technical brief

Security
in HP Web Jetadmin

This technical brief discusses the security mechanisms available in HP Web Jetadmin 6.5.

Overview

HP Web Jetadmin is a web-based software utility for installing, configuring, and managing network-connected devices. Since it can install devices, change the configuration of devices, and create print queues to print to devices, security becomes an issue. Setting security on printers is important for many reasons including:

- reducing printer down time
- reducing helpdesk calls
- minimizing troubleshooting visits
- minimizing consumable usage

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.

Securing 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 should be considered.

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

- HTTP port
- Allow list
- User profiles

Naturally, a firewall is the first form of security that should be employed to keep unwanted internet users from browsing to any web server within an intranet, including HP Web Jetadmin.

HTTP Port

To keep unwanted users from within the intranet from browsing to an installation of HP Web Jetadmin, the HTTP port number can be changed under *Preferences, Network, HTTP* (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, this port number can be changed by the administrator to any desired number in order to keep unwanted users from having the ability to browse to the installation of HP Web Jetadmin.

Allow List

HP Web JetAdmin provides an Allow List to control which IP addresses (individual or range) or host names can have access to an installation of HP Web Jetadmin. This Allow List can be configured under *Preferences, Network, HTTP* (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 Allow List is configured.

User Profiles

User Profiles are perhaps the strongest 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 what parts of HP Web JetAdmin are

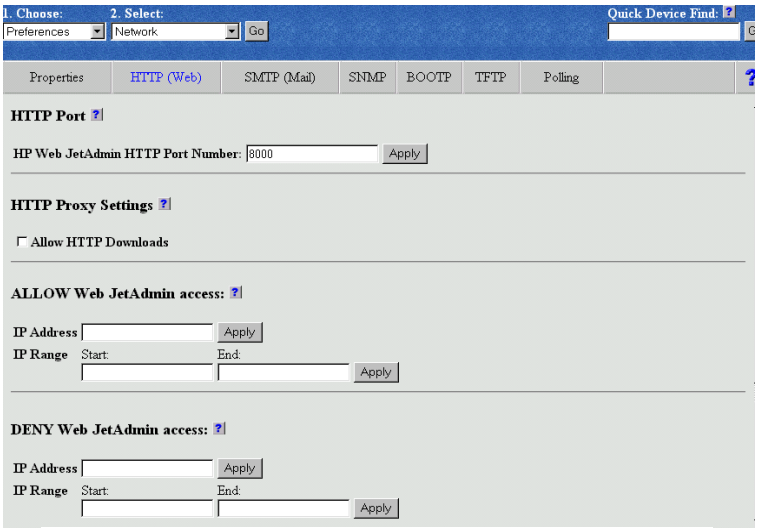

Figure 1

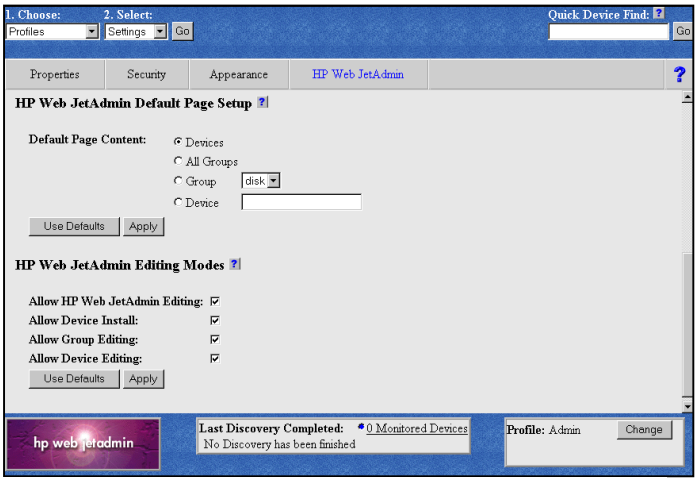

Figure 2

available to users

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 number of new profiles that can be created. The box in the lower right hand corner of the HP Web Jeradmin screen indicates which profile is currently in use (see Figure 2).

The default profile is the profile that HP Web JetAdmin automatically uses whenever anyone initially accesses it, and is defined by the administrator. If users do not have access to the default profile, they can select other profiles in the lower right hand portion of the screen.

Under *Profiles, Settings HP Web Jetadmin*, profiles can be quickly edited by allowing or denying access to four main permissions (see Figure 2):

- Allow Group Editing - controls the ability to make changes to existing device groups or create new groups.
- Allow Device Editing - controls the ability to make configuration changes to devices.
- Allow HP Web Jetadmin Editing - controls the ability to make configuration changes to HP Web Jetadmin itself.
- Allow Device Install - controls the ability to install new devices using HP Web Jetadmin.

By allowing or denying a combination of these four permissions, User Profiles can tailor access to HP Web JetAdmin features according to the needs of the person or group. For example, a Help Desk 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. The Admin Profile always has these four permissions and cannot be changed.

In addition, under *Profiles, Settings, Security,* profiles can be very finely tailored to the needs of various types of users (see Figure 3). There are several main permission categories of which a profile can allow or deny

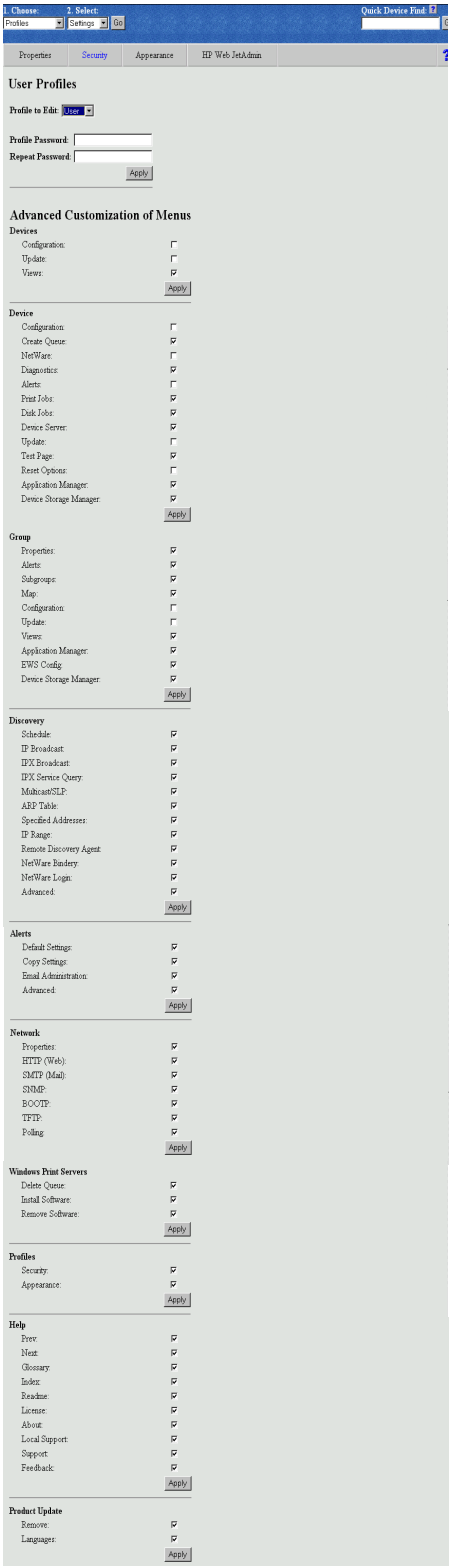

Figure 3

access to individual items that pertain to that category:

- Device
- Devices
- Groups
- Discovery
- Alerts
- Network
- Windows Print Servers
- Profiles
- Help
- Product Update

The individual items under each category determine which controls will appear in the user interface. For example, the *Device* section will control what type of device editing options will appear in the user interface, with each individual setting determining which tabs will appear on the menu bar.

These individual permission items provide a much more granular level of profile creation than the group permission levels described earlier.

Securing a Printer

While an installation of HP Web Jetadmin contains several methods for securing itself against unwanted access, controlling individuals from downloading HP Web Jetadmin from the web and using it to install and configure printers can be a challenge.

Setting security on the printer itself is probably the strongest form of security that can be enabled to avoid unwanted access to a networked printer. Users can access printers in a variety of methods, but setting security at the device level is effective no matter which technique is used to access the printer.

For example, configuration of a device can be accomplished through a variety of utilities including:

- HP Web Jetadmin
- HP Jetadmin

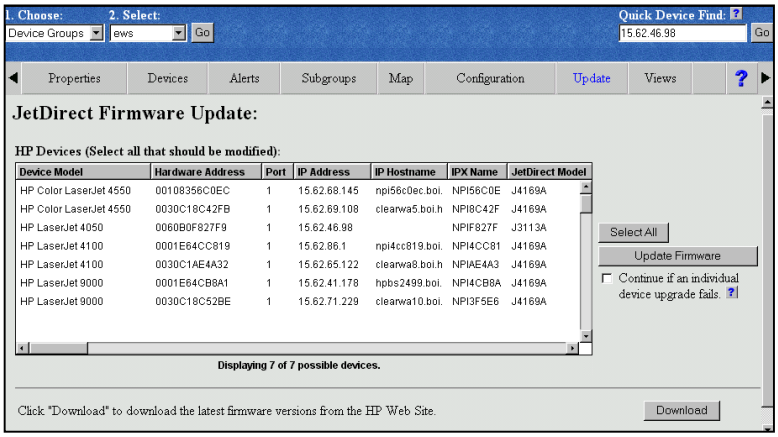

Figure 4

- HP Install Network Printer Wizard
- Telnet
- Embedded Web Server
- Any SNMP utility

With all of these avenues for potentially changing device configuration, 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.

Direct HP Web Jetadmin Device Security

HP Web Jetadmin provides multiple methods for securing devices against unwanted access including:

- upgrade the HP Jetdirect firmware to the highest level
- disable all unused protocols
- specify an administrator password
- specify an SNMP Set Community name
- lock the control panel

These are all techniques for enabling security that HP Web Jetadmin provides directly in the HP Web Jetadmin interface itself.
Other security techniques, such as:

- disable all unused services
- set access control list

are provided indirectly in HP Web Jetadmin by linking to the device Embedded Web Server page, and will be discussed later. Either way, administrators have the luxury of using a single tool to enforce desired device security mechanisms.

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 by selecting the *Upgrade* tab while viewing either a single device, a group of devices, or the list of all devices (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

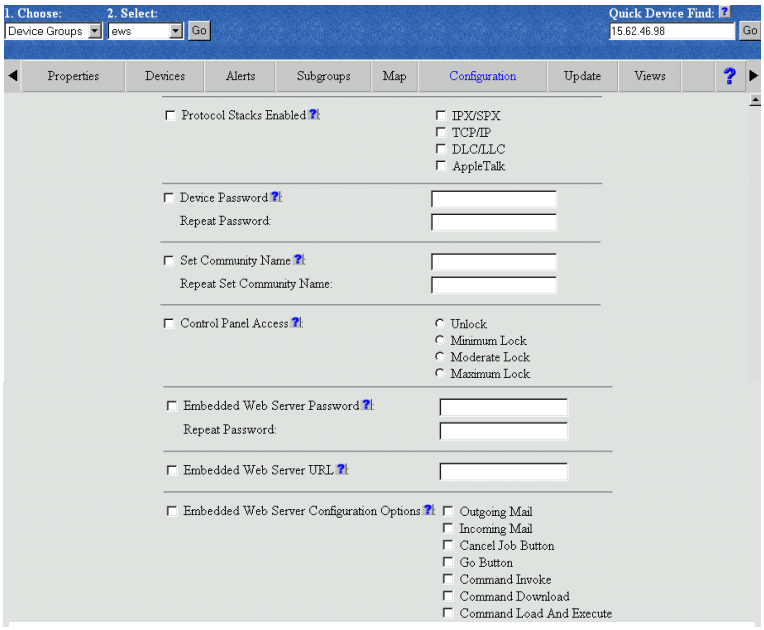

Figure 5

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 the *Configuration* tab while viewing either a single device, a group of devices, or the list of all devices (see Figure 5).

Set Administrator Password

Three methods exist for setting an administrator password on a printer to deter unwanted configurations of the printer:

- HP Jetdirect password
- HP Jetdirect EWS
- Printer EWS

Both the HP Jetdirect password and the printer EWS password can be set directly in the HP Web Jetadmin interface.

The HP Jetdirect password is set under the *Configuration* tab when viewing a device or group of devices in HP Web Jetadmin (see Figure 5). It is stored on the HP Jetdirect device and is verified during any attempts at device modification through any of the following utilities:

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

The HP Jetdirect password will only prevent configuration through HP utilities such as those listed above. Other SNMP utilities will still be able to change the configuration of the device because they will not check for the presence of this password. The HP Jetdirect password is not case sensitive and is saved across a power cycle.

Note: The HP Jetdirect password actually sets the same object on the HP Jetdirect device as the HP Jetdirect EWS password. Therefore, setting one actually sets the other. For example, if the HP Jetdirect password is set on a device, the password will be required when attempting to change device configuration via HP Jetdirect EWS.

HP Web Jetadmin can also cache the HP Jetdirect password after it is initially entered for the rest of the web browser session to avoid having to enter the same password multiple times.

The printer Embedded Web Server password can be set on printers with EWS capability directly in the HP Web Jetadmin interface by using two techniques, both of which can configure the password on multiple devices simultaneously

- under the EWS Config tab if the EWS Configuration Management plug-in has been installed (see Figure 6)
- selecting the *Configuration* tab while viewing a group of devices or the list of all devices (see Figure 5)

The printer EWS password will prevent users from changing printer configurations while browsing directly to the printer and accessing the

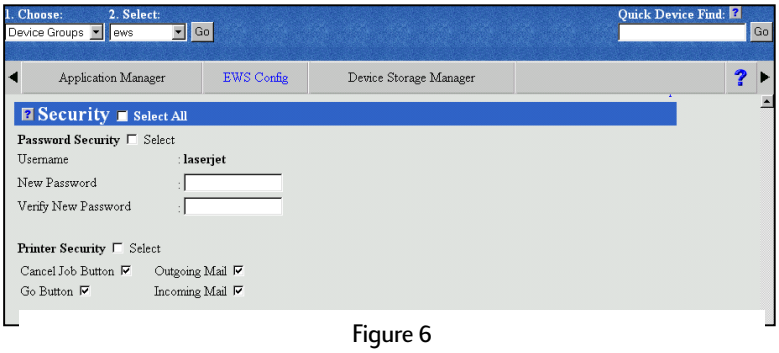

Figure 6

Embedded Web Server. This password is separate from the HP Jetdirect password and the HP Jetdirect EWS password.

Selecting the *Configuration* tab while viewing a group of devices or the list of all devices is a quick and easy way to assign consistent device passwords to more than one device at the same time (see Figure 5). Both the HP Jetdirect password and the printer EWS password can be set in batches from this screen.

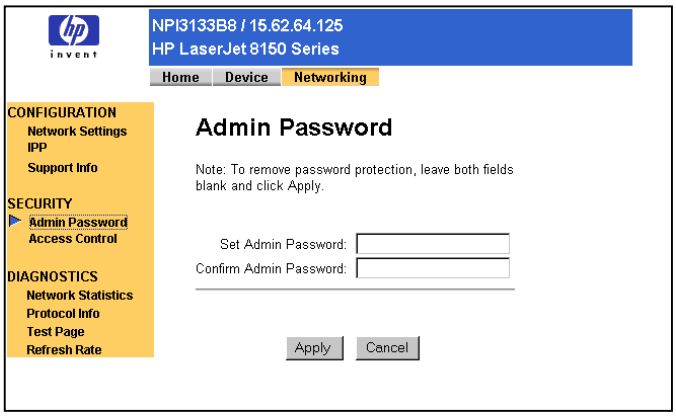

Figure 7

Specify SNMP Set Community Name

HP Web Jetadmin allows for setting the SNMP Set Community which is used to prevent unauthorized changes to devices via SNMP. This option can be set on individual devices by selecting *Configuration, Security* while viewing a single device or it can be set in batches by selecting the *Configuration* tab while viewing a group of devices or the list of all devices (see Figure 5). Only the users that have knowledge of the Set Community Name can make changes via SNMP. 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.

Lock Printer Control Panel

A printer control panel can be locked remotely through HP Web Jetadmin to keep unauthorized users from walking up to the printer and making changes on the control panel (see Figure 5). Users can still read the settings on the control panel but would not be able to change settings.

Most devices with control panel lock capability will offer the ability to define the level of access as either minimum, moderate, or maximum. The definitions for the different levels of access will depend on the device.

Indirect HP Jetadmin Device Security

As mentioned previously, HP Web Jetadmin can also provide access to other device security methods indirectly by linking to the device Embedded Web Server. The HP Web Jetadmin window remains open while launching the Embedded Web Server screen for a device.

In addition to providing additional security methods to prevent against unwanted device configuration, the device Embedded Web Server screens also provide 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

Fortunately, security methods exist under the HP Jetdirect Embedded Web Server that can prevent unwanted printing from users utilizing these various printing techniques.

Note: Most of the following security techniques are only available under the HP Jetdirect Embedded Web Server interface for the following HP Jetdirect products:

- HP Jetdirect 610n: J4169A, J4167A
- HP Jetdirect 175x: J6035A

Previous HP Jetdirect products may

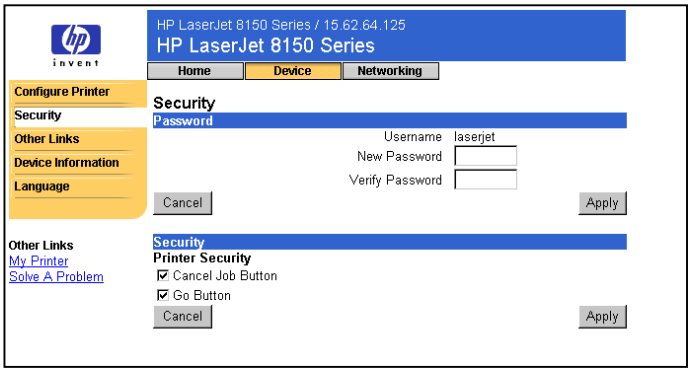

Figure 8

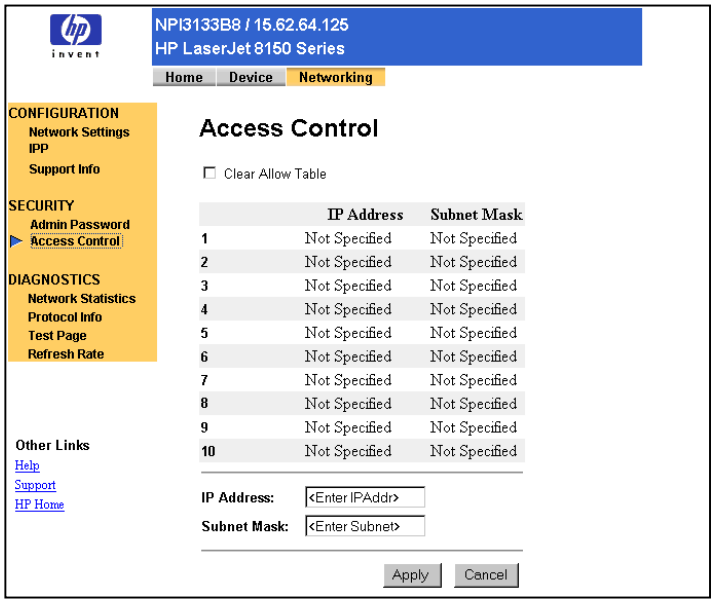

Figure 9

not contain all of the following security techniques under EWS. However, telnet can still be used to enable many of these options, as long as recent firmware exists on the HP Jetdirect device.

HP Jetdirect EWS Password

The HP Jetdirect EWS password is set on a device by selecting the *Device Server* tab while viewing a device in HP Web Jetadmin (see Figure 7). Selecting the *Device Server* tab actually launches a separate window for the HP Jetdirect Embedded Web Server interface, but HP Web Jetadmin remains open for a quick return. This password is verified during any attempts at device modification when browsing to the HP Jetdirect EWS. Information pertaining to the device can still be viewed through EWS but cannot be changed.

Note: The HP Jetdirect EWS password actually sets the same object on the HP Jetdirect device as the HP Jetdirect password. Therefore, setting one actually sets the other. For example, if the HP Jetdirect EWS password is set on a device, the password will be required when attempting to change device configuration via HP Jetadmin, HP Web Jetadmin, etc.

Printer EWS Password

The printer Embedded Web Server password can be set on a device by selecting the *Device Server* tab when viewing a printer that has EWS capability (see Figure 8), in addition the fact that it can be set from within the HP Web Jetadmin interface as mentioned earlier. This password will prevent users from changing printer configurations while browsing directly to the printer and accessing the Embedded Web Server. Selecting the *Device Server* tab actually launches a separate window for the printer Embedded Web Server interface, but HP Web Jetadmin remains open for a quick return.

Access Control List

The HP Jetdirect Embedded Web Server page to which HP Web Jetadmin links provides an additional security technique called the Access Control List. This option is accessed by selecting *Access Control* under *Security* (see Figure 9).

The Access Control List specifies a range of IP addresses that can establish TCP connections with the HP Jetdirect device.

The access control list affects printing as well as management. HP Web Jetadmin typically uses TCP packets during management of devices, while port monitors, such as the HP TCP/IP Standard Port Monitor, typically use TCP packets to send print jobs. These utilities will not be able to configure devices or print to devices if they are excluded from the Access Control List.

Disable Unused Services

Additional techniques for either configuring a device or printing to a device can be disabled through the HP Jetdirect EWS interface to provide even more security against unwanted device access. These additional techniques can be accessed by selecting *Advanced Settings* under *Network Settings* (see Figure 10).

The following techniques can be enabled/disabled:

- SLP Config: Service Location Protocol. Used primarily for IP Multicast discovery.
- Telnet Config: telnet is used for device configuration.
- 9100 Printing: TCP Port 9100 printing, used by Microsoft port monitors such as the HP TCP/IP Standard Port Monitor, HP Jetdirect Port Monitor, Microsoft Standard Port Monitor.
- FTP Printing: File Transfer Protocol printing
- LPD Printing: Line Printer Daemon printing
- IPP Printing: Internet Printing Protocol

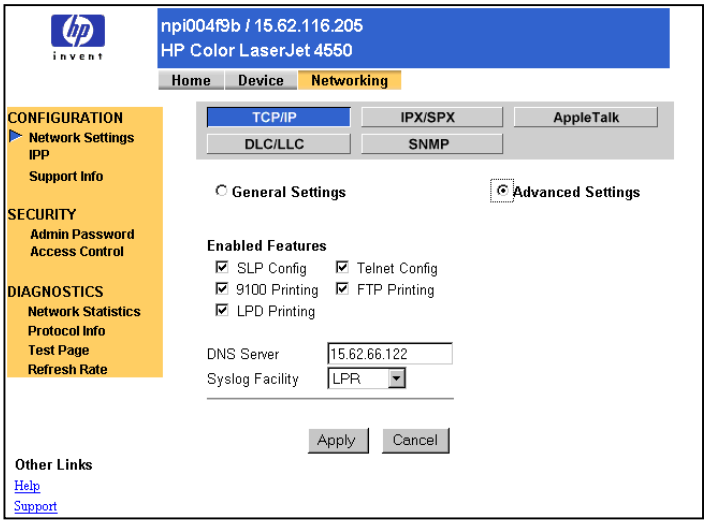

Figure 10

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.

Appendix A

This table displays security methods that HP Web Jetadmin provides (directly or indirectly) to protect devices against unwanted access. The first section displays security methods to protect against unwanted device configuration methods, while the second section displays security methods to protect against unwanted printing methods.

Configuration Method	Security Method	Description
HP Web Jetadmin	HP Jetdirect password	HP Web Jetadmin checks for the presence of this password on the HP Jetdirect device before allowing configuration to occur.
	Set Community Name	HP Jetdirect device will not allow SNMP SET REQ commands (which HP Web Jetadmin uses for device configuration) without this password.
	Access Control List	Will not allow TCP packet access unless IP address is included in the Access Control List. HP Web Jetadmin uses TCP packets to initiate connections to devices
HP Jetadmin	HP Jetdirect password	HP Jetadmin checks for the presence of this password on the HP Jetdirect device before allowing configuration to occur.
	Set Community Name	HP Jetdirect device will not allow SNMP SET REQ commands (which HP Jetadmin uses for device configuration) without this password.
	Access Control List	Will not allow TCP packet access unless IP address is included in the Access Control List. HP Jetadmin uses TCP packets to initiate connections to devices.
HP Install Network Printer Wizard	HP Jetdirect password	HP Install Network Printer Wizard checks for the presence of this password on the HP Jetdirect device before allowing configuration to occur.
	Set Community Name	HP Jetdirect device will not allow SNMP SET REQ commands (which HP Install Network Printer Wizard uses for device configuration) without this password.
	Access Control List	Will not allow TCP packet access unless IP address is included in the Access Control List. HP Install Network Printer Wizard uses TCP packets to initiate connections to devices.
Telnet	Disable telnet access	telnet access, used for device configuration, can be disabled under the HP Jetdirect EWS.
Any SNMP Utility	Set Community Name	HP Jetdirect device will not allow SNMP SET REQ commands from any utility without this password.
	Disable Unused protocols	Disabling unused protocols, such as IPX/SPX, can keep unwanted device configurations from occurring through SNMP utilities.

Printing Method	Security Method	Description
HP TCP/IP Standard Port Monitor	Access Control List	Will not allow TCP packet access unless IP address is included in the Access Control List. HP TCP/IP Standard Port Monitor uses TCP packets to send print jobs.
	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.
HP IPX/SPX Standard Port Monitor	Disable Unused protocols	Disabling unused protocols, such as IPX/SPX, can keep unwanted printing from occurring through the HP IPX/SPX Standard Port Monitor.
HP Jetdirect Port Monitor	Access Control List	Will not allow TCP packet access unless IP address is included in the Access Control List. HP Jetdirect Port Monitor can use TCP packets to send print jobs.
	Disable Port 9100 printing	Port 9100 printing, which HP Jetdirect Monitor can utilize to send print jobs, can be disabled.
	Disable Unused protocols	Disabling unused protocols, such as IPX/SPX, can keep unwanted printing from occurring through the HP Jetdirect Port Monitor configured to use IPX/SPX.
Microsoft Standard Port Monitor	Access Control List	Will not allow TCP packet access unless IP address is included in the Access Control List. Microsoft Standard Port Monitor uses TCP packets to send print jobs.
	Disable Port 9100 printing	Port 9100 printing, which Microsoft 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 Microsoft Standard Port Monitor, can be disabled.
LPD (LPR Port)	Disable LPD printing	LPD, which is typically used in UNIX environments for printing, and is used by the Microsoft Windows NT LPR Port, can be disabled.
FTP	Disable FTP printing	FTP (file transfer protocol) printing can be disabled.
IPP	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.