Designjet Printer series

Security features

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

July 2013 Edition

Table of Contents

1. Introduction & Overview

This document is aimed at providing an overview of the security features supported by HP Designjet printers as of February 2012.

The security features described in this document make the HP Designjet printer series particularly well suited to being deployed into environments where network, data, access control, and security are important.

The following is a table summarizing the new and existing security features of HP Designjet printers series and how they are implemented using the Embedded Web Server and/or HP Web JetAdmin (WJA). Please make sure that the printer has the latest firmware version to benefit from all security features.

Note: If the printer is not listed in the table then these features are not implemented.

	Z6200	Z3200	Z2100/Z5200ps
Hide information to user			
Control panel lock	EWS	N/A	N/A
Hide IP from fp	FP	N/A	N/A
EWS multilevel	EWS	EWS (1 level)	N/A
Printer access control	N/A	N/A	N/A
Exclude personal info. From accounting	EWS	EWS	EWS (Z5200ps only)
Disable features			
Disable USB drive	N/A	N/A	N/A
Disable fmw update thru USB	N/A	N/A	N/A
Disable interfaces	EWS	N/A	N/A
Disable direct print with ePrint&Share (USB Printing)	N/A	N/A	N/A
Disable internet connection	N/A	N/A	N/A
Disable ePrint Center connectivity	N/A	N/A	N/A
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA
Wizard setup configuration	N/A	N/A	N/A
Data access			
Secure file erase	WJA	WJA	WJA (Z2100 only)
Secure disk erase	WJA/FP	WJA/FP	N/A
External HDD	Yes	No	No
Communications security			
IPSec	EWS	EWS/WJA + JetDirect	EWS/WJA + JetDirect
SNMPv3	EWS	EWS/WJA + JetDirect	EWS/WJA + JetDirect
CA/JD Certificates	EWS/WJA	EWS + JetDirect	EWS + JetDirect
Encrypt web comms	EWS/WJA	EWS/WJA + JetDirect	EWS/WJA + Jetdirect

	T7100	T1500/T920	T2300/T1300	T790	T120/T520
Hide information to user					
Control panel lock	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	N/A
EWS multilevel	EWS	EWS/FP/WJA	EWS/FP	EWS / FP (1 level)	EWS (1 level)
Hide IP from fp	FP	FP	FP	FP	N/A
Printer access control	N/A	EWS/FP/WJA	EWS/FP	EWS/FP	N/A
Exclude personal info. From accounting	EWS	EWS/WJA	EWS	EWS	N/A
Disable features					
Disable USB drive	N/A	EWS/FP/WJA	EWS/FP	EWS/FP	N/A
Disable fmw update thru USB	N/A	EWS/FP	EWS/FP	EWS/FP	N/A
Disable interfaces	EWS	EWS/FP/WJA	EWS/FP (USB printing only)	EWS / FP (USB printing only)	EWS/FP
Disable direct print with ePrint&Share (USB Printing)	N/A	EWS/FP	FP	FP	N/A
Disable ePrint Center connectivity	N/A	EWS/FP	FP	FP	EWS/FP
Disable internet connection	N/A	EWS/FP/WJA	EWS/FP	EWS/FP	EWS/FP
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA
Wizard setup configuration	N/A	EWS	N/A	N/A	N/A
Data access					
Secure file erase	WJA	EWS/FP/WJA	WJA	WJA	N/A
Secure disk erase	WJA/FP	EWS/FP/WJA	WJA/FP	WJA/FP (PS models)	N/A
External HDD	Yes	No	Yes	PS only	No
Communications security					
IPSec	EWS	EWS/FP/WJA	EWS/WJA	EWS/WJA	EWS
SNMPv3	EWS	EWS/FP/WJA	EWS	EWS	N/A
CA/JD Certificates	EWS/WJA	EWS/WJA	EWS/WJA	EWS	N/A
Encrypt web comms	EWS/WJA	EWS/FP/WJA	EWS/WJA	EWS/WJA	EWS

	T1200	T770	Z3100	Z3100ps	4020/4520	T1100/T1120	Z6100	T620
Hide information to user								
Control panel lock	EWS/WJA	WJA	N/A	N/A	WJA	EWS	EWS	N/A
EWS multilevel	EWS	N/A	N/A	EWS (1 level)	EWS	EWS	EWS	N/A
Hide IP from FP	FP	FP	N/A	N/A	FP	FP	FP	N/A
Printer access control	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Exclude personal info. from accounting	EWS	EWS	N/A	N/A	EWS	EWS	EWS	N/A
Disable features								
Disable USB drive	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable fmw update thru USB	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable interfaces	EWS	EWS	EWS	N/A	EWS	EWS	EWS	N/A
Disable direct print with ePrint&Share (USB Printing)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable ePrint Center connectivity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable internet connection	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA
Data access								
Secure file erase	WJA	WJA	WJA	WJA	WJA	WJA	WJA	N/A
Secure disk erase	WJA/FP	WJA/FP (HD)	N/A	FP	FP	WJA/FP	WJA/FP	WJA/FP
External HDD	Yes	HD ver (from fw 6.0.0.6)	No	No	No	No	No	No
Communications security								
IPSec	EWS/WJA	EWS/WJA	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect
SNMPv3	EWS	EWS	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS+ Jetdirect	EWS + Jetdirect	EWS + Jetdirect
CA/JD Certificates	EWS	EWS	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect
Encrypt web comms	EWS	EWS	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect

2. Security features available for Large Format scanners

The Multi function printers (MFPs) are made of two main parts: The printer and the scanner. For the printer, the table above applies, for the scanner please refer to the following table:

	DJ 4500MFP/T1100MFP HD-MFP Series DJ4520 Scanner, DJ 4500 Scanner, HD Scanner	T1120 SD-MFP	T2300 emfp
Firewall	Yes	Yes	Yes
Antivirus installation	Closed systems with very low risk of being infected by a virus, no antivirus is required		
Disable FTP & WebAccess	Yes	No	Yes
Access to images in scanner through network	Yes, by default (FTP & EWS - Read only)	No	No
Microsoft Security patches	Yes through scanner SW update		Not needed (Linux based)
Install scanner software into a separate PC	Possible but not official process	No	No

3. Security Concepts explanation

3.1 Secure File Erase

Secure File Erase is a feature that manages how files are deleted from the printer's hard disk.

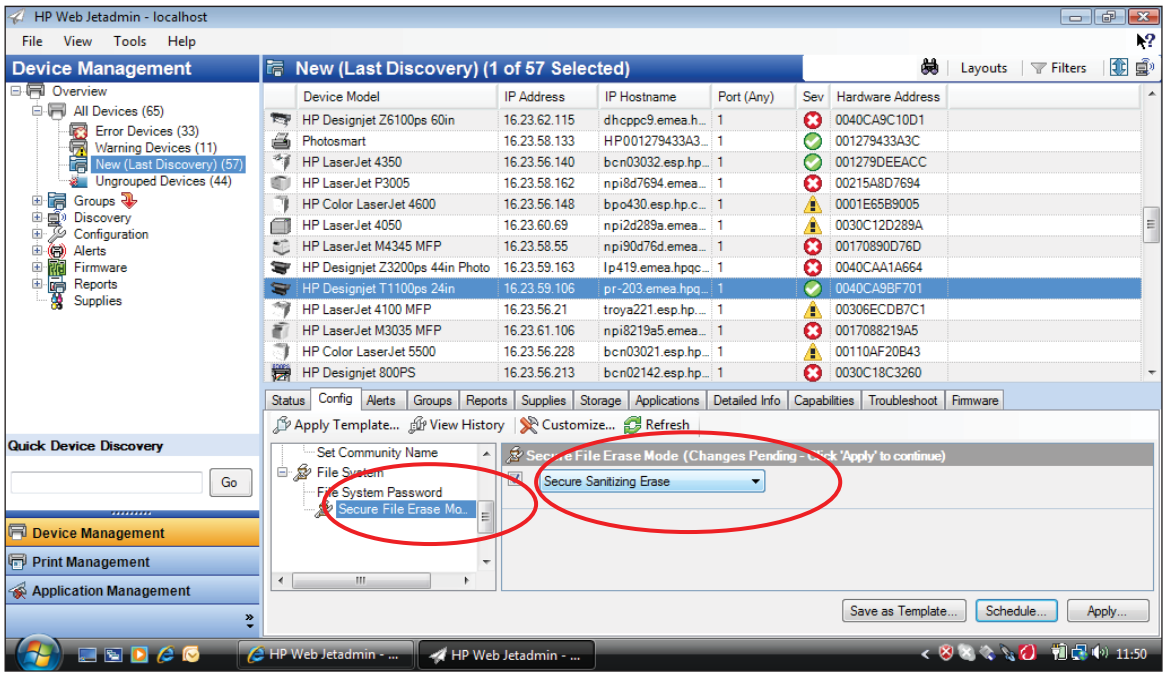
There are three security modes to the Secure Files Erase feature. These settings can be changed in the Web JetAdmin.

- **Non-Secure Fast Erase:** All file pointers to the data (table indexes) are erased. Temporary data remains on the Hard Disk Drive until the disk space it occupies is needed for another purpose, and is then overwritten. This is the fastest mode of operation and is the default for all printers.
- **Secure Fast Erase:** File pointers are erased and the disk space where the temporary job was stored is also overwritten with a fixed character pattern. This mode of operation is slower than Non-Secure Fast Erase, but all data is overwritten.
- **Secure Sanitizing Erase:** File pointers are erased and the disk space where the temporary job was stored is repetitively overwritten using an algorithm that prevents any residual data. This mode of operation may affect product performance. The Secure Sanitizing Erase mode of operation meets the US Department of Defense 5220-22.m requirements for clearing and sanitization of disk media. When the Secure Sanitizing Erase feature is enabled, all temporary files that might contain sensitive data are erased with this method, no temporary files are left after a job has completed (scan, copy, or print).

Furthermore, if storing jobs in the printer is not required; set the number of jobs to be stored in the printer's queue to 0. To configure this setting perform the following:

- Go to the printer's front panel
- Select the "setup" menu
- Select "job management setup"

For further information, refer to the printer's user manual as the actual menu options might change for a specific printer. The following is an example of how to change the 'Secure File Erase' setting for the HP Designjet T1100 printer.

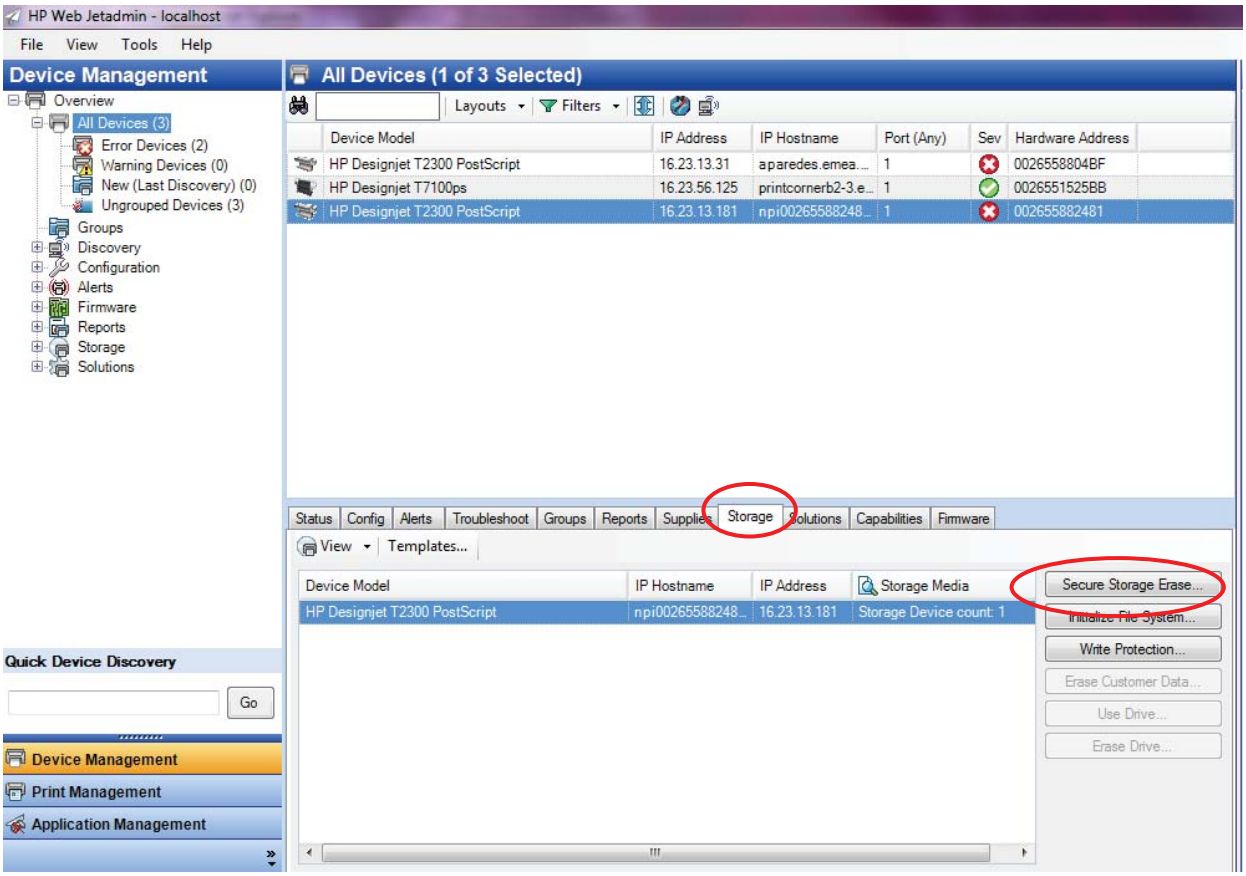


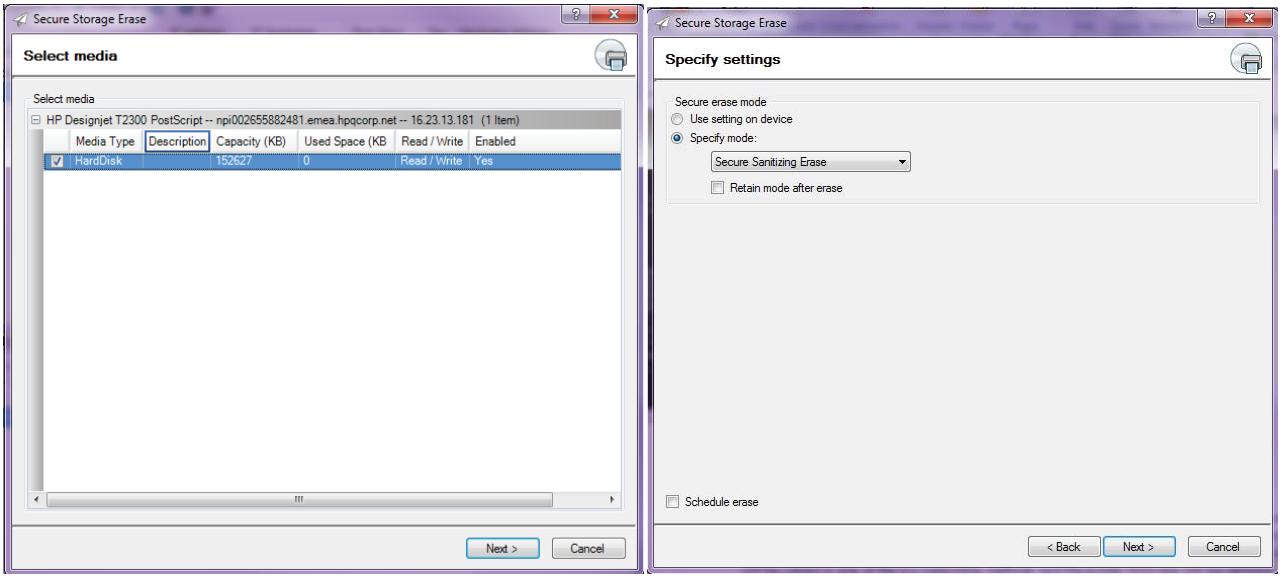
Secure Disk Erase

In either of the two secure methods described above, (Secure Fast Erase and Secure Sanitizing Erase), there is also the option to sanitize the whole disk. The sanitizing method removes any user data in a secure manner, so the device can be moved out from a secure location to unsecure location. All disk erasing will be done via the same level of security erase.

This setting can only be used via Web JetAdmin, or the Front Panel “Service menu” which is only accessible with the help of an HP Support representative.

- **HP Web JetAdmin access**: The user interface that manages the Secure File Erase and Secure Disk Erase functionality is the HP Web JetAdmin. This is the same functionality that is used in the Web JetAdmin device plug-ins for LaserJet printers, this would enable setting the same global options across a fleet of HP LaserJet’s and HP Designjets. The following example shows how to configure the HP Designjet T2300 using the Web JetAdmin. Note that in the Web JetAdmin this option is called “Secure Storage Erase”.

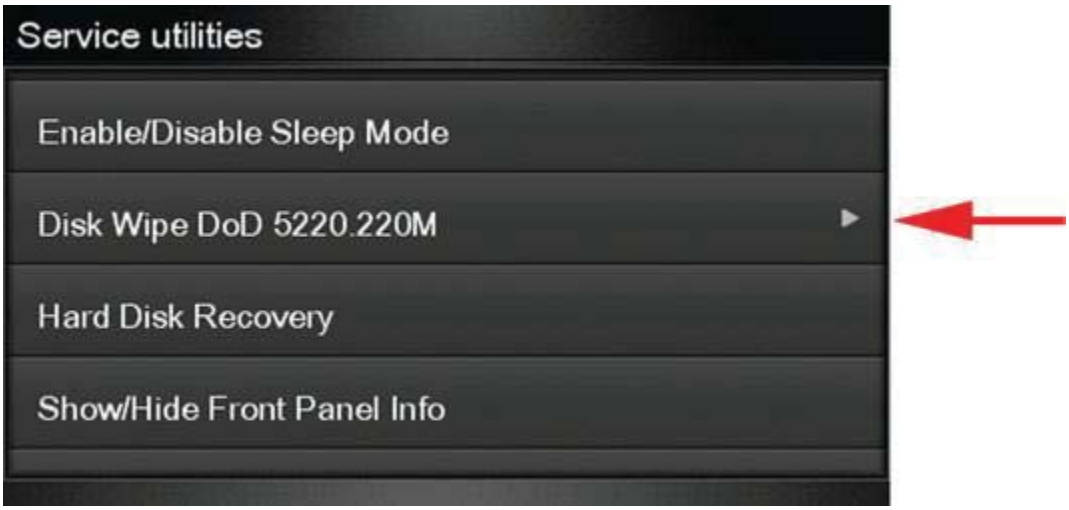


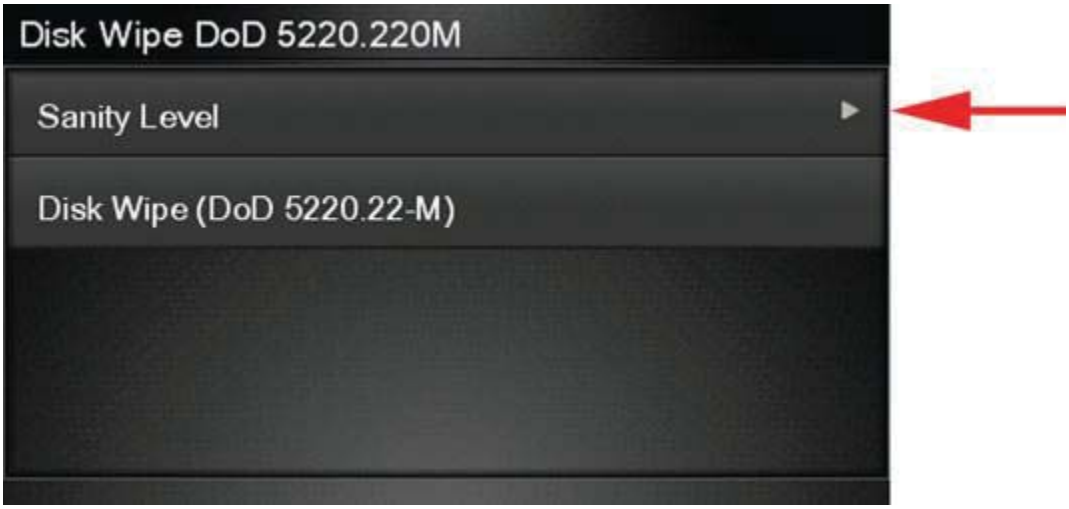


- **Printer's Front Panel access:** Once the "Service Menu" is entered with the help of an HP Support representative, perform the Secure Disk Erase by using the same 3 options that are in Web JetAdmin. Note that the name of the feature in the front panel is **Disk Wipe DoD 5220.220M**, and the three options are called "Insecure Mode", "1-pass mode" and "5-pass mode"

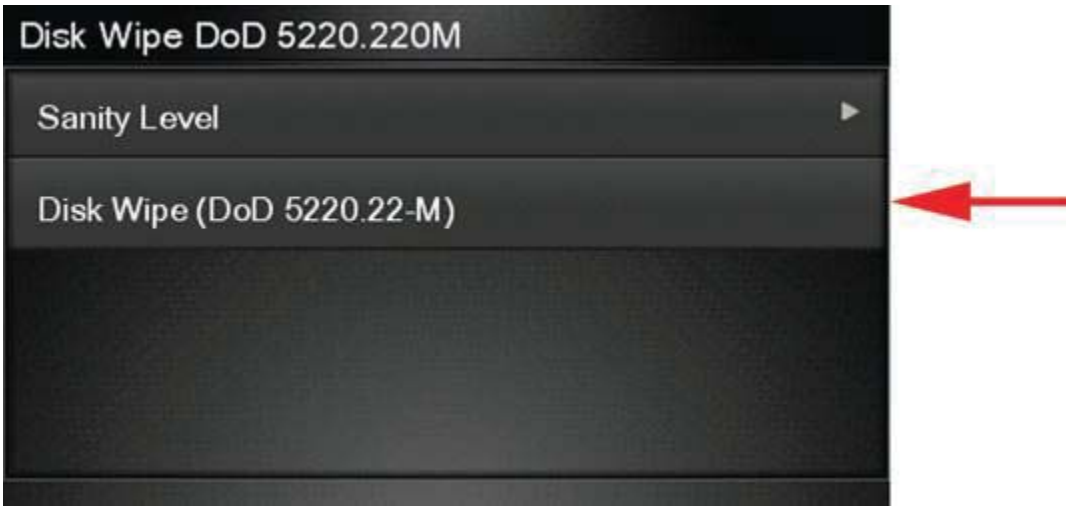
First, select the security level, and then perform the erase operation. The printer will warn that it is a process which deletes all data and takes a long time, when accepted; the printer begins the process and displays a progress bar until complete, all data will be wiped in one of the two selectable methods and the printer's firmware will be restored.

The following screens show how to perform a secure hard disk erase in the HP Designjet T2300 printer:




Disk Wipe DoD 5220.220M
Sanity Level
Disk Wipe (DoD 5220.22-M)


Sanity Level
Insecure Mode
1-Pass Mode
5-Pass Mode

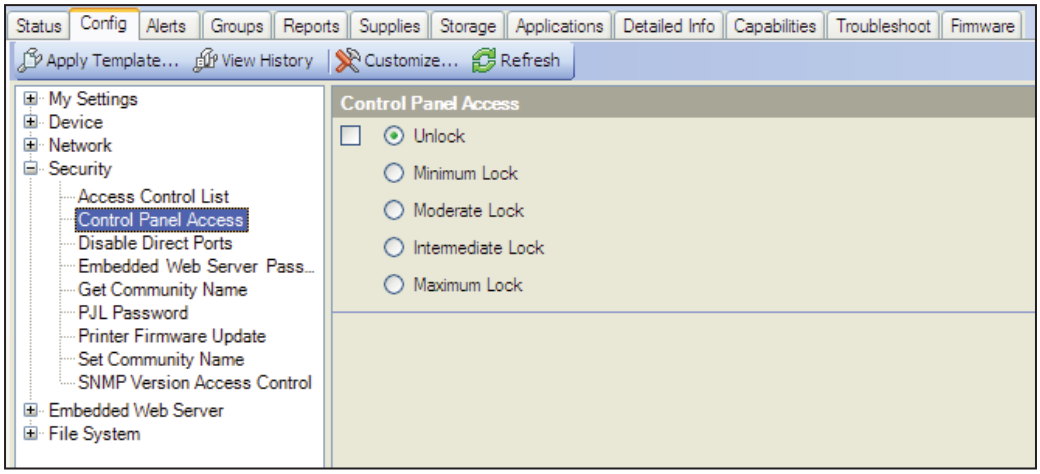

Disk Wipe DoD 5220.220M
Sanity Level
Disk Wipe (DoD 5220.22-M)

3.2 Control Panel Access Lock

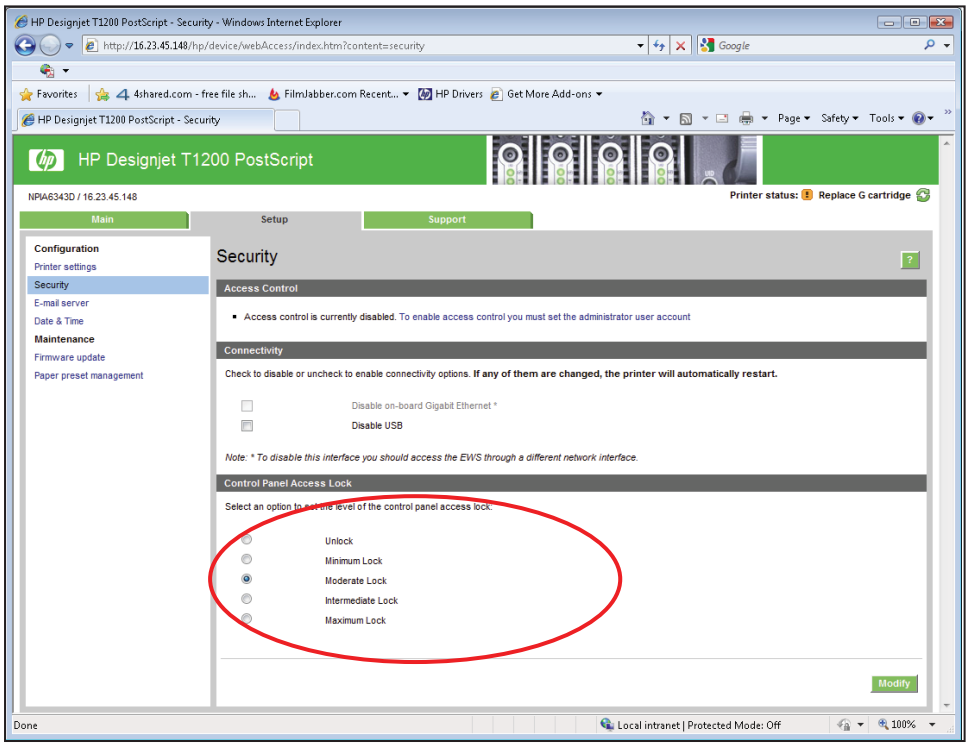
The control panel access is a feature intended for IT administrators, which allows them to lock the device's control panel using the HP Web JetAdmin or the printers Embedded Web Server (depending on the printer model). This feature prevents unauthorized users from accessing the control panel and changing the printer's settings. Administrators can specify the level of access as follows:

- Unlock
- Minimum lock
- Moderate lock
- Intermediate lock
- Maximum lock

This option can be enabled from the HP Web JetAdmin as shown below:



This option can be enabled from the T1200 Embedded Web server as shown below:



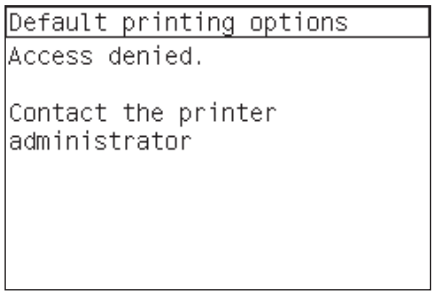
The following table shows the different levels access and what they enable or disable:

	Retrieve Job	Information	Paper handling	Configure Designjet	Diagnostics
Maximum	OK	----	----	----	----
Intermediate	OK	OK	----	----	----
Moderate	OK	OK	OK	----	----
Minimum	OK	OK	OK	OK	OK

- Maximum Lock – Denies access to all options.
- Intermediate Lock – Denies access to the paper and ink supplies handling options, maintenance options, and demo prints, on top of the Moderate Lock. Only viewing printer and supplies information is allowed.
- Moderate Lock – Denies access to all printer settings, the job queue, information and service prints, and the printer log, on top of Minimum Lock. For ePrinters, the setting also locks access to these 5 security features:
    - Disable USB drive
    - Disable firmware update through USB
    - Disable direct print using ePrint&Share
    - Disable ePrint connectivity
    - Disable internet connection
- Minimum Lock – Denies access to the Resets options, Enable/Disable connectivity options, and the Service Menu.

Note: With the Moderate or Maximum locks set it is not permitted to load/unload paper or replace printheads/ink cartridges without first unlocking the front panel. These options should only be set in specific circumstances where the implications are known and understood.

When the Control Panel is locked, the applicable menus show a 'lock' symbol in the front panel. If a user attempts to enter in a "locked" menu entry, a warning message is displayed:



3.3.1 Deadlock: Front Panel locked + EWS password forgotten

Under certain circumstances, a printer might be blocked if the control panel has been locked and the administrator has lost the password needed to unlock it. This could happen if the front panel is locked through the printer's Embedded Web Server and the Administrative password in the EWS is lost. In this situation, it would not be possible to unblock the front panel from the Embedded Web Server and it would not be possible to reset the Embedded Web Server from the front panel.

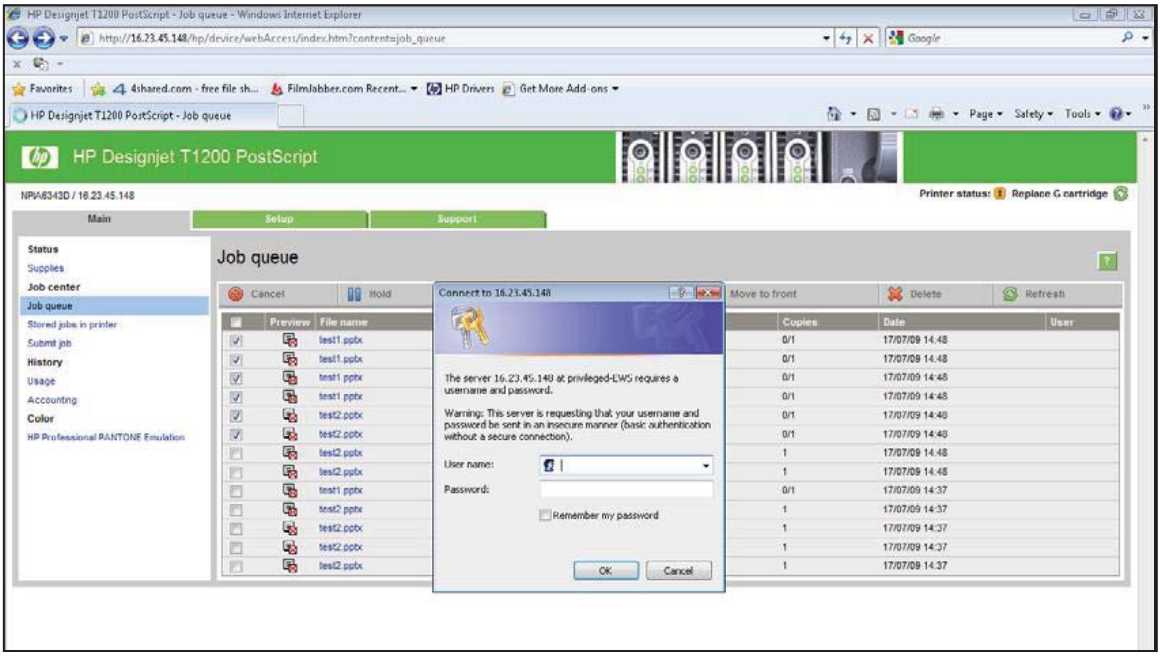
With HP Designjet Printers there is a menu option accessible to users with the guidance of Customer Support agents. Contact HP Support in case of problems related to deadlock.

Embedded Web Server (EWS) multilevel access

The Embedded Web Server is a powerful tool which enables direct management of a device such as an HP LaserJet printer or an HP Designjet printer, however with no security in place, this tool also has the potential to have a negative effect on many features as they can be configured using just a web browser and knowledge of the IP connection to the printer. To solve this situation we have implemented two levels of access to our compatible HP Designjet printers as follows:

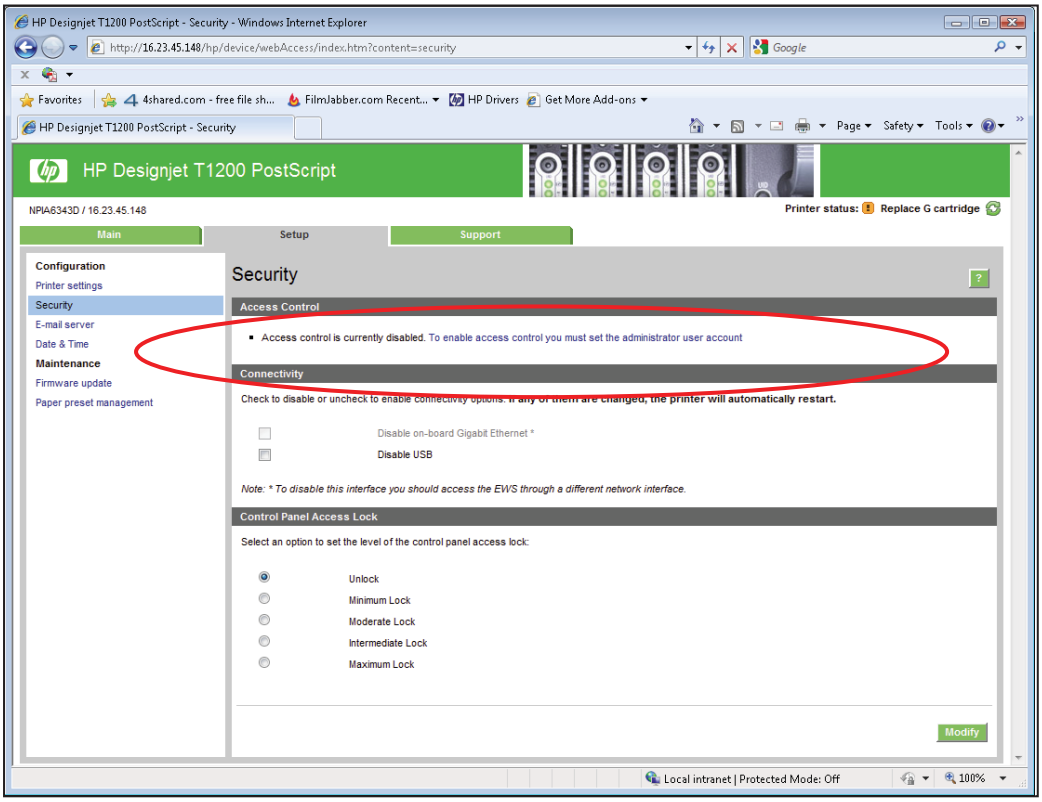
The Security page enables users to:

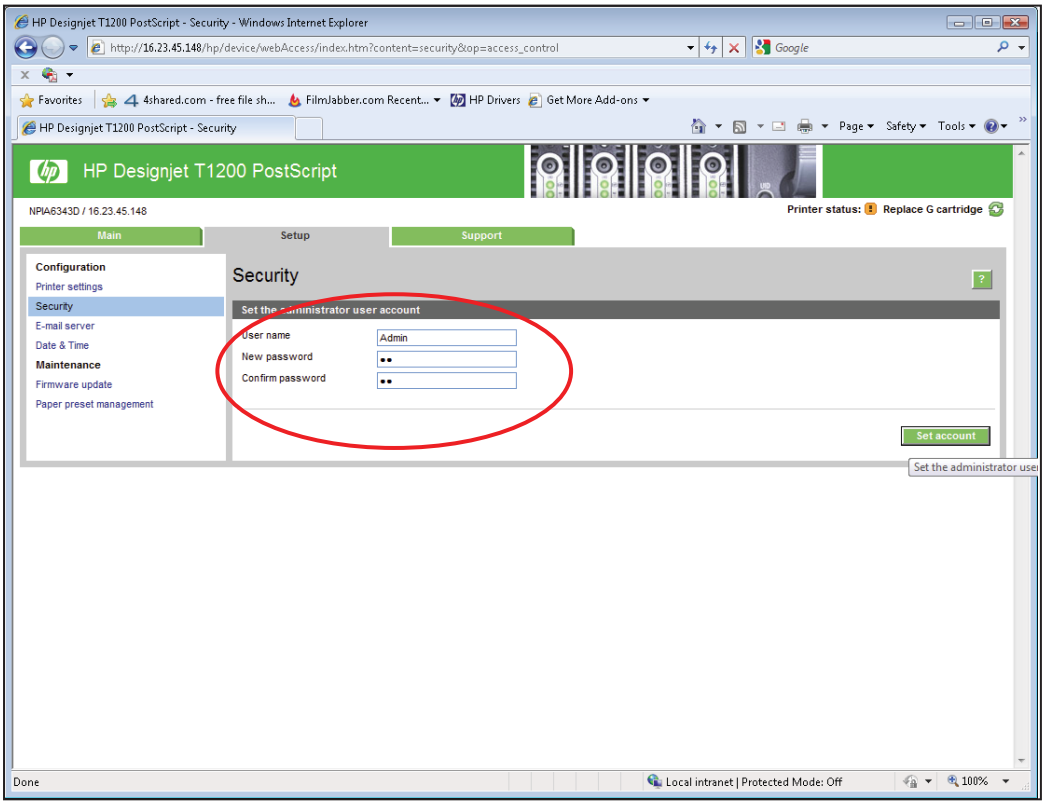
- Restrict access to the printer by setting an administrator user account
- Define two levels of access: Administrator and Guest
- If the two levels of access have been set, and without having either of the passwords; access to EWS information will not be permitted, see below:

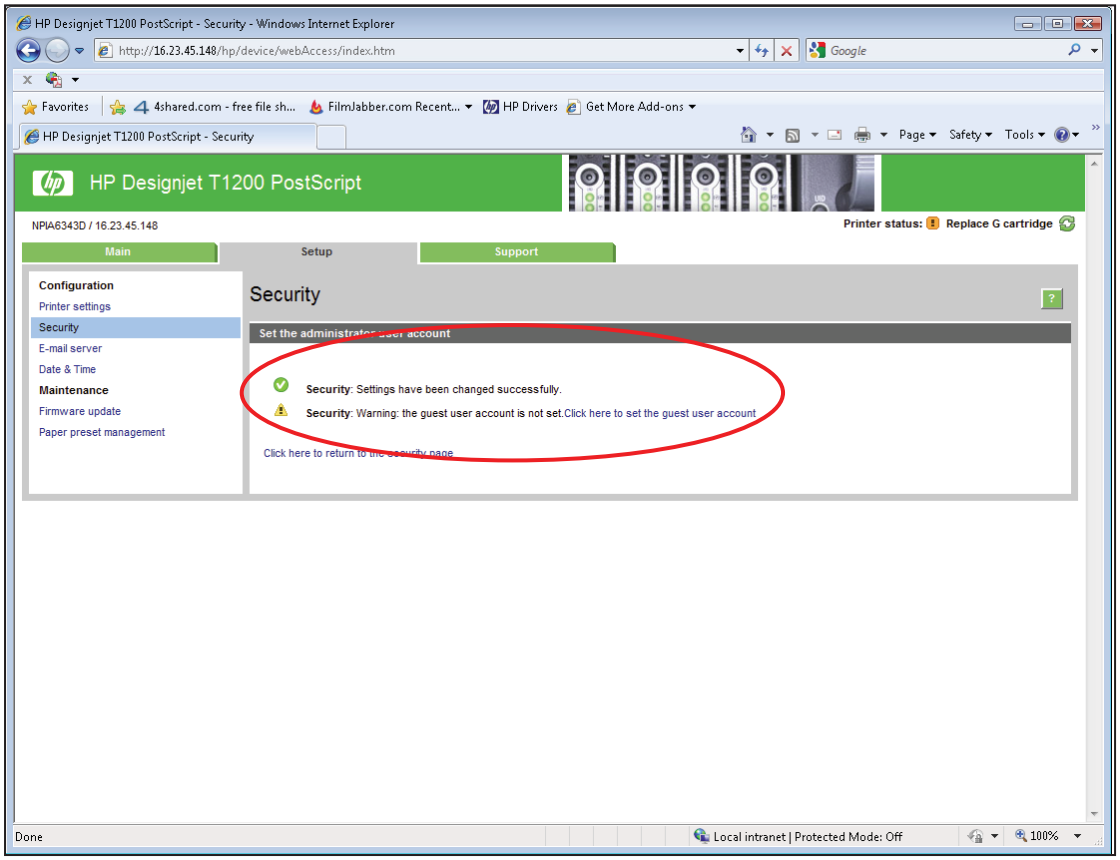


Administrator password
Access control is enabled by setting the “Admin account password”, specifying a password for the user account at Admin level. The Admin password must then be provided in order to perform any of the following **restricted operations**:

- Cancel, delete or preview a job in the job queue
- Delete a stored job
- Clear accounting information
- Change printer’s settings on the Device Setup page
- Update printer's firmware
- Change printer's date and time
- Change security settings
- View protected printer information pages


HP Designjet T1200 PostScript - Security - Windows Internet Explorer
http://16.23.45.148/hp/device/webAccess/index.htm?content=security
HP Designjet T1200 PostScript
NPIA6343D / 16.23.45.148
Printer status: Replace G cartridge
Main
Setup
Support
Configuration
Printer settings
Security
E-mail server
Date & Time
Maintenance
Firmware update
Paper preset management
Security
Access Control
Access control is currently disabled. To enable access control you must set the administrator user account
Connectivity
Check to disable or uncheck to enable connectivity options. If any of them are changed, the printer will automatically restart.
Disable on-board Gigabit Ethernet *
Disable USB
Note: * To disable this interface you should access the EWS through a different network interface.
Control Panel Access Lock
Select an option to set the level of the control panel access lock:
Unlock
Minimum Lock
Moderate Lock
Intermediate Lock
Maximum Lock
Modify


HP Designjet T1200 PostScript - Security - Windows Internet Explorer
http://16.23.45.148/hp/device/webAccess/index.htm?content=security&op=access_control
HP Designjet T1200 PostScript
NPIA6343D / 16.23.45.148
Printer status: Replace G cartridge
Main
Setup
Support
Configuration
Printer settings
Security
E-mail server
Date & Time
Maintenance
Firmware update
Paper preset management
Security
User name
Admin
New password
Confirm password
Set account
Done

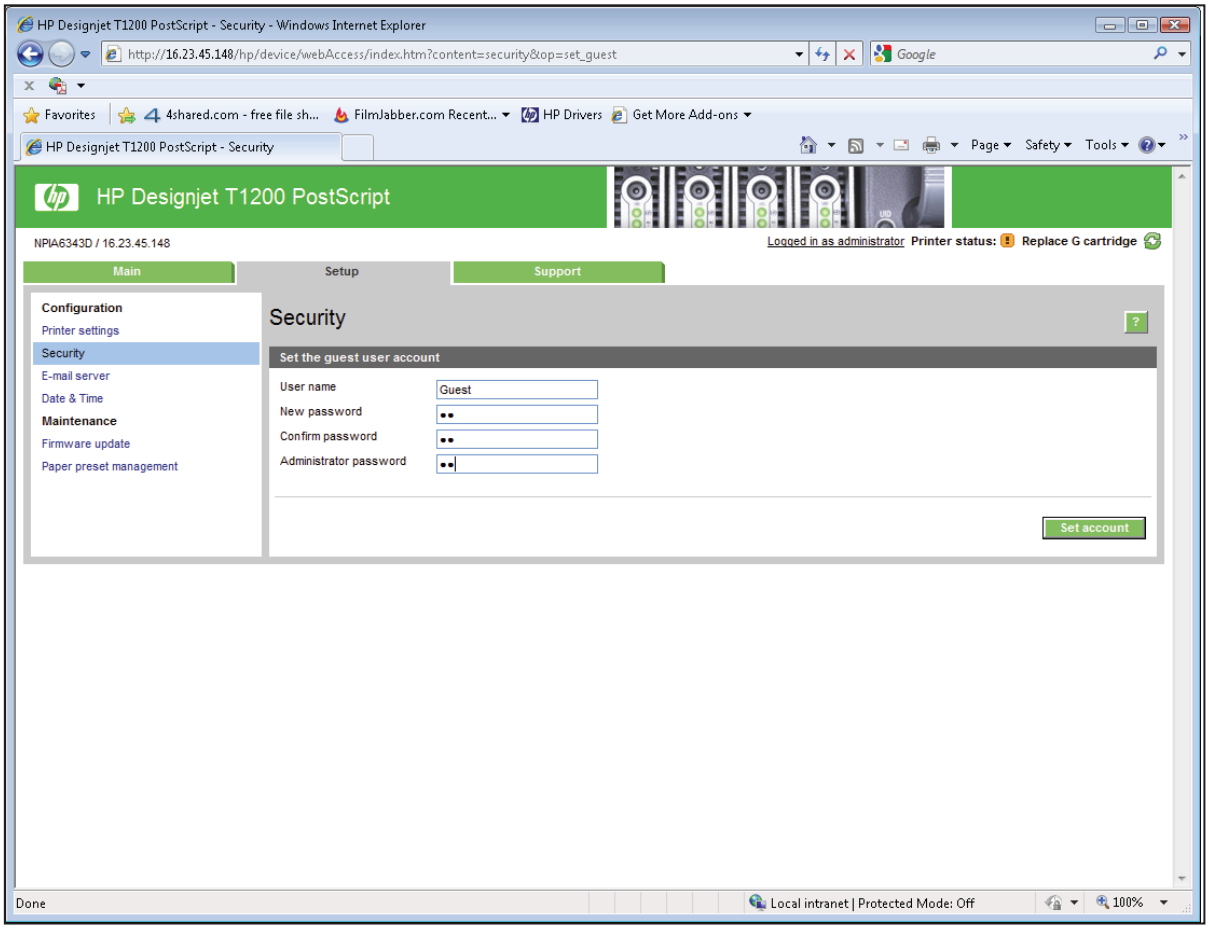


If there is no administrator account, restricted operations can be accessed without a password.

3.4.1 Guest password

Once the administrator user account has been set, the administrator can also set the guest user account by specifying a password for the guest.

If the guest user account is set, a username and password are required for **all** EWS operations: users indentified as guests have access to restricted operations, whilst users identified as administrators have access to all operations.
If the guest account is not set, a username and password are not required for unrestricted operations.



Notes:

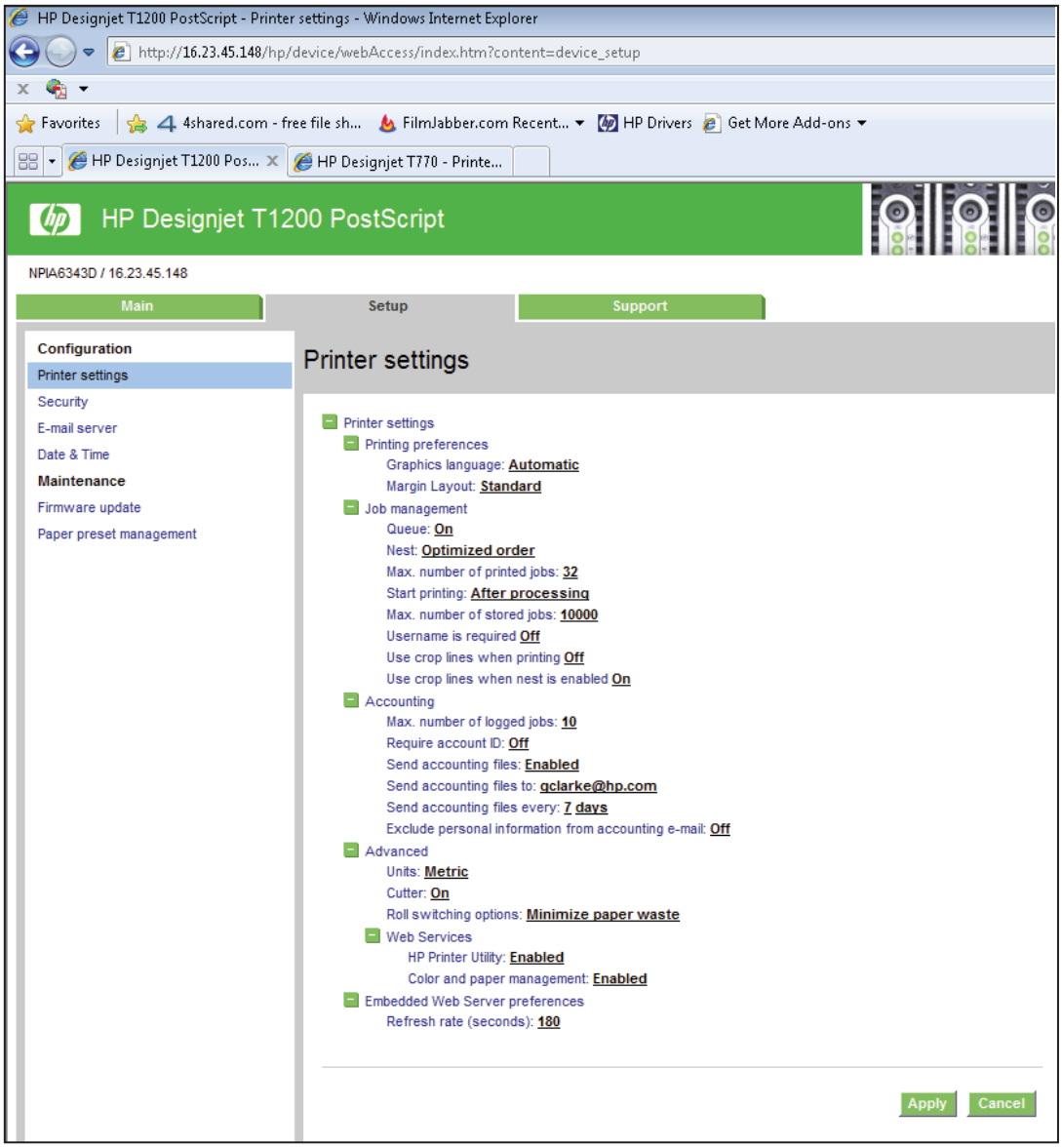
- Some printers only have 1-level password access to the Embedded Web Server.
- The networking tab of the Embedded Web Server allows setup of another password. If the printer has an EWS 1-level or multi-level password, then the networking password is common with the general EWS password. If the EWS does not have password capabilities then the networking password is only used for controlling access to the networking area of the EWS.
- For most printers that have a EWS password capability, it is also possible to setup the admin password through Web JetAdmin, however only one level can be set so that Guest password cannot be setup from Web JetAdmin.

3.3 Exclude personal info from accounting

Enable or disable the printer to send an e-mail containing accounting information; if this setting is enabled, it is imperative to also fill in the destination of the report using the Send accounting files to setting and also configure the e-mail server on the **Setup Page**.

In some cases customers prefer not to send personal data from the printers via email and so the option Exclude Personal information from accounting e-mail is now available in the Embedded Web server. If this option is selected, accounting e-mails will not contain personal information (user name, job name, account ID will be left blank in the accounting file sent by email from the printer).

Typically this option is used for managed print or pay-per-use contracts to ensure that only the data (counters) relevant for billing are being sent by the printer. Personal information about who printed which file is not required for billing purposes, and can be excluded from the accounting email. This personal information is typically used for cost allocation within a company.

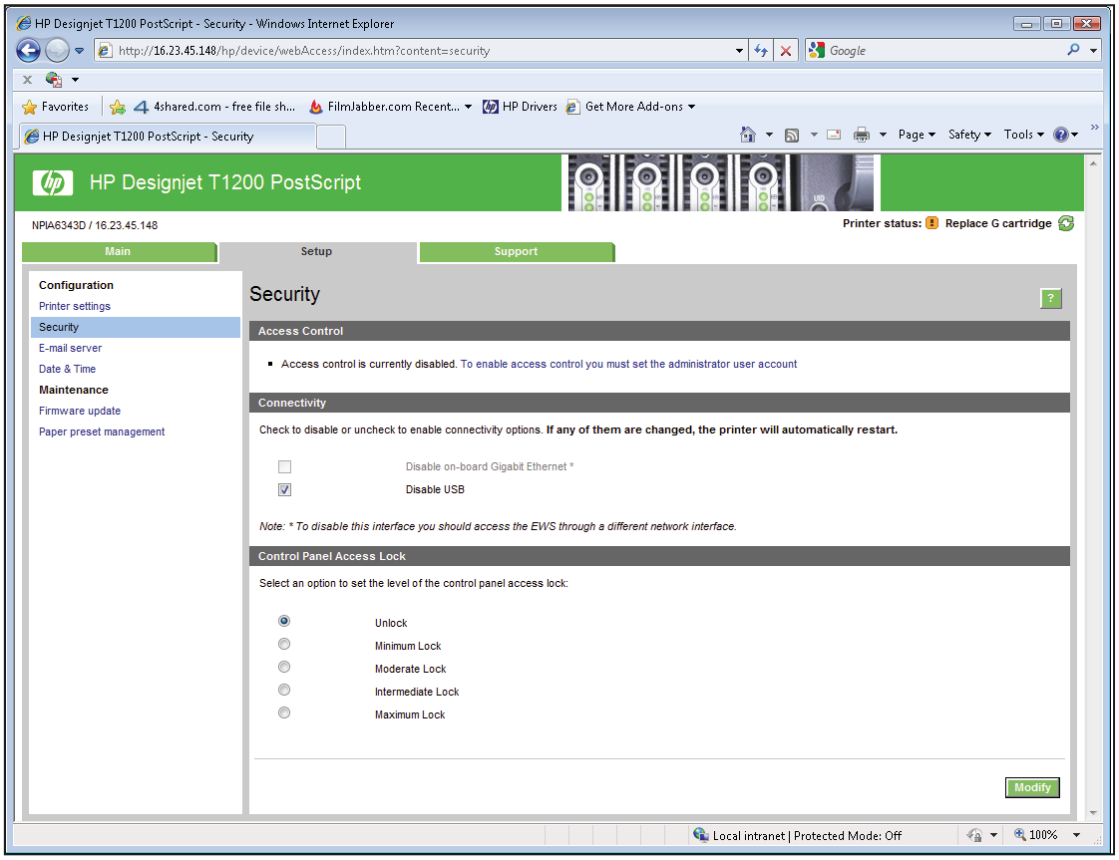


3.4 Disable connectivity interfaces

Depending on the printer series, there are some ports that can be disabled to prevent unauthorized printing and possible data theft.

It may be desirable to disable the USB printing port to avoid people from connecting a laptop directly into the printer and printing through the USB.

If a JetDirect card is installed to add extra security features, then disabling the onboard Ethernet may be required.

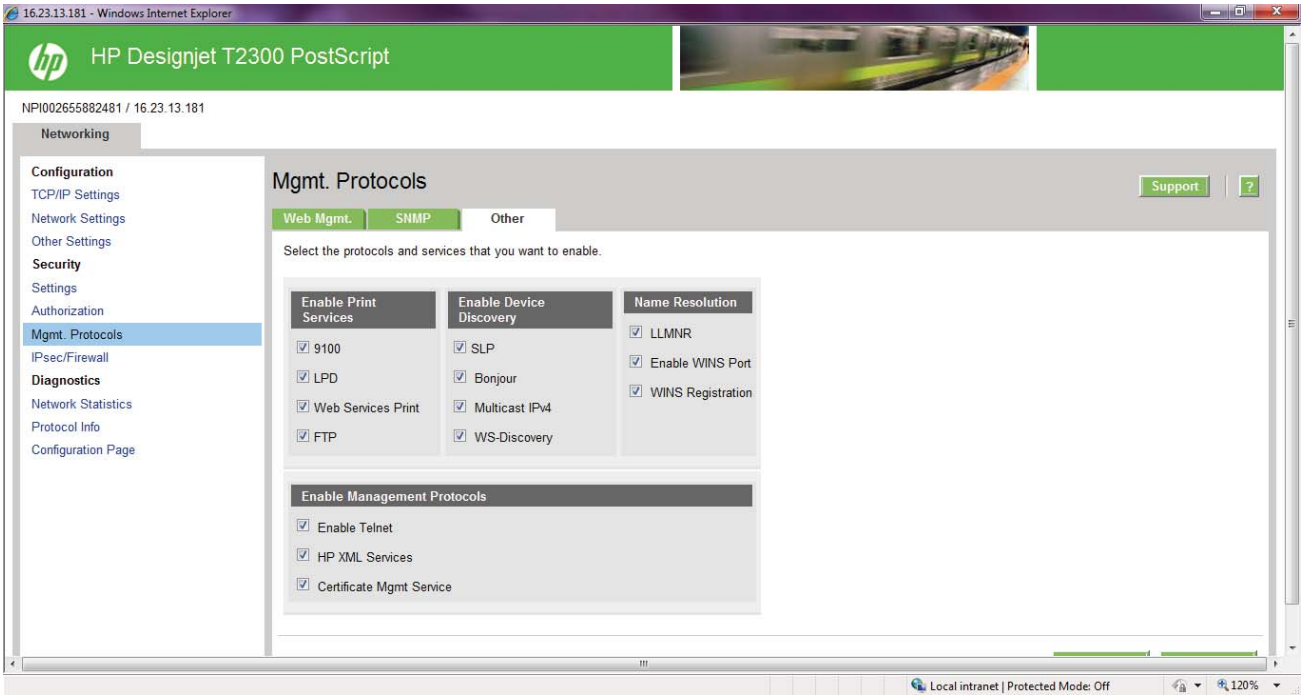


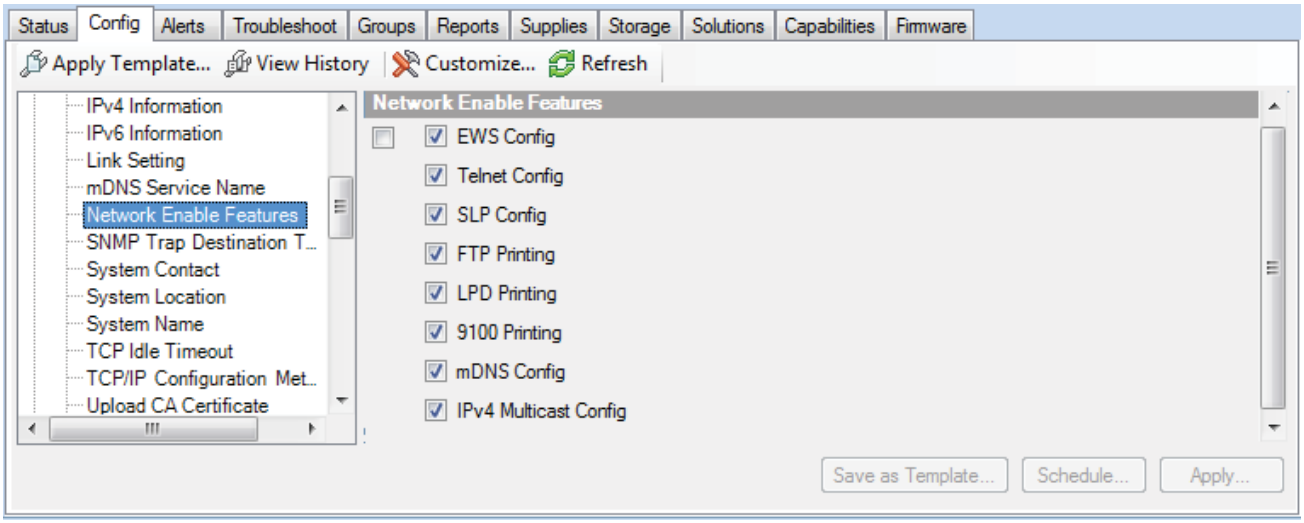
If a connectivity option is enabled or disabled, the printer will automatically restart. Keep in mind that disabling a connectivity option could cut off network access to the printer. As a security measure, disabling the connection used to access the Embedded Web server is not permitted.

Note: Contact HP support in case the printer's front panel is locked and cannot be unlocked.

3.5 Disable protocols

In some cases, disabling all protocols that are not planned on being used to access the printer may be required, for example, to prevent users from sending files through the ftp, or connecting through telnet to manage the printer network settings. Disable unused protocols through the Mgmt. protocols option in the Embedded Web Server or Network enable features in Web JetAdmin.





3.6 IPSec

A Firewall or IP Security (IPsec) policy allows the control of traffic to or from the device using network-layer protocols. Either a firewall or IPsec / firewall pages will appear depending on whether IPsec is supported by the print server and device. If IPsec is not supported, firewall pages will be displayed and a firewall policy can be configured.

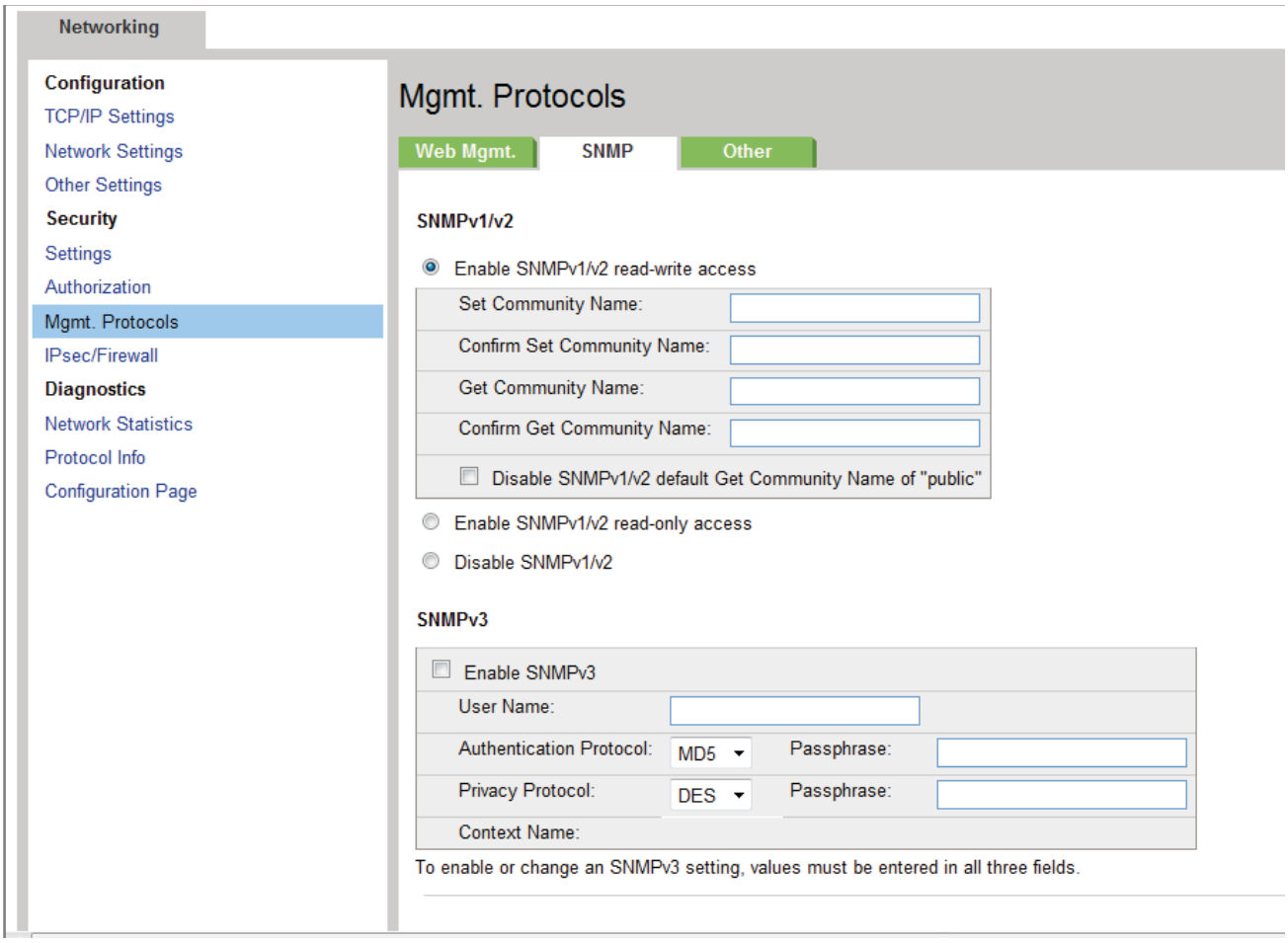
Note: Before enabling a firewall or IPsec policy, make sure there is secure access to the configuration management settings (for example, through an administrator password). This will ensure t policy is not easily disabled through Telnet, control panel menus, or other management tools.

Firewall: A firewall policy consists of up to 10 rules, where each rule specifies the IP addresses and services allowed by the print server and device. To add a rule, click 'Add Rule'. This setting runs a wizard to help configure each rule.
IPsec / Firewall: An IPsec / firewall policy consists of up to 10 rules. As with a firewall policy, each rule specifies the IP addresses and services allowed by the print server and device. With IPsec support, one can apply IPsec authentication and encryption protocols for those addresses and services. To add a rule, click 'Add Rule'. This runs a wizard to help configure each rule.

For a detailed description of wizard settings and additional help, click **Jetdirect IPsec/Firewall Help**.

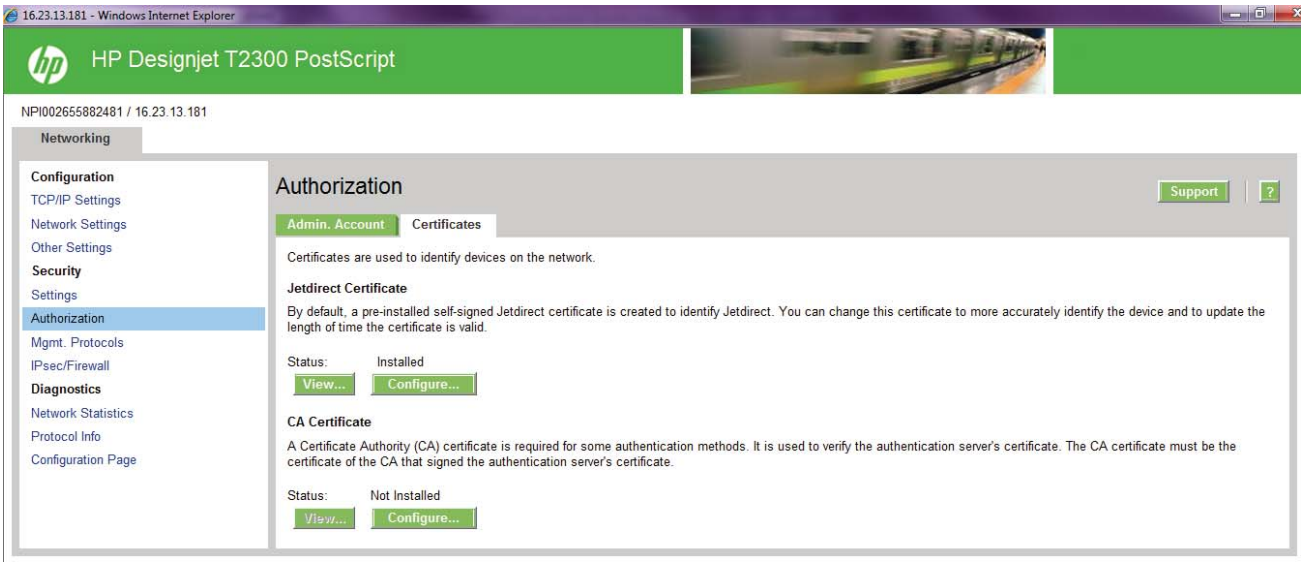
3.7 SNMPv3

Enable and disable the SNMP v3 agent from the printer. An account may be set up that allows a management application to access the SNMP v3 agent.



3.8 CA/JD Certificates

Request, install, and manage digital certificates on the HP JetDirect print server. Certificates are used to identify the JetDirect print server both as a valid Web server for network clients, and as a valid client requesting access on a secure network. By default, the JetDirect print server contains a self-signed preinstalled certificate.



3.9 Hide IP from front panel

Some printers includes an option in the Service Menu, accessible with the help of an HP Support agent only, that allows hiding all IP information from the printer's front panel.

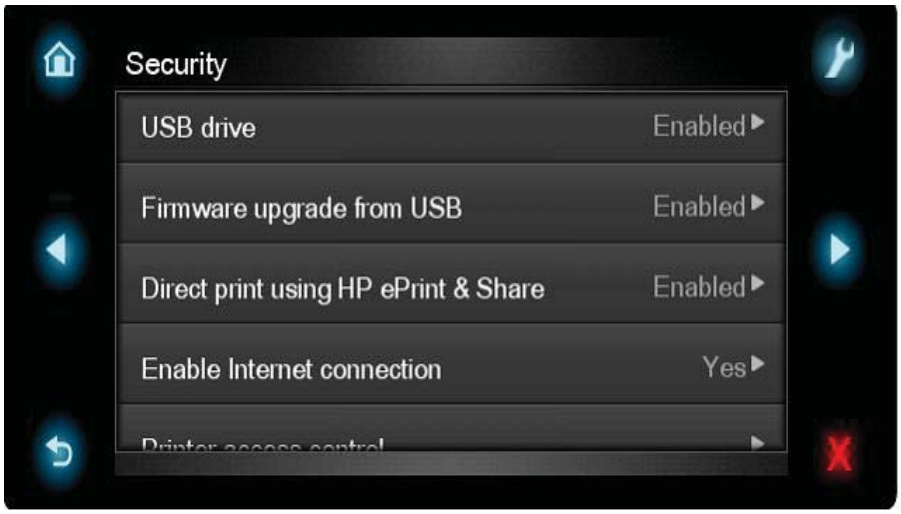
3.10 Encrypt web communications

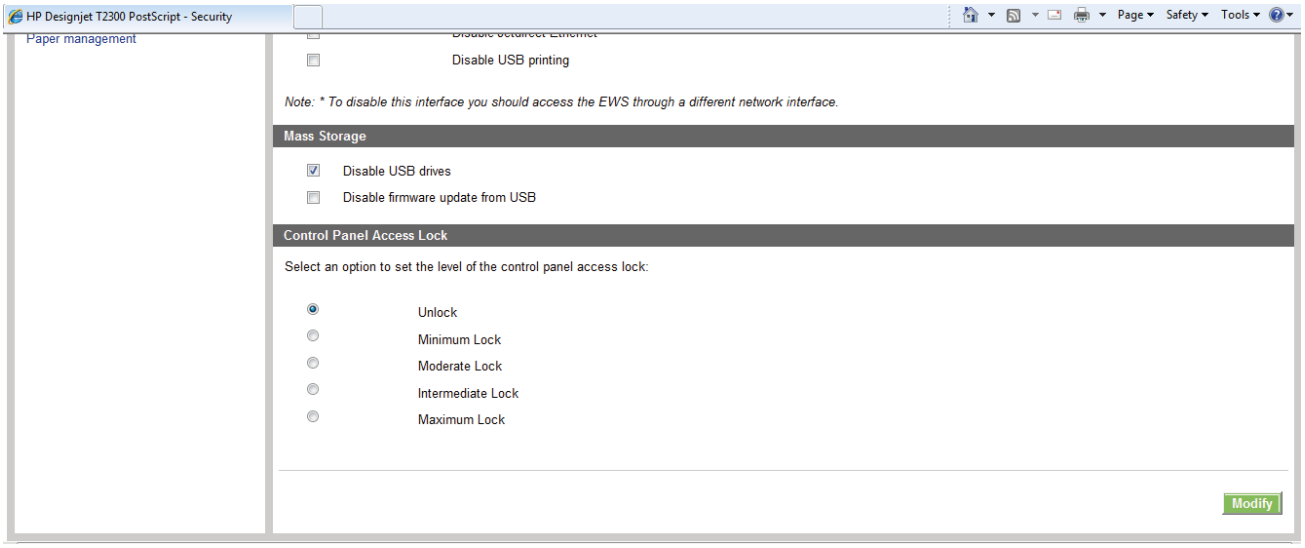
Securely manage the network device using a Web browser and the HTTPS protocol. To authenticate the HP JetDirect Web Server when HTTPS is used, configure a certificate, or use the pre-installed, self-signed X.509 Certificate. The encryption strength specifies what ciphers the web server will use for secure communications. Supported cipher suites are DES, RC4, 3DES.

By enabling encryption, the web server encrypts all web communication, forcing all connections to use HTTPS. Enabling encryption can also be configured to allow both HTTP (unencrypted) and HTTPS connections. In secure environments, choose to encrypt all web communications. Otherwise, sensitive management data (Administrator Password, SNMP Community Names, and secret keys) may be compromised.

3.11 Disable USB drive

Use this option to disable the USB drive preventing somebody connecting a device to print or to scan images.





3.12 Disable firmware update through USB

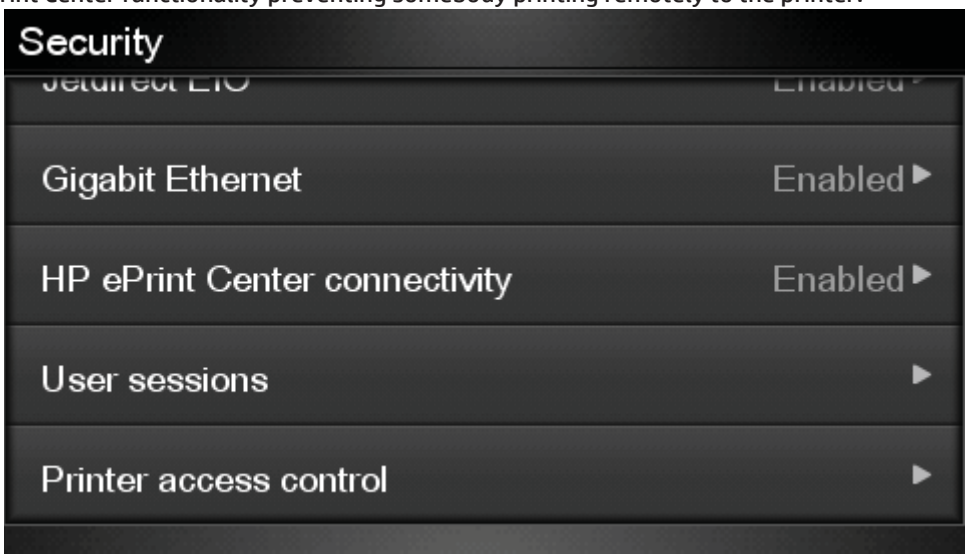
Disable the possibility of upgrading the printer by installing the firmware via a USB device.

3.13 Disable direct print using ePrint&Share

In some printers, when connecting a computer directly with a USB cable, one can print without installing any driver, this can be done by launching the ePrint&Share application that resides inside the printer. This feature can disable direct printing so that printing through the USB cannot be done unless the driver (or ePrint&Share) is installed in the computer.

3.14 Disable ePrint Center connectivity

Disables the ePrint Center functionality preventing somebody printing remotely to the printer.



3.15 User sessions

Allows setting a timeout so that open sessions to ePrint&Share from the printer front panel are automatically closed if they are not used.

3.16 Disable internet connection

Disable the direct connection of the printer to the internet. This option would also prevent the printer from automatically performing firmware upgrades.

3.17 Printer Access control

For some printers, when setting an Embedded Web Server admin password, it is also preventing access to certain front panel features. The features protected in the front panel are:

- Network connectivity & Internet Connectivity
- Control firmware upgrades
- Reset factory defaults
- External hard disk connection
- Security

If a user loses the admin password, it is not possible to reset it so the printer would be locked. There is a service menu option to reset the admin password.

3.18 External hard disk (EHD)

Some printers allow the connection of an external hard disk. Any HP Designjet printer with an internal hard disk uses it for four main purposes:

- Store the printer's firmware & resources (media profiles, demo plots, diagnostic plots)
- Virtual memory for job processing
- Job storage/queue
- Storage for printer's accounting data

The HP Designjet External Hard Disk was designed to fulfill one specific use for those security conscious customers that want to preserve the confidentiality of the jobs being printed in their HP Designjet printers.

How the system works

1. Connect the External Hard Disk (EHD) into the printer's USB host port.
2. The printer will detect the EHD and will ask the customer for permission to install it. When the customer accepts, the printer will perform the following step:
3. A copy will be made of all the customer's information that is stored in the internal HD and copied to the external HD.
4. The customer's internal HD partition will be deleted after a highly secure erasing process (DoD 5220.22-M).
5. The printer will be configured to use the EHD as the repository for ALL customer jobs (including the temporary processing storage area).
6. Once the EHD has being installed, all the customer jobs will ALWAYS be stored in the EHD
7. When the printer is switched off, as a security measure, the EHD can be removed and kept in a secure location.

Notes:

- Once the printer has an EHD installed it can no longer be initialized without it.
- If for any reason the installed EHD is no longer available (the customer loses the EHD, or the EHD is broken), there is a mechanism (through a special bootmode controlled with an specific front panel key combination) that reconfigures the printer to work without the EHD. However in that particular case, all the information stored in the EHD is lost.
- Once the EHD is installed on a particular printer, it becomes fully tied to it. It is not possible to move this EHD to another HP Designjet printer without losing the stored information. When the printer detects an EHD that has been installed on a different printer, it will advise the customer about it. If the customer decides to go ahead and use the EHD on a different printer, the printer will erase the contents of the EHD (once again, using the highly secure DoD 5220.22-M process)
- The EHD has its own software based encryption mechanism that prevents anyone reading the contents of the EHD, for instance, by plugging it into a PC. The encryption system is not a standard one and cannot be considered as an extremely secure encryption mechanism (such as the standard encryption system DES, RSA, FIPS 140...), but it does add a level of security that makes it difficult when trying to read the contents by just connecting the disk to a PC.

The EHD is not intended to be used as an USB memory stick, that is, to copy documents from a PC, plug it into the printer and to print them.

3.19 Jetdirect Security Wizard (HP T920-T1500 only)

The HP Jetdirect Security Configuration Wizard allows a user to configure security settings for HP Jetdirect print server management. There are 3 levels of Network Security that can be set:

Basic

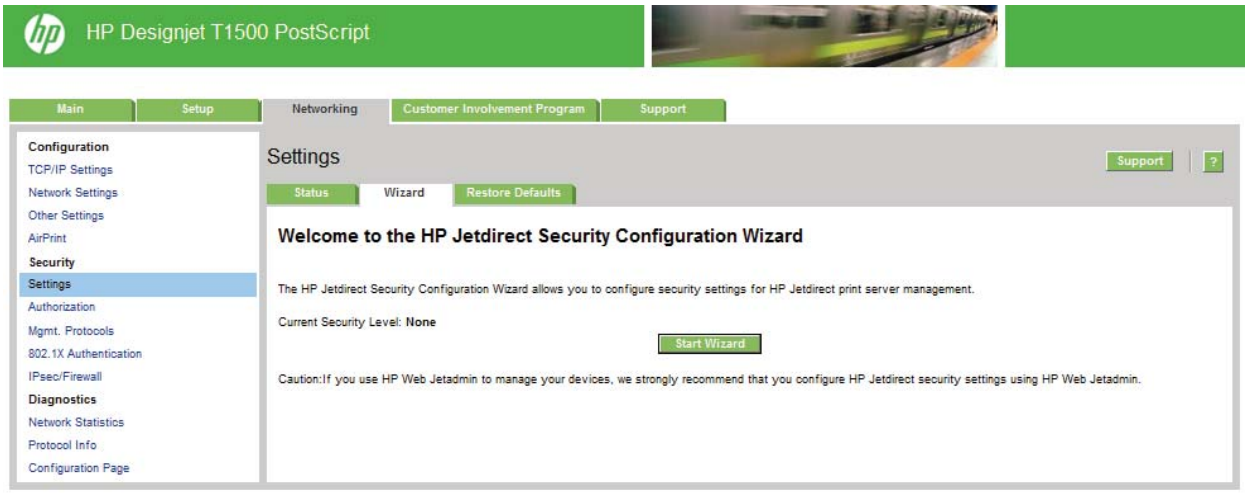
Configure Admin password shared with other tools such as Telnet and SNMPv1/v2

Enhanced

Disables unsecure management protocols (FTP, Telnet, RCFG, SNMP v1/v2c)
Enable SNMPv3
Enable SNMPv1/v2 read only access

Custom

Manually adjust all the settings



4. Designjet Security features vs LaserJet

Some security features are available only after installing a JetDirect 635n or similar.

4.1 Access Control list

This feature lets one determine the access control list (ACL), which is used to specify the IP addresses on a network that are allowed access to the device. The ACL is normally used for security purposes and supports up to 10 entries. The device blocks communications from all other addresses. If the list is empty, any system is allowed access. By default, host systems with HTTP connections (such as web browser or IPP connections) are allowed access regardless of ACL entries. This allows hosts to access the device when proxy servers or Network Address Translators (NATs) are used. However, unfiltered access by HTTP hosts may be disabled by clearing the Check ACL for HTTP checkbox.

Host systems that have access are specified by their IP host or network address. If the network contains subnets, an address mask may be used to specify whether the IP address entry is for an individual host system or a group of host systems. For an individual host system, the mask “255.255.255.255” is assumed and is not required.

CAUTION! A user may lose the ability to communicate with the device 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.

4.2 802.1X Authentication

802.1X is an IEEE Standard for port-based Network Access Control. It provides an authentication mechanism to devices that want to connect to a LAN.

For most 802.1X networks, the infrastructure components (such as LAN switches) must use 802.1X protocols to control a port's access to the network. If these ports do not allow partial or guest access, the print server may need to be configured with your 802.1X parameters prior to connection.
To configure initial 802.1X settings before connecting to a network, use an isolated LAN, or a direct computer connection using a cross-over cable.

The supported 802.1X authentication protocols and associated configuration depend on the print server model and firmware version. For more information on 802.1X features please click **here**.

5. Designjet Security features vs LaserJet

HP LaserJet printers have some security features that are not yet available in HP Designjet printers.
As a brief comparison, please find the comparison between HP LJ 9050 series and Designjet T1200 series.

Security Feature	L9050	DJ T1200
Authentication Manager	Yes	No
Control panel lock	Yes	Yes
Device Password	Yes	Yes
Direct Connect Ports (USB/IEEE 1284)	Yes	Yes
File erase mode	Yes	Yes
File system access settings	Yes	No
File system password	Yes	WJA only
Job Held Timeout	Yes	No
Job Retention	Yes	No
PJL Password	Yes	No
Remote FW upgrade	Yes	Yes

6. Glossary

Active Directory (AD)	An advanced, hierarchical directory service that comes with Microsoft Windows servers (version 2000 or later). It is LDAP-compliant and built on the domain naming system (DNS) used on the Internet. Workgroups are given domain names, exactly like Web sites, and any LDAP-compliant client – such as Windows, Mac, or Unix – can gain access.
Adobe PostScript	Developed by Adobe, this is the standard page description language (PDL) for the graphics arts industry and commercial printing. Many printing devices support PostScript with a built-in PostScript interpreter
Color Access Control	Settings to determine which users and/or applications are allowed to print in color
Device Password (LJ feature)	This is equivalent to the designjet's web server password. It helps protect the printer from unauthorized access through remote applications
Domain Naming System (DNS)	Converts host names and domain names into IP addresses on the internet or on local networks that use the TCP/IP protocol.
Embedded Web Server (EWS)	The EWS resides on a hardware device (such as an HP Designjet) or in the printer firmware. The EWS allows you to review, configure, and change settings on an HP Designjet after inputting an IP address into a Web browser from the computer
File System Access settings (LJ feature)	File system access settings: The File System Access options allows to completely disable many of the access points to the printer's data storage system. These access points are for various types of usage for the printer. The options are: • PJL disk access • SNMP disk access • NFS disk access • PS disk access HP recommends enabling PS Disk Access to allow to print PS files, and disable the rest
File System Password (LJ feature)	The File System Password feature helps protect the printer's data storage system options from unauthorized access. With the File System password configured, the printer requires the password before it will allow configurations to features that affect the data storage system. Some of these features are the Secure disk erase mode, the Secure Storage Erase feature, and the File System Access options.
Hide IP address from front Panel	Option in the Service Utilities menu of the front panel to show/not show the Internet Protocol (IP) address of your printer. In that way, only registered users or network administrations will know the correct address to submit jobs to the printer
HP Web Jetadmin	Web-based fleet management software tool for remote installation, configuration, problem resolution, proactive management, and reporting. For more information go to; www.hp.com/go/webjetadmin
IP multicast	A one-to-many transmission of data over an IP network.
IPSec	Internet Protocol Security (IPsec) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. In our case, IPsec is used to protect data flows between the host and the printer.
Job Held Timeout (LJ feature)	This feature is part of the Job Retention feature. It limits a held job to the selected time, and then the printer deletes it. A user should select a reasonable timeout value for this setting to allow enough time for a user to walk to the printer to print a job or to allow time for jobs to print in a queue.

Job Retention (LJ feature)	This feature provides job retention options such as private job and hold job. A user will be able to ensure that they are present during printing to provide privacy for documents in the printer output bins.
Multicast DNS (mDNS)	Also known as Bonjour or Rendezvous, mDNS uses IP multicast with DNS to provide the capabilities of a DNS server for service discovery in a small network that does not have a DNS server.
PJL Password (LJ feature)	The PJL password feature helps protect the printer from unauthorized configurations through Print Job Language (PJL) commands. It does not affect ordinary print jobs. Once the PJL password is configured, the MFP requires it before it will process any of these commands
Remote Firmware Upgrade (LJ feature)	This service allows an administrator to use a custom application to upgrade the printer's firmware remotely. Since HP recommends using HP Web Jetadmin to upgrade MFP firmware, one should disable Remote Firmware Upgrade.
Simple Network Management Protocol (SNMP)	This is a network monitoring and control protocol.
SNMPv3	SNMP (Simple Network Management protocol) allows users to manage the printer using SNMP management tools, such as HP Web JetAdmin. SNMP is also the protocol for communicating from the printer to the Windows driver. SNMPv3 provides security through user authentication and data encryption
Subnet	A logical division of a local area network, which is created to improve performance and provide security. A subnet limits the number of nodes that compete for bandwidth.
Authentication Manager (LJ feature)	It allows administrators to secure Device Functions by requiring users to log in with a specific Log In Method for each Function. For example, users may be required to log in with an Access Code or PIN to make copies yet be required to log in with a username and password to send e-mails. **Log In Methods:** The following Log In Methods are available with the latest device firmware upgrade: **Group 1 PIN:** Requires users to input a numeric code for access when at the control panel of the device. The numeric code entered by the walk up user is compared to the first of two PINs stored on the device by the Administrator. When the PIN is entered correctly, the user can proceed. **Group 2 PIN:** Requires users to input a numeric code for access when at the control panel of the device. The numeric code is compared to the second of two PINs stored on the device by the Administrator. **LDAP:** Lightweight Directory Access Protocol, Requires users to input a username and password that are verified by an LDAP server. **HP Digital Send Service (if available):** Also known as DSS. Requires users to enter credentials that are verified by the HP Digital Send Service software. (HP Digital Send Service software must be available to use this Log In Method. If no DSS server is associated with this device, walk-up users will not be required to authenticate before using the device.) **Kerberos:** Requires users to enter a username and password to be verified by a Windows Server.

For more information

About HP Designjet printers: www.hp.com/go/designjet

About HP WebJetAdmin: www.hp.com/go/webjetadmin

July 2013