

Security

in HP Web Jetadmin



Table of Contents:

Overview	1
Preventing Access to HP Web Jetadmin	2
HTTP Port	2
Access List	2
User Profiles	3
Preventing Printer Access	4
Network Security	5
Individual Access	5
Physical Access	8
File System	9
MFP Access	10
Color Access Control	14
Encryption	15
Upgrade HP Jetdirect Firmware	16
Summary	17

Overview

HP Web Jetadmin is a powerful web-based software utility for installing, configuring, and managing network-connected devices. Since it can install and configure devices, it must be able to secure itself against unwanted access. Not only can it secure itself against unwanted users, it can also secure the devices it manages against unwanted access.

Securing devices is important for many reasons:

- reduces printer down time
- reduces helpdesk calls
- minimizes troubleshooting visits
- minimizes consumable usage

Fortunately, HP Web Jetadmin offers several levels of authentication and privacy to secure devices and itself against unwanted access.

Preventing Access to HP Web Jetadmin

HP Web Jetadmin is a web-based tool that can be installed on one machine and accessed from any other machine within the intranet via an ordinary browser. Since it has the power to install and configure devices, security against unwanted users is typically desired. While a firewall can protect the internal network from external access, users inside the firewall could still potentially access an installation unless security measures are present.

HP Web Jetadmin offers the following types of security to ensure only desired users within the intranet have access to an installation of HP Web Jetadmin:

- HTTP Port
- Access List
- User Profiles

HTTP Port

To keep unwanted users within the intranet from browsing to an installation of HP Web Jetadmin, the HTTP port number can be changed by selecting *HTTP (Web)* under the *General Settings* folder in the *Navigation* tree (see Figure 1).

HP Web Jetadmin defaults to using port 8000 in order to not conflict with any other web service on the machine that may be using the typical port 80. However, the port number can be changed by the administrator in order to keep unwanted users from having the ability to browse to the installation of HP Web Jetadmin.

Access List

HP Web Jetadmin provides an *access list* to control which IP addresses (individual or range) or host names can have access to an installation of HP Web Jetadmin. The *access list* can be configured by selecting *HTTP (Web)* under the *General Settings* folder in the *Navigation* tree (see Figure 1). As a precaution to prevent losing access to HP Web Jetadmin entirely, a web browser running on the machine where HP Web

The screenshot shows the 'Network Settings -- HTTP' configuration window. It contains the following sections and fields:

- HTTP Port:** HP Web Jetadmin HTTP Port Number: 8000 [Apply]
- HTTP Proxy Settings:**
 - Allow HTTP Downloads
 - Provide Hewlett-Packard with additional information on HP Web Jetadmin installation information. Click here to view [HP's privacy policy](#).
 - HTTP Proxy Server: web-proxy.boi.hp.com
 - HTTP Proxy Port: 8088
 - Use Proxy Authentication
 - Proxy User: []
 - Proxy Password: []
 - Note: HP Web Jetadmin supports basic authentication to the proxy server. If basic authentication is not available, the necessary files can be downloaded using the browser.
 - [Apply]
- Order for HP Web Jetadmin Access:** None - Open to All Clients Allow then Deny Deny then Allow
- Allow HP Web Jetadmin Access:**
 - IP Hostname:
 - IP Address: [Apply]
 - IP Range: Start: [] End: [] [Apply]
- Deny HP Web Jetadmin Access:**
 - IP Hostname:
 - IP Address: [Apply]
 - IP Range: Start: [] End: [] [Apply]

Figure 1 – HTTP Network Settings

Jetadmin is installed can always access it regardless of how the access list is configured.

A list of individuals who can access HP Web Jetadmin can be created, as well as a list of individuals who cannot access HP Web Jetadmin. The access list can be enabled as *Allow then deny* or *Deny then allow* with the latter always taking precedence. For example, if

Allow then deny is selected, and the same IP address appears in both the *allow* and *deny* lists, the IP address will be denied because that would be the last action performed on the lists.

User Profiles

User profiles are a widely used form of security that HP Web Jetadmin offers to keep unwanted users from gaining access to an installation of HP Web Jetadmin. User profiles can control who has access to an installation of HP Web Jetadmin and what parts of HP Web Jetadmin are available to users under a particular profile. Features can be hidden from certain user profiles and enabled for others.

Passwords are assigned to the profiles to provide authentication against unwanted access (see Figure 2). In addition to unique profile passwords created by HP Web Jetadmin, Microsoft Windows domain passwords can be associated to profiles (see Figure 3). With this technique, HP Web Jetadmin prompts users for their Windows domain user name and password before allowing access to a particular profile.

Windows domain authentication simplifies the following tasks:

- User account administration: there is no longer a need to maintain a specific profile for each user in order to ensure separate passwords.
- Login procedure for users: users are not required to learn a new password, they merely use their existing Windows domain user name and password.

There are two user profiles defined by default in HP Web Jetadmin:

- *Admin* - can view and configure all available items.
- *User* - can view most items, but cannot configure settings unless configured to do so.

The *User* profile can be edited at will, but only the password can be changed on the *Admin* profile. Also, there is no limit to the

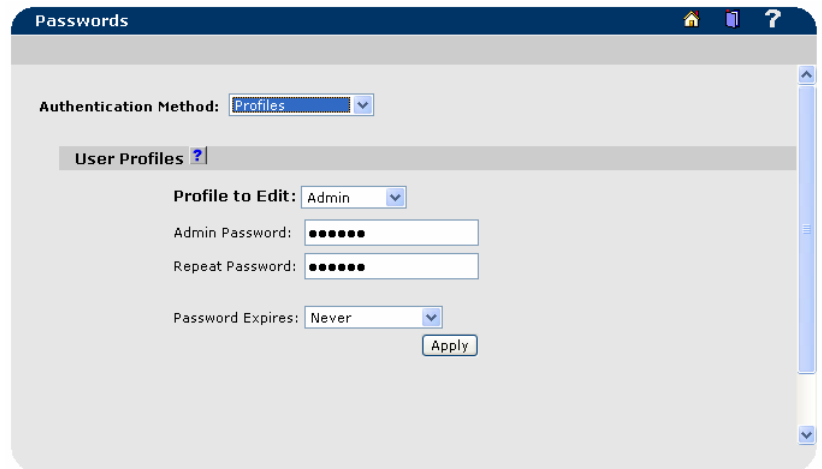


Figure 2 – Profile Passwords

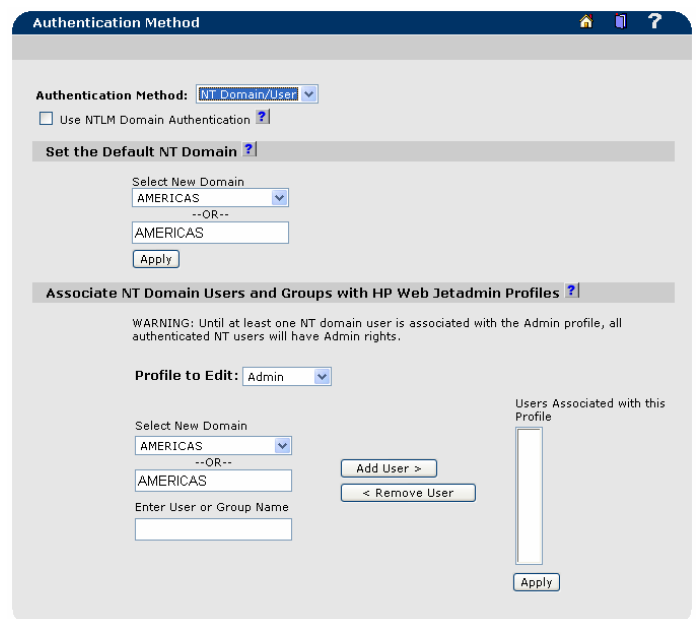


Figure 3 – Profiles – NT Authentication

number of new profiles that can be created.

As an extra precaution, whether installing HP Web Jetadmin as a new version or upgrading over a previous version, the installer will prompt for passwords to be set on any existing profiles whereby passwords have not been previously set.

Each profile can be edited to define which features are made available to users logging in under a particular profile. For example, a *Helpdesk* profile could be created that allows for editing of groups and editing of devices, but does not allow editing of HP Web Jetadmin configuration settings or device installation.

Preventing Printer Access

While an installation of HP Web Jetadmin contains several methods for securing itself against unwanted access, there is still a possibility that devices can be configured with other installations of HP Web Jetadmin or other SNMP utilities. Therefore, setting security on the devices themselves becomes an important form of security to restrict unwanted access to a networked device. Users can access devices through a variety of methods and protocols, but setting security at the device level is effective no matter which technique is used to access the device. For example, configuration of a device can be accomplished through a variety of utilities including:

- HP Web Jetadmin
- Telnet
- Embedded Web Server
- Any SNMP utility

Protocols in use by these and other utilities to perform configuration changes on printers may include:

- SNMP over UDP – changes of PML objects
- SNMP over UDP – changes of PML objects
- RFU file through Port 9100 over TCP – printer firmware upgrades
- PJI file through Port 9100 over TCP – changes of PML objects
- PCL file through Port 9100 over TCP – changes of PML objects
- NFS over TCP – changes to storage (such as hard disk)

In addition to providing additional security methods to prevent against unwanted device configuration, HP Web Jetadmin also provides security against unwanted printing access. For example, printing can occur to printers using the following techniques, among others:

- HP Standard Port Monitor
- HP Jetdirect Port
- Microsoft Standard Port Monitor
- LPD
- FTP
- IPP

Finally, MFP devices contain unique functionality to which it may be desirable to control who has access to which functionality. Fortunately, HP Web Jetadmin contains multiple methods of securing MFP functionality against unwanted access.

Network Security

An excellent place to begin to lock down a printer against unwanted access is to disable any unused network paths or protocols used to access the device.

Disable Unused Protocols

An unused protocol could be considered a back door for unauthorized use and configuration. Disabling unused protocols also helps to minimize network traffic. Once a protocol is disabled, no activity is allowed on that protocol. Therefore, printing and management applications that utilize a disabled protocol will no longer function correctly. HP Web Jetadmin provides the ability to disable protocols either individually or in batches by selecting *Configuration, Network, Protocol Stacks* (see Figure 4).

Disable Unused Services

Additional avenues for either configuring a device or printing to a device can be disabled in HP Web Jetadmin to provide even more security against unwanted device access.

The following services can be enabled/disabled by selecting *Configuration, Network, Enable Features* while viewing a device Status page in HP Web Jetadmin (see Figure 5):

- Service Location Protocol (SLP) - used for IP Multicast discovery
- Telnet - used for device configuration
- Port 9100 - used by Microsoft port monitors such as the HP TCP/IP Standard Port Monitor, HP Jetdirect Port Monitor, Microsoft Standard Port Monitor
- File Transfer Protocol (FTP) – used for configuration and printing
- Line Printer Daemon (LPD) – used for printing
- Internet Printing Protocol (IPP) – used for printing

Individual Access

Once unused paths and protocols to access a device had been disabled, it is time to restrict who can access the device via the open paths and protocols. Techniques are available in Web Jetadmin to restrict either machines or individuals from accessing the device through various paths and protocols.

HP Jetdirect Access Control List

An access control list (or host access list) is used to specify the IP addresses that are allowed TCP access to the device. The list supports up to 10 entries. If the list is empty, then any system is allowed access. By default, host systems with HTTP connections, such as Web browser or Internet Printing Protocol connections, are allowed access regardless of access control list entries. This allows hosts to



Figure 4 – Disable Unused Protocols

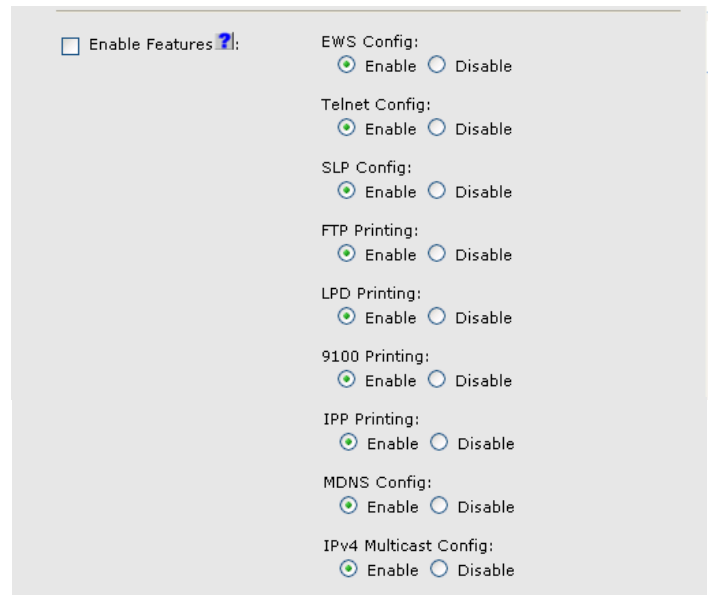


Figure 5 – Disable Unused Services

access the device when Proxy Servers or Network Address Translators are used. However, unfiltered access by HTTP hosts may be disabled by clearing the *Allow Web Server (HTTP) access* checkbox (see Figure 6).

CAUTION: The ability to communicate with the device may be lost if the system is not properly specified in the list, or access through HTTP is disabled. If communications with the device is lost, restoring network settings to factory-default values may be required.

HP Web Jetadmin allows for adding or removing addresses from the Access Control List by selecting *Configure, Network* when viewing a Status page for a single device (see Figure 6).

Access Control List ?:

	Save	IP Address	Mask
1.	<input checked="" type="checkbox"/>		
2.	<input checked="" type="checkbox"/>		
3.	<input checked="" type="checkbox"/>		
4.	<input checked="" type="checkbox"/>		
5.	<input checked="" type="checkbox"/>		
6.	<input checked="" type="checkbox"/>		
7.	<input checked="" type="checkbox"/>		
8.	<input checked="" type="checkbox"/>		
9.	<input checked="" type="checkbox"/>		
10.	<input checked="" type="checkbox"/>		

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 clearing the checkbox below.

Allow Web Server (HTTP) access

Figure 6 – Access Control List

Credentials/Passwords

Credentials, or passwords, can be assigned to devices so that only individuals who present the proper credentials can access the device. Various versions of HP Jetdirect firmware have allowed for configuring several passwords including:

- HP Jetdirect password – an object residing on the HP Jetdirect device that software such as HP web Jetadmin will query before allowing an SNMP Set Request operation.
- Printer EWS password – an object residing on the printer that will deter unwanted printer configurations using HTTP (EWS).
- Telnet password – an object residing on the HP Jetdirect device that will deter unwanted changes in HP Jetdirect configuration using telnet.

Depending upon the HP Jetdirect device and the revision of the Jetdirect firmware, these passwords may be the same or different. For newer HP Jetdirect firmware, such as 22.xx.xx or greater, all three passwords are synched up so that setting one sets them all.

Device Password

HP Web Jetadmin allows for setting a Device Password by selecting *Configuration, Security* while viewing the Status page of a device (see Figure 7). This Device Password will effectively set all three objects mentioned above for newer HP Jetdirect firmware since they are synched.

Note: Future versions of HP Web Jetadmin may no longer use the HP Jetdirect password as a form of security to deter unwanted SNMP Set request attempts. It will be recommended to use either the Set Community Name or SNMPv3 if it is desired to stp unwanted configuration

Device Password ?:

Repeat Password:

Set Community Name ?:

Repeat Set Community Name:

Figure 7 - Passwords

of the device using SNMP.

The Printer EWS Password can also be set when browsing directly to the printer IP address where it is labeled as the Administrator Password. Again, setting the Administrator Password here will effectively set the HP Jedirect Password and the Telnet Password on newer HP Jetdirect devices. The telnet password can also be set through a telnet session to the printer. Once any of these mechanisms are set on newer HP Jetdirect firmware, any attempts at device modification through any of the following utilities will require knowledge of the password:

- HP Web Jetadmin
- HP Jetadmin
- HP Install Network Printer Wizard
- HP Jetdirect Embedded Web Server
- Printer Embedded Web Server
- Telnet

The administrator password will only prevent configuration through HP utilities such as those listed above because they are the only ones to check for the presence of this password.

SNMP Set Community Name

The Set Community Name is an object that resides on the HP Jetdirect device, and is often used to secure the printer against unwanted SNMP Set Request attempts. HP Web Jetadmin allows for setting the SNMP Set Community Name on individual devices by selecting *Configuration, Security* while viewing a single device (see Figure 7), or it can be set in batches by selecting *Configuration* while viewing a group of devices or the list of all devices. Only the users that have knowledge of the Set Community Name can make changes via SNMP. An advantage to the Set Community name over the HP Jetdirect Password is that any SNMP utility, not just HP utilities such as HP Web Jetadmin, must contain this Set Community Name before parameter modification can be performed. The Set Community Name parameter can have a maximum length of 32 characters.

The Set Community Name can be synced up with the other administrator passwords in HP Jetdirect firmware versions 22.x.x or greater.

PJL Password

PJL (Printer Job Language) is a command language that can be used to enable features of the printer or make configuration changes. Typically, PJL is used at the beginning of a print job to prepare the printer to print the job. However, PJL can also be used to make configuration changes to the printer over PML. Setting the PJL password locks access to changing configuration via PJL. The PJL password can be set under *Configuration, Security* in single and multiple configuration in HP Web Jetadmin (see Figure 8).

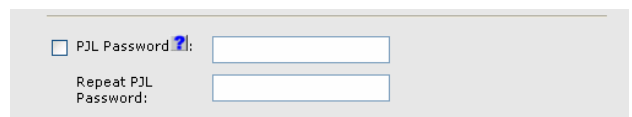
The image shows a screenshot of a web interface for configuring a PJP Password. It consists of two input fields. The first field is labeled "PJP Password" with a small blue question mark icon to its right. The second field is labeled "Repeat PJP Password:" and is positioned directly below the first field. Both fields are empty and have a light gray border.

Figure 8 – PJP Password

Store Credentials

Credentials such as *Set Community Name* or *Device Password* can be securely stored in HP Web Jetadmin per profile per device to be used for subsequent configuration attempts on the devices selected, including scheduled configurations (see Figure 9). This eliminates the need to enter passwords at the time of the scheduled configuration if passwords are required and unknown.

The *Store Credentials* button at the bottom of the page is NOT writing any credentials to devices. Rather, it is storing those credentials in HP Web Jetadmin in order to be used for subsequent configuration attempts.

Rather than prompting for device credentials as the configuration attempt is made on each device, if a password does not exist in HP Web Jetadmin for a particular profile attempting to make a configuration, the attempt on the device will be postponed and the next device will be attempted. The log file can be visited at a later date to enter the credentials, then re-attempt the configuration.

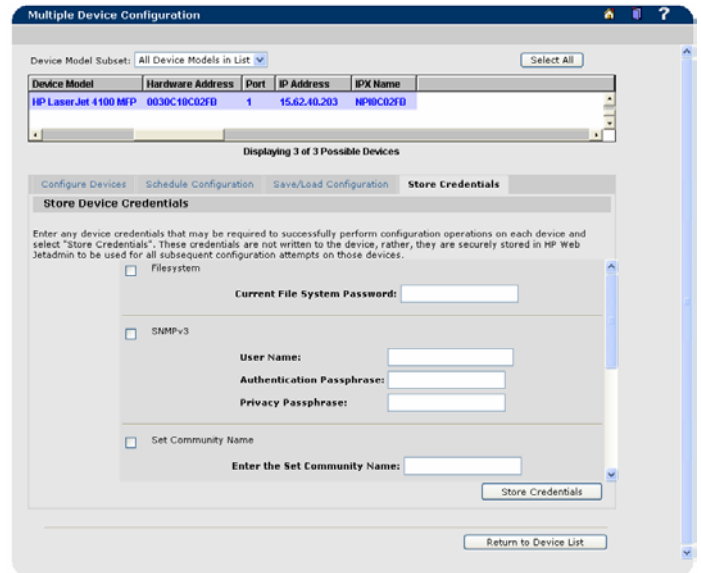


Figure 9 – Store Credentials

When a Web Jetadmin configuration is attempted on a device with credentials that don't match stored credentials, it logs an Invalid Credentials failure. The same is true when a Web Jetadmin configuration is attempted on a device for which no credentials are stored. In the logged entry is a link named "invalid credentials" which launches a screen to allow for entering the credentials.

Configuration attempts can be automatically retried at a configurable frequency and number of attempts, in which case any new credentials that are stored in HP Web Jetadmin will be attempted again. Any time a device password, set community name, SNMPv3 credential, etc. is configured on a device through HP Web Jetadmin, it will also be placed in the HP Web Jetadmin password store for subsequent use.

Physical Access

Even though unused network path and protocols have been disabled and user access restricted through used paths and protocols, unwanted individuals could still physically access the device to change configurations or print.

Control Panel Lock

HP Web Jetadmin can lock the control panel on the printer, preventing unauthorized users from accessing it and changing the settings via the front panel (see Figure 10). The following number of values may be present, depending upon the printer:

- 0 - no levels available
- 2 - unlock, maximum lock,
- 4 - unlock, minimum lock, moderate lock, maximum lock
- 5 - unlock, minimum lock, moderate lock, intermediate lock, maximum lock

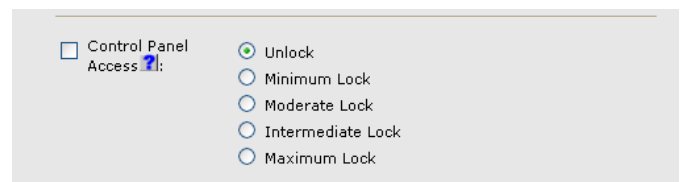


Figure 10 – Control Panel Lock

For example, typical menu items locked for an HP LaserJet 4345MFP include:

Minimum:

The Configure Device menu is not locked, but the following sub-menus are:

System Setup

I/O

Resets

Moderate:

Configure Device

Diagnostics

Intermediate:

Paper Handling

Configure Device

Diagnostics

Maximum:

Almost everything, including the Stop button.

Disable Direct Ports

With network access secured against unwanted access and the control panel locked, it may also be desired to prohibit the ability of an individual to walk up to a printer, connect a cable to one of the direct ports such as USB or LPT, and print a document. HP Web Jetadmin provides the ability to disable direct ports so printing would not be possible through those ports. To disable direct ports, select *Configuration, Security* in either single or multiple configuration in HP Web Jetadmin (see Figure 11).



Figure 11 – Disable Direct Ports

File System

Secure File Erase Modes can be applied to determine the behavior of a secure storage erase operation and the erase operation that a printer automatically performs to make space available on a hard disk drive for incoming print jobs. The erase operations are designed to add available space to a device's hard disk drive and to prevent unauthorized users from accessing confidential information from a device's hard disk drive or other erasable storage device.

Three levels of erasure are supported:

- 1) Non-Secure Fast Erase: erases the file system references to operations, such as completed print jobs. By erasing the references, space on the hard disk drive is made available. Data is retained on disk until overwritten due to freed up status. This is the fastest erase mode and the default mode.
- 2) Secure Fast Erase: erases the file system references to file operations and provides one layer of masking to hide data stored on the hard disk drive or other erasable storage devices. Information is overwritten with identical character pattern. This is slower than non-secure erase, but all data is over written.
- 3) Secure Sanitizing Erase: erases the file system references to operations and provides multiple layers of masking to hide data stored on the hard disk drive or other erasable storage devices. It is a secure, repetitive algorithm used to overwrite all file information and remove any residual data persistence.

To securely erase a disk, a file system password is required. HP Web Jetadmin provides an interface to initially configure or change the file system password (see Figure 12). As with any PML object

configured through an SNMP SET, an SNMP SET Community Name can be applied to the device, or an HP Jetdirect password, in order to deter unwanted access or changing of the password.

Secure Storage Erase (wipe disk) erases the file system references to operations and provides multiple layers of masking to hide data stored on the hard disk drive or other erasable storage devices. It entirely erases storage media in a device using the file erase mode described above. Media include hard disks and compact flash. HP Web Jetadmin provides an interface that will allow the immediate or scheduled execution of the operation in batch or single device mode.

A password is used to protect the configuration of the secure file erase modes and file system external access and to protect the execution of wipe disk. HP Web Jetadmin will allow for initially configuring and changing the password in both batch and single device configuration.

Access control for external PJJ, PML, PostScript, and NFS requests to read or write to the file system are also provided by HP Web Jetadmin (see Figure 9). An interface is provided for enabling/disabling access to the file system for each of these mechanisms. The user will be required to supply the file system password to configure access. NFS is used to manage the contents of a printer hard disk using the HP Device Storage Manager plug-in to HP Web Jetadmin. Disabling NFS will force the Device Storage Manager to use PJJ to manage the disk.

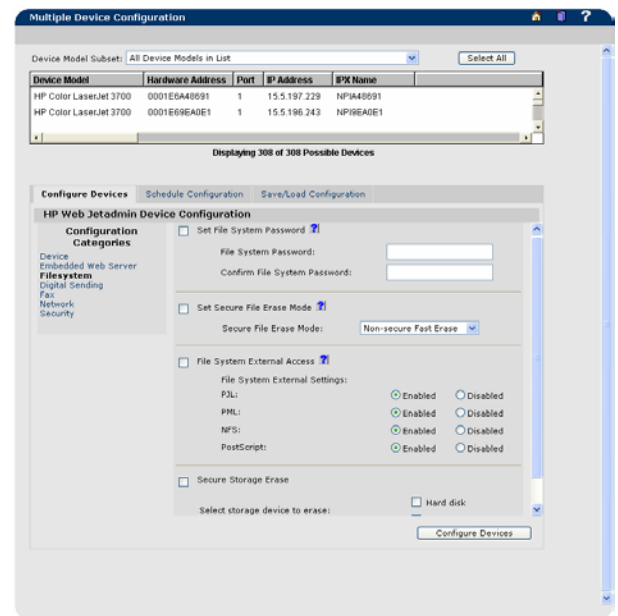


Figure 12 – File System

MFP Access

HP MFP access controls can require users to be authenticated before accessing MFP functions via the device control panel and can restrict access to digital sending functions and digital sending e-mail destinations based on the user. HP MFPs can also control access to installed functions and installed applications based on the user.

All HP MFPs and digital senders offer server-based Windows NTLM, LDAP, Kerberos, and Novell authentication and authorization that integrates into existing infrastructure to help manage user access, prevent unwanted printing and digital sending, and help secure access to the management utility to prevent unwanted device configurations.

HP Web Jetadmin provides the ability to configure authentication methods in single or multiple configuration modes, then assign those particular authentication methods to be used for certain MFP functions using the Authentication Manager plug-in, an optional component to HP Web Jetadmin that can be installed through Product Update.

Kerberos

Kerberos Authentication can be accessed in Web Jetadmin under *Configuration, Security* to configure the device (multi-function peripheral or digital sender) to authenticate users to a Kerberos Realm (see Figure 13). When Kerberos authentication is selected as the Log In Method for one or more Device Functions on the Authentication Manager page, the user at the device must enter valid credentials (username, password, and realm) to gain access to those functions. Authentication consists of two interdependent parts. First, the device verifies the user's credentials with the KDC. After the device user has supplied valid credentials and has been authenticated, the device searches for the user's e-mail address and name. If either step fails, the user is denied access to the functions that have been configured to require Kerberos authentication.

Use the Kerberos Authentication page to set up the parameters that are used to access the LDAP server and searches for the user's information. The Kerberos Default Realm is the fully qualified domain name of the Kerberos realm (domain). The Kerberos Server Hostname can be the same as the Kerberos Default Realm if a DNS service is available (Domain Name Service) is used and correctly configured. The device will use DNS to look up the first available KDC (Kerberos Domain Controller) on the network. If DNS is not available, the IP address of the Kerberos Server may be used. The Kerberos Server Port is the default IP port used by the Kerberos authentication method. Note that the default is port 88, but this can be different in different network environments. The LDAP Server Bind Method determines how the device will access the LDAP server. The only available method currently supported for Kerberos authentication is the Kerberos bind method.

The Credentials configuration section is used to determine which credentials will be used to bind (authenticate) to the LDAP server.

- When Use Device User Credentials is selected, the device users credentials (entered at the control panel of the device) will be used to access the LDAP server. This method has the advantage of not having to store a username and password, which may expire, in the device.
- When Use Public Credentials is selected and user credentials are not available, the Username and Password entered will be used to access the LDAP server. This method should be used if for some reason device users do not have read access to the LDAP data.

The LDAP Server is typically the same as the Kerberos Server in the Windows Active Directory Environment. The Port is the IP port used by the LDAP protocol to communicate with the LDAP server. This is typically port 389 or port 3268.

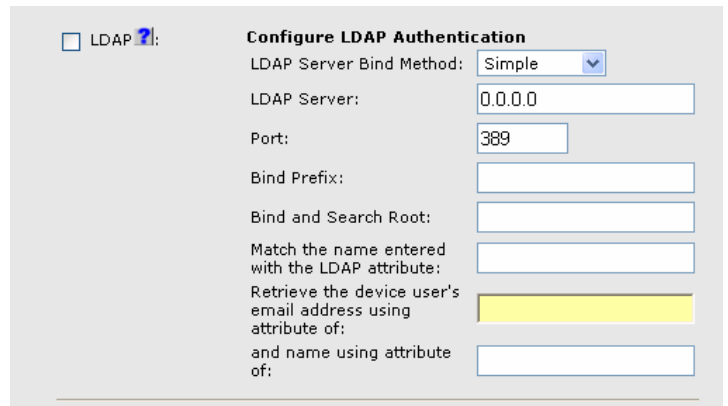
The Search Root is the Distinguished Name (DN) of the entry in the LDAP directory structure where address searching is to begin. A DN is made up of ' attribute=value ' pairs, separated by commas.

Figure 13 – Kerberos Authentication

When searching for the device user's information in the LDAP database, the contents of the attribute specified in this field are compared to the username that was typed during authentication. In the Windows Active Directory environment, this attribute is typically sAMAccountName. After the device user has been located in the LDAP database, the user's e-mail address is retrieved from the database by using the LDAP attribute specified in the Retrieve the device user's e-mail address using attribute of field. In the Windows Active Directory environment, this attribute is typically mail.

LDAP

Kerberos Authentication can be accessed in Web Jetadmin under *Configuration, Security* to configure a Lightweight Directory Access Protocol (LDAP) server to authenticate device (multifunction peripheral, digital copier, or digital sender) users. When LDAP authentication is selected as the Log In Method for one or more Device Functions on the Authentication Manager page, the user at the device must enter valid credentials (username and password) to gain access to those functions.



LDAP ?:

Configure LDAP Authentication

LDAP Server Bind Method: Simple

LDAP Server: 0.0.0.0

Port: 389

Bind Prefix:

Bind and Search Root:

Match the name entered with the LDAP attribute:

Retrieve the device user's email address using attribute of:

and name using attribute of:

Figure 14 – LDAP Authentication

Authentication consists of two interdependent parts. First, the device verifies the user's credentials with the LDAP server. After the device user has supplied valid credentials and has been authenticated, the device searches for the user's e-mail address and name. If either step fails, the user is denied access to the functions that have been configured to require LDAP authentication.

The LDAP Server Bind Method setting determines how the device will access the LDAP server.

- Simple - The selected LDAP server does not support encryption. Note that the password, if any, will be sent unencrypted across the network.
- Simple over SSL - The selected LDAP server supports encryption using the Secure Sockets Layer (SSL) protocol. All data, including the username and password, will be encrypted. The LDAP server must be set up to support SSL, including configuring a certificate that establishes its identity. Also, the device network interface must be configured with a Certificate Authority (CA) certificate to validate the LDAP server. The CA certificate is configured on the Networking tab of the Web interface. In some LDAP server configurations, a client certificate is also required and is configured on the same Networking tab.

The LDAP Server setting is the host name or IP address of the LDAP server to be used to authenticate device users. When using SSL, the name or address typed here must match the name in the certificate that the server sends. Multiple servers can be included in this field by separating their addresses with a vertical bar ('|', ASCII 0x7c) character. This feature can be used, for example, to specify primary and backup servers. The network interface only supports a single Certificate Authority (CA) certificate, so all the LDAP servers in the list must use the same CA. The Port setting refers to the TCP/IP port number on which the server is processing LDAP requests. Typically, this is port 389 for Simple binds or 636 for Simple over SSL binds.

Group PIN

Pin Authentication can be accessed in Web Jetadmin under *Configuration, Security* to control the usage of certain features from the front control panel of select MFP devices. Pin Authentication is one method in which Administrators can choose how users should authenticate to access these certain features. Depending upon which features are enable, the user will be prompted to enter a Pin number to receive access to the following features:

- Copy
- Color Copy
- Send to Email
- Send to Fax
- Send to Folder

Two Pin Numbers are able to be defined for the control of the features listed above.

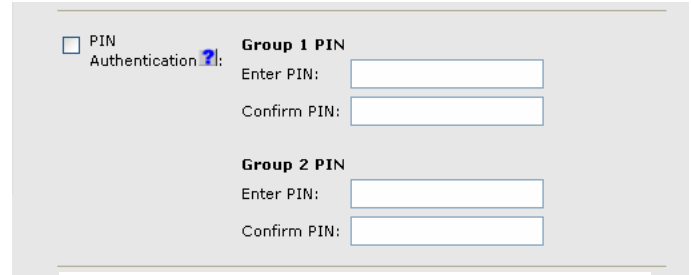
The most frequent request for Pin Authentication is to limit/lockout color copies. This feature would allow administrators to require end users to enter a pin numbers to receive access to the color copy feature. The Authentication Manager can be used to display three methods of authentication to be applied to certain MFP functions:

1. Use external Digital Send Service (if available)
2. LDAP
3. PIN

Authentication Manager

Authentication Manager is an application that can be installed into HP Web Jetadmin via Product Update. Once installed, it is accessed from the drop-down menu for a single device or list of devices (see Figure 16). Authentication Manager allows administrators to secure device functions by requiring users to log in with a specific log in method for each function. For example, users may be required to log in with an Access Code or PIN to make copies yet be required to log in with a username and password to send e-mails.

The following log in methods are available:

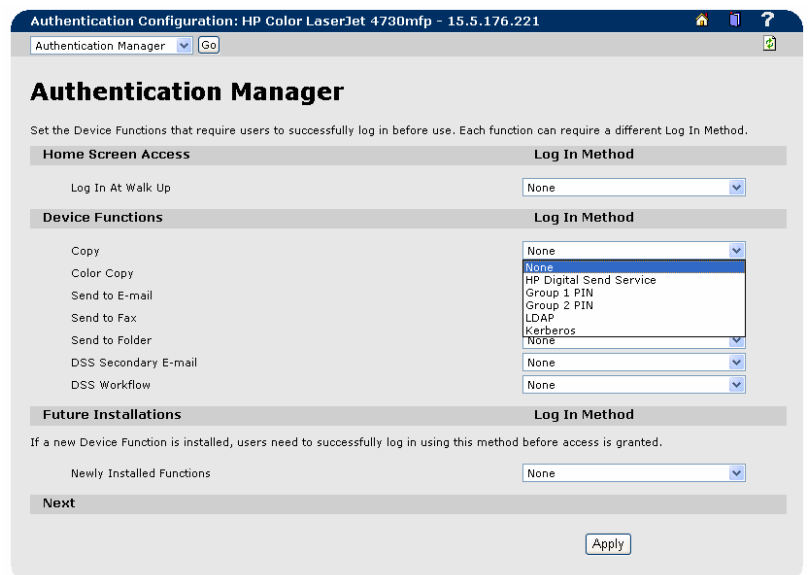


PIN Authentication ?

Group 1 PIN
Enter PIN:
Confirm PIN:

Group 2 PIN
Enter PIN:
Confirm PIN:

Figure 15 – Group PIN Authentication



Authentication Configuration: HP Color LaserJet 4730mfp - 15.5.176.221

Authentication Manager Go

Authentication Manager

Set the Device Functions that require users to successfully log in before use. Each function can require a different Log In Method.

Home Screen Access	Log In Method
Log In At Walk Up	None

Device Functions	Log In Method
Copy	None
Color Copy	None
Send to E-mail	None
Send to Fax	None
Send to Folder	None
DSS Secondary E-mail	None
DSS Workflow	None

Future Installations	Log In Method
Newly Installed Functions	None

Next

Apply

Figure 16 – Authentication Manager

- Group 1 PIN: Requires users to input a numeric code for access when at the control panel of the device. The numeric code entered by the walk up user is compared to the first of two PINs stored on the device by the Administrator. When the PIN is entered correctly, the user can proceed.
- Group 2 PIN: Requires users to input a numeric code for access when at the control panel of the device. The numeric code is compared to the second of two PINs stored on the device by the Administrator.
- LDAP: Lightweight Directory Access Protocol, Requires users to input a username and password that are verified by an LDAP server.
- HP Digital Send Service (if available): Also known as DSS. Requires users to enter credentials that are verified by the HP Digital Send Service software. *(HP Digital Send Service software must be available to use this Log In Method. If no DSS server is associated with this device, walk-up users will not be required to authenticate before using the device.)*
- Kerberos: Requires users to enter a username and password to be verified by a Windows Server.

The Authentication Manager allows administrators to secure the following Functions:

- Copy: The user can make copies of the document on this device.
- Color Copy: The user can make color copies of the document on this device.
- Send E-mail: The user can scan a document and send it as an attachment to an e-mail.
- Send Fax: The user can scan and fax the document.
- Send to Network Folder: The user can scan a document and send it to a network folder.
- DSS Secure E-Mail: The user can scan a document and send it securely to a 3rd party secure solution via the DSS server. *(HP Digital Send Service software must be available to use this Function. This Function encrypts the document between the device and the DSS server.)*
- DSS WorkFlow: The user can scan a document and send it to a specific destination via the DSS server. *(HP Digital Send Service software must be available to use this Function.)*

Color Access Control

HP Web Jetadmin provides the ability to configure color access control functions whereby color printing can be restricted on individual users or groups, as well as by specific applications such as Web browsers, to help prevent users from wasting color on jobs that should be output in black and white. In addition, HP Web Jetadmin can install pre-configured printer drivers that limit printing to monochrome only when creating shared print queues on Microsoft Windows machines. If necessary, it is also possible to disable color printing and copying entirely until it's needed for special projects.

A list of users who can print in color can be created by selecting Configuration, Security when viewing a Device Status page in HP Web Jetadmin (see Figure

The screenshot shows the HP Web Jetadmin configuration page for Color Access Control. It is organized into three main sections:

- Restrict Color Use:** A checkbox is present. To its right are three radio buttons: 'Enable Color' (selected), 'Color if Allowed', and 'Disable Color'.
- User Permission:** A checkbox is present. To its right is a 'Default User Permission' dropdown menu set to 'Color'. Below this is a table with columns for 'User Name', 'Permissions', and 'User Name'. There are '>>' and '<<' buttons for adding and removing users, a 'Delete' button, and a 'Color' dropdown menu. Below the table is an 'Import Configuration File' section with a text input field and a 'Browse...' button.
- Application Permission:** A checkbox is present. To its right is a 'Default Application Permission' dropdown menu set to 'Color'. Below this is a table with columns for 'Application Name', 'Permissions', and 'Application Name'. There are '>>' and '<<' buttons for adding and removing applications, a 'Delete' button, and a 'Color' dropdown menu. Below the table is an 'Import Configuration File' section with a text input field and a 'Browse...' button.

Figure 17 – Color Access Control

17). A list of users can also be imported from a .csv file if desired. The format of the .csv file should contain one users per line followed by either "black" or "color" to assign printing privileges. Any imported list will remove and overwrite existing entries in the list configured on the printer. Up to 50 users can be imported in the list and configured on the printer.

A list of applications that will have color access can also be created in the designated area under Configuration, or a list of applications can be imported from a file. The same format rules apply to this list as apply for the list of users. One application must be specified per line, followed by either "black" or "color" to assign printing privileges. Up to 10 applications can be imported and configured on the printer.

Encryption

Assigning passwords can keep unwanted users from accessing HP Web Jetadmin and/or printers. However, in many cases these passwords can be compromised by using network sniffing or tracing tools to view the passwords. Fortunately, password encryption is possible in HP Web Jetadmin to secure the passwords.

Secure Sockets layer (SSL)

Secure Sockets Layer (SSL) communication is supported for secure communication between the web browser and the HP Web Jetadmin installation. This optional SSL access encrypts all communication between the web browser and the HP Web Jetadmin host machine using HTTPS instead of HTTP. This prevents persons from intercepting information and learning sensitive information such as passwords. SSL communication is based on a digital certificate that can originate from two sources: self-signed and third-party Certificate Authority (CA). A self-signed certificate is issued by HP Web Jetadmin itself. Alternately, HP Web Jetadmin can request a certificate from a third-party CA such as Verisign (see Figure 18).

HTTPS

HTTPS can also be enabled for the HP Jetdirect device to configure whether the device will require Secure HTTP (HTTPS) only, or allow both HTTPS and standard HTTP, for browser-based management (see Figure 19). Secure Hyper Text Transfer Protocol (HTTPS) provides secure, encrypted management

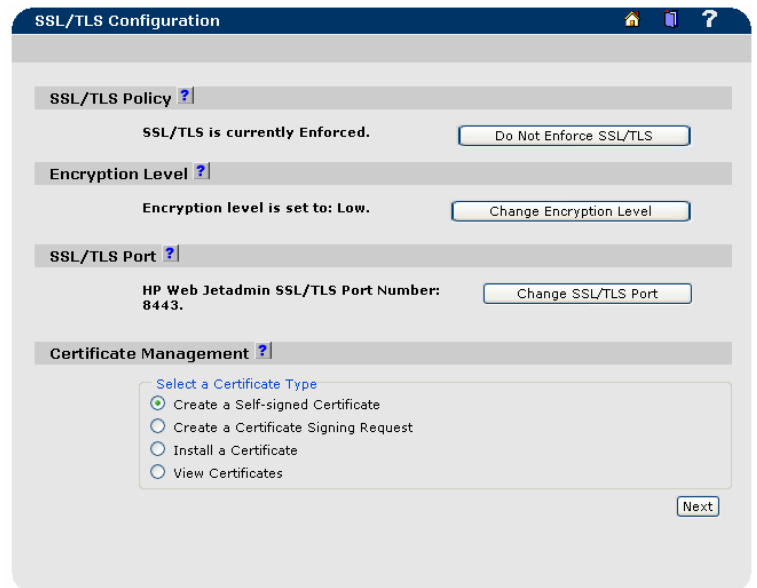


Figure 18 – SSL (Secure Sockets Layer)

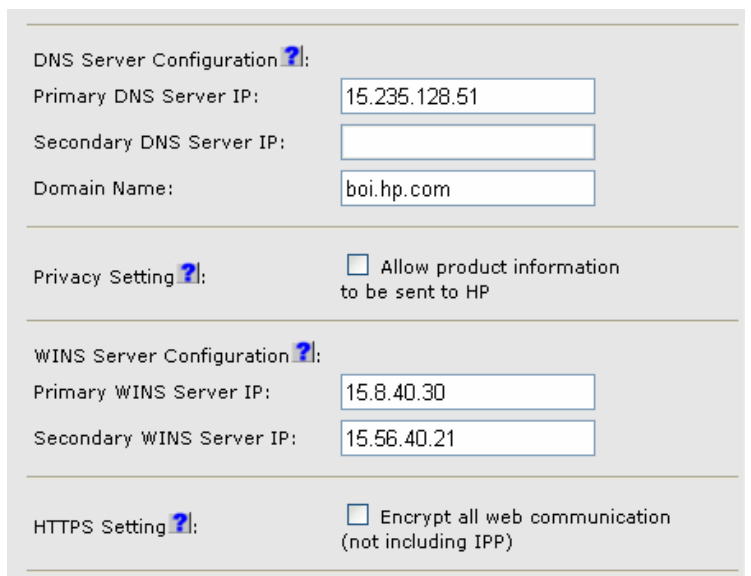


Figure 19 - HTTPS

communications between the embedded Web server on the device and a Web browser. If non-secure communications (HTTP) are used with a device that is configured to require HTTPS only, the browser will be redirected to use HTTPS. Automatic redirection of the browser for HTTPS may be transparent depending on the browser's capabilities. If both HTTPS and HTTP are allowed, the browser communications will be routed to the device's HTTPS or standard HTTP port as appropriate.

SNMPv3

HP Web Jetadmin uses SNMPv1 to retrieve information pertaining to devices, but can also use SNMPv3 for configuring parameters on SNMPv3 capable HP Jetdirect devices. SNMPv3 allows the communication between the HP Jetdirect device and HP Web Jetadmin to be encrypted and authenticated to eliminate interception and alteration.

HP Web Jetadmin can be used to enable SNMPv3 on multiple devices simultaneously. When HP Web Jetadmin enables SNMPv3 on a device, it can either enforce read/write capabilities for SNMPv3, but leave read access open for SNMPv1 to enable discovery by management tools, or it can disable SNMPv1 entirely (see Figure 20). If the latter is configured, both read and write access will be blocked under SNMPv1. However, HP Web Jetadmin will still be able to discover the device and manage it if the credentials are supplied under *Discovery, Properties* and clicking the link for Discover SNMPv3 Enabled Devices (see Figures 21 and 22).

Upgrade HP Jetdirect Firmware

As HP Jetdirect firmware is enhanced or revised, performance and security issues are proactively addressed. Always keep the firmware on the HP device at the latest revision level to ensure maximum security. HP Web Jetadmin provides the ability to upgrade HP Jetdirect firmware either individually or in batches (see Figure 23).

Figure 20 – SNMPv3

Figure 21 – SNMPv3 Discovery

Figure 22 – SNMPv3 Credentials for Discovery

The ability to disable printer firmware upgrades is also possible in HP Web Jetadmin under the *Security* section of single and multiple device configuration. The object named Printer Firmware Update can be disabled so that all attempts at upgrading printer firmware are rejected (see Figure 24). If the printer is configured with passwords explained earlier in this paper, this object can be changed to value of enabled only by individuals who know the password in order to perform a printer upgrade.

Summary

Unwanted changes in device configuration can make setting security a priority. Fortunately, HP Web Jetadmin offers multiple levels of security to provide LAN administrators the control needed to customize and protect device management on their networks. Not only can it secure itself against unwanted users, it can also secure the devices themselves against unwanted access through any utility. See Appendix A for a table of typical device access points and how HP Web Jetadmin can provide security against those access points.

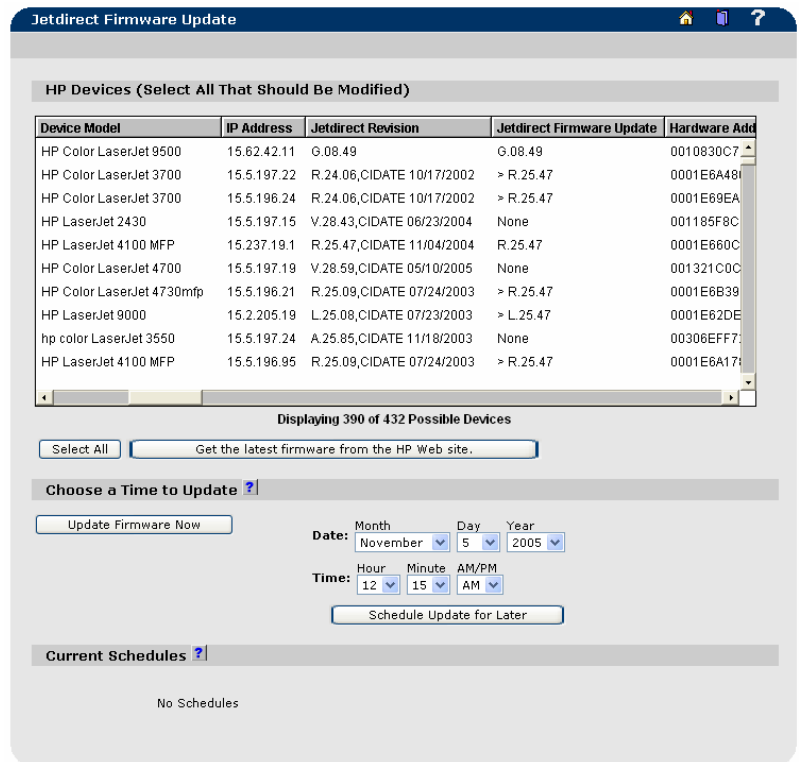


Figure 23 – Multiple HP Jetdirect Firmware Upgrade

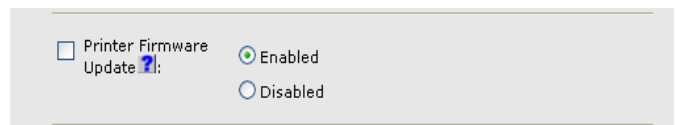


Figure 24 – Disable Printer Firmware Update

Appendix A

Security Method	Description
Device password	HP Web Jetadmin checks for the presence of a device password before allowing configuration or firmware updates to occur.
Set Community Name	An HP Jetdirect device will not allow SNMP SET REQ commands (which HP Web Jetadmin uses for device configuration) without this password.
Access Control List	Specifies the IP addresses that are allowed access to the device
Disable telnet access	Telnet access, used for HP Jetdirect device configuration, can be disabled.
Disable unused protocols	Disabling unused protocols, such as IPX/SPX, can keep unwanted device configurations from occurring through SNMP utilities.
Disable PJJ access	Disables PJJ access to the printer file system only. PJJ in print jobs is still accepted.
Disable NFS access	Disables NFS access to the printer file system. The Device Storage Manager plug-in requires NFS for management of fonts, forms, macros, and stored jobs.
Disable PML access	Disables PML access to the printer file system. Regular PML objects over SNMP are still accepted.
Disable Postscript	Disables Postscript access to the printer file system.
File system password	Required to set secure file erase modes, securely erase storage, disable file system access.
Secure file erase modes	Determines the behavior of a secure storage erase operation and the erase operation that a printer automatically performs to make space available on a hard disk
Secure storage erase	Entirely erases storage media in a device using the file erase modes described above.
SSL (Web Jetadmin)	Encrypts the communication between client and HP Web Jetadmin server using HTTPS.
HTTPS (device)	Encrypts the communication between client and HP Jetdirect device interface.
SNMPv3	Encrypts all SNMP SET REQUESTS to the HP Jetdirect device.
Disable Port 9100 printing	Port 9100 printing, which HP TCP/IP Standard Port Monitor utilizes by default to send print jobs, can be disabled.
Disable LPD printing	LPD, which can be enabled (LPR) as a print method under the HP Standard TCP/IP Port Monitor, can be disabled.
Disable FTP printing	FTP (file transfer protocol) printing can be disabled.
Disable IPP printing	Internet Printing Protocol, or printing directly from the web, available as a separate utility from HP for Microsoft Windows NT, and available by default under Microsoft Windows 2000, can be disabled.
Control panel lock	Disables users from performing front panel control panel operations.

© November 2006 Hewlett-Packard Development Company, L.P. The information contained in this document is subject to change without notice. HP makes no warranty of any kind with respect to this information. HP specifically disclaims the implied warranty of merchantability and fitness for a particular purpose. HP shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in conjunction with the furnishing or use of this information. Microsoft, Windows, and Windows NT/2000/XP are registered trademarks of Microsoft Corporation in the USA, and other countries. All other brand and product names are trademarks or registered trademarks of their respective companies.