

HP Jetdirect Security Guidelines



Table of Contents:

- Introduction 1
- HP Jetdirect Overview 2
- What is an HP Jetdirect? 3
- How old is Your HP Jetdirect? 4
- Upgrading 5
- HP Jetdirect Administrative Guidelines 6
- HP Jetdirect Hacks: TCP Port 9100 7
- HP Jetdirect Hacks: Password and SNMP Community Names 9
- HP Jetdirect Hacks: Firmware Upgrade 9
- HP Jetdirect Hacks: Sniffing Print Jobs and Replaying Them 10
- HP Jetdirect Hacks: Printer/MFP access 10
- Recommended Security Deployments: SET 1 11
- Recommended Security Deployments: SET 2 12
- Recommended Security Deployments: SET 3 18
- Recommended Security Deployments: SET 4 28
- Further Reading 33

Introduction

The availability of public information on the Internet for hacking HP Jetdirect products has prompted customers to ask HP about how they can protect their printing and imaging devices against such attacks and what is HP doing about preventing those attacks. In all fairness, some of this public information is of rather poor quality and inflammatory; however, some websites detailing the attacks and the vulnerabilities on HP Jetdirect are informative and raise valid concerns that need to be addressed. It is the purpose of this whitepaper to address customer concerns about these attacks and vulnerabilities and to recommend proper security configurations to help customers protect their printing and imaging devices. This whitepaper is only a small part of a broad initiative within HP to educate our customer base about printing and imaging security. Resources such as The Secure Printing website (<http://www.hp.com/go/secureprinting>) provide a great deal of information for customers about products, solutions, as well as configuration recommendations. In general, a lot of this information can be put to use on existing HP Jetdirect products, mainly because HP Jetdirect was

one of the first print servers to widely implement security protocols such as SSL/TLS, SNMPv3, 802.1X, and IPsec.

If you are new to security and secure configurations, it is important to remember that 'security' is a process. Today's security configurations and protocols that are thought to be unbreakable for the next few years may in fact be broken later today. At one extreme, the best security available for imaging and printing devices is to never unpack them once you buy them. At the other extreme, the worst security available is unboxing them, powering them up, getting a configuration page to find the IP address, adding them to your desktop computer system or printer spooler, and then forgetting about them. Does that last part sound like your printing and imaging security strategy?

One of the challenges HP Jetdirect has in terms of security is actually the result of being "plug-n-play" and reliable. As we will find out, "plug-n-play" and "security" often do not belong in the same sentence. Hundreds of thousands, and perhaps a few million HP Jetdirect products have been in use for years and have never had their firmware updated or their configuration changed. In today's increasingly security focused environment, we know that this is not a sound practice for maintaining the proper operation of an infrastructure, regardless of the type of device in question.

HP Jetdirect Overview

Years ago, the world networked printers by connecting them via parallel ports or serial ports to computers called spoolers. These spoolers then shared the printers via networking protocols such as LPD to clients on the network. The length limits of serial and parallel based cables prohibited printers from moving too far from the spoolers.

The incredible print quality of the HP LaserJet printers compared to other technologies at the time fueled an unprecedented growth in the printing industry. The complexity and capability of printers increased and the need to connect to a spooler in order to share printers became a burden. HP Jetdirect was designed to allow users to share printers on the network without the need of direct attachment to a spooler. While migrating to networking printers, the goal was to have the same ease of use as a directly connected printer. HP Jetdirect would automatically initialize all protocols to the best of its ability in order to allow users to print to Jetdirect immediately. Popular HP tools, such as Jetadmin, simplified configuration of HP Jetdirect devices by taking advantage of proprietary protocols as well as well-known default security settings.

At the time HP Jetdirect was introduced, there was a variety of competition in the market place regarding protocol suites and networking infrastructure. Protocol suites such as AppleTalk, DLC/LLC, and IPX/SPX were deployed widely and had as much market share as TCP/IP. In addition, Token-Ring, FDDI, LocalTalk, ATM, and other ways of transporting frames had been adopted (or hyped) almost as much as Ethernet. During this growth period in network printing, functionality within HP Jetdirect was designed to promote 'Ease-of-Use', to reduce support calls, and to provide a rich customer experience regardless of the protocol or networking infrastructure they were using. In short, HP Jetdirect was designed to be "plug-n-play" on the network and behave as if the printer was directly connected to your PC.

Fast forwarding to the present, we have clear winners in intranet networking connectivity: TCP/IP and Ethernet. An 'Ease of Use' design criterion now has an arch nemesis: 'Security'. Customers are starting to ask how to deploy printing and imaging devices securely rather than how to deploy them as fast and painlessly as possible.

What is an HP Jetdirect?

When printers were directly connected to network spoolers, often a simple hardware protocol was used to send data from the PC to the printer. Centronics mode on a parallel port would be an example. As customers demanded faster data transfer speeds and richer status, these protocols became more complex as in IEEE 1284.4. In short, a printer had direct connect ports (e.g., serial, parallel) that implemented a hardware protocol and converted encapsulated data into just data for printer consumption. As customers began to network their printers, HP decided to embark on a strategy that still remains in use to this day: Use a smart networking card to implement the various networking infrastructure components to convert encapsulated network data into data for printer consumption. Thus, the HP Jetdirect was born – one of the first Networking Protocol offload engines. Let's refer to Figure 1 – Functional Diagram

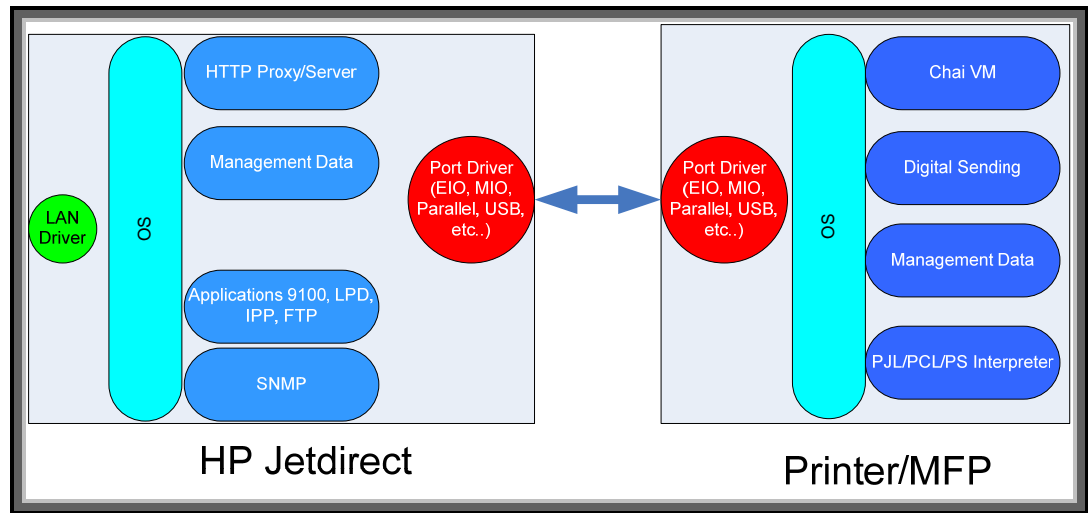


Figure 1 - Functional Diagram

In Figure 1, you can see the standard diagram of an offload engine. This diagram is by no means comprehensive, but does convey the difference between HP Jetdirect and Printer/MFP platforms. Why is this diagram important? First and foremost, we can understand what HP Jetdirect can do to help in the security of your printing infrastructure. Secondly, we can also understand what HP Jetdirect cannot do. As an example, some information on the Internet conveys that the P.JL parser is implemented on HP Jetdirect. Based upon this diagram, we know that is false. Upgrading your HP Jetdirect card to provide your printer more P.JL parsing protection is not going to be a good investment. Upgrading your HP Jetdirect card to control who can and who cannot interact with your printer is a good investment.

How old is Your HP Jetdirect?

Once in a while, when doing an inventory of a network, an administrator may discover some network connected devices that rather old but are still working. The same is true for printers and HP Jetdirect devices. An easy way to get an inventory of your HP Jetdirect devices is to use the HP Download Manager available here: http://www.hp.com/go/dlm_sw. This utility allows you to discover printers and their HP Jetdirect devices on the network. For an in-depth management platform, try HP Web Jetadmin available here: <http://www.hp.com/go/webjetadmin>. Keep in mind, you don't have to update the firmware on your HP Jetdirect products if you don't want to (HP does recommend it), but for this particular section we simply want to find HP Jetdirect devices and based upon their product number, see how old they are. Refer to Table 1 – HP Jetdirect Aging

Description	Date Released
Microsoft Windows for Workgroups 3.11	February 1994
HP Jetdirect J2550A, J2552A MIO Print Servers	May 1994
Microsoft Windows 95	August 1995
HP Jetdirect J2550B, J2552B MIO Print Servers	November 1996
HP Jetdirect J3110A, J3111A EIO Print Servers	October 1997
HP Jetdirect J3263A 300X External Print Server	January 1998
HP Jetdirect J3113A 600n EIO Print Server	January 1998
Microsoft Windows 98	June 1998
HP Jetdirect J3258A 170x External Print Server	September 1998
Microsoft Windows 2000 Professional	February 2000
HP Jetdirect J4169A 610n EIO Print Server	October 2000
Microsoft Windows XP	October 2001
HP Jetdirect J6057A 615n EIO Print Server	April 2002
Microsoft Windows 2003 Server	April 2003
HP Jetdirect J7934A 620n EIO Print Server	April 2004
HP Jetdirect J7961A 635n EIO Print Server	October 2005

Table 1 – HP Jetdirect Aging

Table 1 is by no means complete. Many Jetdirect cards were introduced before 1994; however, some popular HP Jetdirect products are listed there and compared to some of the Microsoft Windows introduction dates. It would be rare to find a reputable security analyst willing to spend time discussing the security issues associated with Microsoft Windows for Workgroups 3.11 and Microsoft Windows 95 in today's environment. When viewing public information about the security vulnerabilities of HP Jetdirect devices, be sure to keep in mind how old the devices may be.

At the time of this writing (August 2007), migrating to Microsoft Windows XP SP2 and Microsoft Windows 2003 SP2 is very important to get the most security protection for desktops and servers. Microsoft provides many guidelines to the proper configurations of their products and many security consultants make a living by helping customers deploy these configurations. Customers are willing to carry this expense because the security of their data is very important to them. If your printing infrastructure is important to you, should you not consider upgrading it and implementing recommended security configurations as well? As a point of comparison, some companies place a lot of their faith in a printing infrastructure that they developed in the early 1990s. How many of these customers would also be willing to run Microsoft Windows 95 on their desktops and Microsoft Windows Advanced Server 3.51 on their servers today?

Upgrading

Upgrading your HP Jetdirect devices is by no means a requirement, but is highly recommended. Should a customer choose to do so, HP can provide some guidelines. First, if the HP Jetdirect device was introduced before the year 2000, HP recommends that it be upgraded to a newer model. Some security features of the models that are available for customers to purchase as of August 2007 are shown in Table 2 – HP Jetdirect Models:

HP Jetdirect	Security Features
J3258G 170x External Parallel Print server	Non-Cryptographic Security, not upgradeable to newer firmware after purchase
J6035G 175x External USB 1.1 Print Server	Non-Cryptographic Security, not upgradeable to newer firmware after purchase
J3263G 300x External Print server	Non-Cryptographic Security, upgradeable after purchase
J7983G 510X External 3-Port Print Server	Non-Cryptographic Security, upgradeable after purchase
J7942G en3700 External USB 2.0 Print Server	SSL/TLS for Management, SNMPv3, 802.1X PEAP.
J7934G 620n EIO 10/100 Print Server	SSL/TLS for Management, SNMPv3, 802.1X PEAP.
J7949E Embedded Jetdirect 10/100 (not for sale individually, comes installed on the formatter for certain printers/MFP devices)	Running V.33.14 or later firmware: SSL/TLS for Management, SNMPv3, 802.1X PEAP.
J7982E Embedded Jetdirect 10/100 (not for sale individually, comes installed on the formatter for certain printers/MFP devices)	Firewall, SSL/TLS for Management, SNMPv3, 802.1X PEAP, 802.1X EAP-TLS.
J7997G 630n EIO 10/100/1000 Print Server	Firewall, SSL/TLS for Management, SNMPv3, 802.1X PEAP, 802.1X EAP-TLS.
J7961G 635n EIO 10/100/1000 IPv6/IPsec Print Server	IPsec/Firewall, SSL/TLS for Management, SNMPv3, 802.1X PEAP, 802.1X EAP-TLS

Table 2 - HP Jetdirect Models

In Table 3 – Discontinued HP Jetdirect Models, some popular HP Jetdirect devices that are no longer being sold by HP and their security capabilities are shown.

HP Jetdirect	Security Features
J4100A 400n 10/100 MIO Print server	Non-Cryptographic Security, upgradeable after purchase
J4106A 400n 10Mbps MIO Print server	Non-Cryptographic Security, upgradeable after purchase
J3110A 600n 10Mbps EIO Print server	Non-Cryptographic Security, upgradeable after purchase
J3111A 600n 10Mbps EIO Print server	Non-Cryptographic Security, upgradeable after purchase
J3113A 600n 10/100 EIO Print server	Non-Cryptographic Security, upgradeable after purchase
J4169A 610n 10/100 EIO Print Server	SSL/TLS for Management, SNMPv3
J6057A 615n 10/100 EIO Print Server	SSL/TLS for Management, SNMPv3

Table 3 - Discontinued HP Jetdirect Models

As you can see, replacing a discontinued 400n MIO model with a new external parallel port print server like the 300X will not upgrade the security capabilities of the Jetdirect device. Printers that have an MIO slot like the LaserJet IIIsi and LaserJet 4si have been discontinued for many years. Printers and MFPs with an EIO slot are still being sold today. The EIO slot was introduced on the HP LaserJet 4000 almost ten years ago. One of the great features of having an EIO based printer is the ability to install a J7961G 635n IPv6/IPsec print server. Using this product, we can take an older printer like the HP LaserJet 4000 and give it the latest in networking protocol and security support. This flexibility will come in handy as we evaluate the various attacks employed against HP Jetdirect and some ways to counteract those attacks. For companies with a lot of EIO based printers, proper deployment of the 635n can protect their printer/MFP investment and increase the security of their printing and imaging infrastructure.

HP Jetdirect Administrative Guidelines

In the material that follows, this whitepaper will be addressing some public information available about vulnerabilities or attacks against HP Jetdirect. In order to properly recommend configurations for HP Jetdirect, four different administrative guidelines will need to be used. These administrative guidelines come from the four main HP Jetdirect product lines, referred to as SETs.

- **SET 1:** The 170x, 300x, 500x, 510x, 400n, 600n models. The administrative guideline for securing these devices is located here: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj05999>. As a reminder, these devices do not have cryptographic security capability.
- **SET 2:** The 610n, 615n, 620n, 625n, en3700, and Embedded Jetdirect (J7949E) models. SET 2 can use the administrative guideline referenced for SET 1 products, but a more updated administrative tool available via the EWS for securing these devices is located here: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj07576>
- **SET 3:** The 630n and Embedded Jetdirect (J7982E, J7987E, J7991E, and J7992E) models. SET 3 can use the administrative guideline referenced for SET 2 products, but have additional security by means of a Firewall. The Firewall can allow/drop packets on the basis of IPv4/IPv6 addresses as well as service types.
- **SET 4:** The 635n model and the CM8000 Color MFP series (J7974E). These models have the most security capability in HP Jetdirect's product line.

With security configurations, one must be careful not to lock the front door and leave your windows open. In many cases, one must "lock down" several things before securing one thing can be effective. Before using the techniques presented here, the administrator **at the very least** should do the following:

- Update all HP Jetdirect firmware to the highest level. One of the easiest ways to perform this operation is to use the HP Download Manager available at http://www.hp.com/go/dlm_sw. Using Internet Mode, the HP Download Manager will automatically indicate which devices need to be upgraded. HP recommends always upgrading only a few devices and performing an evaluation of those devices on your network before upgrading all devices to the latest firmware.
- An Embedded Web Server (EWS) password has been specified
- The default SNMPv1/v2c SET Community Name has been changed
- All non-active protocols have been disabled (e.g., IPX/SPX, AppleTalk)
- Mark any product that cannot be firmware upgraded to the highest level as a security risk.

- A guideline to popular HP Jetdirect devices and the firmware they should be running as of August of 2007 is shown in Table 4:

HP Jetdirect Product Number	Firmware Version
J7949E Embedded Jetdirect	V.33.14/V.33.15
J4100A 400n 10Mbps MIO Print server	K.08.49
J4106A 400n 10Mbps MIO Print server	K.08.49
J3110A 600n 10Mbps EIO Print server	G.08.49
J3111A 600n 10Mbps EIO Print server	G.08.49
J3113A 600n 10/100 EIO Print server	G.08.49
J4169A 610n 10/100 EIO Print Server	L.25.57
J6057A 615n 10/100 EIO Print Server	R.25.57
J3263A/J3263G 300x External Print server	H.08.60
J3265A 500X External 3-Port Print Server	J.08.60
J7983G 510X External 3-Port Print Server	J.08.60
J7942A/J7942G en3700 External USB 2.0 Print Server	V.28.22
J7934A/J7934G 620n EIO 10/100 Print Server	V.29.20
J7960A/J7960G 625n EIO 10/100/1000 Print Server	V.29.29
J7961A/J7961G 635n EIO 10/100/1000 IPv6/IPsec Print Server	V.36.11

Table 4 – Jetdirect Firmware Versions

NOTE: For some Embedded Jetdirect products, you'll need to upgrade the printer/MFP firmware to update the JDI firmware.

Now that we covered enough background information, let's look at some of the reported vulnerabilities and attacks on HP Jetdirect.

HP Jetdirect Hacks: TCP Port 9100

TCP port 9100 was one of the first ways developed for sending print data to a printer. Some public references talk about a print protocol that exists on TCP port 9100. There isn't one. Raw data delivered to the TCP layer on the HP Jetdirect device is sent to the printer as if it had been delivered over a parallel port, serial port, or any other port. TCP port 9100 is the fastest and most efficient way of delivering data to a printer using the TCP/IP protocol suite.

The most common hack for TCP Port 9100 is send a job to that port that has some PJI commands in it. These PJI command can do a variety of things, one of the most common ones being to change the control panel display. Remember that HP Jetdirect is stripping off the TCP/IP headers and presenting this data directly to the printer. The printer is processing the PJI (data) as if the printer was directly connected to a PC. Many years ago, printer drivers would use the PJI command suite to control the printer in a variety of ways. As we can see, in the networking world, there is a potential for misuse.

How does an Administrator prevent TCP Port 9100 from being misused? Based upon what we've learned about HP Jetdirect so far, we know we have to control who can and who cannot establish a TCP connection to TCP Port 9100. Table 5 shows us some options, presented in the form of the least amount of security (option 1) to higher levels of security (options > 1):

Which hosts need to print?	Options
Only computers on the same subnet as HP Jetdirect	<p>Option 1) For SET 1/2/3/4. Eliminate the default gateway (set to 0.0.0.0). This doesn't prevent HP Jetdirect from receiving packets from other subnets, but does prevent the responses from returning to those remote subnets. As a result, TCP connections cannot be formed.</p> <p>Option 2) For SET 1/2/3/4. Setup an access control list with the IP address and mask for the local subnet.</p> <p>Option 3) For SET 3. Setup a rule to protect print traffic using the Firewall.</p> <p>Option 4) For SET 4. Setup a rule to protect print traffic using the IPsec.</p>
Ten or less individual computers on different subnets	<p>Option 1) For SET 1/2/3/4. Setup an access control list for each individual IP address with a mask of 255.255.255.255.</p> <p>Option 2) For SET 3. Setup a rule to protect print traffic using the Firewall</p> <p>Option 3) For SET 4. Setup a rule to protect print traffic using IPsec</p>
All hosts in the company.	<p>Option 1) For Set 1/2/3/4. Setup an access control list for the network ID assigned to your company. As an example, for HP's internal network, there would be two entries: IP - 15.0.0.0 mask - 255.0.0.0 and IP -16.0.0.0 mask - 255.0.0.0.</p> <p>Option 2) For SET 3. Setup a rule to protect print traffic using the Firewall</p> <p>Option 3) For SET 4. Setup a rule to protect print traffic using IPsec</p>

Table 5 – Access Control

Because there are many print protocols supported over TCP, the next logical step is to disable all print protocols that the administrator doesn't use. How to disable these protocols can be found in the administrative guidelines for the appropriate product SET.

It is important to note that all TCP/IP traffic to any device (not just HP Jetdirect) that is not cryptographically protected is subject to IP address spoofing and Man-in-the-Middle (MITM) attacks. These attacks can target any TCP/IP traffic. Also, some cryptographic protections can be used but may not be deployed correctly. For instance, if you are relying on SSL/TLS to protect your data, you need to have the certificates used by SSL/TLS to be properly signed by a trusted Certificate Authority. Otherwise, SSL/TLS is subject to MITM attacks as well because it depends on a robust PKI to successfully authenticate the server endpoint (and optionally the client endpoint).

What about the user at work that is allowed to print but keeps changing the display or doing other mischief with the printer using TCP Port 9100? Well, that really is no different then if they were printing personal items at work, running the printer out of consumables with large print jobs, etc... If

they are trusted to establish a print connection, they are trusted to print. Some additional protections can be provided, in the form of Color Access Controls using HP's Universal Print Driver (UPD), which allow an administrator to control the amount of color being used by a user. In addition, HP's Web Jetadmin includes functionality called Report Generator which facilitates reports on users and their how their printing behavior. This functionality is useful for auditing and understanding printer usage.

HP Jetdirect Hacks: Password and SNMP Community Names

HP Jetdirect password and SNMP Community Name behavior has definitely evolved over the years. An excellent resource for the history and current behavior is located here:

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00004828>.

In short, keep your firmware updated on your HP Jetdirect, use the latest client software from HP, and upgrade to the latest Web Jetadmin management software. After you have upgraded all software and firmware, change your passwords on these devices to something new. This process will help make your HP Jetdirect devices behave the same regarding their password handling.

To better protect passwords from passive sniffing, consider using SSL/TLS. SET 2/3/4 support automatic redirection to SSL/TLS and prevents HTTP from being used to access the EWS (if the administrator so desires). However, when using SSL/TLS, be sure to update the HP Jetdirect certificate to a certificate issued by a trusted CA to properly avoid MITM attacks. Also, consider migrating to SNMPv3. HP Web Jetadmin can be configured to use SNMPv3 automatically. HP Jetdirect devices that belong to SET 2, 3, or 4 support SNMPv3.

HP Jetdirect Hacks: Firmware Upgrade

A nice overview of the various methods used by HP Jetdirect to upgrade firmware is described here:

http://www.hp.com/go/webjetadmin_firmware.

All HP Jetdirect firmware files follow the same basic format: a recovery partition and a main functionality partition. In case of an upgrade programming failure (due to a network outage, client lockup, printer powered down during the upgrade, etc...), HP Jetdirect will be able to recover, albeit with less functionality. This behavior allows an administrator to restart the upgrade process from the recovery partition and regain full functionality without having to contact HP support.

There are three common ways of updating HP Jetdirect firmware:

- HP Download Manager / HP Web Jetadmin
- FTP
- Embedded Web Server

When using HP Download Manager or HP Web Jetadmin, the application issues an SNMP SET to the HP Jetdirect device. If the application has proper credentials, it can populate the firmware upgrade MIB table with TFTP server information. HP Jetdirect uses this information to start a TFTP client and pull down the download file. These applications use the well-known default SNMP community names. However, if an administrator has configured the SNMP SET community name, then the application must know it to successfully set the TFTP MIB objects for firmware upgrade. Customers can also utilize SNMPv3 for additional security and HP Web Jetadmin makes using SNMPv3 easy. Also note that applications such as the HP Download Manager and HP Web Jetadmin are digitally signed by Hewlett-Packard as proof of their source.

The ability to use FTP to upgrade the firmware of HP Jetdirect devices is described here:

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj07129>. At the end of the document is a Security section detailing the security precautions available for FTP firmware upgrades. Essentially: if a password has been specified, it is required to be entered to utilize FTP

firmware upgrades; if telnet has been disabled to avoid plain-text transmission of the password, FTP upgrades are also disabled.

The ability to use the EWS to upgrade HP Jetdirect devices is described here:

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj07572>. How the EWS is protected determines how the HP Jetdirect firmware upgrade capability is protected. For users of the EWS, HP recommends setting the redirect from HTTP to HTTPS, using a properly signed certificate, and of course specifying a good password.

HP Jetdirect Hacks: Sniffing Print Jobs and Replaying Them

Easily available network tools that can perform effective MITM attacks against the TCP/IP protocol suite has caused a lot of concern among customers. Let's review what a MITM attack against the TCP/IP protocol suite does. A node intercepts IP packets from a node by pretending to be another node and then forwards the IP packets to the next correct node so it may end up at the final destination as if no interception had taken place; also, this MITM node intercepts packets traveling in the opposite direction (from the destination back to the source) in the same manner. What this means is that the MITM node has a copy of all the data sent between that source and that destination. If the MITM node has a copy of a PDF file that was sent between an email client and email server, it can use Adobe Acrobat Reader to open it. If the MITM node has a copy of a text document that was sent between an FTP client and an FTP server, it can open it with a text editor. If the MITM node has a copy of a print job, it can "open" it by sending it to a printer. In some cases, as with PostScript or simple text, a print job can be opened using other applications without having to send it to a printer. While a valid vulnerability, it is nonetheless a general vulnerability of the TCP/IP protocol suite and is not a vulnerability specific to printing.

Passive sniffing attacks are where another node on the network can record conversations. These attacks are analogously similar to using a listening device hidden in a conference room to record a meeting conversation. Active attacks are also used to force network infrastructure equipment to behave in a manner that allows passive sniffing. This active/passive behavior is analogously similar to a person not being able to plant the listening device in the conference room and instead pulling a fire alarm in the building then recording the conversation of the individuals leaving the conference room. Properly deployed cryptographic protocols are a good defense against passive and active sniffing attacks. Networking infrastructure equipment can be configured to help hinder active attacks. Port access controls, such as 802.1X, help protect against unauthorized connections. In addition, many switch vendors offer various flavors of ARP protection and monitoring since ARP poisoning is a fundamental step in MITM attacks.

The defense against TCP/IP MITM attacks is the proper deployment of cryptographic protocols such as IPsec and SSL/TLS with a properly signed HP Jetdirect certificate. HP recommends the proper deployment of IPsec (SET 4) as a solution to this general vulnerability with the TCP/IP protocol suite.

HP Jetdirect Hacks: Printer/MFP access

Up until now, we have discussed HP Jetdirect security primarily. Some publicly available applications interface directly with the printer/MFP's PDL library over a print connection. These tools often claim to bypass HP Jetdirect security. However, as we've seen from our functional diagram, HP Jetdirect controls the networking stack and does not parse PDL and cannot be configured to block PDL commands. However, printer/MFPs can be configured to provide a lot of security too. HP recommends following NIST checklist as a guideline to all customers concerned about printer/MFP security: http://www.hp.com/united-states/business/catalog/nist_checklist.html.

Recommended Security Deployments: SET 1

The HP Jetdirect products denoted by SET 1 do not have any cryptographic security capability. As a result, a BOOTP/TFTP configuration is recommended as we can specify several control parameters via the TFTP configuration file. This configuration file allows for a great deal of power with very little administration overhead once configured. Many customers associate BOOTP/TFTP with UNIX or Linux environments; however, there are many free BOOTP and TFTP servers for Windows and setup is fairly easy. An example UNIX configuration will be provided here.

```
picasso:\
:hn:\
:ht=ether:\
:vm=rfc1048:\
:ha=0001E6123456:\
:ip=192.168.40.39:\
:sm=255.255.255.0:\
:gw=192.168.40.1:\
:lg=192.168.40.3:\
:T144="hpn/picasso.cfg":\
:T151="BOOTP-ONLY":
```

This configuration provides the following:

- Syslog server: 192.168.40.3
- TFTP configuration file: picasso.cfg under the subdirectory of "hpn" of the TFTP daemon's home directory
- Forces HP Jetdirect to remain with BOOTP and not transition to DHCP if a BOOTP server is unavailable.

An example of the contents of the TFTP configuration file picasso.cfg:

```
# Allow subnet 192.168.40.0 access
allow: 192.168.40.0 255.255.255.0
#
# Disable Telnet
telnet-config: 0
#
# Disable the embedded Web server
ews-config: 0
#
# disable unused protocols
ipx/spx: 0
dlc/lc: 0
ethertalk:0
#
# Set a password
passwd: Security4Me3
#
# Disable SNMP
# use with caution – breaks SNMP management tools
snmp-config:0
#
# if SNMP must be enabled, comment out the "snmp-config" command and
# uncomment out the following:
# set-community-name: Security4Me3
# get-community-name: notpublic
# default-get-community: 0
#
# parameter file
parm-file: hpn/pjlprotection
#
```


The TFTP configuration file points to a parameter file called “pjlprotection”. This file is sent to the printer on power-up. Here is a sample content for the pjlprotection file:

```
<ESC>%-12345X@PJL <CR><LF>
@PJL COMMENT **Set Password** <CR><LF>
@PJL COMMENT **& Lock Control Panel**<CR><LF>
@PJL JOB PASSWORD = 7654 <CR><LF>
@PJL DEFAULT PASSWORD = 1776 <CR><LF>
@PJL DINQUIRE PASSWORD <CR><LF>
@PJL DEFAULT CPLOCK = ON <CR><LF>
@PJL DINQUIRE CPLOCK <CR><LF>
@PJL EOJ <CR><LF>
<ESC>%-12345X
```

Recommended Security Deployments: SET 2

For the HP Jetdirect products that are in SET 2, the security wizard is recommended for non HP Web Jetadmin users. The security wizard can be access via the Networking tab, “Settings” in the left-hand navigation bar, and then the “Wizard” tab. A sample configuration is shown here:

NOTE: be sure to use HTTPS when navigating to this page. Press the “Start Wizard” button to begin the wizard.



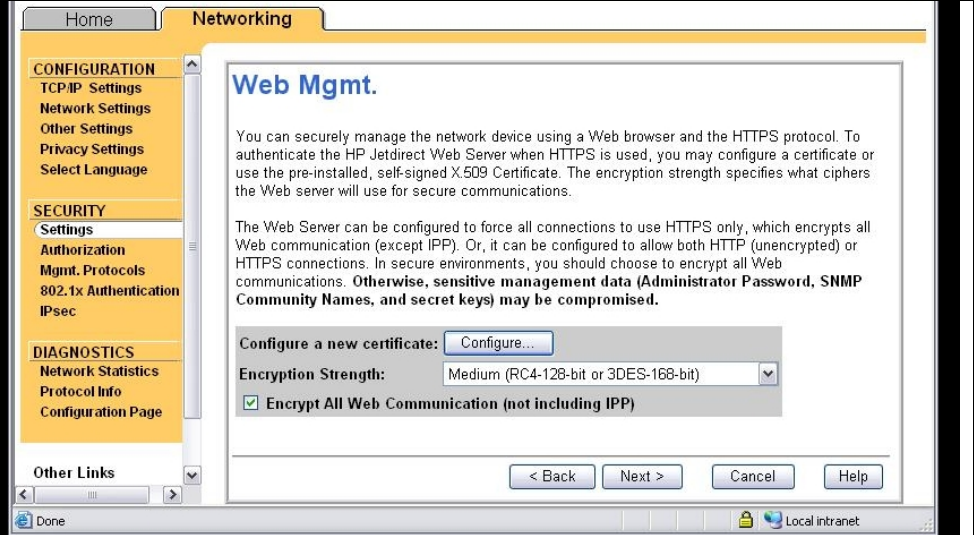
The Security level you want to implement on Jetdirect. Here, we are going to choose “Custom Security” to show all the options that are available to a customer.



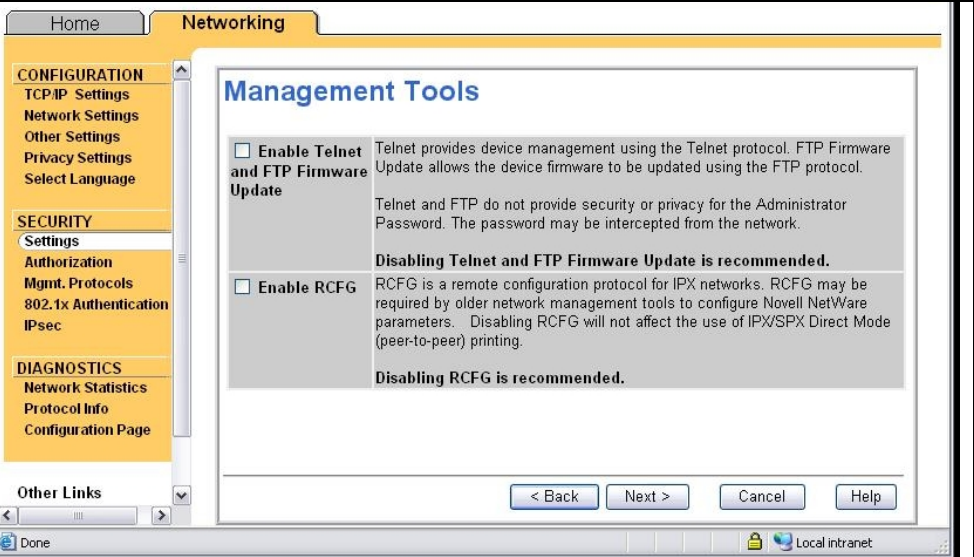
First and foremost, set a password.

The screenshot shows a web-based configuration interface for a network device. The main navigation bar at the top has 'Home' and 'Networking' tabs. On the left, a sidebar menu is organized into sections: 'CONFIGURATION' (with sub-items: TCP/IP Settings, Network Settings, Other Settings, Privacy Settings, Select Language), 'SECURITY' (with sub-items: Settings, Authorization, Mgmt. Protocols, 802.1x Authentication, IPsec), and 'DIAGNOSTICS' (with sub-items: Network Statistics, Protocol Info, Configuration Page). Below the menu is an 'Other Links' section. The main content area is titled 'Administrator Account' and contains the following text: 'Use the fields below to set or change the Administrator Password. When set, the Administrator Password will be required before you can access and change configuration parameters. To disable the Administrator Password, leave the entries blank.' Below this text are three input fields: 'User Name:' with the value 'Admin', 'Password:' with a masked field of 10 dots, and 'Confirm Password:' with a masked field of 10 dots. At the bottom of the main area are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The browser's status bar at the bottom shows 'Done' on the left and 'Local intranet' on the right.

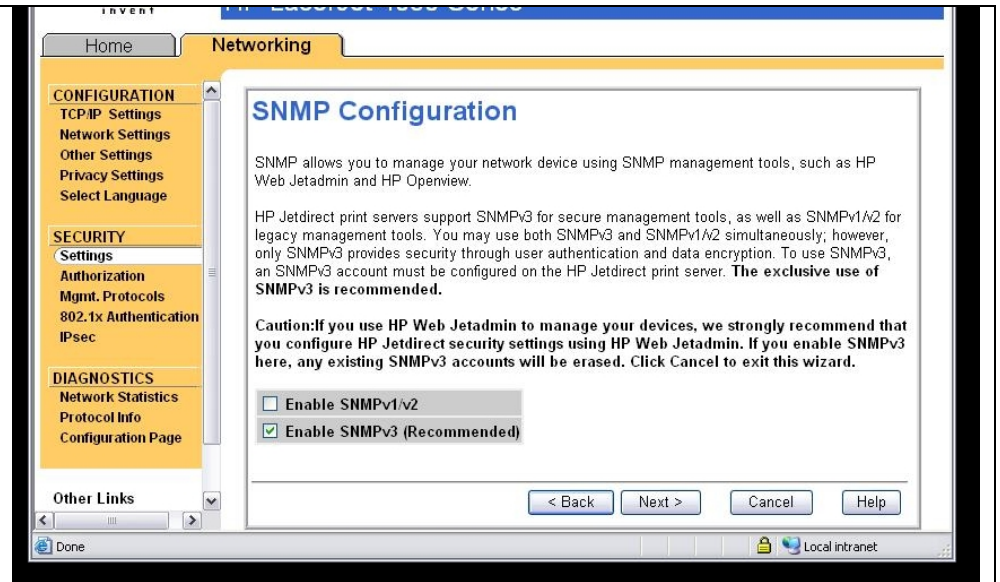
Change the Encryption Strength to "Medium" and check the "Encrypt All Web Communication" checkbox. This checkbox forces HTTPS to be used for all web communication.



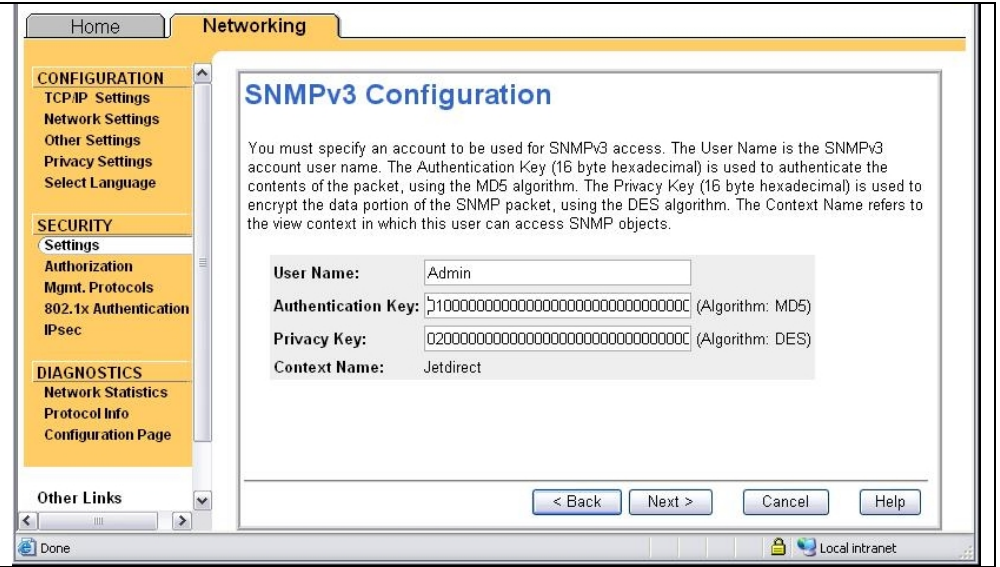
Uncheck "Enable Telnet and FTP Firmware Update" and "Enable RCFG".



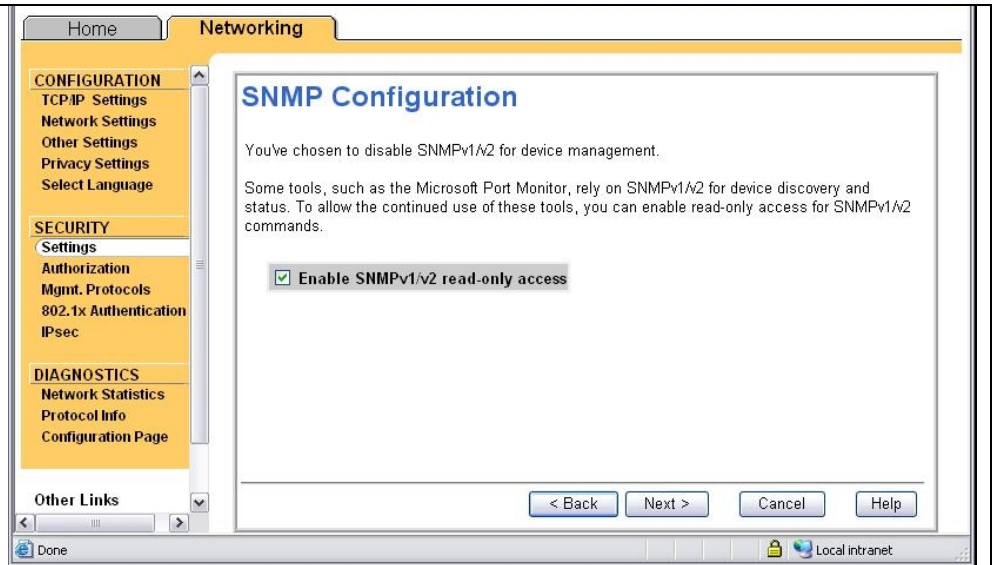
Uncheck "Enable SNMPv1/v2" and check "Enable SNMPv3".



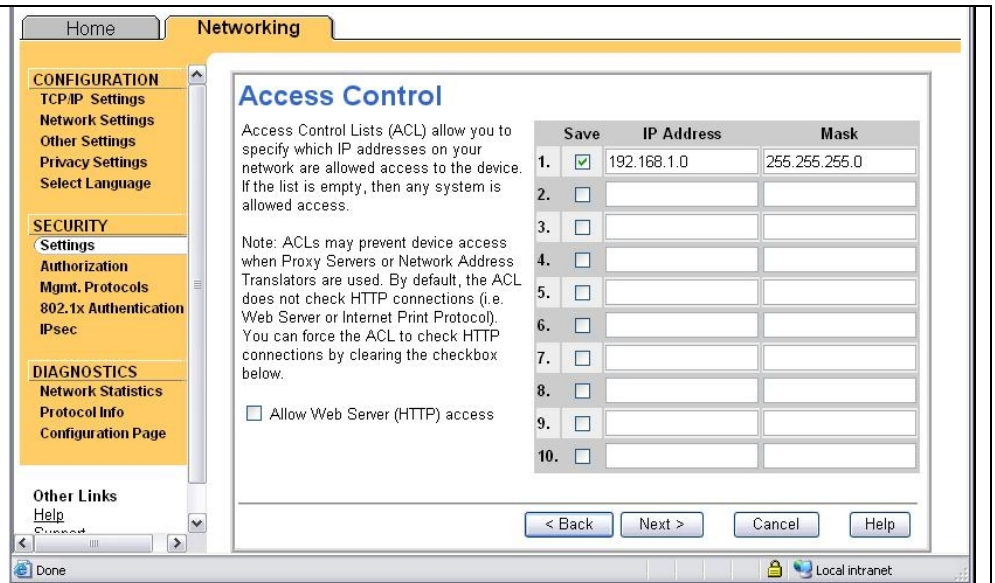
Provide SNMPv3 parameters.



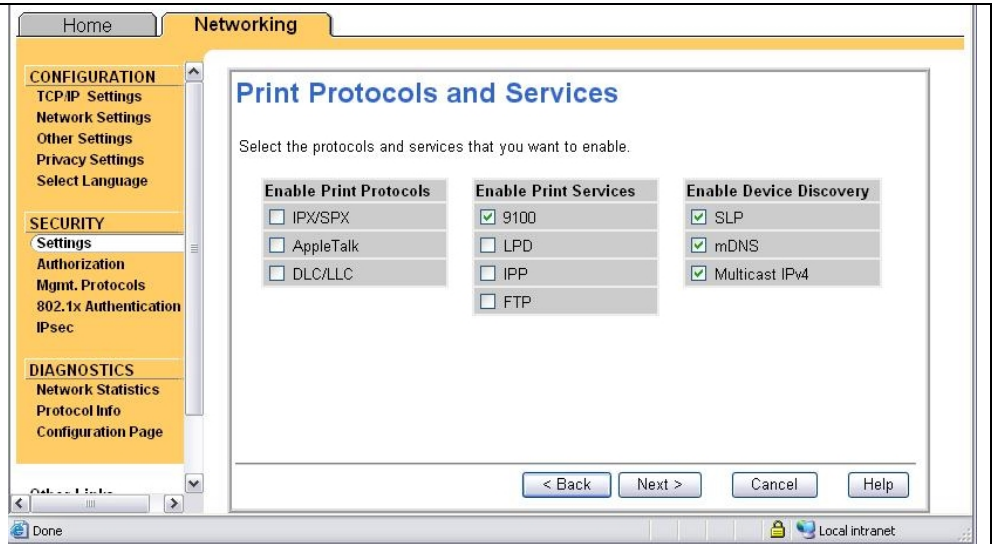
Based upon the customer's environment, read only SNMPv1/v2c access may need to be granted. Some tools such as the HP Standard Port Monitor use SNMPv1/v2c for status.



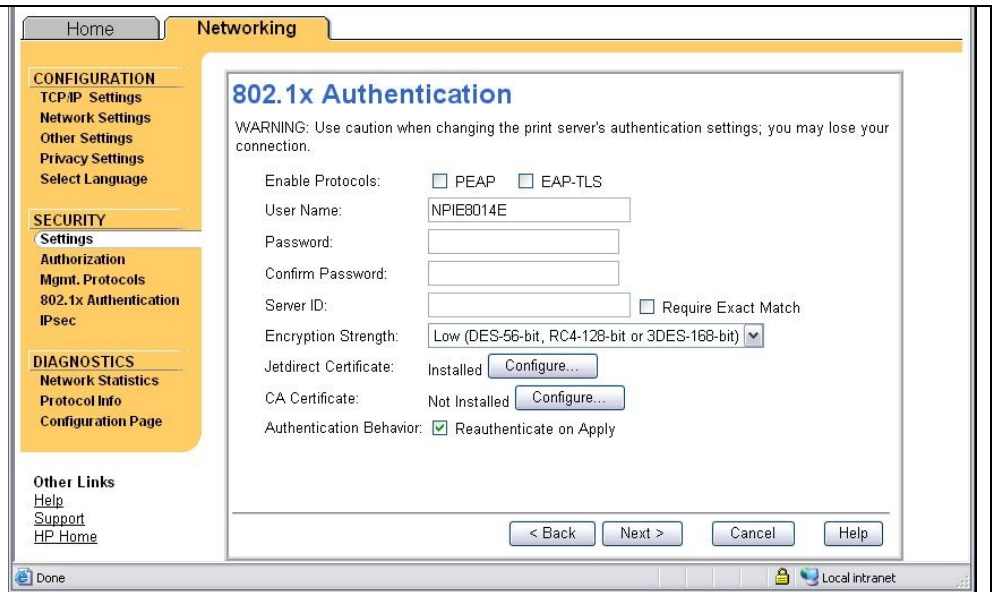
Setup an Access Control List entry. This is another customer environment specific entry. In this example, the subnet 192.168.1.0 is protected by the ACL. Uncheck "Allow Web Server (HTTP) access" to force HTTP checking to be done in the ACL.

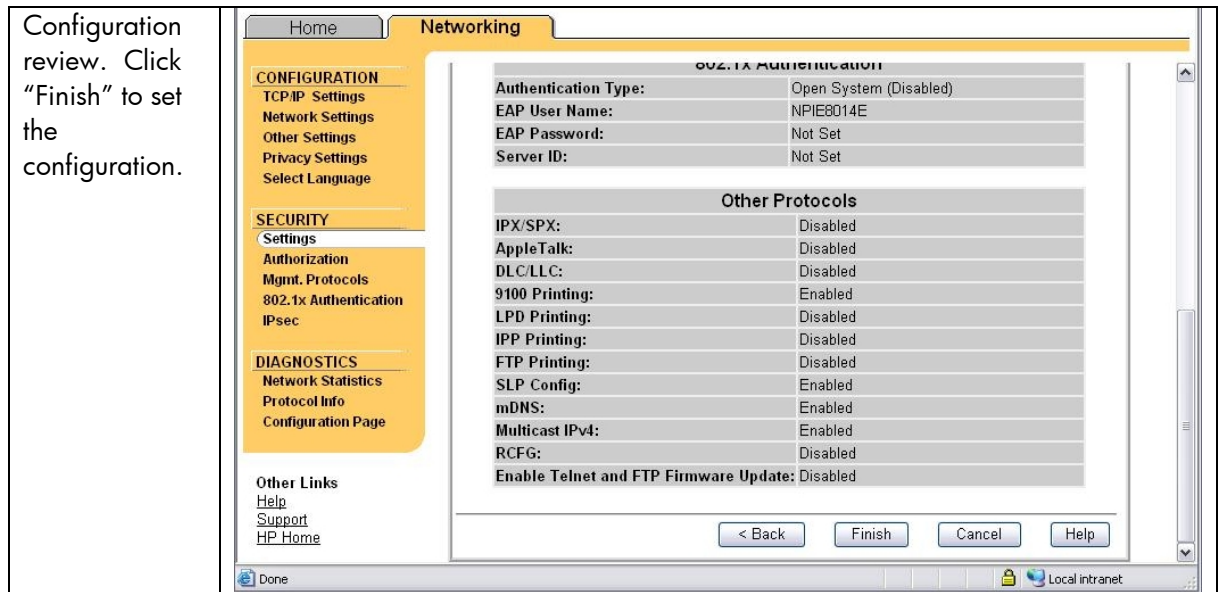
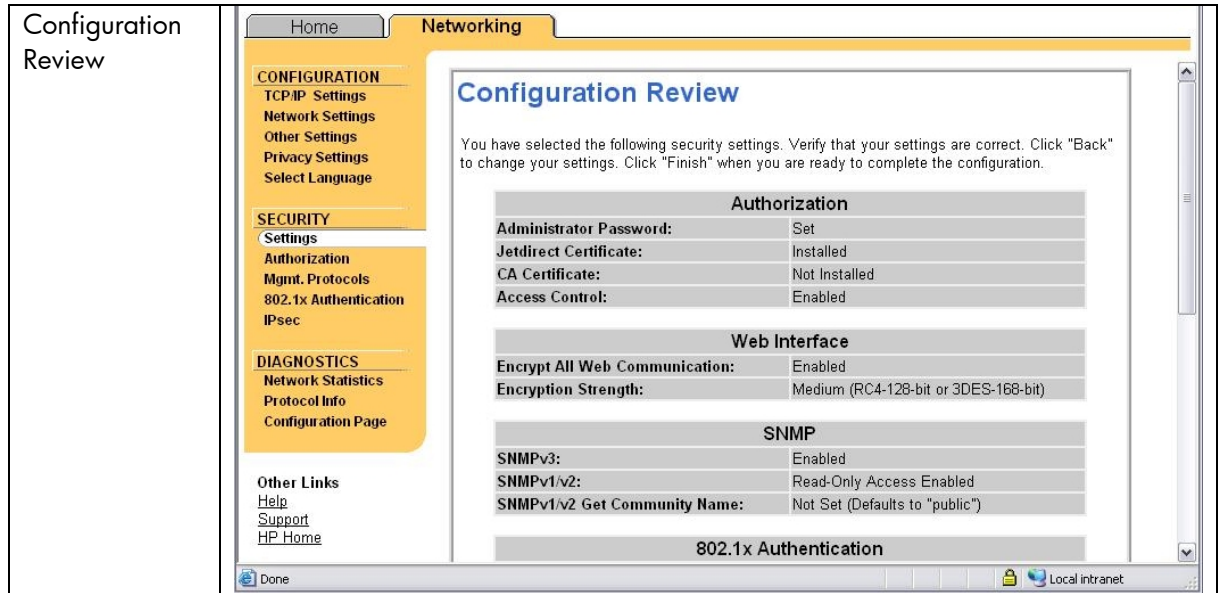


Disable unused print protocols and services. Allowing device discovery helps in device management, but may not be required in all environments.



802.1X authentication can also be done. Special equipment is required. For a complete discussion of 802.1X, see HP Jetdirect whitepapers on the topic. For now, this configuration step is skipped.





Recommended Security Deployments: SET 3

First and foremost, SET 3 configuration needs to have the Security Wizard for SET 2 executed. Once the Security Wizard configuration has been completed, then we can begin the Firewall configuration. A sample Firewall configuration is shown where the management protocols are restricted to a specific IP subnet range:

Be sure that you are using HTTPS before navigating to this page. Select the drop down box for the Default Rule to be "Allow" and then click "Add Rules..."

Firewall Policy

Enable Firewall

Firewall Rules

Rule	Enable	Match Criteria		Action on Match
		Address Template	Services Template	Action
1	<input type="checkbox"/>			
2	<input type="checkbox"/>			
3	<input type="checkbox"/>			
4	<input type="checkbox"/>			
5	<input type="checkbox"/>			
6	<input type="checkbox"/>			
7	<input type="checkbox"/>			
8	<input type="checkbox"/>			
9	<input type="checkbox"/>			
10	<input type="checkbox"/>			

Default Rule: All IP Addresses | All Services | Allow

Add Rules... **Delete Rules...** **Advanced**

Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.

Apply **Cancel**

We have a specific administrator subnet defined for printing and imaging devices. Click the "New" button so we can be very specific about what addresses can manage the device.

Rule 1 : Specify Address Template

Specify the Address Template that will be applied to this rule. Predefined templates listed below contain common address choices. Select a predefined template or click 'New' to define your own.

Address Templates:

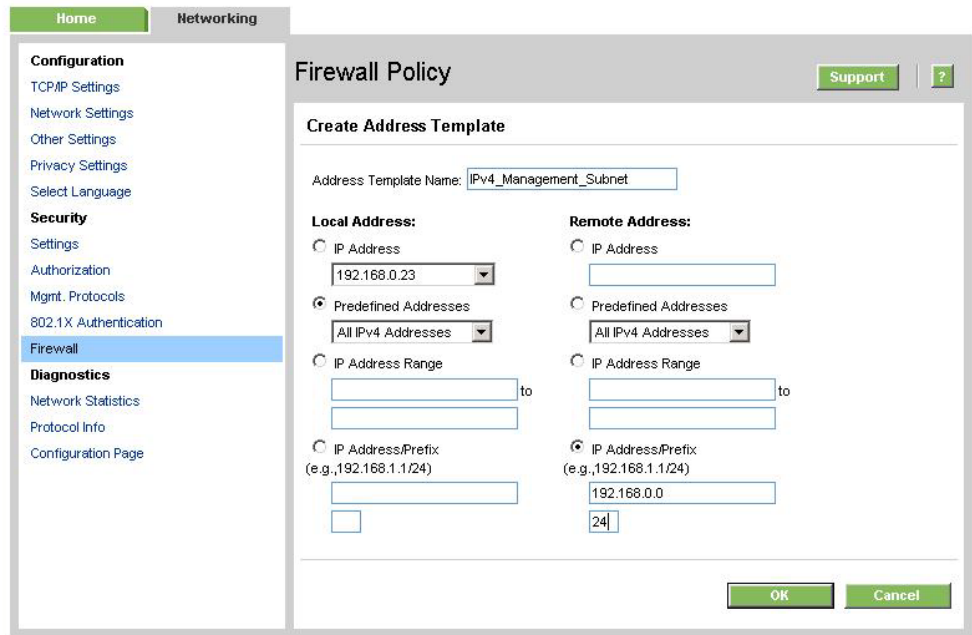
- All IP Addresses
- All IPv4 Addresses
- All IPv6 Addresses
- All link local IPv6
- All non link local IPv6

New **View...** **Delete**

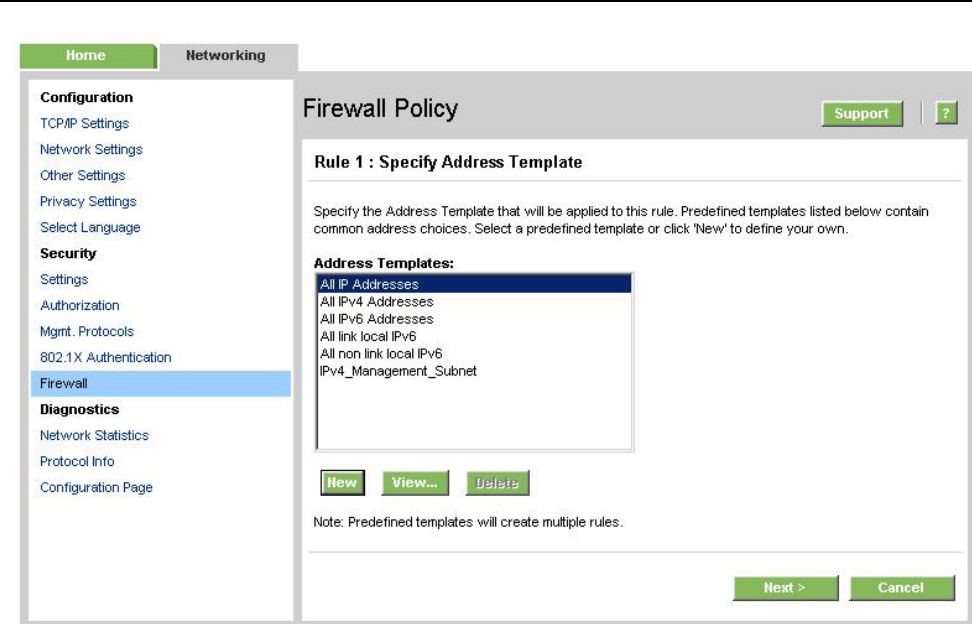
Note: Predefined templates will create multiple rules.

Next > **Cancel**

We'll define the IPv4 address range first. Select "All IPv4 Addresses" for Local Address and then we specified the 192.168.0/24 subnet for the Remote Address. We've also named this address template very clearly.



Now for IPv6. Click "New" again. NOTE: If IPv6 is not used on your network, go to TCP/IP settings and disable IPv6 for increased security. You can also skip which use IPv6 in this configuration.



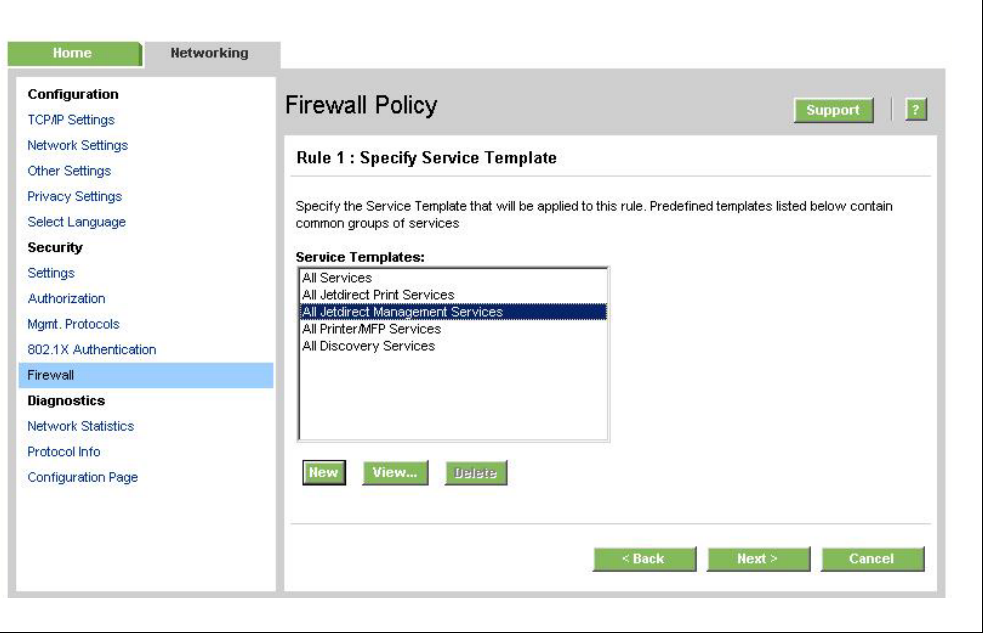
Select the appropriate IPv6 addresses and name the address template.

The screenshot shows the 'Firewall Policy' configuration page. On the left is a navigation menu with sections: Configuration (TCP/IP Settings, Network Settings, Other Settings, Privacy Settings, Select Language), Security (Settings, Authorization, Mgmt. Protocols, 802.1X Authentication, Firewall), and Diagnostics (Network Statistics, Protocol Info, Configuration Page). The 'Firewall' section is highlighted. The main area is titled 'Firewall Policy' and contains a 'Create Address Template' dialog. The dialog has a text field for 'Address Template Name' containing 'IPv6_Management_Subnet'. It is divided into 'Local Address' and 'Remote Address' sections. In the 'Local Address' section, the 'Predefined Addresses' radio button is selected, and a dropdown menu shows 'All IPv6 Addresses'. In the 'Remote Address' section, the 'IP Address/Prefix' radio button is selected, with a text field containing '2001:0DB8::' and a dropdown for prefix length set to '64'. 'OK' and 'Cancel' buttons are at the bottom right.

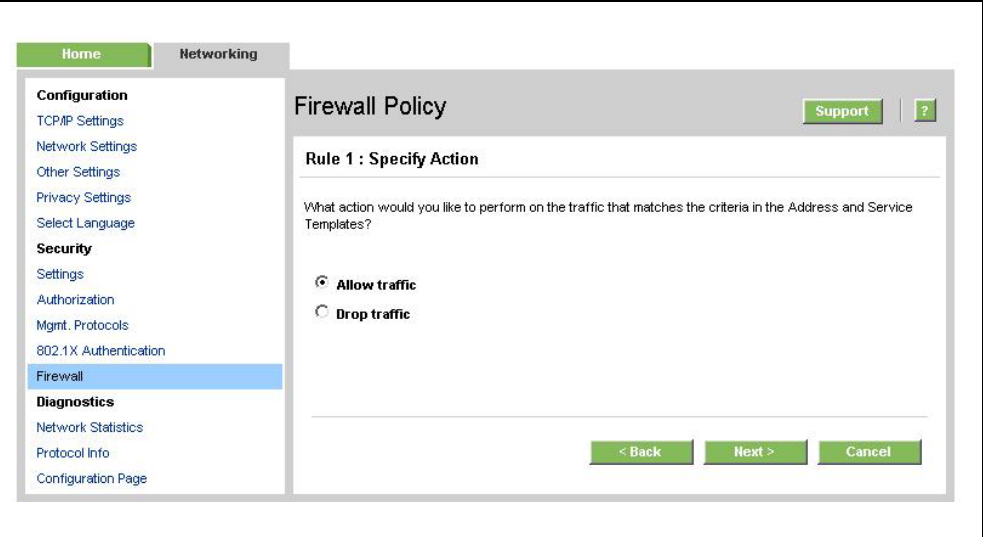
Now that we have the address templates, let's create a rule. Rules are processed in priority order from 1 – 10. Let's create an IPv4 rule first. Select the IPv4 address template you created, then click "Next".

The screenshot shows the 'Firewall Policy' configuration page, similar to the previous one. The main area is titled 'Rule 1 : Specify Address Template'. It contains a text area with the instruction: 'Specify the Address Template that will be applied to this rule. Predefined templates listed below contain common address choices. Select a predefined template or click 'New' to define your own.' Below this is a list box titled 'Address Templates:' containing the following items: All IP Addresses, All IPv4 Addresses, All IPv6 Addresses, All link local IPv6, All non link local IPv6, IPv4_Management_Subnet (highlighted), and IPv6_Management_Subnet. Below the list are 'New', 'View...', and 'Delete' buttons. A note at the bottom states: 'Note: Predefined templates will create multiple rules.' 'Next >' and 'Cancel' buttons are at the bottom right.

We are concerned with management services, so select the service template "All Jetdirect Management Services". Click "Next".



Select "Allow Traffic". Click "Next"



Select "Create another rule".

The screenshot shows the 'Firewall Policy' configuration page. On the left is a navigation menu with sections: Configuration (TCP/IP Settings, Network Settings, Other Settings, Privacy Settings, Select Language), Security (Settings, Authorization, Mgmt. Protocols, 802.1X Authentication, Firewall), and Diagnostics (Network Statistics, Protocol Info, Configuration Page). The 'Firewall' option is selected. The main content area is titled 'Firewall Policy' and includes a 'Support' button and a '?' icon. Below is the 'Rule Summary' section, which contains a table of 'Firewall Rules'.

Match Criteria			Action on Match
Rule	Address Template	Services Template	Action
1	IPv4_Management_Subnet	All Jetdirect Management Services	Allow traffic
2			
3			
4			
5			
6			
7			
8			
9			
10			
Default Rule	All IP Addresses	All Services	Allow

Below the table, there is a note: 'To return to the beginning of the Firewall Wizard and create an additional Firewall rule, click 'Create Another Rule'. To apply all rules, click 'Finish'.' A warning message follows: 'Warning: An invalid Firewall configuration can result in the device being inaccessible over the network. To recover from this condition physical access to the device is required. For internal print servers, the Jetdirect menu on the control panel of the printer will contain a reset option. For external printer servers, the administrator may perform a cold reset of the device. See your printer manual for instructions on how to perform a cold reset.' Another warning: 'Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.' At the bottom are four buttons: '< Back', 'Create Another Rule', 'Finish', and 'Cancel'.

Select the IPv6 address template you created and then click "Next".

The screenshot shows the 'Firewall Policy' configuration page at the 'Rule 2 : Specify Address Template' step. The navigation menu is the same as in the previous screenshot. The main content area is titled 'Firewall Policy' and includes a 'Support' button and a '?' icon. Below is the 'Rule 2 : Specify Address Template' section, which contains a text box for specifying the address template. Below the text box is a list of 'Address Templates' with a scrollable list box containing the following options: All IP Addresses, All IPv4 Addresses, All IPv6 Addresses, All link local IPv6, All non link local IPv6, IPv4_Management_Subnet, and IPv6_Management_Subnet. The 'IPv6_Management_Subnet' option is selected. Below the list box are three buttons: 'New', 'View...', and 'Delete'. A note below the buttons reads: 'Note: Predefined templates will create multiple rules.' At the bottom are two buttons: 'Next >' and 'Cancel'.

Select the "All Jetdirect Management Services" service template. Click "Next".

The screenshot shows the 'Firewall Policy' configuration interface. The left sidebar has 'Firewall' selected under the 'Security' section. The main content area is titled 'Rule 2 : Specify Service Template'. It contains a list of service templates: 'All Services', 'All Jetdirect Print Services', 'All Jetdirect Management Services' (highlighted), 'All Printer/MFP Services', and 'All Discovery Services'. Below the list are 'New', 'View...', and 'Delete' buttons. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

Select "Allow Traffic". Click Next.

The screenshot shows the 'Firewall Policy' configuration interface. The left sidebar has 'Firewall' selected under the 'Security' section. The main content area is titled 'Rule 2 : Specify Action'. It contains the question 'What action would you like to perform on the traffic that matches the criteria in the Address and Service Templates?' and two radio button options: 'Allow traffic' (selected) and 'Drop traffic'. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

We have allowed management traffic from our IPv4/IPv6 administrative subnet. Now we must create a rule to throw away all other management traffic. Click "Create another rule".

The screenshot shows the 'Firewall Policy' configuration page. On the left is a navigation menu with sections: Configuration, Security, and Diagnostics. The 'Firewall' option under Security is highlighted. The main content area is titled 'Firewall Policy' and includes a 'Rule Summary' section with a table of 'Firewall Rules'.

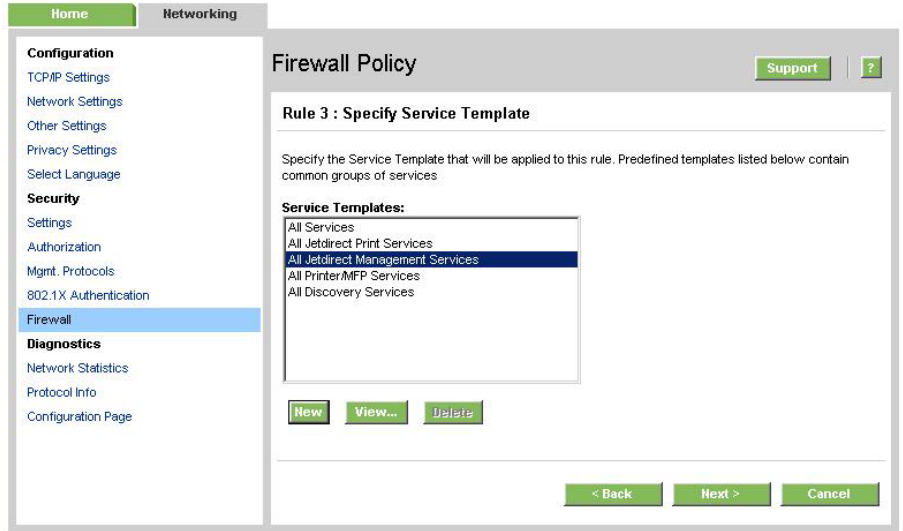
Rule	Match Criteria		Action on Match
	Address Template	Services Template	Action
1	IPv4_Management_Subnet	All Jetdirect Management Services	Allow traffic
2	IPv6_Management_Subnet	All Jetdirect Management Services	Allow traffic
3			
4			
5			
6			
7			
8			
9			
10			
Default Rule	All IP Addresses	All Services	Allow

Below the table, there are instructions: 'To return to the beginning of the Firewall Wizard and create an additional Firewall rule, click 'Create Another Rule'. To apply all rules, click 'Finish'.' A warning message states: 'Warning: An invalid Firewall configuration can result in the device being inaccessible over the network. To recover from this condition physical access to the device is required. For internal print servers, the Jetdirect menu on the control panel of the printer will contain a reset option. For external printer servers, the administrator may perform a cold reset of the device. See your printer manual for instructions on how to perform a cold reset.' Another warning says: 'Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.' At the bottom are buttons: '< Back', 'Create Another Rule', 'Finish', and 'Cancel'.

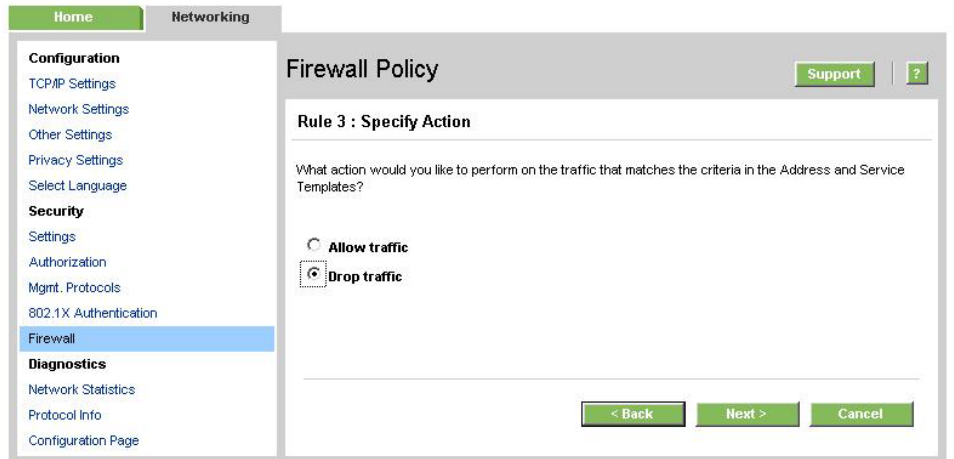
Here we select "All IP addresses" which encompasses both IPv4 and IPv6. Click "Next".

The screenshot shows the 'Rule 3 : Specify Address Template' configuration page. The navigation menu on the left is the same as in the previous screenshot, with 'Firewall' highlighted. The main content area is titled 'Rule 3 : Specify Address Template' and includes instructions: 'Specify the Address Template that will be applied to this rule. Predefined templates listed below contain common address choices. Select a predefined template or click 'New' to define your own.' Below this is a list of 'Address Templates' with 'All IP Addresses' selected. The list includes: All IP Addresses, All IPv4 Addresses, All IPv6 Addresses, All link local IPv6, All non link local IPv6, IPv4_Management_Subnet, and IPv6_Management_Subnet. There are buttons for 'New', 'View...', and 'Delete'. A note at the bottom says: 'Note: Predefined templates will create multiple rules.' At the bottom right are buttons for 'Next >' and 'Cancel'.

Again, select "All Jetdirect Management Services" for the service template and then click "Next".



Select "Drop". Click "Next".



We can now see our policy. Rules are processed from 1 to 10. If a packet comes from or is going to our defined IPv4/IPv6 subnet, the rule will match and it will be allowed. Otherwise, if it is a management service, it will be dropped. All other traffic will be allowed (the default rule is allow). Click "Finish".

Home Networking

Configuration
 TCP/IP Settings
 Network Settings
 Other Settings
 Privacy Settings
 Select Language

Security
 Settings
 Authorization
 Mgmt. Protocols
 802.1X Authentication
Firewall

Diagnostics
 Network Statistics
 Protocol Info
 Configuration Page

Firewall Policy

Support ?

Rule Summary

Firewall Rules:

Match Criteria			Action on Match
Rule	Address Template	Services Template	Action
1	IPv4_Management_Subnet	All Jetdirect Management Services	Allow traffic
2	IPv6_Management_Subnet	All Jetdirect Management Services	Allow traffic
3	All IP Addresses (IPv4)	All Jetdirect Management Services	Drop traffic
4	All IP Addresses (IPv6)	All Jetdirect Management Services	Drop traffic
5			
6			
7			
8			
9			
10			
Default Rule	All IP Addresses	All Services	Allow

To return to the beginning of the Firewall Wizard and create an additional Firewall rule, click 'Create Another Rule'. To apply all rules, click 'Finish'.

Warning: An invalid Firewall configuration can result in the device being inaccessible over the network. To recover from this condition physical access to the device is required. For internal print servers, the Jetdirect menu on the control panel of the printer will contain a reset option. For external printer servers, the administrator may perform a cold reset of the device. See your printer manual for instructions on how to perform a cold reset.

Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.

< Back Create Another Rule Finish Cancel

Select "Yes" for Enable Policy. HTTPS failsafe can be used when trying out configurations. If this is your first firewall configuration, you may want to enable it, and then disable it once it has been tested. Click "Ok"

Home Networking

Configuration
 TCP/IP Settings
 Network Settings
 Other Settings
 Privacy Settings
 Select Language

Security
 Settings
 Authorization
 Mgmt. Protocols
 802.1X Authentication
Firewall

Diagnostics
 Network Statistics
 Protocol Info
 Configuration Page

Support ?

The Firewall Policy has not been enabled.
 Would you like to enable the policy now?
 Yes No

Would you like to enable the Failsafe Option?
 This option ensures HTTPS remains accessible even if it is blocked by the Firewall policy. This allows the administrator to test the policy without inadvertently locking themselves out of the device. It is recommended that the Failsafe Option be disabled once the policy has been successfully tested.
 Yes No

Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.

OK

Recommended Security Deployments: SET 4

First and foremost, SET 4 configuration needs to have the Security Wizard for SET 2 executed. Once the Security Wizard configuration has been completed, then we can begin the IPsec configuration. Let's go through the same process as we did with SET 3, only this time, we'll simply say that all IP addresses must use IPsec to utilize a management protocol. If an end station tries to communicate with a management protocol to Jetdirect without using IPsec, the packets are dropped by the IP layer.

Be sure that you are using HTTPS before navigating to this page. Select "Allow" for the default rule and then click "Add Rules...".

The screenshot shows the 'IPsec/Firewall Policy' configuration page. On the left is a navigation menu with sections: Configuration (TCP/IP Settings, Network Settings, Other Settings, Privacy Settings), Security (Settings, Authorization, Mgmt. Protocols, 802.1X Authentication, IPsec/Firewall), and Diagnostics (Network Statistics, Protocol Info, Configuration Page). The 'IPsec/Firewall' option is selected. The main area is titled 'IPsec/Firewall Policy' and includes a 'Support' link and a help icon. Below the title is a checkbox for 'Enable IPsec/Firewall'. A table titled 'IPsec/Firewall Rules' has columns for 'Rule', 'Enable', 'Address Template', 'Services Template', and 'Action'. The table contains 10 rows, all with 'Enable' checkboxes unchecked. Below the table are buttons for 'Add Rules...', 'Delete Rules...', and 'Advanced'. A dropdown menu shows 'Default Rule' set to 'All IP Addresses', 'All Services', and 'Allow'. A warning message states: 'Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.' At the bottom are 'Apply' and 'Cancel' buttons.

Select "All IP Addresses" and click "Next".

The screenshot shows the 'Rule 1: Specify Address Template' configuration page. The navigation menu is the same as in the previous screenshot. The main area is titled 'IPsec/Firewall Policy' and includes a 'Support' link and a help icon. Below the title is the heading 'Rule 1: Specify Address Template'. A text block explains: 'Specify the Address Template that will be applied to this rule. Predefined templates listed below contain common address choices. Select a predefined template or click 'New' to define your own.' Below this is a list of 'Address Templates': 'All IP Addresses', 'All IPv4 Addresses', 'All IPv6 Addresses', 'All link local IPv6', and 'All non link local IPv6'. The 'All IP Addresses' option is selected. Below the list are buttons for 'New', 'View...', and 'Delete'. A note states: 'Note: Predefined templates will create multiple rules.' At the bottom are 'Next >' and 'Cancel' buttons.

Select "All Jetdirect Management Services". Click "Next".

The screenshot shows the 'IPsec/Firewall Policy' configuration page. The left sidebar is under the 'Networking' tab, with 'IPsec/Firewall' selected. The main content area is titled 'Rule 1 : Specify Service Template'. It contains a list of service templates: 'All Services', 'All Jetdirect Print Services', 'All Jetdirect Management Services' (highlighted), 'All Printer/MFP Services', and 'All Discovery Services'. Below the list are 'New', 'View...', and 'Update' buttons. A warning message states: 'Warning: Only the 'All Services' template will protect applications added to the device after IPsec/Firewall rules have been saved. Otherwise, a new rule must be created to protect that new network application with the IPsec/Firewall policy.' At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Select "Require traffic to be protected with an IPsec/Firewall Policy". Click "Next".

The screenshot shows the 'IPsec/Firewall Policy' configuration page. The left sidebar is under the 'Networking' tab, with 'IPsec/Firewall' selected. The main content area is titled 'Rule 1 : Specify Action'. It contains the question 'What action would you like to perform on the traffic that matches the criteria in the Address and Service Templates?' and three radio button options: 'Allow traffic to pass without IPsec/Firewall protection', 'Drop traffic', and 'Require traffic to be protected with an IPsec/Firewall policy.' (which is selected). At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

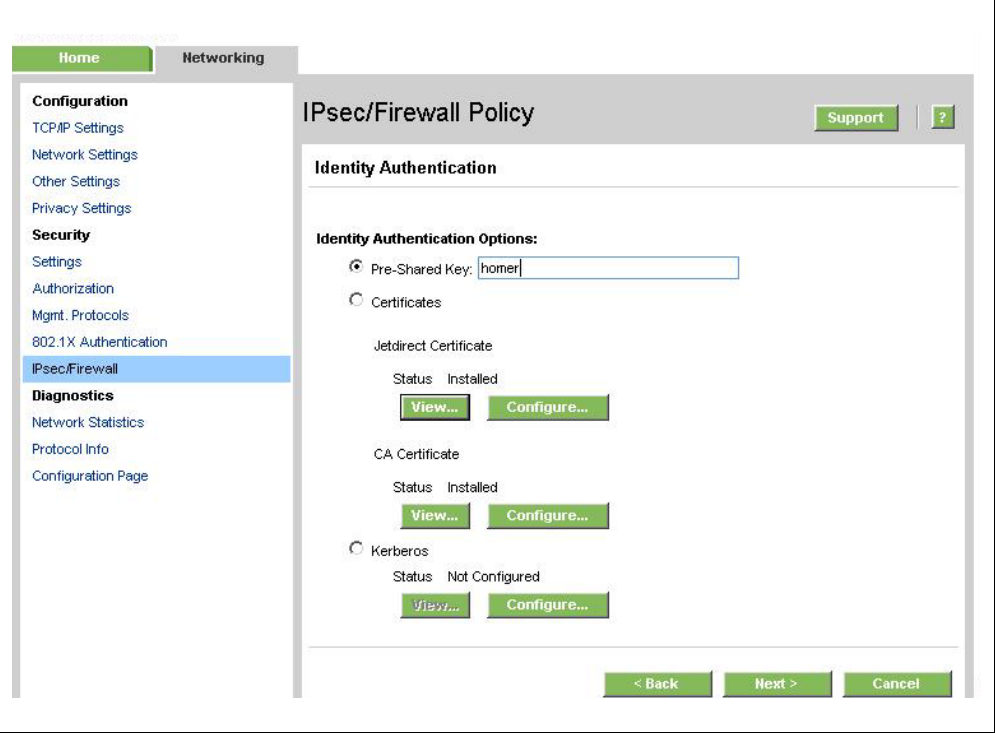
Click "New".

The screenshot shows the 'IPsec/Firewall Policy' configuration page. The left sidebar has a menu with categories: Configuration, Security, and Diagnostics. Under 'Configuration', 'IPsec/Firewall' is selected. The main content area is titled 'Rule 1 : Specify IPsec/Firewall Template'. It contains a text box with instructions: 'Specify the IPsec/Firewall Template that will be applied to this rule. Click 'New' to create an IPsec/Firewall template, or select a previously defined template.' Below this is a large empty box labeled 'IPsec/Firewall Templates:'. At the bottom of this box are three buttons: 'New', 'View...', and 'Delete'. At the bottom of the main content area are three buttons: '< Back', 'Next >', and 'Cancel'. There are also 'Support' and '?' buttons in the top right corner.

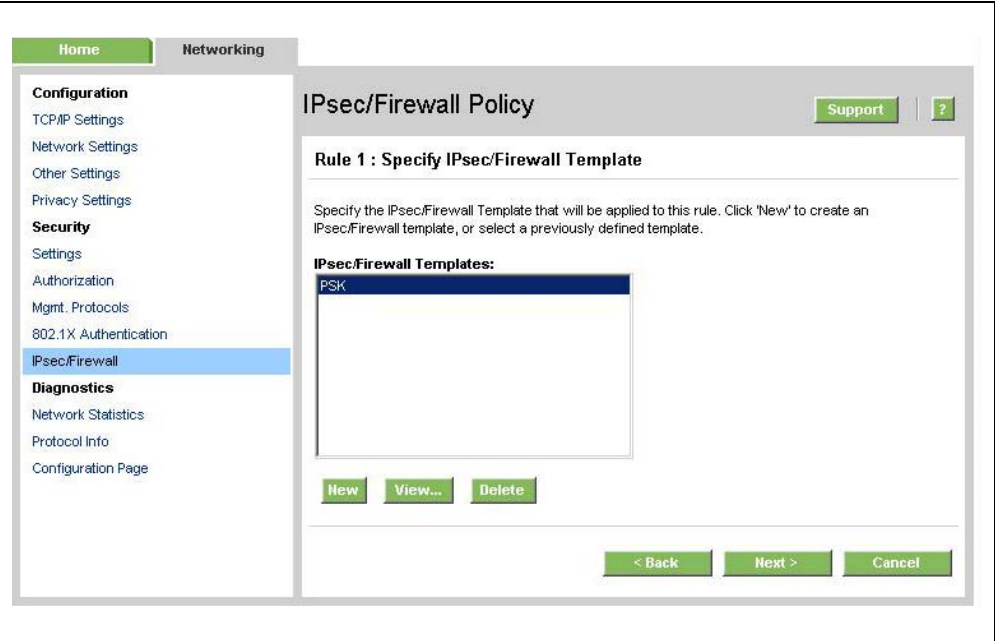
Name the IPsec Template. Some Jetdirect models may require you to configure IKE parameters. However, this model has a quick set of IKE defaults that can be used. The one selected is for more emphasis on Interoperability and less on Security. Click "Next".

The screenshot shows the 'Create IPsec Template' configuration page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Create IPsec Template'. It has a text input field for 'IPsec Template Name' with the value 'PSK'. Below this is the 'Authentication Type' section, which has two radio buttons: 'Internet Key Exchange Version 1 (IKEv1)' (selected) and 'Manual Keys'. Under 'Internet Key Exchange Version 1 (IKEv1)', there is a 'Set IKE Defaults' section with a dropdown menu showing 'High interoperability/Low security'. Below the dropdown is a 'Preview IKE Defaults' button. At the bottom of the main content area are two buttons: 'Next >' and 'Cancel'. There are also 'Support' and '?' buttons in the top right corner.

For example purposes only, Pre-Shared Key Authentication is used. HP does not recommend using Pre-Shared Key Authentication. Certificates or Kerberos is highly recommended. Click "Next".



Select the IPsec template you just created. Click "Next".



Here is our IPsec policy. If a management protocol is to be used, it must use IPsec. All other traffic is allowed based upon the default rule. Click "Finish".

IPsec/Firewall Policy

Rule Summary

IPsec/Firewall Rules:

Rule	Match Criteria		Action on Match
	Address Template	Services Template	Action
1	All IP Addresses (IPv4)	All Jetdirect Management Services	PSK
2	All IP Addresses (IPv6)	All Jetdirect Management Services	PSK
3			
4			
5			
6			
7			
8			
9			
10			
Default Rule	All IP Addresses	All Services	Allow

To return to the beginning of the IPsec/Firewall Wizard and create an additional rule, click 'Create Another Rule'. To apply all rules, click 'Finish'.

Warning: An invalid IPsec/Firewall configuration can result in the device being inaccessible over the network. To recover from this condition physical access to the device is required. For internal print servers, the Jetdirect menu on the control panel of the printer will contain a reset option. For external printer servers, the administrator may perform a cold reset of the device. See your printer manual for instructions on how to perform a cold reset.

Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.

< Back Create Another Rule Finish Cancel

Select "Yes" to enable the IPsec policy. You can also choose to have a failsafe if you would like. Click "OK".

The IPsec/Firewall Policy has not been enabled.
Would you like to enable the policy now?
 Yes No

Would you like to enable the Failsafe Option?
This option ensures HTTPS remains accessible even if it is blocked by the IPsec/Firewall policy. This allows the administrator to test the policy without inadvertently locking themselves out of the device. It is recommended that the Failsafe Option be disabled once the policy has been successfully tested.
 Yes No

Warning: Changing IPsec/Firewall settings may result in temporary loss of connection.

OK

Further Reading

802.1X: <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00731218/c00731218.pdf>

IPsec: <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01048192/c01048192.pdf>

IPv6: <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00840100/c00840100.pdf>

Using the networking infrastructure to better protect your printing and imaging devices:

<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00707837/c00707837.pdf>