Security

in HP Web Jetadmin

whitepaper

Table of Contents:

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

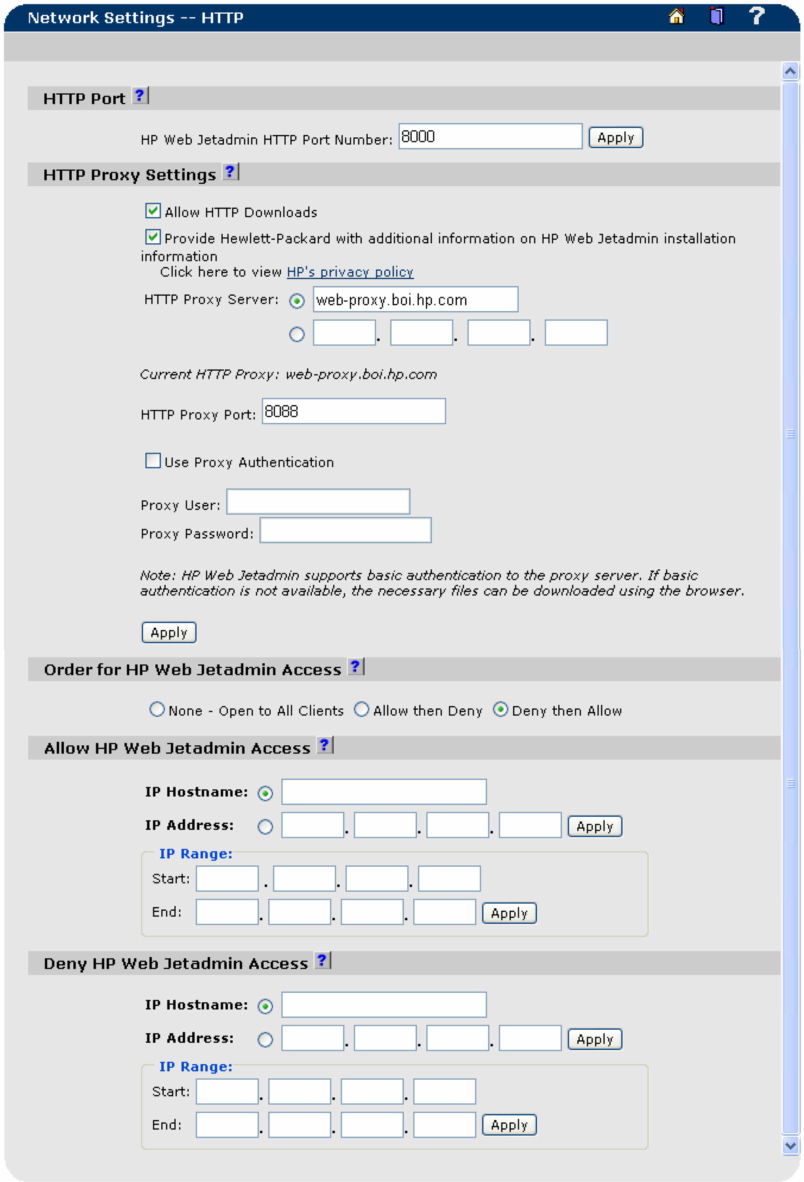
HP Web Jetadmin is a web-based tool that can be installed on one machine and accessed from any other machine within the intranet via an ordinary browser. Since it has the power to install and configure devices, security against unwanted users is typically desired. While a firewall can protect the internal 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).



Network Settings -- HTTP

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

○ . . .

Current HTTP Proxy: 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]

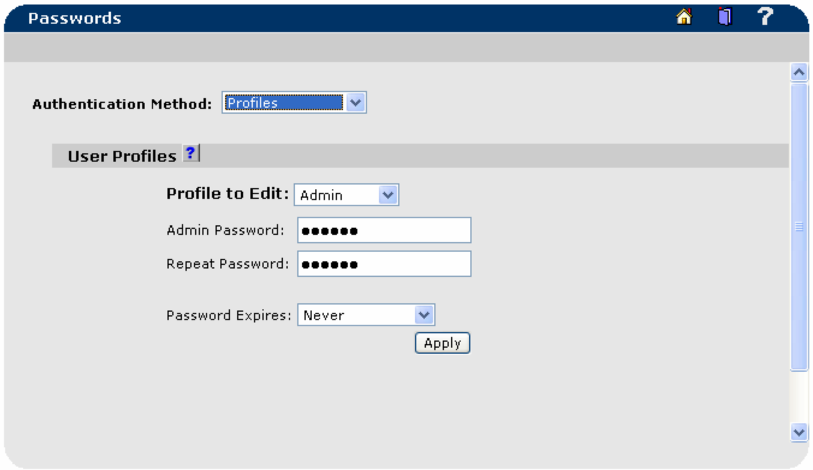
Figure 1 – HTTP Network Settings

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 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.


Passwords

Authentication Method: Profiles

User Profiles

Profile to Edit: Admin

Admin Password: ●●●●●●

Repeat Password: ●●●●●●

Password Expires: Never

Apply

Figure 2 – Profile Passwords

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.

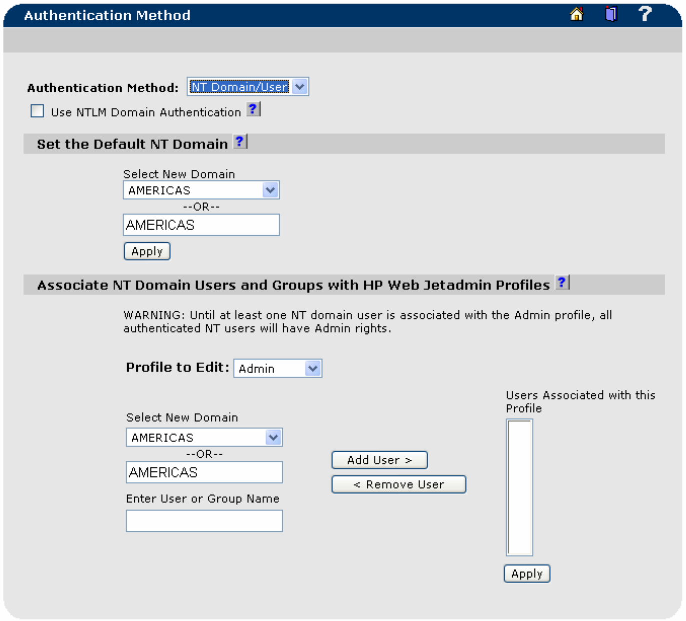
Passwords are assigned to the profiles to provide authentication against unwanted access (see Figure 2). In addition to unique profile passwords created by HP Web Jetadmin, Microsoft Windows domain passwords can be associated to profiles (see Figure 3). With this technique, HP Web Jetadmin prompts users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


Authentication Method

Authentication Method: NT Domain/User

□ Use NTLM Domain Authentication

Set the Default NT Domain

Select New Domain

AMERICAS

--OR--

AMERICAS

Apply

Associate NT Domain Users and Groups with HP Web Jetadmin Profiles

WARNING: Until at least one NT domain user is associated with the Admin profile, all authenticated NT users will have Admin rights.

Profile to Edit: Admin

Select New Domain

AMERICAS

--OR--

AMERICAS

Enter User or Group Name

Add User >

< Remove User

Users Associated with this Profile

Apply

Figure 3 – Profiles – NT Authentication

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 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
- PJL 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

With all of these avenues for potentially changing device configurations or printing to devices, setting security at the device level is the surest way of eliminating access to the device. Fortunately, there are several security mechanisms that can be enabled on the device to address all of these various forms of access. HP Web Jetadmin provides multiple methods for securing devices against unwanted access including:

- upgrade the HP Jetdirect firmware
- disable all unused protocols
- lock the control panel
- disable file access
- disable unused services
- disable printer firmware upgrades
- specify an administrator password
- specify an SNMP Set Community name
- secure the printer disk

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 4).

Disable Unused Protocols

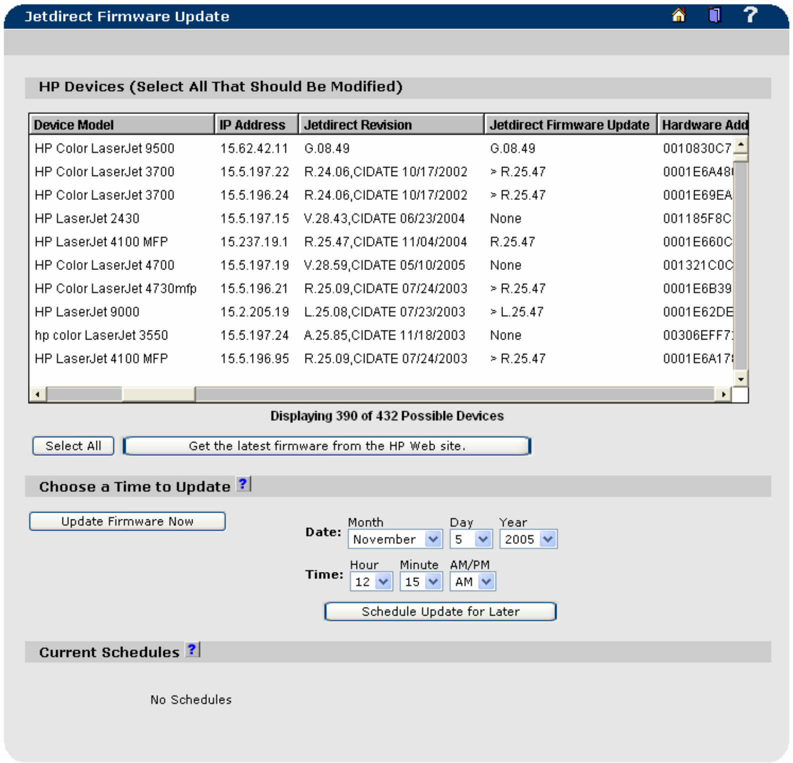
An unused protocol could be considered a back door for unauthorized use and configuration. Disabling unused protocols also helps to minimize network traffic. Once a protocol is disabled, no activity is allowed on that protocol. Therefore, printing and management applications that utilize a disabled protocol will no longer function correctly. HP Web Jetadmin provides the ability to disable protocols either individually or in batches (see Figure 5).

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. 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

Examples of typical menus locked or unlocked with each level may include (depending upon the printer model):



Jetdirect Firmware Update

HP Devices (Select All That Should Be Modified)

Device Model	IP Address	Jetdirect Revision	Jetdirect Firmware Update	Hardware Add
HP Color LaserJet 9500	15.62.42.11	G.08.49	G.08.49	0010830C7
HP Color LaserJet 3700	15.5.197.22	R.24.06,CIDATE 10/17/2002	> R.25.47	0001E6A48
HP Color LaserJet 3700	15.5.196.24	R.24.06,CIDATE 10/17/2002	> R.25.47	0001E69EA
HP LaserJet 2430	15.5.197.15	V.28.43,CIDATE 06/23/2004	None	001185F8C
HP LaserJet 4100 MFP	15.237.19.1	R.25.47,CIDATE 11/04/2004	R.25.47	0001E660C
HP Color LaserJet 4700	15.5.197.19	V.28.59,CIDATE 05/10/2005	None	001321C0C
HP Color LaserJet 4730mfp	15.5.196.21	R.25.09,CIDATE 07/24/2003	> R.25.47	0001E6B39
HP LaserJet 9000	15.2.205.19	L.25.08,CIDATE 07/23/2003	> L.25.47	0001E62DE
hp color LaserJet 3550	15.5.197.24	A.25.85,CIDATE 11/18/2003	None	00306EFF7
HP LaserJet 4100 MFP	15.5.196.95	R.25.09,CIDATE 07/24/2003	> R.25.47	0001E6A17

Displaying 390 of 432 Possible Devices

Choose a Time to Update

Date: Month November Day 5 Year 2005

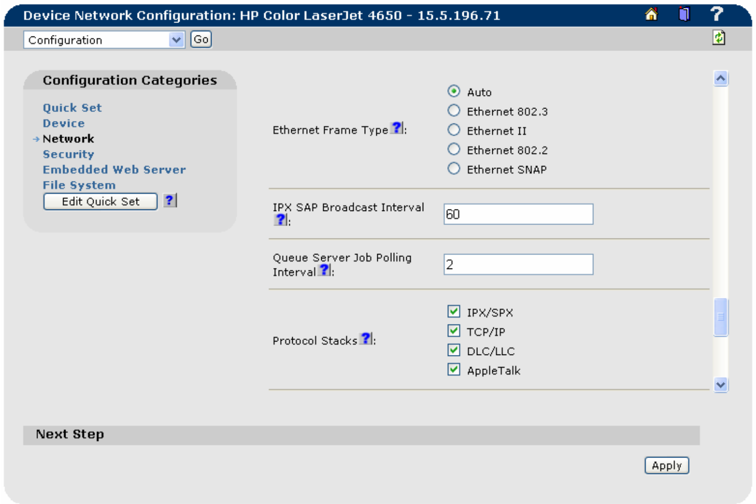
Time: Hour 12 Minute 15 AM/PM AM

Current Schedules

No Schedules

Select All
Get the latest firmware from the HP Web site.
Update Firmware Now
Schedule Update for Later

Figure 4 – Multiple HP Jetdirect Firmware Upgrade



Device Network Configuration: HP Color LaserJet 4650 - 15.5.196.71

Configuration Categories

Ethernet Frame Type: ● Auto ○ Ethernet 802.3 ○ Ethernet II ○ Ethernet 802.2 ○ Ethernet SNAP

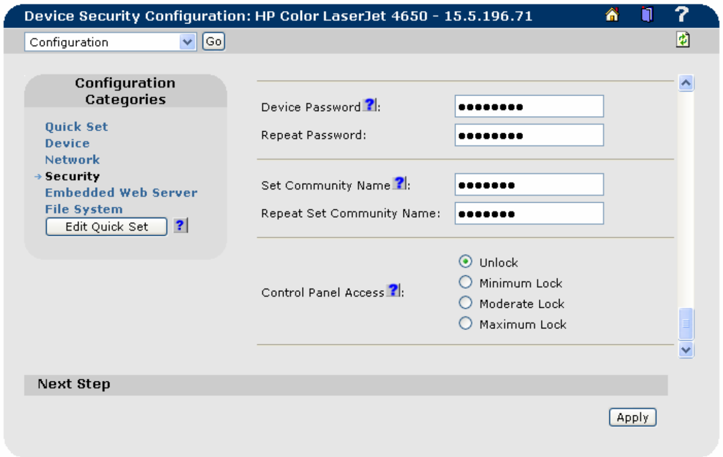
IPX SAP Broadcast Interval: 60

Queue Server Job Polling Interval: 2

Protocol Stacks: ☑ IPX/SPX ☑ TCP/IP ☑ DLC/LLC ☑ AppleTalk

Next Step

Figure 5 – Disable Unused Protocols



Device Security Configuration: HP Color LaserJet 4650 - 15.5.196.71

Configuration Categories

Device Password: ••••••••

Repeat Password: ••••••••

Set Community Name: •••••••

Repeat Set Community Name: •••••••

Control Panel Access: ● Unlock ○ Minimum Lock ○ Moderate Lock ○ Maximum Lock

Next Step

Figure 6 – Control Panel Lock

Minimum control panel lock

Menus that are locked	Menus that are unlocked
Configuration menu	Information menu
IO menu	Paper Handling menu
Resets menu	Print Quality menu
	EIO menu

Moderate control panel lock

Menus that are locked	Menus that are unlocked
Paper Handling menu	Information menu
Print Quality menu	Printing menu
Configuration menu	
IO menu	
EIO menu	
Resets menu	

Maximum control panel lock

Menus that are locked	Menus that are unlocked
Information menu	(None)
Paper Handling menu	
Print Quality menu	
Printing menu	
Configuration menu	
IO menu	
EIO menu	
Resets menu	

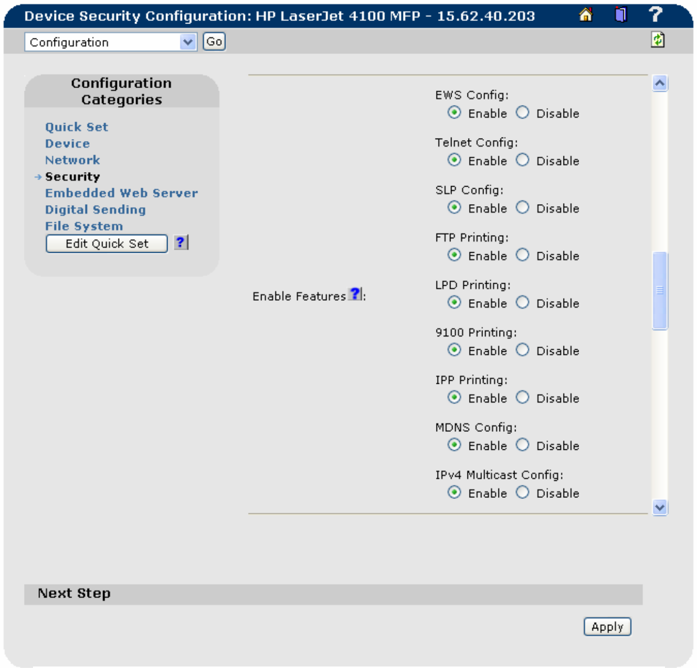
Disable Unused Services

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

The following techniques can be enabled/disabled by selecting *Configuration, Security, Enable Features* while viewing a device Status page in HP Web Jetadmin (see Figure 7):

- 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



Device Security Configuration: HP LaserJet 4100 MFP - 15.62.40.203

Enable Features:

EWS Config: ● Enable ○ Disable

Telnet Config: ● Enable ○ Disable

SLP Config: ● Enable ○ Disable

FTP Printing: ● Enable ○ Disable

LPD Printing: ● Enable ○ Disable

9100 Printing: ● Enable ○ Disable

IPP Printing: ● Enable ○ Disable

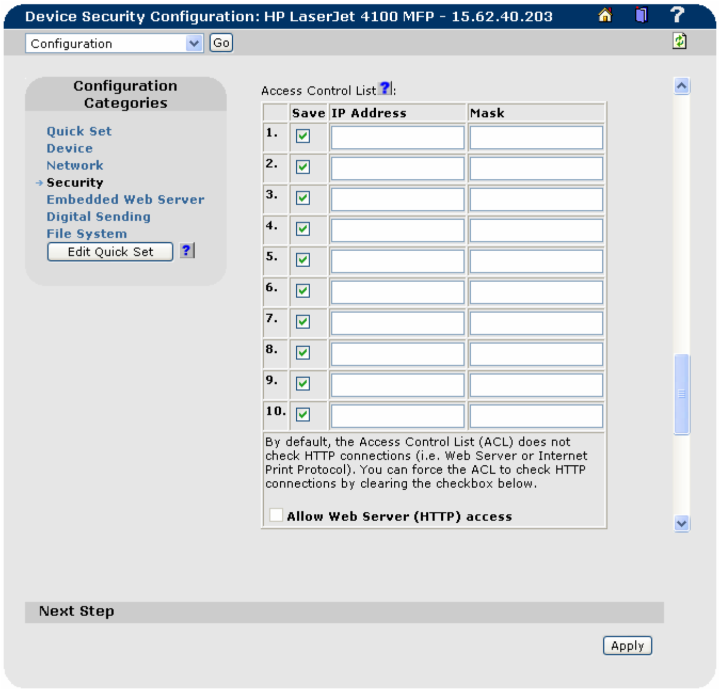
MDNS Config: ● Enable ○ Disable

IPv4 Multicast Config: ● Enable ○ Disable

Figure 7 – Enable Features

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 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 8).



Device Security Configuration: HP LaserJet 4100 MFP - 15.62.40.203

Configuration | Go

Configuration Categories
- Quick Set
- Device
- Network
- Security
- Embedded Web Server
- Digital Sending
- File System

Edit Quick Set

Access Control List:

	Save	IP Address	Mask
1.	☑		
2.	☑		
3.	☑		
4.	☑		
5.	☑		
6.	☑		
7.	☑		
8.	☑		
9.	☑		
10.	☑		

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

Next Step

Apply

Figure 8 – Access Control List

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.

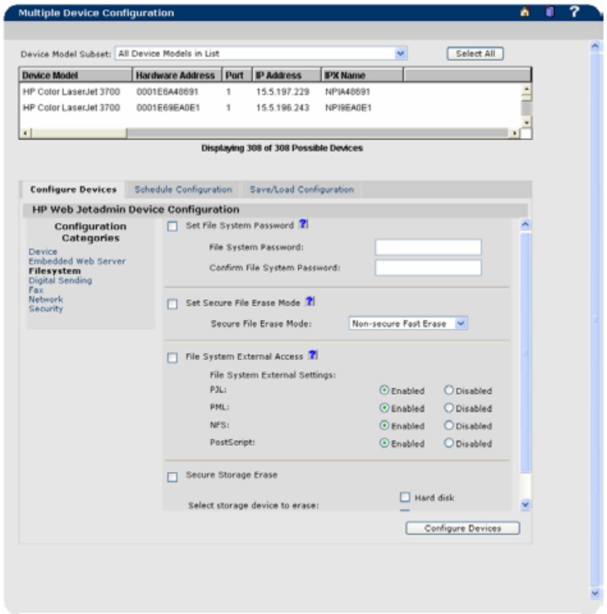
HP Web Jetadmin allows for adding or removing addresses from the Access Control List by selecting Configure, Network when viewing a Status page for a single device (see Figure 8).

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



Multiple Device Configuration

Device Model Subset: All Device Models in List | Select All

Device Model	Hardware Address	Port	IP Address	IPX Name
HP Color LaserJet 3700	0001E6A48691	1	15.5.197.229	NPIA48691
HP Color LaserJet 3700	0001E69EA0E1	1	15.5.196.243	NPI9EA0E1

Displaying 308 of 308 Possible Devices

Configure Devices | Schedule Configuration | Save/Load Configuration

HP Web Jetadmin Device Configuration

Configuration Categories
- Device
- Embedded Web Server
- Filesystem
- Digital Sending
- Fax
- Network
- Security

□ Set File System Password

File System Password:

Confirm File System Password:

□ Set Secure File Erase Mode

Secure File Erase Mode: Non-secure Fast Erase

□ File System External Access

File System External Settings:

PJL:	● Enabled	○ Disabled
PML:	● Enabled	○ Disabled
NFS:	● Enabled	○ Disabled
PostScript:	● Enabled	○ Disabled

□ Secure Storage Erase

Select storage device to erase: □ Hard disk

Configure Devices

Figure 9 – File System

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 9). 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 PJL, 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 PJL to manage the disk.

Credentials/Passwords

Ultimately, to deter unwanted configurations on the printer, credentials, or passwords, should be assigned to a device. Various versions of HP Jetdirect firmware have allowed for configuring several passwords including:

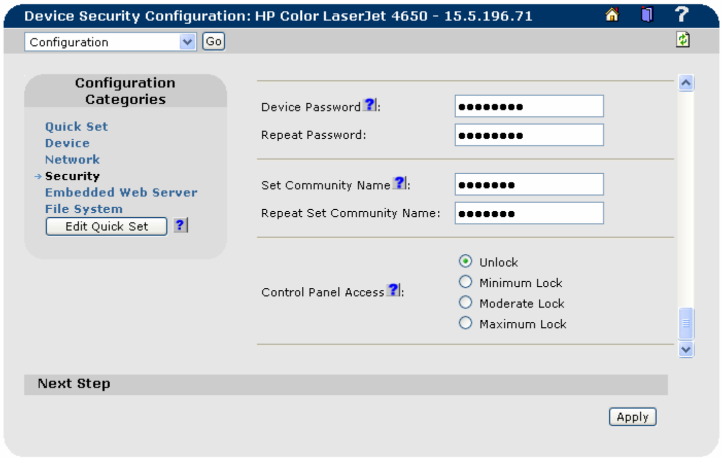
- HP Jetdirect password – an object residing on the HP Jetdirect device that software such as HP web Jetadmin will query before allowing an SNMP Set Request operation.
- Printer EWS password – an object residing on the printer that will deter unwanted printer configurations using HTTP (EWS).
- Telnet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

HP Web Jetadmin allows for setting a Device Password by selecting *Configuration, Security* while viewing the Status page of a device (see Figure 10). 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 Jetadmin will 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 of the device using SNMP.

The Printer EWS Password can also be set when browsing directly


Device Security Configuration: HP Color LaserJet 4650 - 15.5.196.71

Device Password: •••••••••
Repeat Password: •••••••••

Set Community Name: •••••••
Repeat Set Community Name: •••••••

Control Panel Access: ● Unlock ○ Minimum Lock ○ Moderate Lock ○ Maximum Lock

Figure 10 – Setting Credentials on Devices

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 opject 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 10), 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.

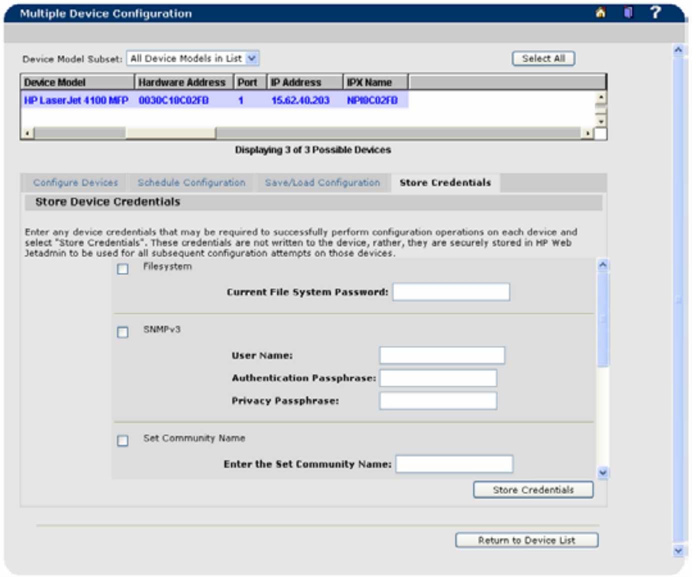
The Set Community Name can be synched up with the other administrator passwords in HP Jetdirect firmware versions 22.x.x or greater.

Store Credentials

Credentials such as *Set Community Name* or *Device Password* can now 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 11). 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.



Device Model Subset: All Device Models in List

Device Model	Hardware Address	Port	IP Address	IPX Name
HP LaserJet 4100 MFP	0030C10C02FB	1	15.62.40.203	NPI0C02FB

Displaying 3 of 3 Possible Devices

Store Device Credentials

Enter any device credentials that may be required to successfully perform configuration operations on each device and select "Store Credentials". These credentials are not written to the device, rather, they are securely stored in HP Web Jetadmin to be used for all subsequent configuration attempts on those devices.

□ Filesystem

Current File System Password:

□ SNMPv3

User Name:

Authentication Passphrase:

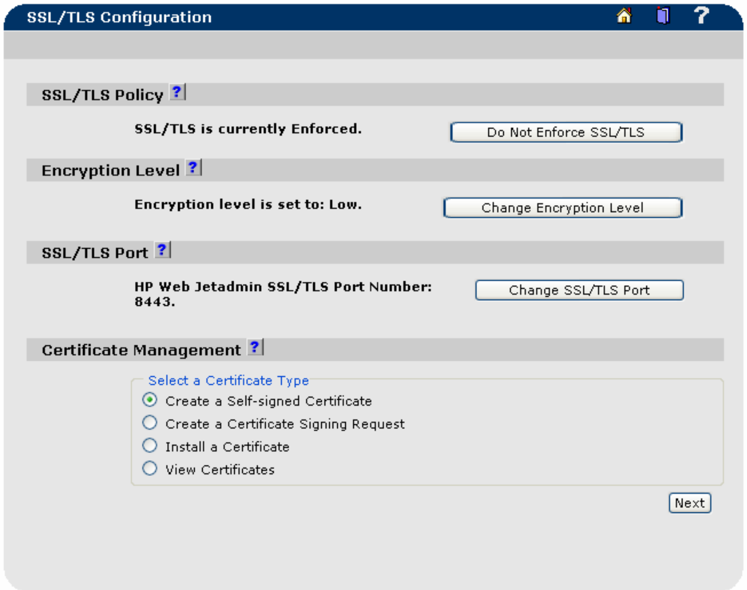
Privacy Passphrase:

□ Set Community Name

Enter the Set Community Name:

Figure 11 – 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.


SSL/TLS Configuration

SSL/TLS Policy ?

SSL/TLS is currently Enforced. [Do Not Enforce SSL/TLS]

Encryption Level ?

Encryption level is set to: Low. [Change Encryption Level]

SSL/TLS Port ?

HP Web Jetadmin SSL/TLS Port Number: 8443. [Change SSL/TLS Port]

Certificate Management ?

Select a Certificate Type
- ● Create a Self-signed Certificate
- ○ Create a Certificate Signing Request
- ○ Install a Certificate
- ○ View Certificates

[Next]

Figure 12 – SSL (Secure Sockets Layer)

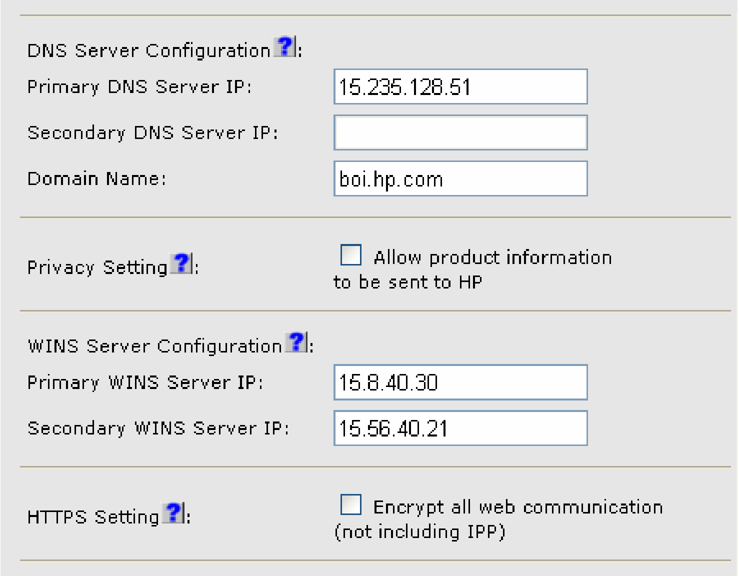
Configuration attempts can be automatically retried at a configurable frequency and number of attempts, in which case any new credentials that are stored in HP Web Jetadmin will be attempted again. Any time a device password, set community name, SNMPv3 credential, etc. is configured on a device through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

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 12).


DNS Server Configuration ?:

Primary DNS Server IP: 15.235.128.51

Secondary DNS Server IP:

Domain Name: boi.hp.com

Privacy Setting ?: □ Allow product information to be sent to HP

WINS Server Configuration ?:

Primary WINS Server IP: 15.8.40.30

Secondary WINS Server IP: 15.56.40.21

HTTPS Setting ?: □ Encrypt all web communication (not including IPP)

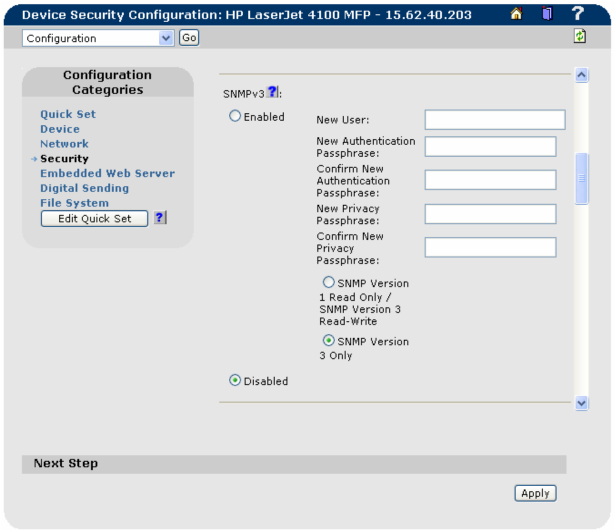
Figure 13 - HTTPS

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 13). Secure Hyper Text Transfer Protocol (HTTPS) provides secure, encrypted management 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.



Device Security Configuration: HP LaserJet 4100 MFP - 15.62.40.203

Configuration [Go]

Configuration Categories
- Quick Set
- Device
- Network
- → Security
- Embedded Web Server
- Digital Sending
- File System

[Edit Quick Set] ?

SNMPv3 ?:

○ Enabled

New User:

New Authentication Passphrase:

Confirm New Authentication Passphrase:

New Privacy Passphrase:

Confirm New Privacy Passphrase:

○ SNMP Version 1 Read Only / SNMP Version 3 Read-Write

● SNMP Version 3 Only

● Disabled

Next Step

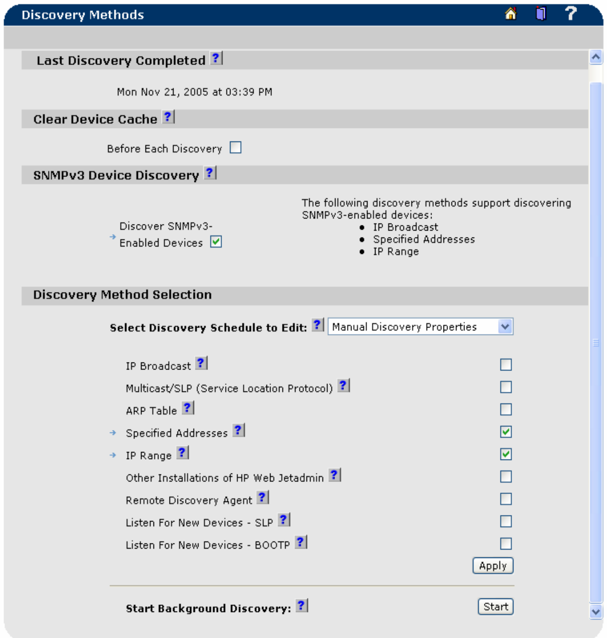
[Apply]

Figure 14 – SNMPv3

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 14). 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 15 and 16).

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.



Discovery Methods

Last Discovery Completed ?

Mon Nov 21, 2005 at 03:39 PM

Clear Device Cache ?

Before Each Discovery □

SNMPv3 Device Discovery ?

→ Discover SNMPv3-Enabled Devices ☑

The following discovery methods support discovering SNMPv3-enabled devices:
- IP Broadcast
- Specified Addresses
- IP Range

Discovery Method Selection

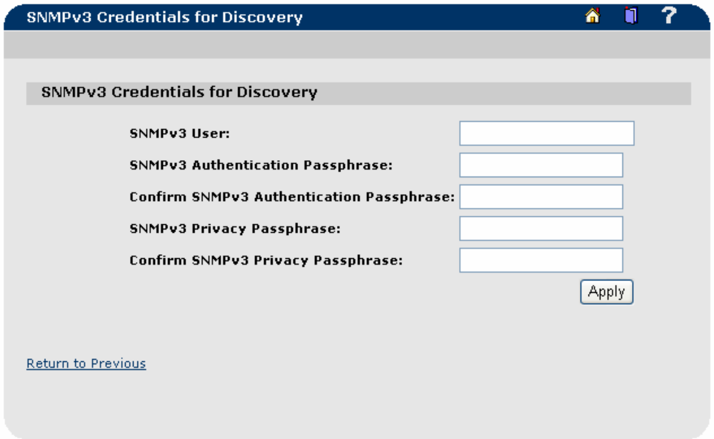
Select Discovery Schedule to Edit: ? Manual Discovery Properties

IP Broadcast ?	□
Multicast/SLP (Service Location Protocol) ?	□
ARP Table ?	□
→ Specified Addresses ?	☑
→ IP Range ?	☑
Other Installations of HP Web Jetadmin ?	□
Remote Discovery Agent ?	□
Listen For New Devices - SLP ?	□
Listen For New Devices - BOOTP ?	□

[Apply]

Start Background Discovery: ? [Start]

Figure 15 – SNMPv3 Discovery



SNMPv3 Credentials for Discovery

SNMPv3 Credentials for Discovery

SNMPv3 User:

SNMPv3 Authentication Passphrase:

Confirm SNMPv3 Authentication Passphrase:

SNMPv3 Privacy Passphrase:

Confirm SNMPv3 Privacy Passphrase:

[Apply]

Return to Previous

Figure 16 – SNMPv3 Credentials for Discovery

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 PJL access	Disables PJL access to the printer file system only. PJL 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.

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.