HP DesignJet and PageWide XL Printers

Security features

September 2017 Edition
Version 11

Table of Contents

1. Introduction & Overview

This document provides an overview of the security and connectivity features supported by HP DesignJet and PageWide XL printers as of April 2017.

The security features described in this document make the HP DesignJet and PageWide XL printer series particularly well suited for deployment in environments where network, data, and access control security are important.

In this document, you will find:

- The description of the features, where to configure them and some recommended values (Section 2, Security concepts explanation).
- The tables summarizing the new and existing security features of the HP DesignJet and PageWide XL printer series and how they are configured using the control panel, Embedded Web Server and/or HP Web Jetadmin (WJA). Please make sure that your printer has the latest firmware version to benefit from all the security features (Section 3, Large Format printers: security features summary).
- The table summarizing the new and existing security features of the HP Scanners compatible with the HP DesignJet and PageWide XL printers (Section 4, Large Format scanners: security features summary).
- The list of ports used by the printer and the effect of keep them blocked (Section 5, Ports used in HP printers).

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

2. Security concepts explanation

2.1 Device security

2.1.1 UEFI secure boot

It prevents the loading of unauthorized operating systems (OS) during system startup. This feature is compliant with the UEFI specification. Non-configurable feature.

2.1.2 Firmware protection

All HP portfolio use signed firmware package, that means firmware packages are digitally signed by the HP Code Signing group.

The printer is able to check the authenticity of any firmware and install only those signed by HP.

It is really important to keep the printer updated with the latest firmware, that provides you the highest security and new features.

The firmware can be updated in various ways, although not all them are available in all the printers:

- Plugging a USB drive with the firmware file in the root folder.
- Sending the firmware file through EWS.
- Sending the firmware file through the port 9100, as any other job.
- Activating the Automatic Firmware Upgrade (AFU): This function connects the printer with the HP server, checks if there is a new firmware and downloads it. The installation should always be launched from EWS or printer control panel.

Despite the signature system, the recommendation is to protect the printer from unauthorized firmware upgrades:

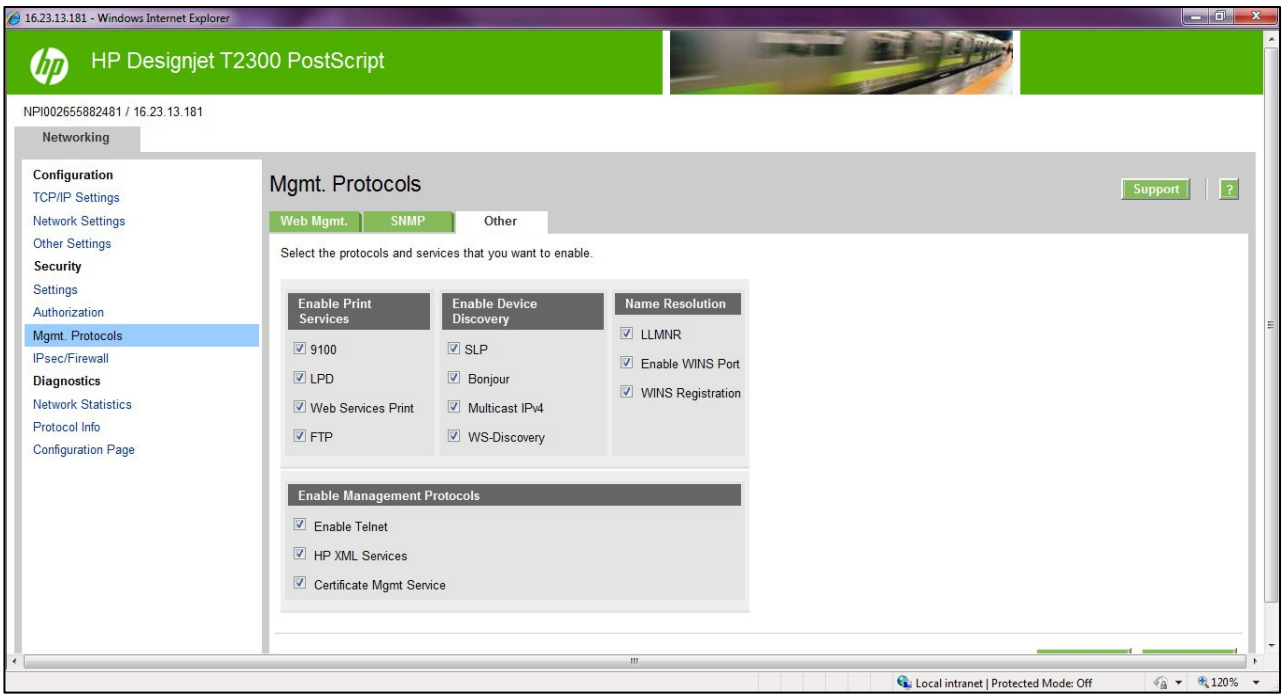
- Protect the EWS access with an admin account (see section 2.2.6, Embedded Web Server (EWS) access control).

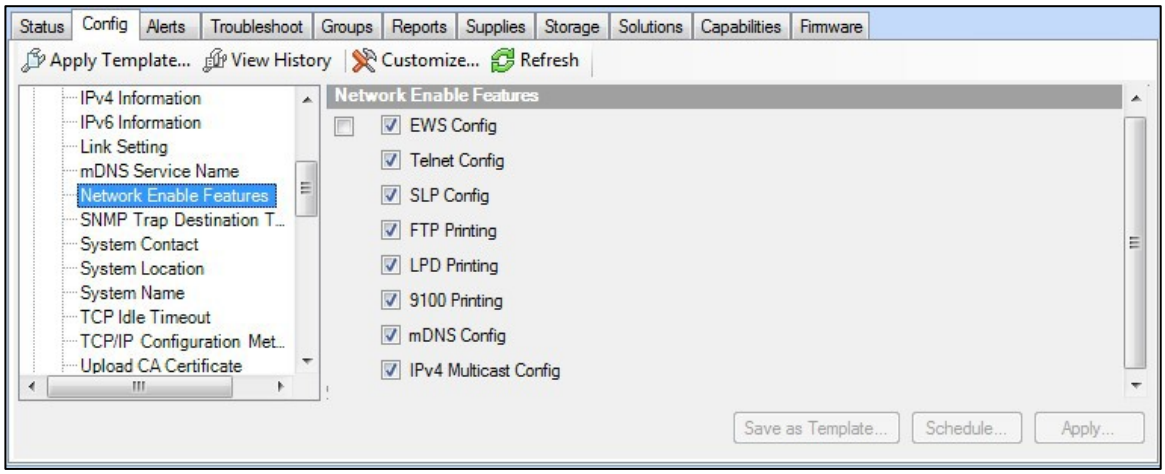
- Disable the firmware upgrade from USB (see section 2.2.7, USB drive control)
- Use the Automatic Firmware Upgrade to download the firmware.

2.2 Device configuration protection

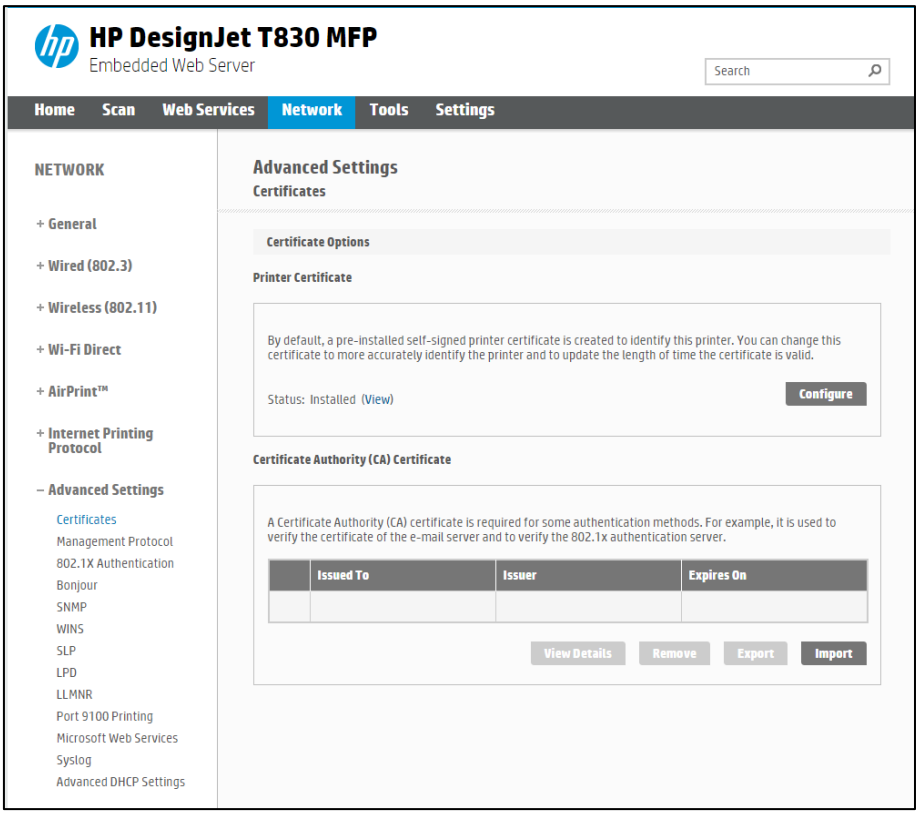
2.2.1 Disable protocols

In some cases, you might want to disable all protocols that you do not plan to use to access your printer. For example, you might prevent users from sending files via ftp or connecting through telnet to manage the printer network settings. You can disable unused protocols through the **Mgmt. Protocols** option in the Embedded Web Server, or the **Network Enable Features** in Web Jetadmin.





In the HP DesignJet T830 MFP/T730 printer, the network Management Protocols can be configured from the **Network > Advanced Settings** menu.



2.2.2 SNMP compatibility

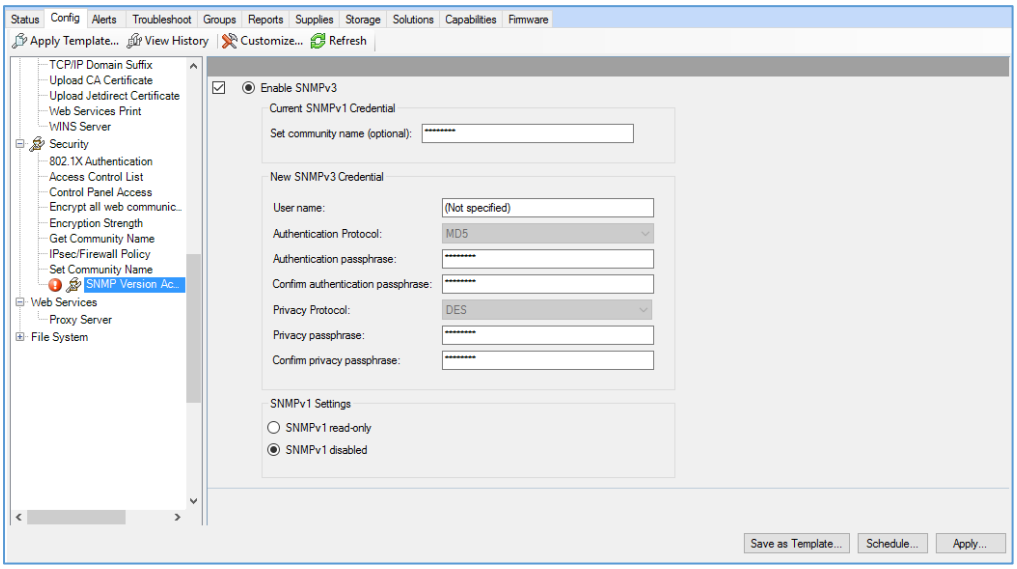
SNMP is a protocol to get printer information and to configure it. SNMPv3 is its encrypted version. Enabling it, only the client applications knowing the keys will be able to access the printer using this protocol.

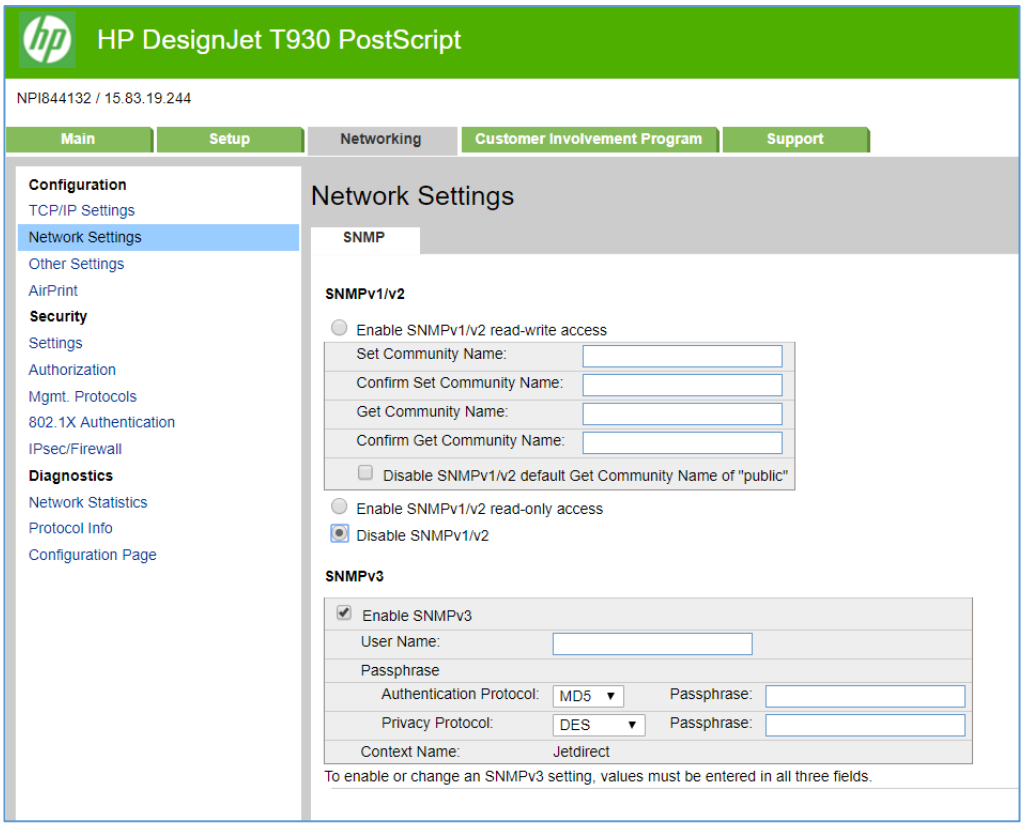
The main benefits of using SNMPv3 are:

- Integrity: protects data flowing from side-to-side from being modified by a third party.
- Authentication: verifies the data source.
- Encryption: protects data from being accessed by a third party.
- Access control: restricts the Managed Device data that can be accessed by each Network Management System.

You can enable and disable the SNMPv3 agent from your printer. You may set up an account that allows a management application to access the SNMPv3 agent.

The recommendation is to work with SNMPv3 and keep SNMPv1/v2 disabled, if your system allows it.





2.2.3 Disable connectivity interfaces

Depending on the printer series, there are some USB network interfaces that can be disabled to restrict access to the printer through these interfaces.

In some products, you can install a Jetdirect card to add extra security features, in this case, you might want to disable the onboard Ethernet.

The **HP Jetdirect 640n** is a print networking device that offers high-speed wired functionality, easy set-up, full manageability, backward compatibility and enterprise-class security features.

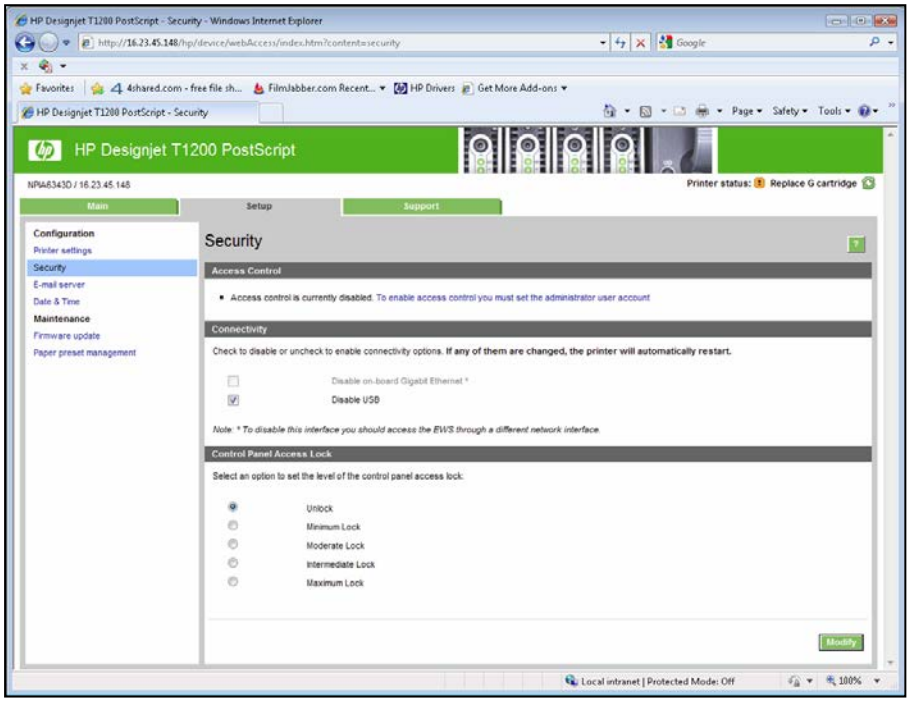
Ideal for enterprise and workgroup SMBs requiring full-featured, secure, and backward-compatible print management of printers and MFPs over shared, wired networks.

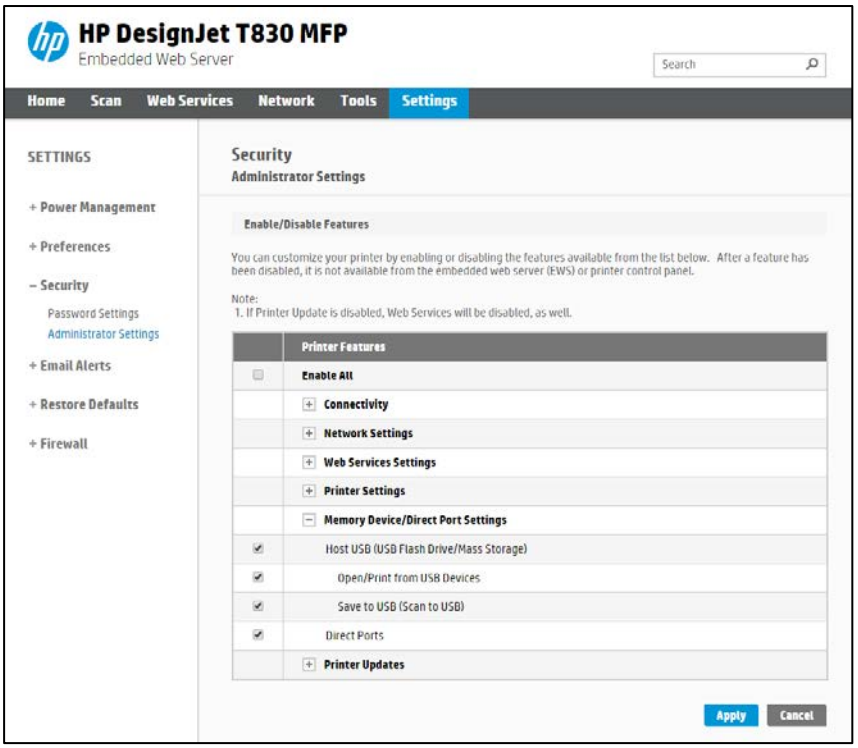
Features: Print at high speed over gigabit networks

- Quickly connect to shared printers and MFPs throughout your office, over a gigabit network.
- Maintain rigorous standards through IPv6 network features: more IP addresses than IPv4 and IPsec security.
- Help reduce administration and operation costs with off-the-shelf functionality and backward compatibility.

See http://www8.hp.com/emea_africa/en/products/print-servers/product-detail.html?oid=5305778 for more information about the Jetdirect card.

If you enable or disable a connectivity option, 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, you cannot disable the connection that you use to access the Embedded Web server.





2.2.4 Control Panel Access

The DesignJet and PageWide technologies allow the printer administrator to locks some features in the control panel of the device. Currently, there are two modes of control access "**Control Panel Access Lock**" and "**Access Control**", depending on the model. To use these features, it is compulsory to define an administrator account and password.

In some printers, when setting an Embedded Web Server admin password, you also restrict access to certain front panel features by default. The protected features on the front panel are:

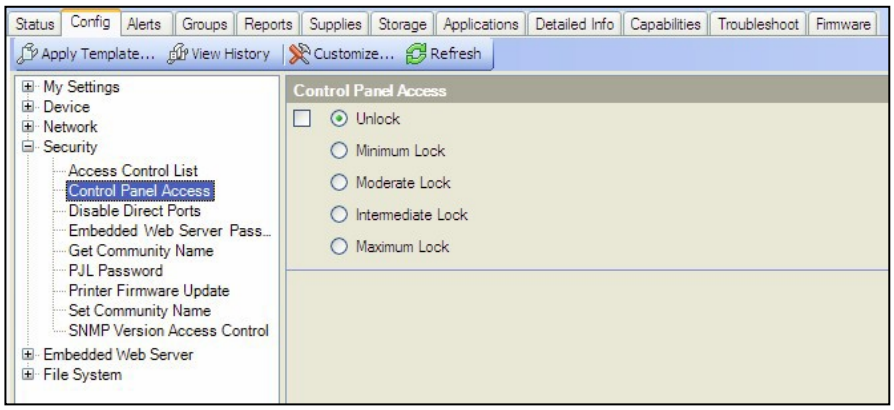
- Network connectivity & Internet connectivity
- Control firmware upgrades
- Reset factory defaults
- External hard disk connection
- Security

2.2.4.1 Control Panel Access lock

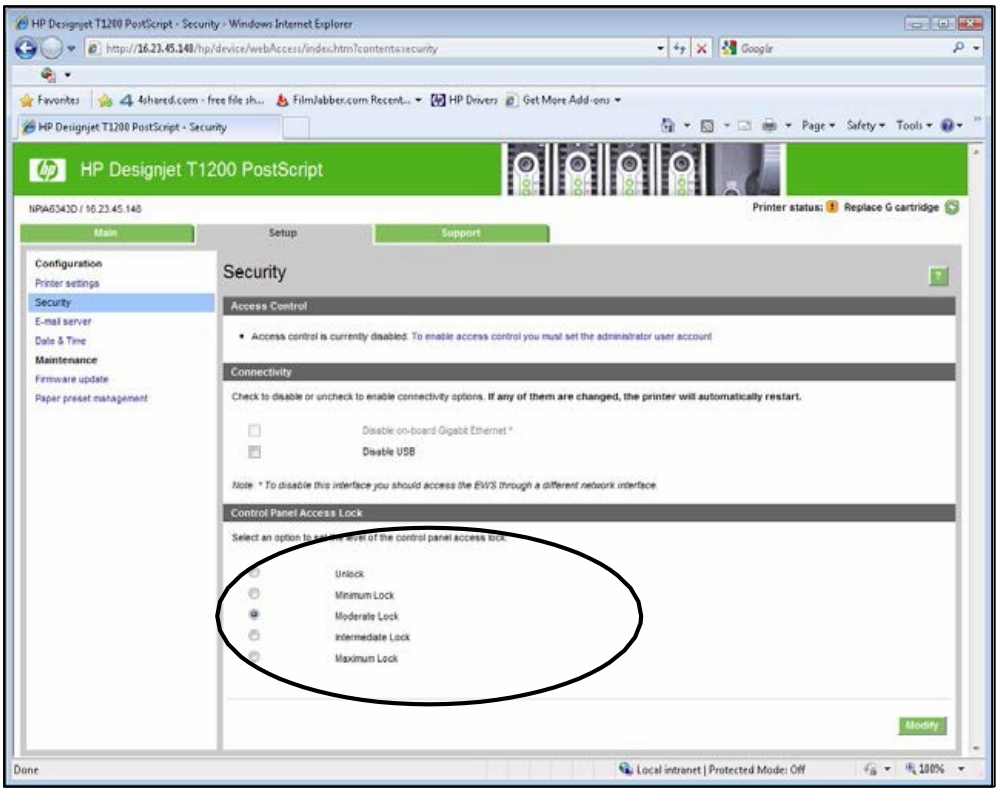
The control panel access lock is a feature intended for IT administrators, which enables them to lock the device's control panel by using either the HP Web Jetadmin or the printer's Embedded Web Server (depending on the printer model). This feature prevents unauthorized users from accessing some features on the control panel. 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 also be enabled from the T1200 Embedded Web Server as shown below:



The following table shows the features enabled or disabled for each lock level:

Lock level	Functionality locked when the Lock level is set
0 – Unlock	
1 – Minimum Lock	Resets, CIP config, Security, Service Menu 1
2 – Moderate Lock	Resets, CIP config, Security config Connectivity, AFU, IDS workflows, System info, Job Queue
3 – Intermediate Lock	Resets, CIP config, Security Connectivity config, AFU, IDS workflows, System info, Job Queue Media mgmt. workflows, Pause printer, Maintenance & IQ workflows
4 – Maximum Lock	Resets, CIP config, Security Connectivity config, AFU, IDS workflows, System info, Job Queue Media mgmt. workflows, Pause printer, Maintenance & IQ workflows Any settings, Connectivity info, IDS info, Paper Info, Cancel jobs, Calibration info

Grouped by categories:

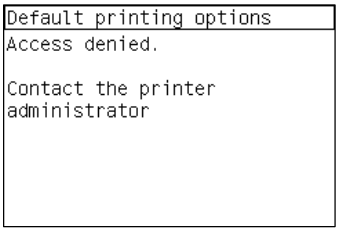
Actions	Permission denied if FP lock level is at least:
Settings App Access	4 - Maximum
Connectivity App Access	4 - Maximum
Connectivity App Details Access	2 - Moderate
Settings App Internet connectivity	2 - Moderate
Settings App Connectivity Troubleshooting	2 - Moderate
IDS App Access	4 - Maximum
IDS App Actions i.e. replacement, alignment, etc.	2 - Moderate
IDS Widget – Access to IDS App	4 - Maximum
IDS Widget – Cartridge Replacement	3 - Intermediate

Settings App Inks Entry Access	3 - Intermediate
Paper App Access	4 - Maximum
Paper App Load Media	3 - Intermediate
Paper App Unload Media	3 - Intermediate
Paper App Change Paper Type	3 - Intermediate
Paper Widget – Access to Paper App	4 - Maximum
Settings App Paper Entry Access	4 - Maximum
Printer Information App Access	4 - Maximum
Printer Information App AFU Access	2 - Moderate
Job Queue App Access	2 - Moderate
Pause printing	3 - Intermediate
Cancel printing	4 - Maximum
Settings App Calibration Info Entry Access	4 - Maximum
Settings App IQ maintenance Entry Access: Test plots, Align PH, IQ	3 - Intermediate
Settings App Maintenance Entry Access	3 - Intermediate
Settings App System Entry Access	2 - Moderate
Settings App CIP Entry Access	1 - Minimum
Settings App Restore Factory Settings	1 - Minimum
Settings App FW Update	2 - Moderate
Settings App Printer Logs	3 - Intermediate
Settings App Allow SNMP	1 - Minimum
Settings App Service Level 1	1 - Minimum – PIN needs to be provided

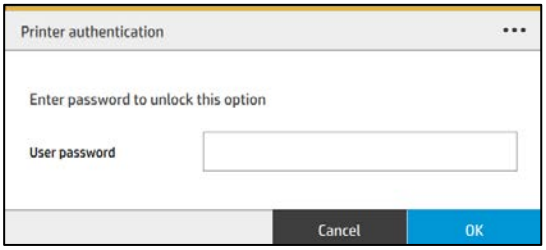
Note: When the **Intermediate** or **Maximum** locks are set, you will not able to load/unload paper or replace printheads/ink cartridges without first unlocking the front panel. These options should only be set in specific circumstances where the implications are known and understood.

Note:*:*None of these levels locks the copy, scan, or print applications.

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



Note: In PageWide XL, when the user attempts to access a "locked" menu, the printer asks for the User password that is not available when the Control Panel Access Lock is used. To insert the Admin password, click on the top left corner.



2.2.4.2 Access Control

The Access Control page is placed in the **Setup** tab, in the subsection called **Access Control**.

This function allows you to manage at least three roles of use (depending on the firmware version), defining which applications are available for each of them.

The Control Panel Access Lock (**Setup > Security**) should be set to unlocked (see 3.5.1. Control Panel Access Lock).

How to configure Access Control

The **Access Control** page has three main sections for the three main actions that can be performed:

- **Sign-in methods**: this section shows the enabled sign-in methods that can be used to sign in to the device.
- **Device user accounts**: in this section you can create, edit or delete the user accounts that are available on the printer.
- **Sign-in and permission policies**: here you can set up the sign-in requirements for specific tasks and restrict user access by role.

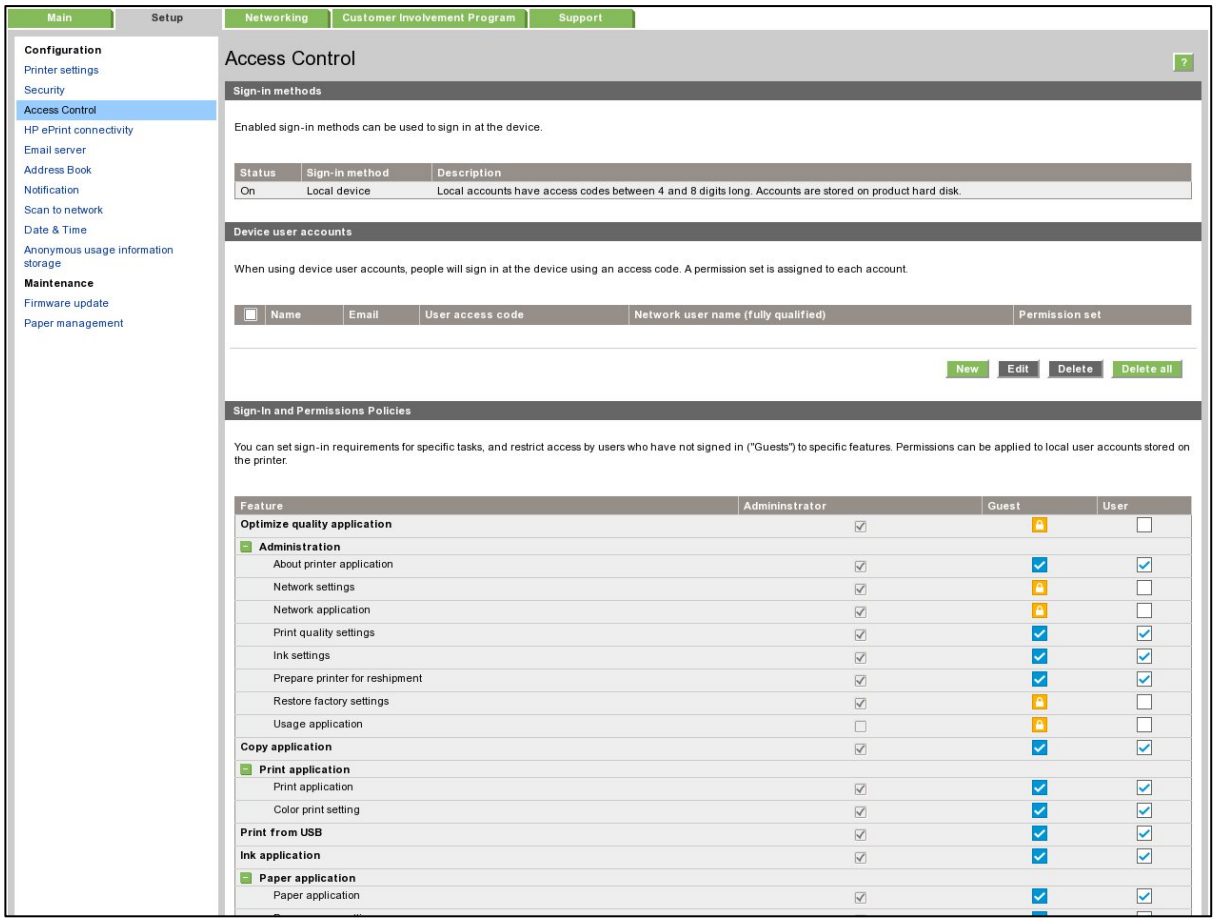


Figure 1 - Access Control page

a. Sign-in methods

This section shows the enabled sign-in methods that can be used to sign in on the device.

Currently, the only available sign-in method is **Local device**, local accounts that have access codes between 4 and 8 digits long and are stored on the product's hard disk.

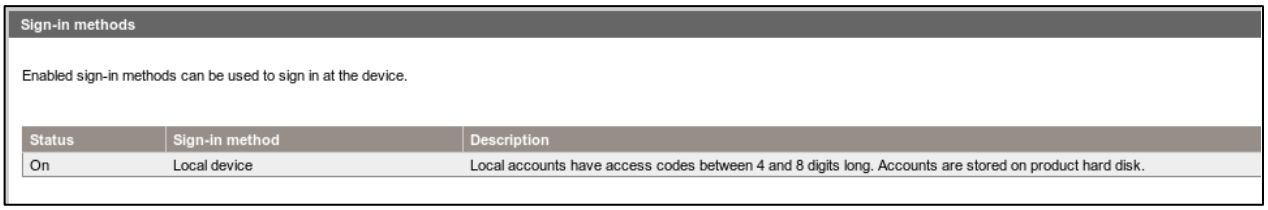


Figure 2 - Sign-in methods

b. Device user accounts

In this section, there are four actions available:

- **New**: to add a new user account.
- **Edit**: to edit the selected user account.
- **Delete**: to delete the selected user account.
- **Delete all**: to delete all the user accounts.

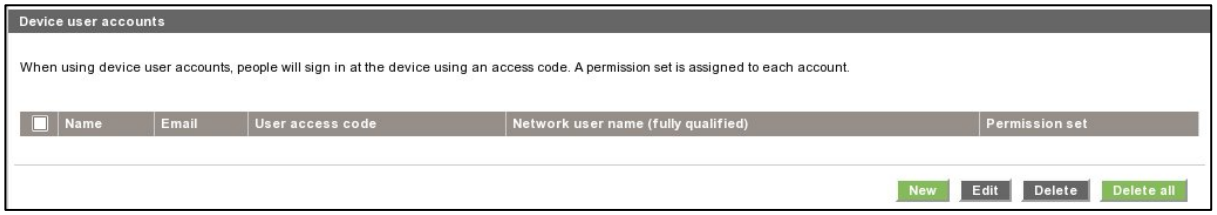


Figure 3 - Empty user accounts list

To add a new user:

- Click the **New** button; a section is expanded. It is required to fill in the **name** and **password** fields.
- It is possible to change the **User access code** and the **Permission** that is set. You can select from the following permission roles.

Admin user	This role has all the access privileges granted to it and cannot be edited.
Device user	This role has some access privileges granted to it that can be edited in the **Access Control** page.
Guest user	This role has some access privileges granted to it that can be edited in the **Access Control** page.

Figure 4 - Creating a user account

After adding the user, you will see the following screen.

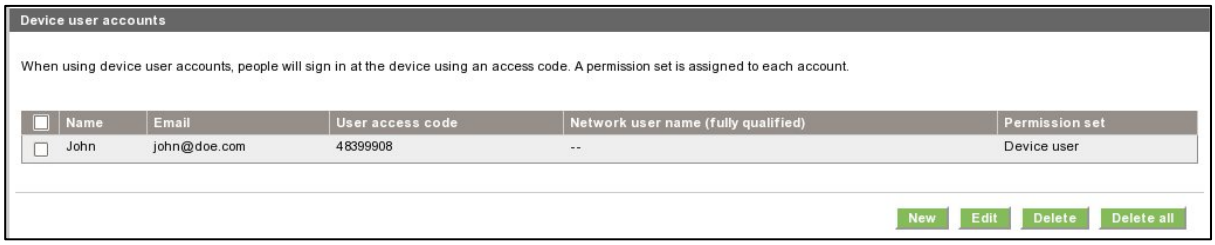


Figure 5 - User accounts list

c. Sign-in and permissions policies

You can change the permissions for the roles **guest** and **user**. Select the permissions and click **Apply**.

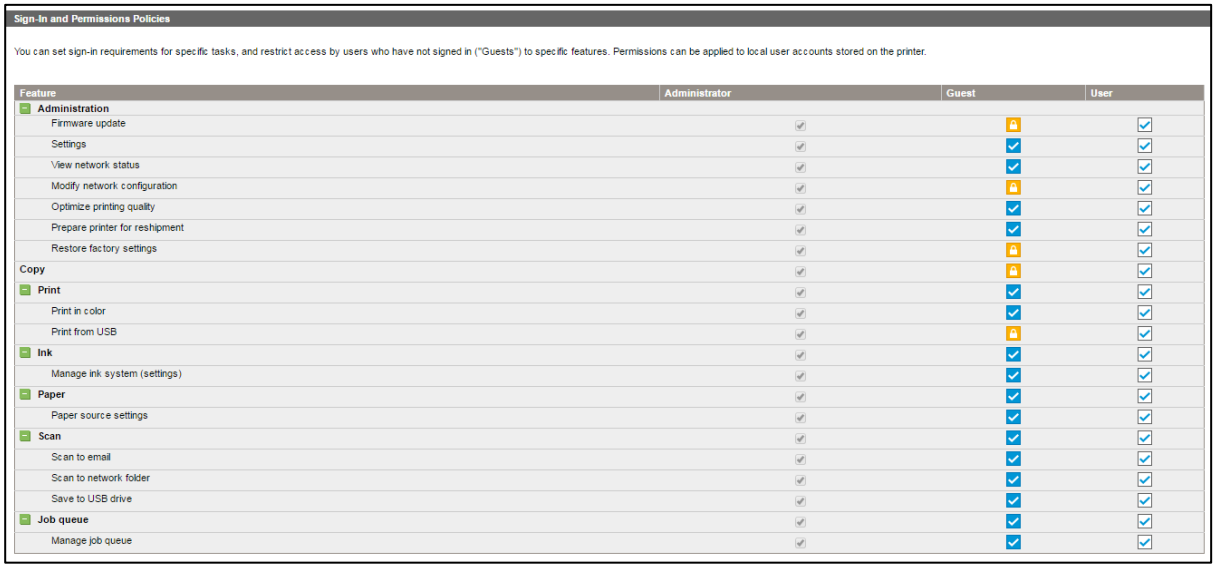


Figure 6 - Defining permissions

Note: Users have at least the **Guest** permission.

Note: Any app that forces the user to log in will cause the **Guest** column to be disabled.

Front Panel log in

When the user clicks on any blocked function for the first time, a window appears. The user must enter in his/her password. Session expiration can be managed in **Settings**.

To log in as *Admin*, click the menu in the corner.

2.2.4.3 Deadlock: Front Panel locked + EWS password forgotten

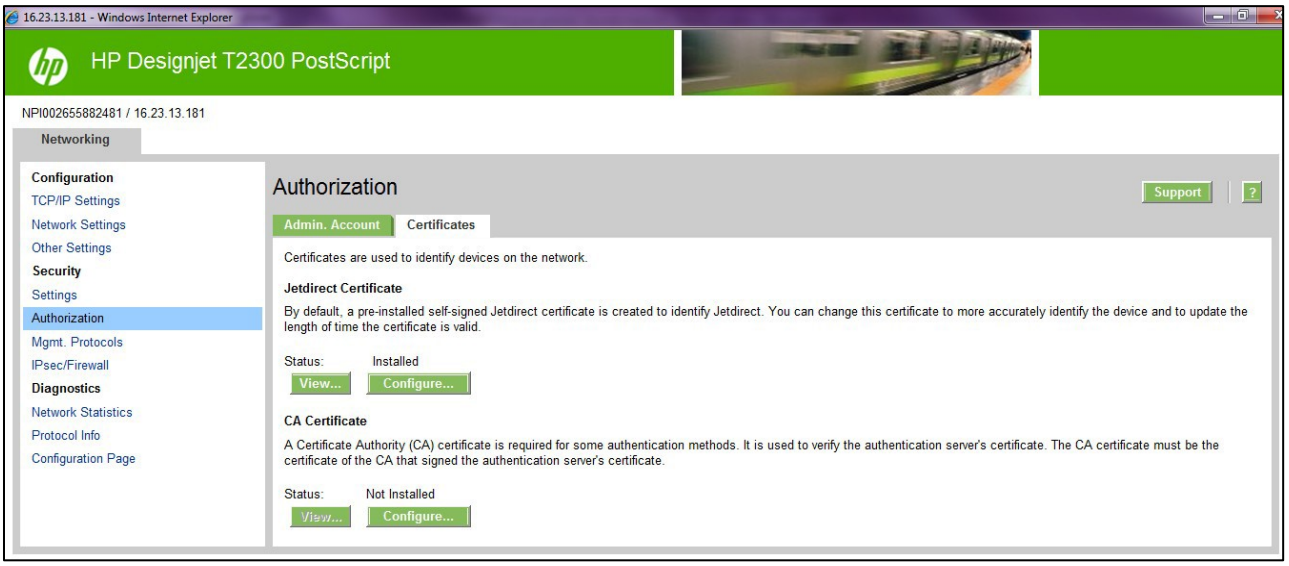
Under certain circumstances, a printer might become inaccessible if the control panel has been locked and the administrator has lost the password needed to unlock it. This could happen if the front panel is locked through the printer's Embedded Web Server and the Administrative password for the EWS is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

Note: If the printer's front panel becomes locked and you are unable to unlock it, then you should contact HP support as soon as possible.

2.2.5 SCL certificates

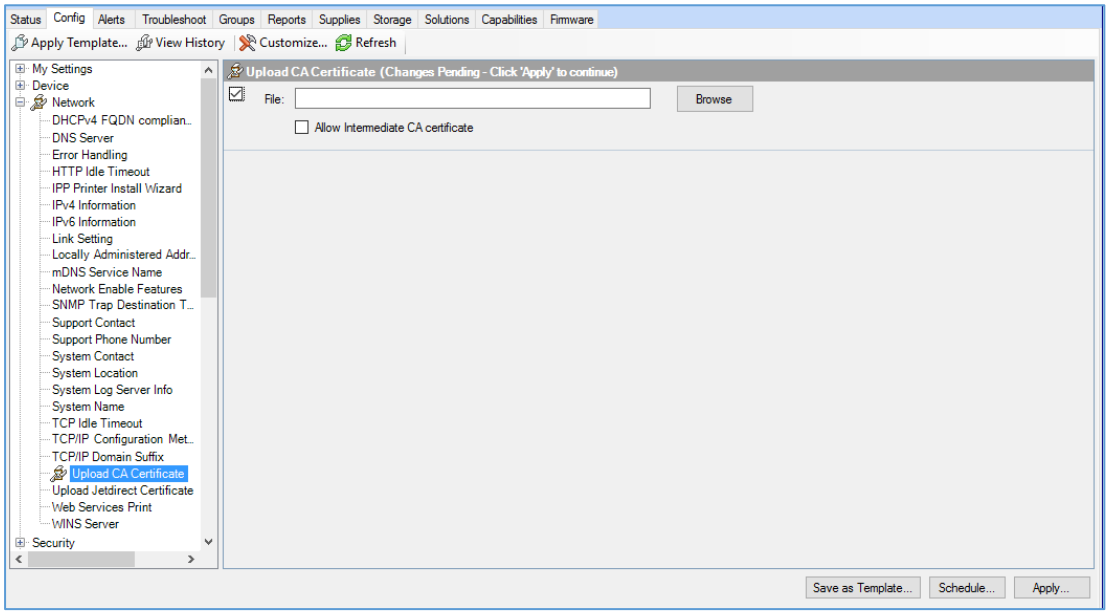
- Jetdirect identity certificate

  You can 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, pre-installed certificate.



- Certificate Authority certificate

  You can install and manage a CA certificates in the printer. The CA certificate is used to validate the identity of the network servers you may connect to, such as SSL or LDAP servers secured with SSL.



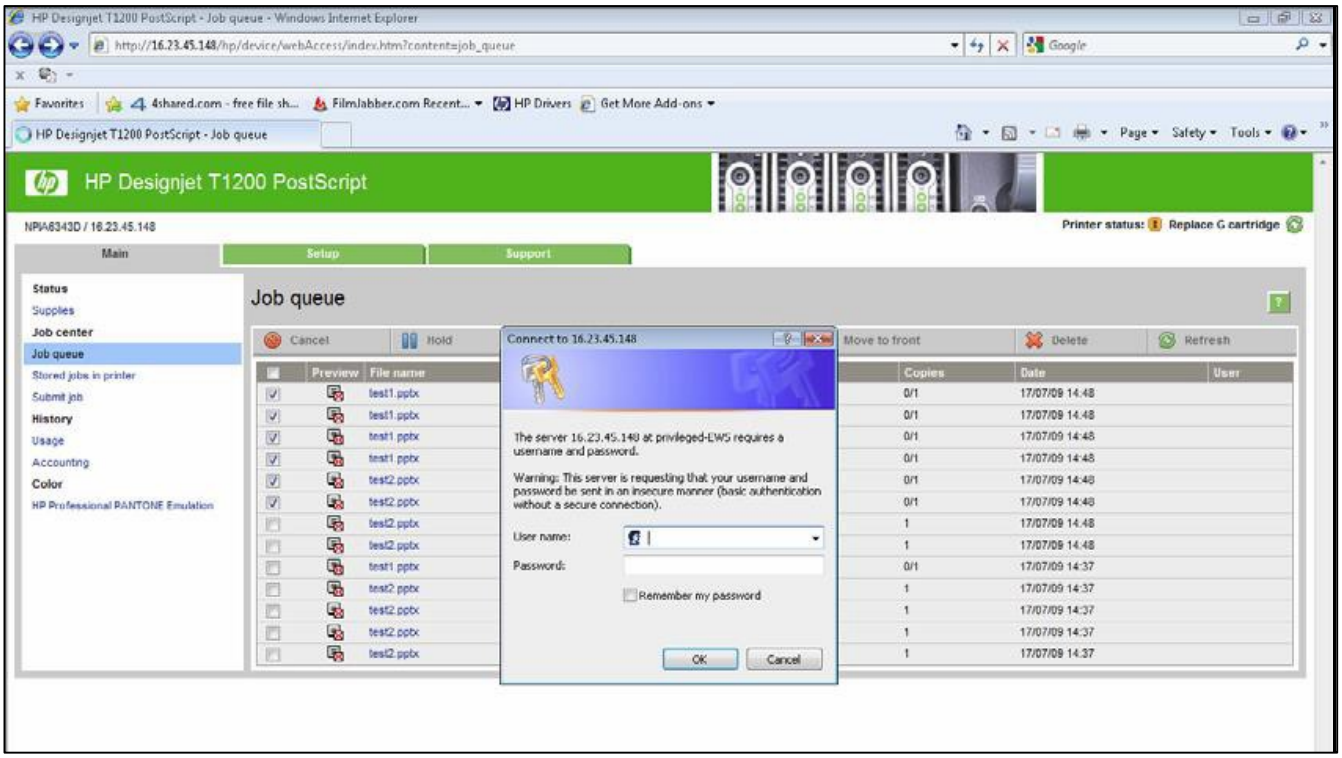
2.2.6 Embedded Web Server (EWS) access control

The Embedded Web Server is a powerful tool which enables direct management of devices such as the HP LaserJet or the HP DesignJet printers. With no security in place, however, 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 knowing the IP address of the printer. To solve this situation, we have implemented two levels of access to our compatible HP DesignJet printers.

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 (Guest account not available in HP PageWide).

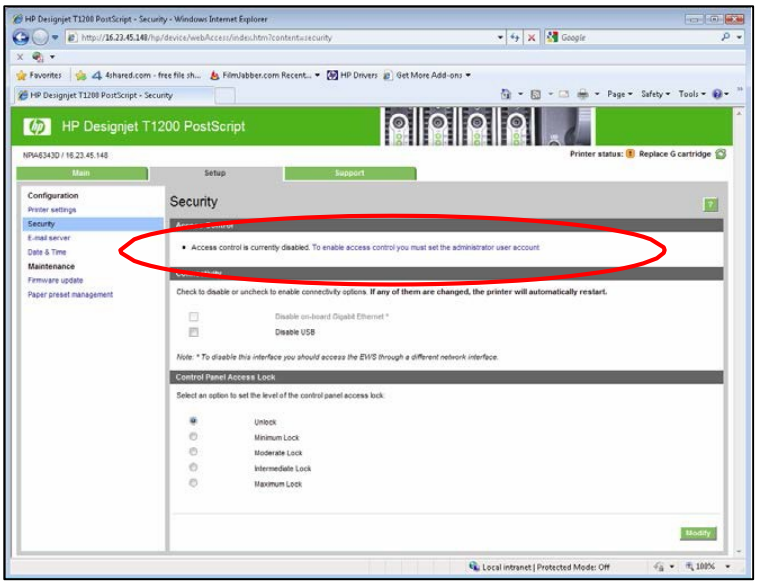
If the two levels of access have been set, and you have neither of the passwords, then you will not be able to gain access to the EWS information, as in the image below.

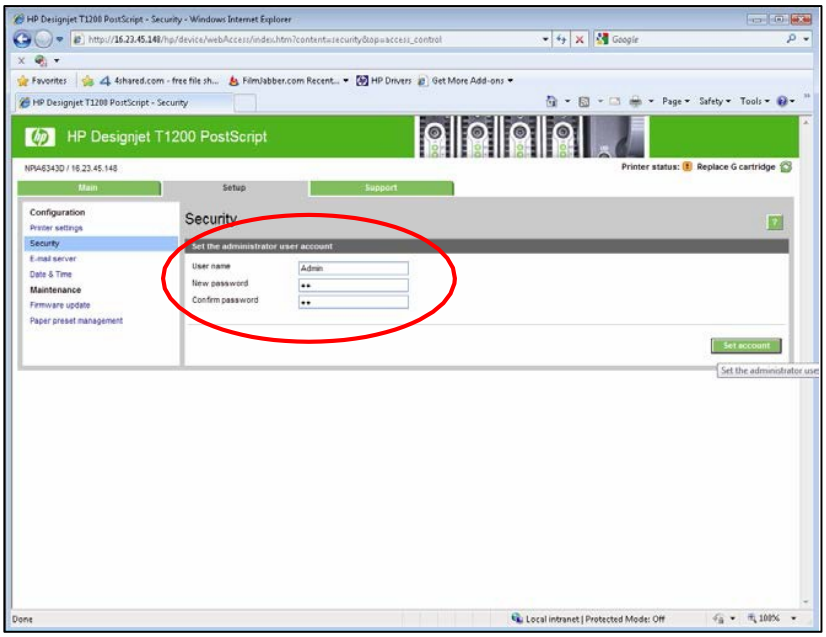


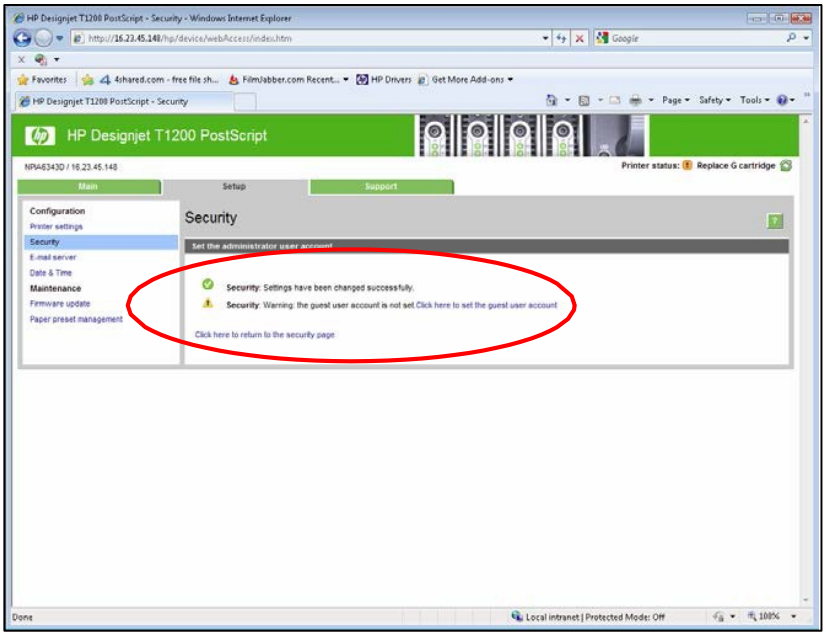
2.2.6.1 Administrator password

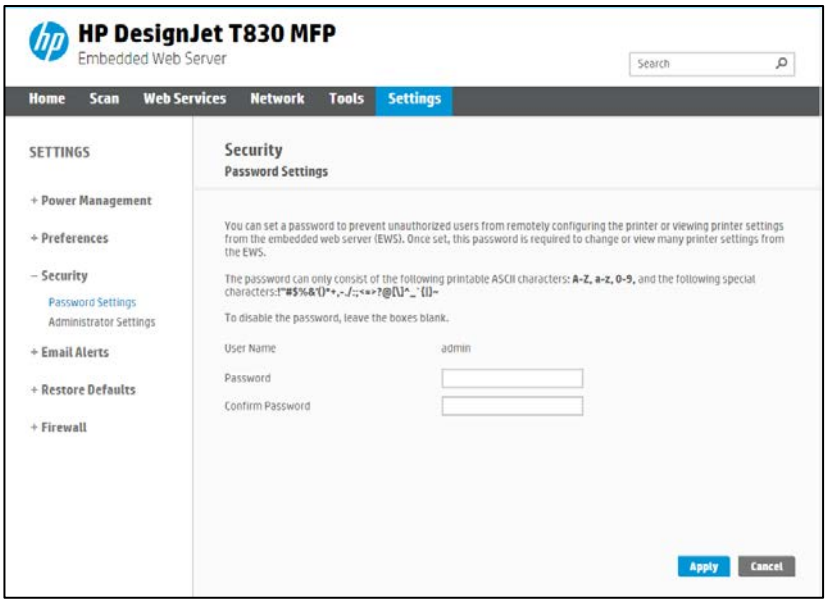
Access control is enabled by setting the **Admin account password**, i.e. specifying a password for the user account at admin level. You must then provide the admin password to perform any of the following **restricted operations**:

- Cancel, delete or preview a job in the job queue.
- Delete a stored job.
- Clear accounting information and configure cost assignment, in some models.
- Change printer settings on the **Device Setup** page.
- Access the **setup** tab to configure the printer.
- View protected printer information pages.
- Access the **Customer Involvement Program** page.
- Access the Service Support.




HP Designjet T1200 PostScript
Security
Set the administrator user account
User name
New password
Confirm password
Set account


HP Designjet T1200 PostScript
Security
Set the administrator user account
Security: Settings have been changed successfully.
Security: Warning: the guest user account is not set.Click here to set the guest user account
Click here to return to the security page


HP DesignJet T830 MFP
Embedded Web Server
Search
Home
Scan
Web Services
Network
Tools
Settings
SETTINGS
+ Power Management
+ Preferences
– Security
Password Settings
Administrator Settings
+ Email Alerts
+ Restore Defaults
+ Firewall
Security
Password Settings
You can set a password to prevent unauthorized users from remotely configuring the printer or viewing printer settings from the embedded web server (EWS). Once set, this password is required to change or view many printer settings from the EWS.
The password can only consist of the following printable ASCII characters: A-Z, a-z, 0-9, and the following special characters:!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
To disable the password, leave the boxes blank.
User Name
admin
Password
Confirm Password
Apply
Cancel

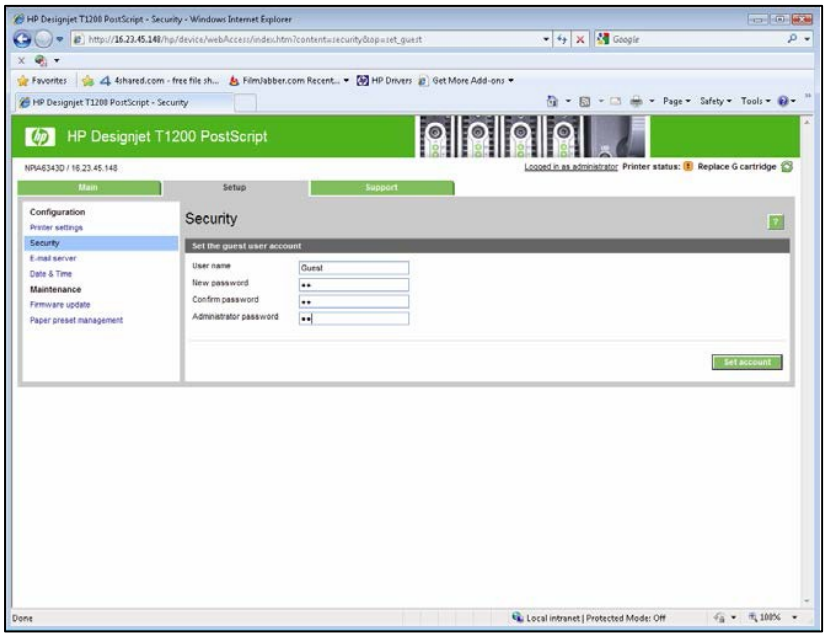
If there is no administrator account, then the restricted operations can be accessed without a password.

2.2.6.2 Guest password

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

If the guest user account is set up, a username and password are required for **all** EWS operations: users identified as guests have access to restricted operations, whilst users identified as administrators have access to all operations.

If the guest account is not set up, 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 asks for another admin account and password. This password is synchronized with the admin password for the complete EWS.
- For most printers that have EWS password capability, it is also possible to setup the **admin** password through Web Jetadmin. Only one level can be set in this way, however, so the **guest** password cannot be set up from Web Jetadmin.
- Passwords have no minimum complexity requirements, the maximum length is 16 characters.
- Printers with touchscreen front panels only allow the use of the limited set of characters shown below (capital letters are also supported).

```
q w e r t y u i o p
a s d f g h j k l _
z x c v b n m @ .

1 2 3 4 5 6 7 8 9 0
, - # ; : " + = * '
! ? < > \ / ( ) @ .

¡ ¿ € £ $ % & ~ [ ]
ñ à á â è é â ê ì í î
ò ó ô ù ú û Ç @ .
```

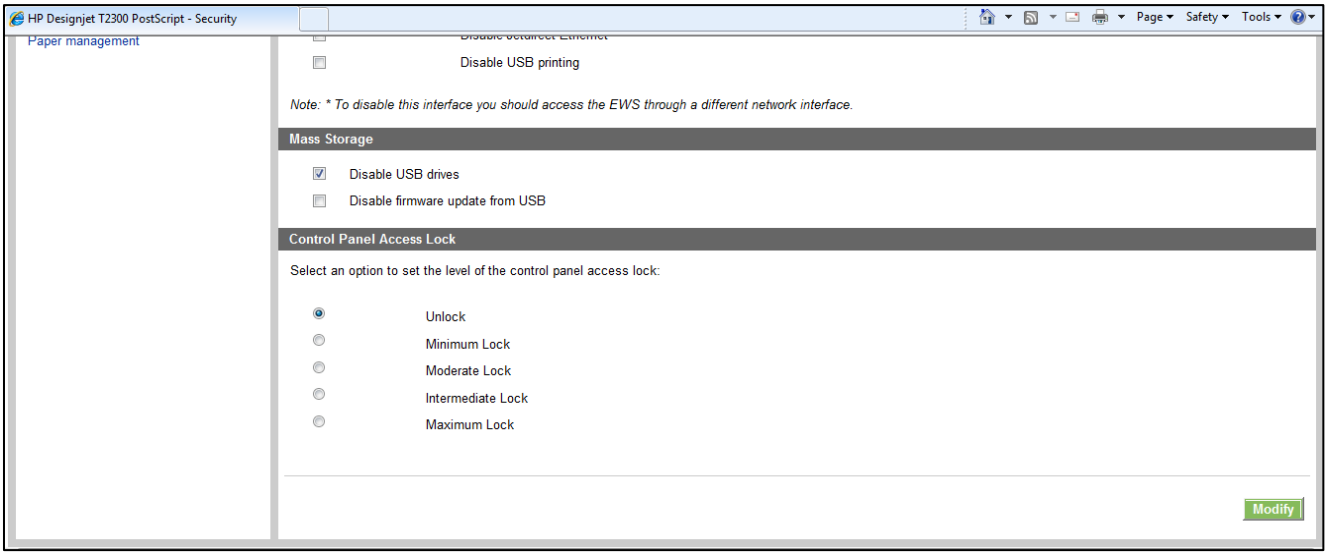
- These limitations do not apply to printers without touchscreen front panels, as the password can be set using EWS.
- Some printer drivers rely on the EWS for creating the preview. In cases where an administrator password is set, the administrator password will be required to access job preview.

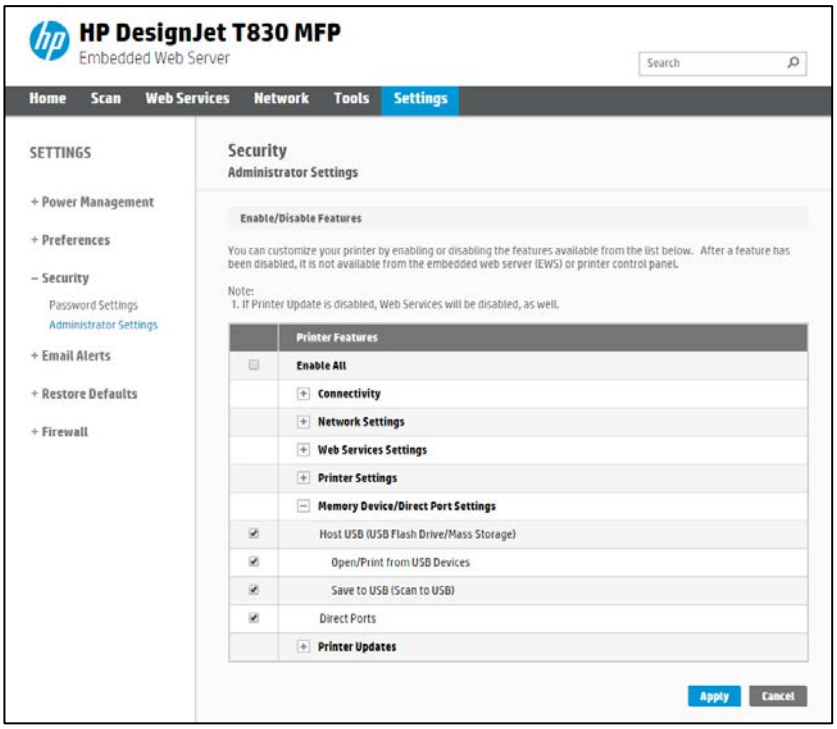
2.2.7 USB drive control

All printers allow you to control the USB use, in two ways:

- USB drive: enable or disable the use of the USB to print or scan.
- Firmware upgrade from USB: enable or disable the possibility of upgrading the firmware from a USB.

These features are available in the control panel, the Embedded Web Server and Web Jetadmin.

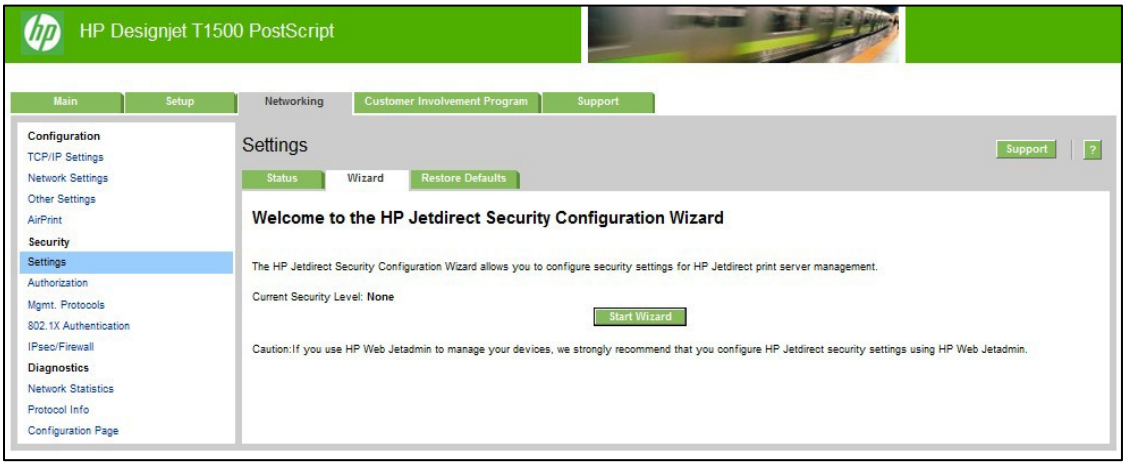




2.2.8 Jetdirect Security Wizard (HP T9x0-T15x0-T25x0-T3500-PageWide XL)

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

Basic	Configure an admin password that is shared on other tools such as Telnet and SNMPv1/v2.
Enhanced	Disable unsecure management protocols (FTP, Telnet, RCFG, SNMP v1/v2c). Enable SNMPv3. Enable SNMPv1/v2 read only access.
Custom	Manually adjust all the settings.



2.2.9 Hide IP from front panel

Some printers include an option in the Service Menu, accessible with the help of an HP Support agent only, that enables you to hide all IP information from the printer's front panel. This prevents that people physically around the printer could obtain the IP and connect to it.

2.3 Data security: encrypted communications

2.3.1 IPSec

A Firewall or IP Security (IPsec) policy enables you to control traffic to or from the device by 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.

Please note: Before you enable a firewall or IPsec policy, you should make sure that access to your configuration management settings is secured (for example, through an administrator password). This will ensure that your policy is not easily disabled through Telnet, control panel menus, or other management tools.

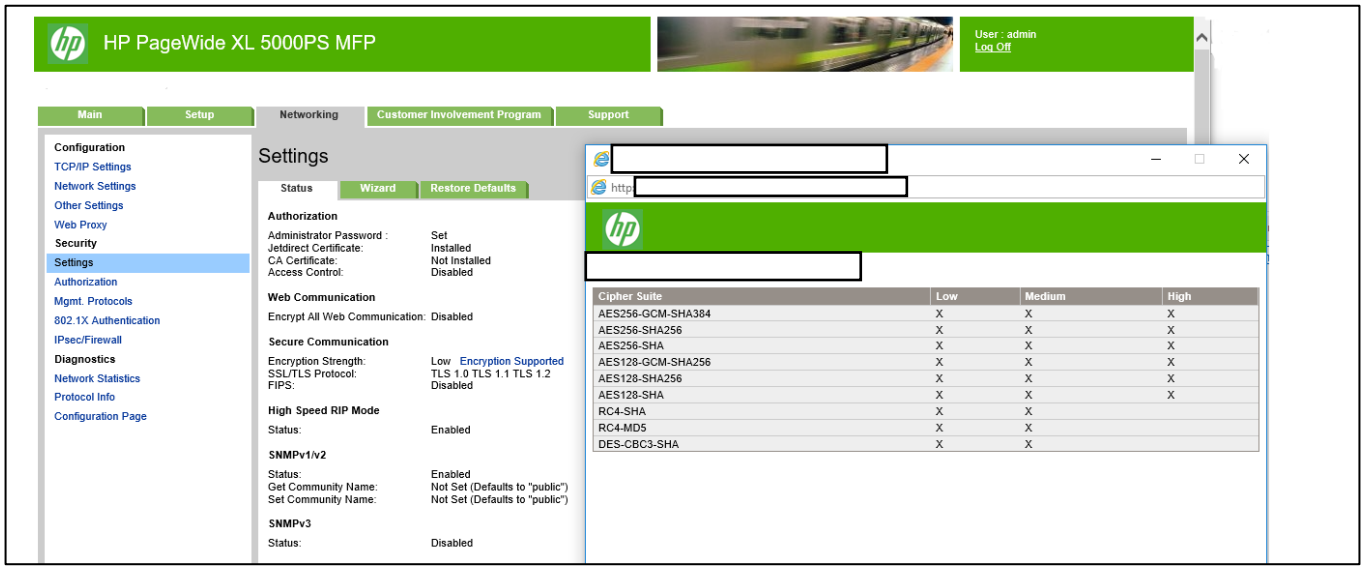
Firewall. Use this page to view or configure a firewall policy. A firewall policy consists of up to 10 rules, where each rule specifies the IP addresses and services that are allowed by the print server and device. To add a rule, click **Add Rule**. This setting runs a wizard that will help you to configure each rule.

IPsec/Firewall. Use this page to view or configure an IPsec/firewall policy. An IPsec/firewall policy consists of up to 10 rules. As with a firewall policy, each rule specifies the IP addresses and services that are allowed by the print server and device. With IPsec support, you can apply IPsec authentication and encryption protocols for those addresses and services. To add a rule, click **Add Rule**. This runs a wizard that will help you to configure each rule.

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

2.3.2 Encrypt web communications

You can securely manage your network-connected printers using a web browser and the HTTPS protocol. To authenticate the HP Jetdirect web server when HTTPS is used, you may configure a certificate, or you may 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 can be checked at EWS.



When you enable encryption, the web server encrypts all web communication, forcing all connections to use HTTPS. You can also configure encryption options to allow both HTTP (unencrypted) and HTTPS connections. In secure environments, you should choose to encrypt all web communications. Otherwise, sensitive management data (administrator password, SNMP community names, and secret keys) may be compromised.

2.3.3 Access control list

This feature lets you determine the access control list (ACL), which is used to specify the IP addresses on your 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! You may lose your ability to communicate with the device if your system is not properly specified in the list, or access through HTTP is disabled. If communication with the device is lost, then it may be necessary to restore the network settings to their factory-default values.

2.3.4 802.1X authentication

802.1X is an IEEE Standard for port-based Network Access Control. It provides an authentication mechanism for 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, then 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 your network, you can use an isolated LAN, or a direct computer connection via a cross-over cable.

The supported 802.1X authentication protocols and associated configuration depend on the print server model and firmware version.

2.4 Authentication

2.5 Protected data in storage

2.5.1 Self-encrypted hard disk

The Self Encrypted hard disk ensures data is automatically encrypted every time data is sent to the printer and is written to the drive. This is achieved using AES 256-bit encryption.

2.5.2 Secure File Erase (SFE)

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

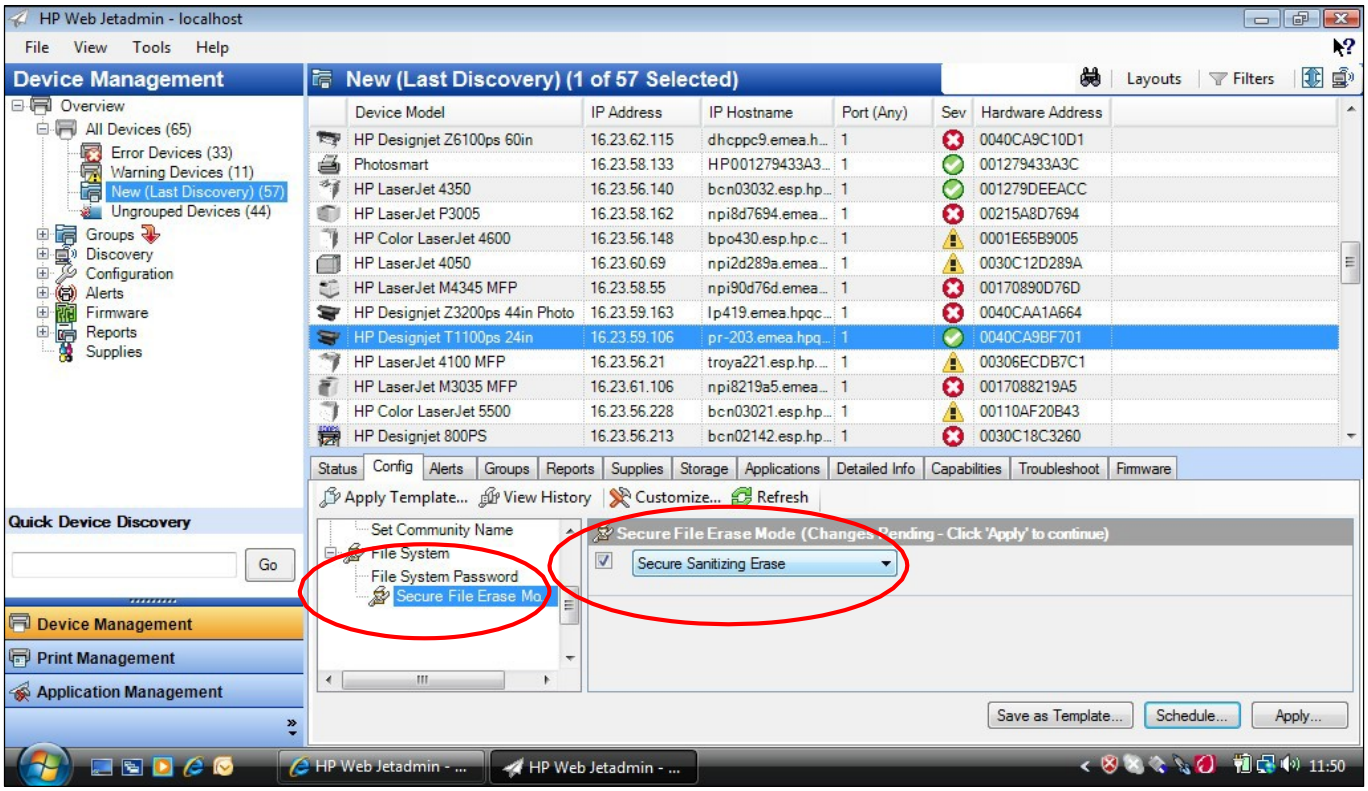
There are three security modes in the Secure Files Erase feature. These settings can be changed via Web Jetadmin, EWS and control panel (via the Service Menu with the HP support representative help).

- Non-Secure Fast Erase: In this mode, 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: In this mode of operation, 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: In this mode of operation, file pointers are erased and the disk space where the temporary job was stored is repeatedly 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 been completed (scan, copy, or print).

Furthermore, if you do not want to store jobs in the printer, you can set the number of jobs to be stored in the printer's queue to 0. To configure this setting, perform the following steps:

- 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 may differ for a specific printer. The following is an example of how to change the **Secure File Erase** setting for the HP DesignJet T1100 printer.

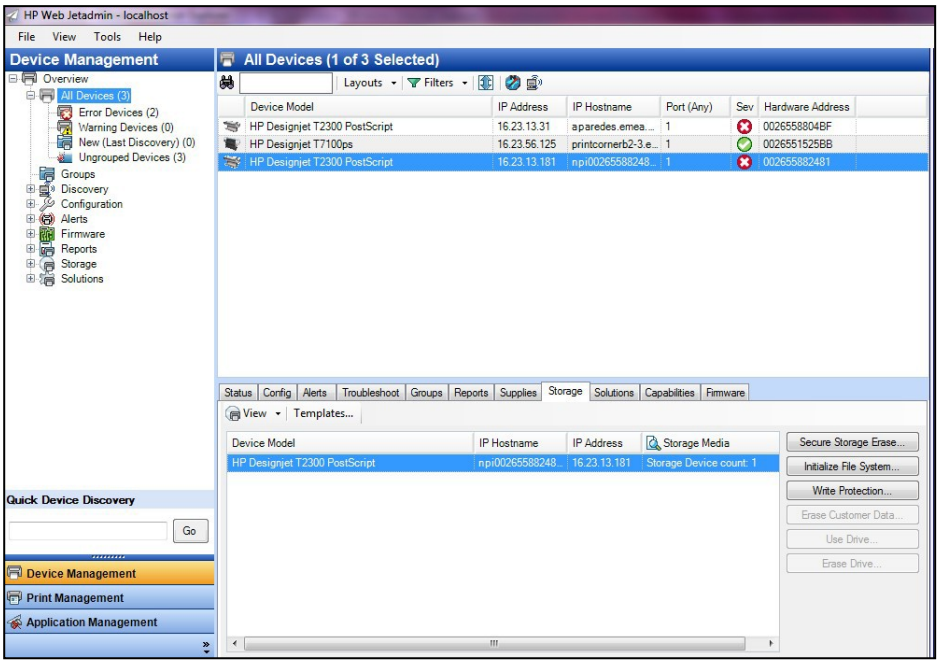


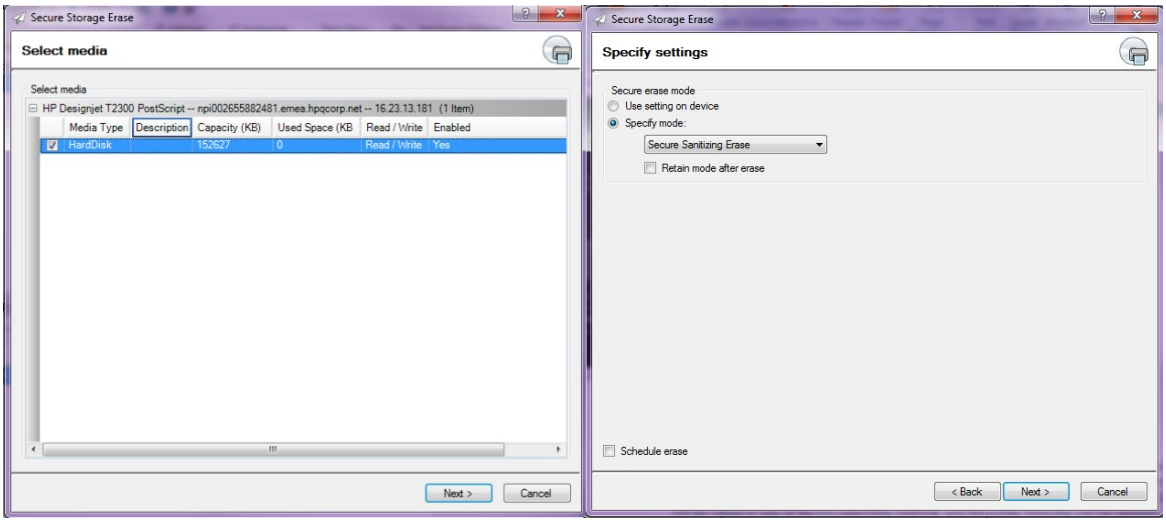
2.5.3 Secure Disk Erase (SDE)

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 that the device can safely be moved from a secure location to an unsecure location. All disk erasing will be carried out via the same level of security erase.

This setting can be used via Web Jetadmin, EWS or the Control Panel's **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, which enables you to set the same global options across your fleet of HP LaserJets 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**.

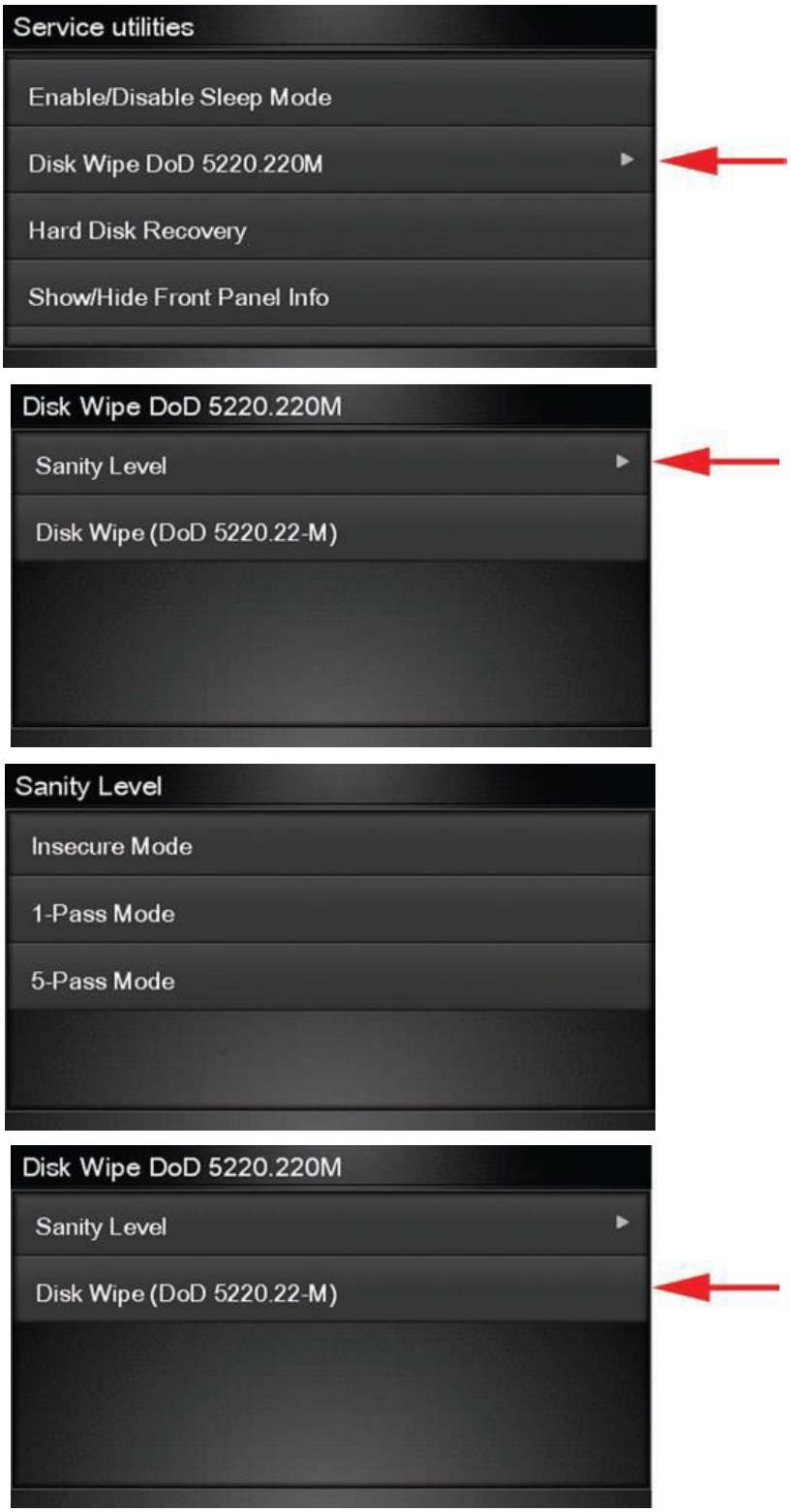




- **Printer Front Panel access:** Once you have entered the **Service Menu** with the help of an HP Support representative, you can perform the **Secure Disk Erase** using the same 3 options that you have in Web Jetadmin. Note that the name of the feature in the front panel is **Disk Wipe DoD 5220.220M**,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

Before you start the erase operation, you must first select the security level (sometimes referred to as sanity level). The printer will then warn you that the erase operation is a process which deletes all data and takes a long time. Once you accept, the printer will begin the process, and will display a progress bar until complete. All data will be wiped using the selected method, and the printer's firmware will be restored to the latest version installed before this operation.

The following screens show how to perform a secure hard disk erase on the HP DesignJet T2300 printer.



2.5.4 Scan to network (HP DesignJet T2500, T2530, T3500 eMFP Series) SMB1

A scanned image may be saved on a USB flash drive or in a network folder. The USB flash drive option requires no preparation, but the network folder option will not work until it has been set up in the following way.

1. Create a folder on a computer that the scanner can access through the network.
2. Create a user account on the same computer for the printer (scanner user).
3. Change the sharing options of the folder, so that it is shared with the *scanner user*, and assign full control of the folder to that user.

4. Create a share name for the folder.

   Note: It is important to complete the above steps before starting the remaining steps below.

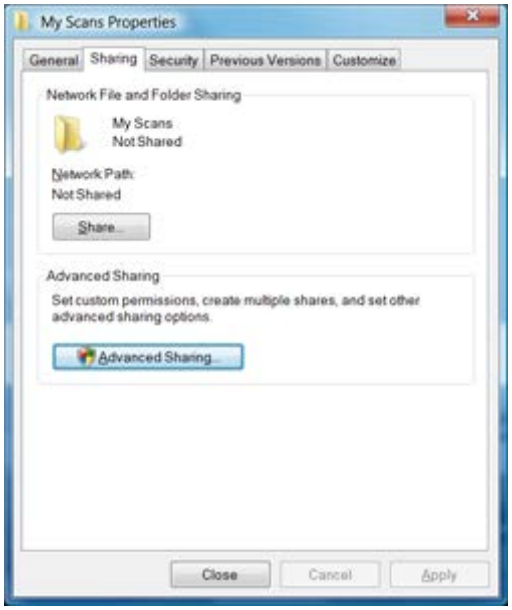
5. In the printer's Embedded Web Server, select the **Setup** tab and then **Scan to network**.
6. On the **Scan to network** page, click **Add folder details**, and fill in the various fields.
   - The **Server name** should contain the network name of the remote computer. This remote computer must be connected in the local network to the printer.
   - The **Folder name** should contain the share name of the folder.
   - The **User name** should contain the name of the *scanner user*.
   - The **User password** should contain the password of the *scanner user*.
   - The **Domain name** should contain the name of the domain in which the user name exists. If the *scanner user* does not belong to any domain, leave this field empty.

   The server and folder names are used to connect to the shared folder by building a network folder path as follows: \\SERVER NAME\FOLDER NAME
7. Click **Apply** to save the configuration.

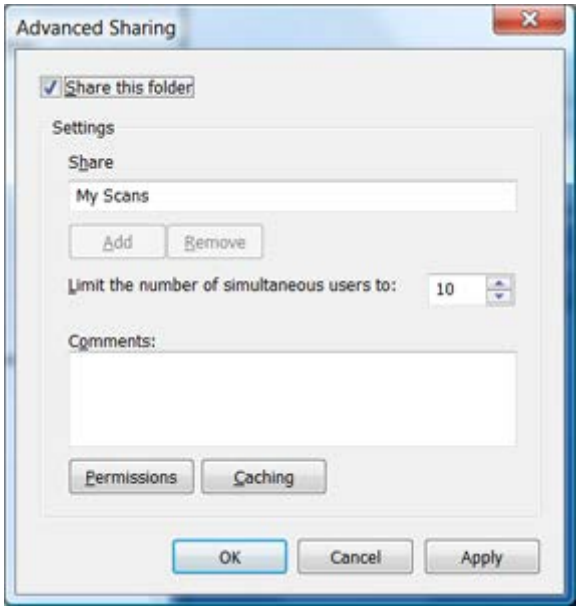
   The printer automatically checks that it can access the network folder.

EXAMPLE: CREATE A SCAN-TO-NETWORK FOLDER USING WINDOWS

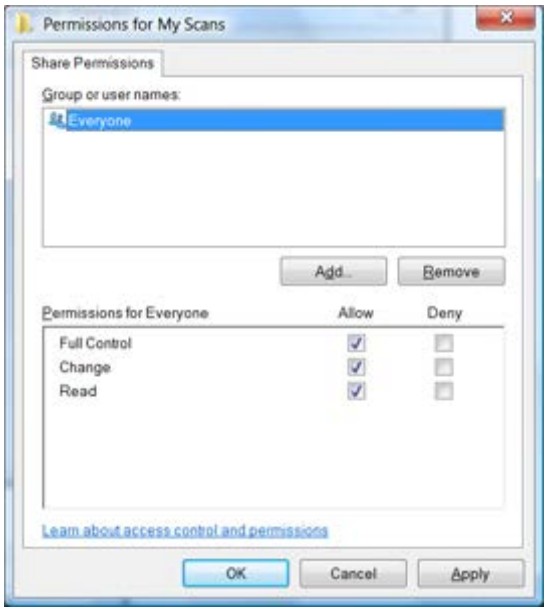
1. Create a new user account for the *scanner user* on the remote computer. You can use an existing user account for this purpose, but it is not recommended.
2. Create a new folder on the remote computer (unless you want to use an existing folder).
3. Right-click the folder and select **Properties**.
4. In the **Sharing** tab, click the **Advanced Sharing** button.



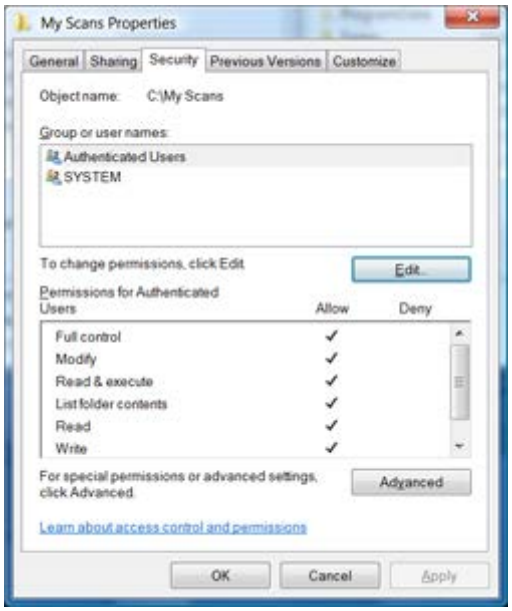
5. Check the **Share this folder** box.



6. You need to ensure that the *scanner user* has full read/write control over the shared folder. To do this, click **Permissions** and grant **Full Control** to the user (or to any suitable group that includes that user).



7. If there is a **Security** tab in the Properties window for your folder, then you must also grant the same user **Full Control** over the folder in the **Securit**y tab. Only some file systems such as NTFS require this.

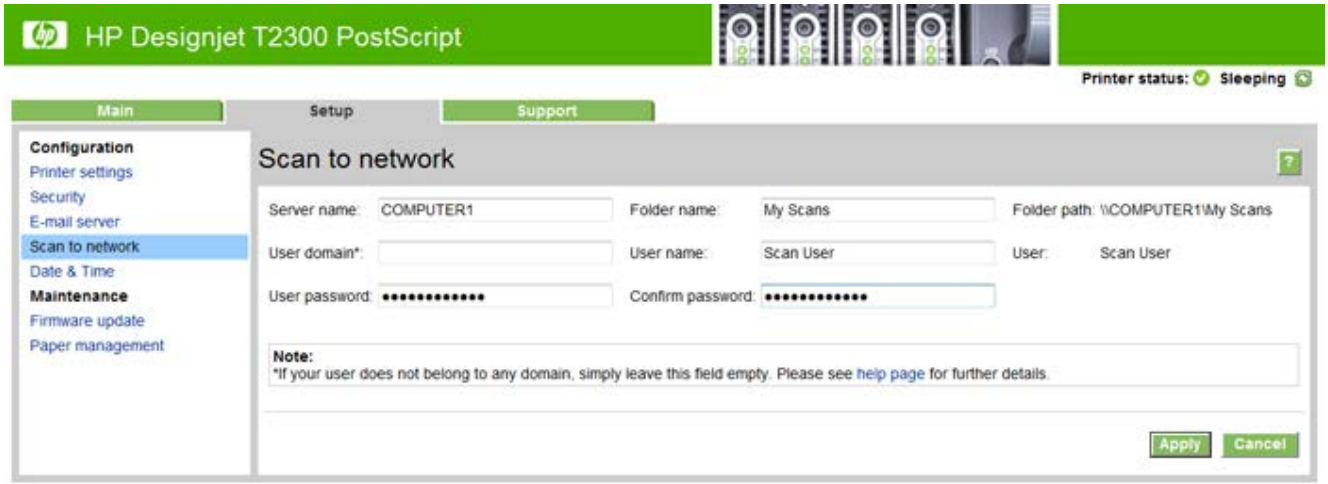


The *scanner user* can now access the folder and write files to it. Next, you must configure the printer to send scans to the folder.

8. In the Home screen of the printer's Embedded Web Server, select the **Scan to network** tab.

9. On the Scan to Network page, click **Add folder details**:

   If the printer has already been configured for scanning to the network and you now want to use a different shared folder, click **Modify**.



Enter the Host name or IP address of the remote computer, the name of the shared folder, and the user

name and password of the *scanner user* that you have already created on the remote computer.

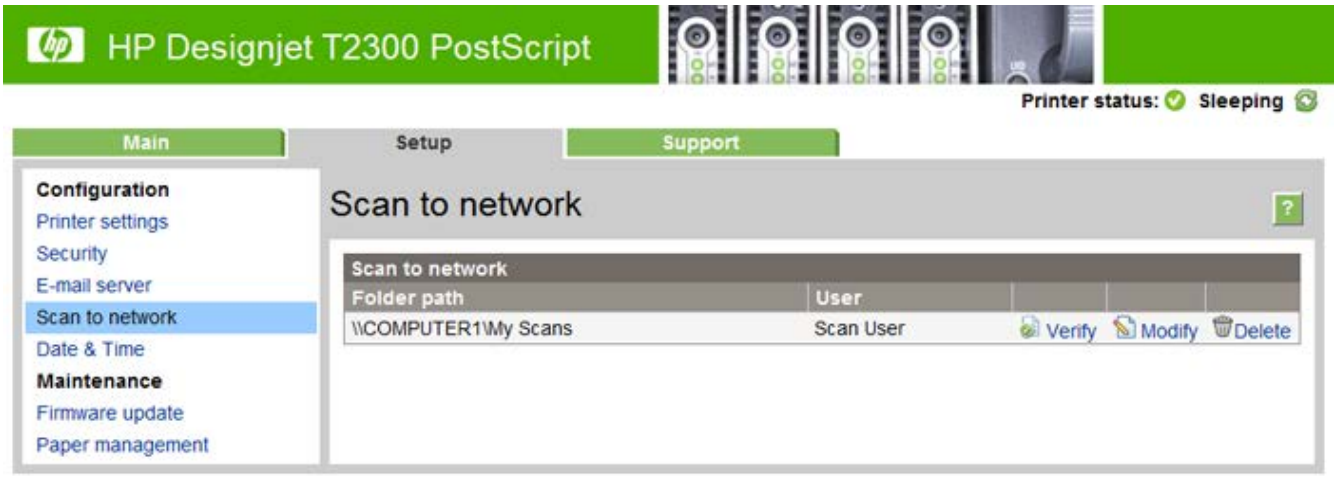
Leave the user domain field empty unless the user is a member of a Windows domain. If the user is only a local user of the remote computer, leave the field empty.

You can use the host name (instead of the IP address) in the server name field only if the shared folder is on a Windows computer in the same local network. This must be a simple name (up to 16 characters long) without a domain suffix (i.e. without any dots in the name). Fully qualified DNS domain names are supported, except for T2300.

10. Click **Apply** to save the configuration.

    The printer automatically checks that it can access the network folder.

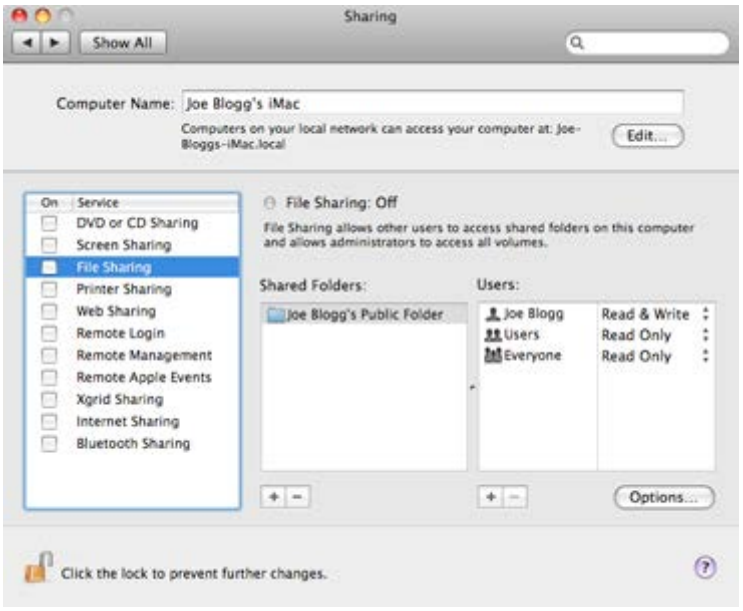
    You can check at any later time that the shared folder remains accessible by clicking **Verify** in the Embedded Web Server. A correctly configured shared folder can become inaccessible if the user's password is changed, or if the shared folder is moved or deleted.



EXAMPLE: CREATE A SCAN-TO-NETWORK FOLDER USING MAC OS

Note: Scan to Network is currently supported on Mac OS 10.9 (Maverick) and previous versions.

1. Create a new user account for the *scanner user* on the remote computer. You can use an existing user account for this purpose, but it is not recommended.
2. Create or choose a folder on the remote computer. By default, Mac OS users have a "Public Folder" that can easily be used for this purpose.
3. Open **System Preferences** and select the **Sharing** icon.



4. Make sure the *scanner user* has **Read & Write** access to the folder.
5. Click **Options**.
6. Check the **Share files and folder using SMB** box, and make sure that the *scanner user* is checked in the **On** column.

7. Click **Done**. You will now see **file sharing** enabled and **Windows sharing: On**.

The *scanner user* can now access the folder and write files to it. Next, you must configure the printer to send scans to the folder.

8. From the Home screen of the printer's Embedded Web Server, select the **Setup** tab and then **Scan to network**.
9. On the **Scan to network** page, click **Add folder details**.

   If the printer has already been configured for scanning to the network and you now want to use a different shared folder, click **Modify**.

Enter the IP address of the remote computer, the name of the shared folder, and the user name and password of the *scanner user* that you have already created on the remote computer.

You cannot use the remote computer's host name as the server name, as this is only supported for computers running Windows. You must use the IPv4 or IPv6 address.

Leave the user domain field empty.

10. Click **Apply** to save the configuration.

    The printer automatically checks that it can access the network folder.

    You can check at any later time that the shared folder remains accessible by clicking **Verify** in the Embedded Web Server. A correctly configured shared folder can become inaccessible if the user's password is changed, or if the shared folder is moved or deleted.

2.5.4.1 Troubleshooting scan to network connectivity issues

If you are unable set the **Scan to network**, try the following:

- Check that you have filled in each field correctly.
- Check that the printer is connected to the network.
- Check that the folder is shared.
- Check that you can put files into the same folder from a different computer on the network, using the printer's logon credentials.
- Check that the printer and the remote computer are on the same network subnet.
- Check that the Firewall does not block de CIFS/SMB ports.
- Try a basic network configuration, connect the printer directly to the computer.

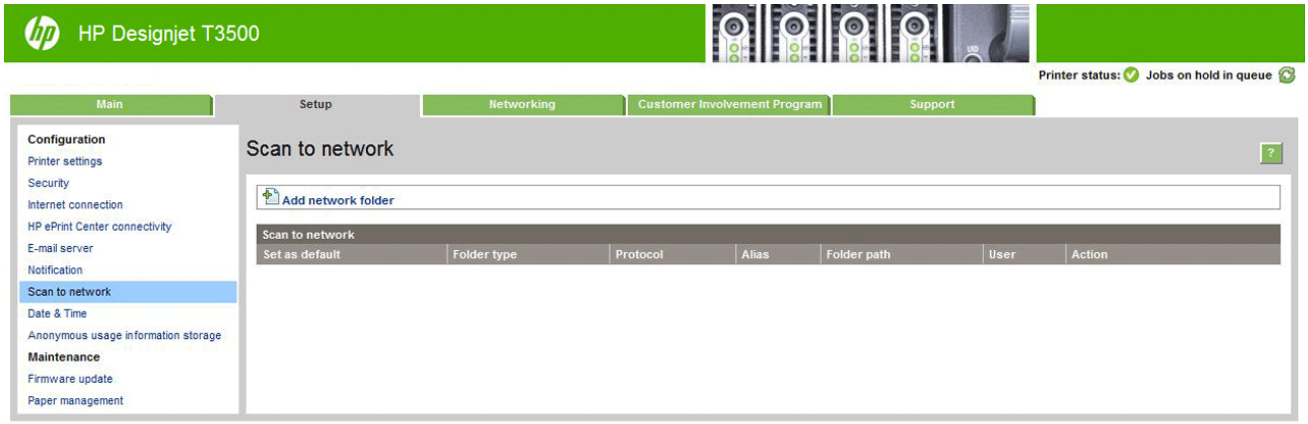
Note:

- Direct hosted SMB traffic (not using NetBIOS) uses port 445 (TCP and UDP).
- NetBIOS over TCP uses the following ports: UDP ports 137,138; TCP ports 137,139.
- **Scan to network** is not supported within the following environments/protocols: Active Directory, SMB 2, SMB 3, Cluster Server environment, Kerberos, NFS and SSPI protocols.

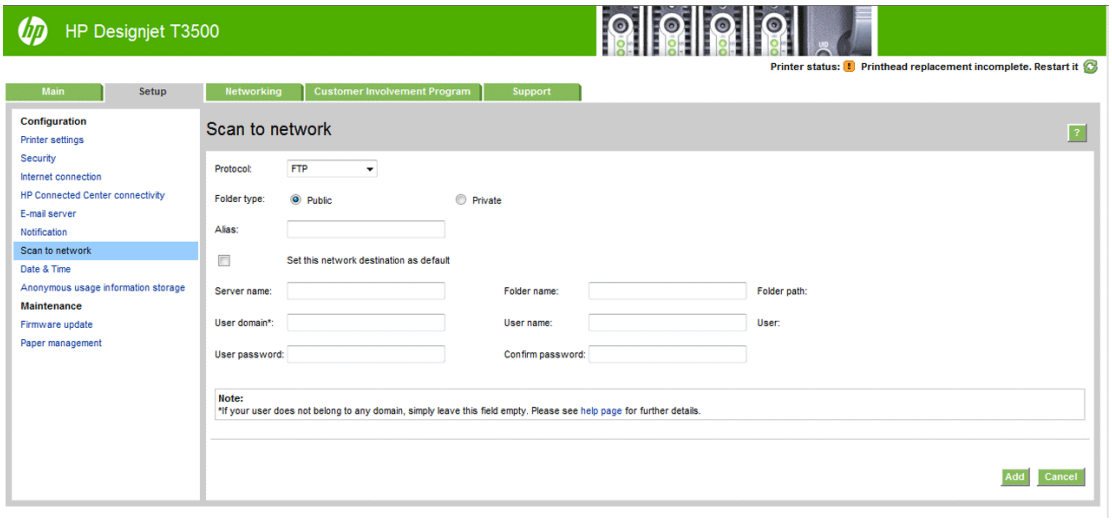
2.5.5 Scan to FTP folder

1. Create a folder on an FTP server.
2. Ensure that you know the server name, user name, and password for the FTP server.

   NOTE: You must complete the above steps for one option or the other before starting the remaining steps below.
3. In the printer's Embedded Web Server, select the **Setup** tab and then **Scan to network**. See *Access the Embedded Web Server*, in the *User Guide*.



   Alternatively, in the HP Utility, select the **Settings** tab and then **Scan to network**. See *Access the HP Utility*, the *User Guide*.
4. On the **Scan to network** page, click **Add folder details**, and fill in the various fields.



- **Protocol** may be FTP or CIFS (Windows).
- **Folder type** may be public or private. The folder type is displayed in both the Embedded Web Server and the front panel with an icon. When you select a private folder, you must enter a password in the front panel.
- **Alias name** is displayed in the front panel when you are choosing the scan destination. It may be different from the network or FTP folder name.
- **Set this network destination as a default**. If you have installed HP DesignJet SmartStream, the option to set it as a destination appears. See the *HP SmartStream User Guide*.
- **Server name** should contain the network name of the remote computer.
- **Folder name** should contain the share name of the folder.
- **User name** should contain the name of the *scanner user* .
- **User password** should contain the password of the *scanner user*.
- **Domain name** should contain the name of the domain in which the user name exists. If the *scanner user* does not belong to any domain, leave this field empty.

The server and folder names are used to connect to the shared folder by building a network folder path as follows: *server name**folder name*.

For a **network folder**, enter the name or IP address of the remote computer, the name of the shared folder, and the user name and password of the *scanner user* that you have already created on the remote computer. Leave the user domain field empty unless the user is a member of a Windows domain. If the user is only a local user of the remote computer, leave the field empty. You can use the name (instead of the IP address) in the server name field only if the shared folder is on a Windows computer in the same local network. This must be a simple name (up to 16 characters long) without a domain suffix (without any dots in the name). Fully qualified DNS domain names are also supported.

For an **FTP folder**, enter the server name, folder name, user name, and password. Leave the user domain empty.

5. Click **Add** to save the configuration.

   Note: If the product has already been configured for scanning to the network and you now want to use a different shared folder, click **Modify**.

6. The printer automatically checks that it can access the network folder. If not, see the printer's *User Guide*.

You can check at any later time that the shared folder remains accessible by clicking **Verify** in the Embedded Web

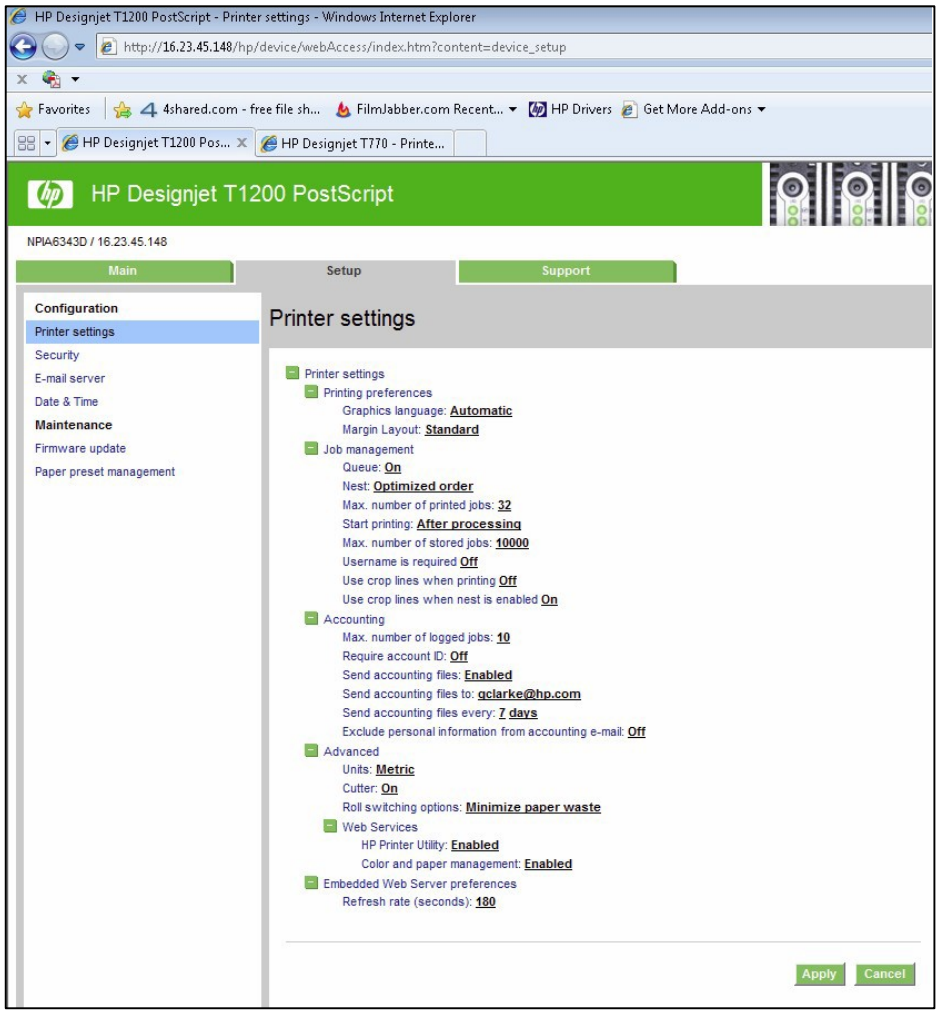
Server. A correctly configured shared folder can become inaccessible if the user's password is changed, or if the shared folder is moved or deleted.

2.5.6 Exclude personal info from accounting

You can enable or disable the option for the printer to send an e-mail containing accounting information. If you enable this setting, you also need to fill in the destination of the report by using the **Send accounting files to** setting. Please note that you also have to configure the e-mail server on the **Setup Page**.

In some cases, customers prefer not to send personal data from the printers via e-mail, and so the option to 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, and account ID will be left blank in the accounting file sent by e-mail from the printer).

This option is typically 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 e-mail. This personal information is typically used for cost allocation within a company.



2.5.7 Disable internet connection

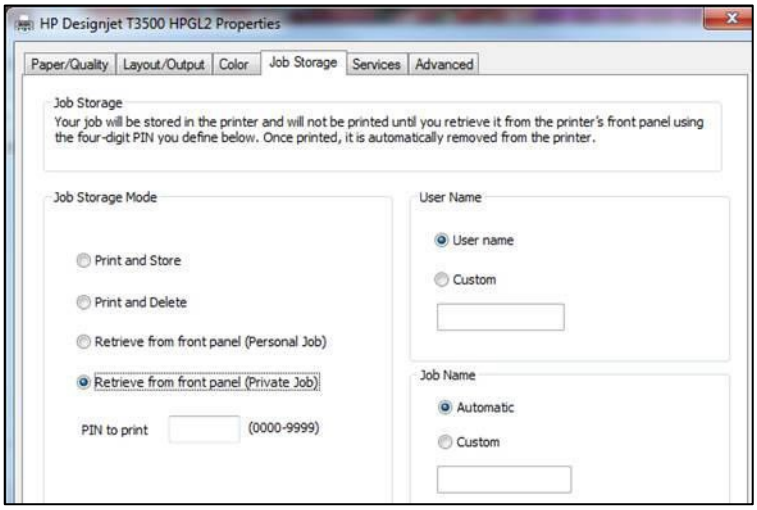
Disable the direct connection of the printer to the internet. This option also prevents the printer from automatically performing firmware upgrades.

2.6 Document security

2.6.1 Job storage and PIN printing

Job storage allows jobs to be stored and then printed when required, it also provides features for setting print jobs as “private”, with a personal identification number (PIN).

To access job storage features, open the printer’s **Properties**, and then select **Printing Preferences**. Click on the **Job Storage** tab where the following job-storage features are available:



Print and Store

- After a job has been printed, it is stored in the printer and more copies can then be printed from the front panel.

Print and Delete

- Once printed, the job is automatically removed from the printer.

Retrieve from front panel (Personal Job)

- Use the **personal job** printing feature to specify that a job cannot be printed until you release it from the printer's front panel.
- To preview it in the Embedded Web Server, you will need to enter the PIN.

Retrieve from front panel (Private Job)

- Use the **private job** printing feature to specify that a job cannot be printed until you release it with a PIN. First, select **Retrieve from front panel (Private Job)**, then the **PIN to print** checkbox will be available. If checked, a 4-digit personal identification number must be set. The PIN is sent to the device as part of the print job. After sending the print job to the device, use the PIN to print the job. Once printed, it is automatically removed from the printer.
- To preview it in the Embedded Web Server or in the front panel, you will need to enter the PIN.

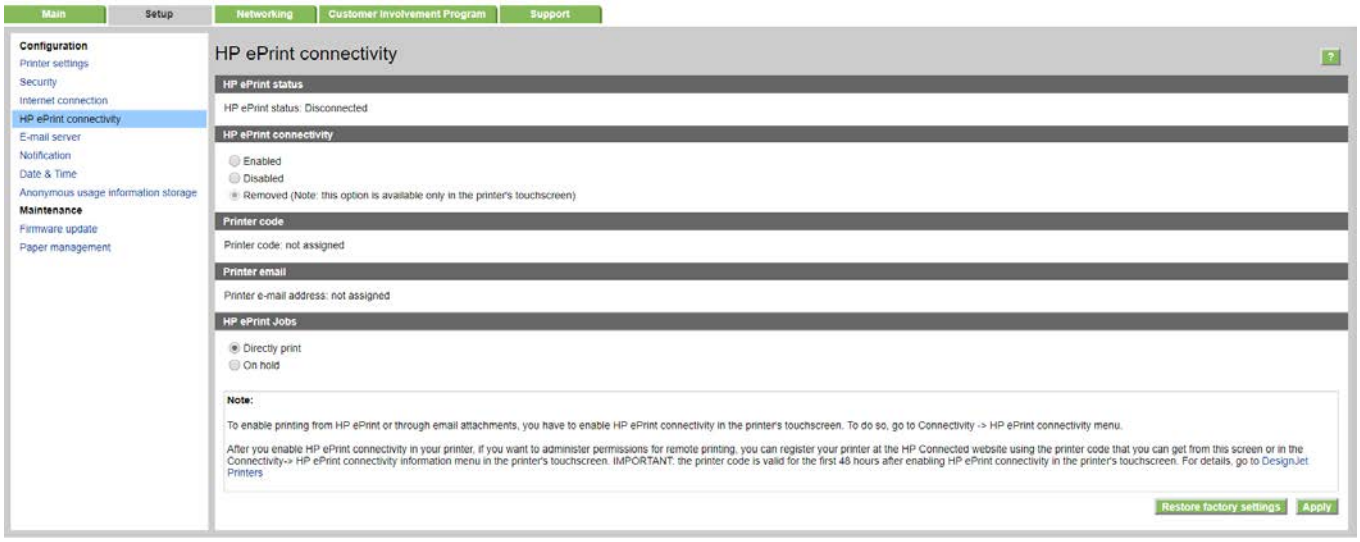
Note: Some Multifunction devices include the **Scan job storage** feature that has two options: **Scan and delete** (the job is not stored in the scan job queue) and **Scan and store** (the job is kept in the scan job queue).

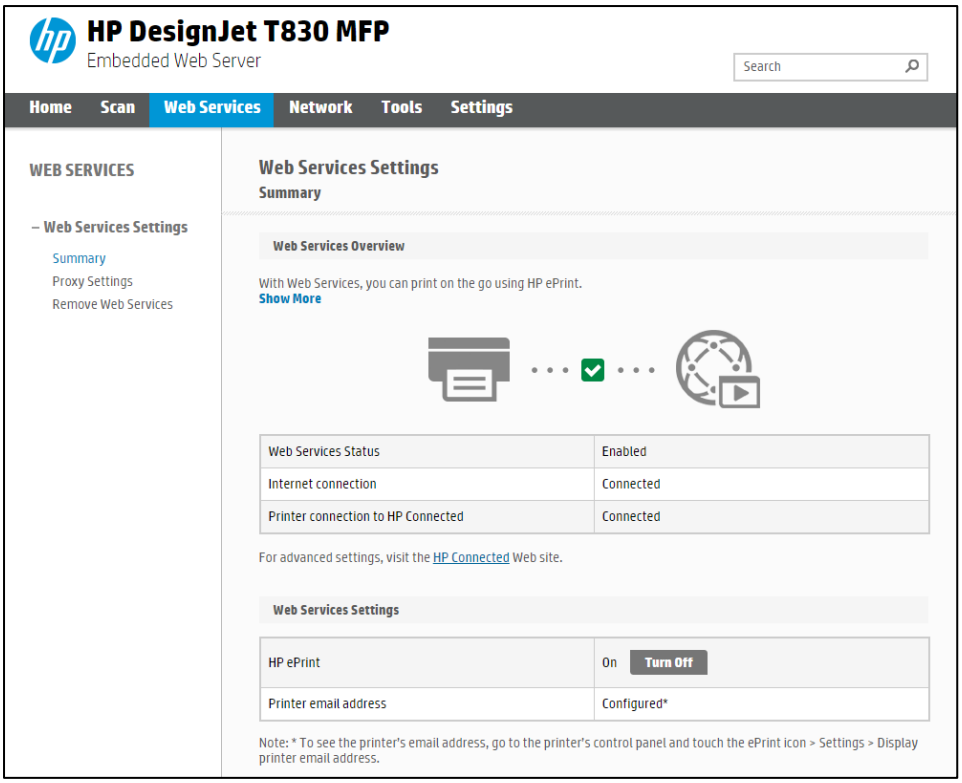
2.6.2 ePrint center connection

The ePrint feature allows the user to print any supported file sending an email. It is available in the front panel and the EWS.

This feature can be disabled, so that users are unable to remotely send items to print.

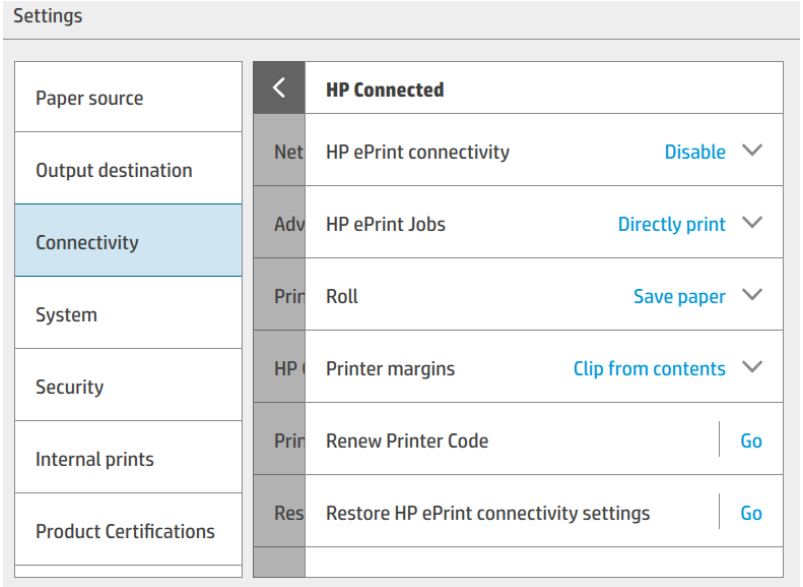

Security
Gigabit Ethernet
Enabled
HP ePrint Center connectivity
Enabled
User sessions
Printer access control


Main
Setup
Networking
Customer Involvement Program
Support
Configuration
Printer settings
Security
Internet connection
HP ePrint connectivity
E-mail server
Notification
Date & Time
Anonymous usage information storage
Maintenance
Firmware update
Paper management
HP ePrint connectivity
HP ePrint status
HP ePrint status: Disconnected
HP ePrint connectivity
Enabled
Disabled
Removed (Note: this option is available only in the printer's touchscreen)
Printer code
Printer code: not assigned
Printer email
Printer e-mail address: not assigned
HP ePrint Jobs
Directly print
On hold
Note:
To enable printing from HP ePrint or through email attachments, you have to enable HP ePrint connectivity in the printer's touchscreen. To do so, go to Connectivity -> HP ePrint connectivity menu.
After you enable HP ePrint connectivity in your printer, if you want to administer permissions for remote printing, you can register your printer at the HP Connected website using the printer code that you can get from this screen or in the Connectivity-> HP ePrint connectivity information menu in the printer's touchscreen. IMPORTANT: the printer code is valid for the first 48 hours after enabling HP ePrint connectivity in the printer's touchscreen. For details, go to DesignJet Printers
Restore factory settings
Apply


HP DesignJet T830 MFP
Embedded Web Server
Search
Home
Scan
Web Services
Network
Tools
Settings
WEB SERVICES
– Web Services Settings
Summary
Proxy Settings
Remove Web Services
Web Services Settings
Summary
Web Services Overview
With Web Services, you can print on the go using HP ePrint.
Show More
Web Services Status
Enabled
Internet connection
Connected
Printer connection to HP Connected
Connected
For advanced settings, visit the HP Connected Web site.
Web Services Settings
HP ePrint
On
Turn Off
Printer email address
Configured*
Note: * To see the printer's email address, go to the printer's control panel and touch the ePrint icon > Settings > Display printer email address.

This functionality is disabled by default.

In PageWide XL, the route to enable it is **Settings > Connectivity > HP Connected > HP ePrint connectivity**. In the same window, you can set the behavior of the printer for this kind of job.



If you want to control the job sent with this path, you can use **Hold the job** and **block the control panel with a password**.

You can also configure who can use this path (which e-mail addresses are allowed or forbidden). This is configured in https://www.hpconnected.com/, an account is needed to do it.

3. Large Format printers: security features summary

GRAPHIC PRINTERS

Model	Z6X00	D5800	Z5400	Z3200	Z2100/Z5200ps	Z2600/Z5600
Device security - Device integrity						
SNMPv3	EWS	EWS	EWS	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS
UEFI Secure Boot	N/A	N/A	N/A	N/A	N/A	N/A
Disable firmware update through USB	N/A	N/A	EWS/FP	N/A	N/A	EWS/FP
Automatic Firmware Upgrade (AFU)	No	EWS	EWS	EWS	EWS	Yes
Device security - Device configuration protection						
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA
Disable physical ports	EWS	EWS	EWS/FP (USB Printing)	N/A	N/A	EWS/FP (USB printing)
Control panel lock	EWS	EWS	EWS/WJA	N/A	N/A	EWS/WJA
Hide IP from Front Panel (FP)	FP	FP	EWS/FP	N/A	N/A	EWS/FP
EWS multilevel	EWS	EWS	EWS	EWS (1 level)	N/A	EWS

Model	Z6X00	D5800	Z5400	Z3200	Z2100/Z5200ps	Z2600/Z5600
Guest Account	Yes	Yes	Yes	Yes	Yes	Yes
Printer access control	N/A	N/A	EWS/FP	N/A	N/A	EWS/FP
Disable USB drive	N/A	N/A	EWS/FP	N/A	N/A	EWS/FP
Wizard setup configuration	N/A	N/A	N/A	N/A	N/A	N/A
CA/JD Certificates	EWS/WJA	EWS/WJA	EWS/WJA	EWS + Jetdirect	EWS + Jetdirect	EWS/WJA
Data security - Encrypted communications						
IPSec Compatibility	EWS	EWS	EWS/WJA	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA
TLS/SSL	No	No	Yes	Only with JD640	Only with JD640	No
Encrypt web communications	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA
Data security – Authentication						
802.1X Authentication	N/A	N/A	N/A	N/A	N/A	N/A
NTLM	N/A	N/A	N/A	N/A	N/A	N/A
Data security - Protected data in storage						
External HDD	Yes	Yes	N/A	N/A	N/A	N/A
Removable HDD	N/A	N/A	Yes	N/A	N/A	Yes
Self-Encrypted hard disk	N/A	N/A	N/A	N/A	N/A	N/A
Secure file erase	WJA	WJA	WJA/FP	WJA	WJA (Z2100 only)	WJA/FP
Secure disk erase	WJA/FP	WJA/FP	WJA/FP	WJA/FP	N/A	WJA/FP
Exclude personal info. from accounting	EWS	EWS	EWS	EWS	EWS (Z5200ps only)	EWS
Disable internet connection	N/A	N/A	EWS/FP	N/A	N/A	EWS/FP
Disable ePrint Center connectivity	N/A	N/A	EWS/FP	N/A	N/A	EWS/FP
Document security – PIN printing						
Job Storage Mode and PIN printing	N/A	N/A	N/A	N/A	N/A	N/A

EWS: Embedded Web Server, **WJA**: Web Jet Admin, **FP**: Front Panel., **N/A**: Not available.

TECHNICAL PRINTERS

Model	T7X00	T3500	T2500/T1500/T920	T2530/T1530/T930	T2300/T1300	T790/T795	T120/T520	T730/T830
Device security - Device integrity								
SNMP configurability ~~v3~~	EWS	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS	EWS	Only SNMPv1 EWS	EWS
UEFI Secure Boot	N/A	Yes	N/A	Yes	N/A	N/A	N/A	N/A
Disable firmware update through USB	N/A	EWS/FP	EWS/FP	EWS/FP	EWS/FP	EWS/FP	N/A	EWS
Automatic Firmware Upgrade (AFU)	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Device security - Device configuration protection								
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA
Disable interfaces	EWS	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/FP (USB printing only)	EWS/FP (USB printing only)	EWS/FP	EWS/FP
Control panel lock	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	N/A	N/A
Hide IP from FP	FP	FP	FP	FP	FP	FP	N/A	N/A
EWS multilevel	EWS	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/FP	EWS/FP (1 level)	EWS (1 level)	EWS (1 level)
Printer access control	N/A	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/FP	EWS/FP	N/A	N/A
Disable USB drive	N/A	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/FP	EWS/FP	N/A	EWS
Wizard setup configuration	N/A	EWS	EWS	EWS	N/A	N/A	N/A	N/A
CA/JD Certificates	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS	N/A	EWS
Data security – Encrypted communications								
IPSec	EWS	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/WJA	EWS/WJA	N/A	N/A

Model	T7X00	T3500	T2500/T1500/T920	T2530/T1530/T930	T2300/T1300	T790/T795	T120/T520	T730/T830
TLS/SSL	Only with JD640	Yes	Yes	Yes	Yes	Only with JD640/YES	N/A	Yes
Encrypt web communications	EWS/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/WJA	EWS/WJA	EWS	EWS
Data security – Authentications								
802.1X Authentication	N/A	Yes	Yes	Yes	Only using Jetdirect Accessory	Only using Jetdirect Accessory	N/A	EWS
NTLM	N/A	V1 and V2	V1 and V2	V1 and V2	V1	N/A	N/A	V1 and V2
Data security – Protected data in storage								
External HDD	Yes	N/A	N/A	N/A	Yes	PS only	N/A	N/A
Removable HDD	N/A	N/A	N/A	N/A	Yes	Yes	N/A	N/A
Self-Encrypted hard disk	N/A	Yes	Rev B	Rev B	Rev B	Reb B (T790)	N/A	N/A
Secure file erase	WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	WJA	WJA	N/A	N/A
Secure disk erase	WJA/FP	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	WJA/FP	WJA/FP (PS	N/A	N/A
Exclude personal info. from accounting	EWS	EWS/WJA	EWS/WJA	EWS/WJA	EWS	EWS	N/A	N/A
Disable internet connection	N/A	EWS/FP/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/FP	EWS/FP	EWS/FP	EWS/FP
Disable ePrint Center connectivity	N/A	EWS/FP	EWS/FP	EWS/FP	FP	FP	EWS/FP	EWS/FP
Document security – PIN printing								
Job storage and PIN printing (Job retention)	N/A	Yes	N/A	Yes	N/A	N/A	N/A	N/A

OLDER TECHNICAL AND GRAPHIC PRINTERS

Model	T1200	T770	Z3100	Z3100ps	4020/4520	T1100/T1120	Z6100	T620
Device security - Device integrity								
SNMPv3	EWS	EWS	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect
UEFI Secure Boot	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable Firmware	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Automatic Firmware Upgrade (AFU)	No	No	No	No	No	No	No	No
Device security – Device configuration protection								
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA
Disable interfaces	EWS	EWS	EWS	N/A	EWS	EWS	EWS	N/A
Control panel lock	EWS/WJA	WJA	N/A	N/A	WJA	EWS	EWS	N/A
EWS multilevel	EWS	N/A	N/A	EWS	EWS	EWS	EWS	N/A
Printer access control	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable USB drive	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Wizard setup configuration	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CA/JD Certificates	EWS	EWS	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect
Data security – Encrypted communications								
IPSec	EWS/WJA	EWS/WJA	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect t	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect
Encrypt web communications	EWS	EWS	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect
Data security – Authentication								
NTLM	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Data security – Protected data in storage								
External HDD	Yes	HD ver (from F/W 6.0.0.6)	N/A	N/A	N/A	N/A	N/A	N/A
Removable HDD	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Self-Encrypted hard disk	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Secure file erase	WJA	WJA	WJA	WJA	WJA	WJA	WJA	N/A

Model	T1200	T770	Z3100	Z3100ps	4020/4520	T1100/T1120	Z6100	T620
Secure disk erase	WJA/FP	WJA/FP (HD)	N/A	FP	FP	WJA/FP	WJA/FP	WJA/FP
Exclude personal info. from accounting	EWS	EWS	N/A	N/A	EWS	EWS	EWS	N/A
Disable internet connection	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
Document security – PIN printing								
PIN Printing	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

PAGEWIDE XL PRINTERS

Model	HP PageWide XL 8000/5000/4500/4000 Printer	HP PageWide XL 5000/4500/4000 Multifunction Printer	HP PageWide XL 4500 Printer and Multifunction Printer TAA Compliant (US Only)
Device security- Device integrity			
SNMPv3	EWS/WJA	EWS/WJA	EWS/WJA
UEFI Secure Boot	Yes	Yes	Yes
Disable firmware (F/W) update through USB	FP/EWS/WJA	FP/EWS/WJA	FP/EWS/WJA
Automatic Firmware Upgrade (AFU)	Yes	Yes	Yes
Device security - Device configuration protection			
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA
Disable interfaces	No	No	No
Control panel lock	EWS/WJA	EWS/WJA	EWS/WJA
Hide IP from Front Panel (FP)	No	No	No
EWS multilevel	Yes (one level)	Yes (one level)	Yes (one level
Printer access control	EWS	EWS	EWS
Disable USB drive	FP/EWS/WJA	FP/EWS/WJA	FP/EWS/WJA
Job Storage Mode and PIN printing	Yes	Yes	Yes
Wizard setup configuration	Yes	Yes	Yes
CA/JD Certificates	EWS//WJA	EWS//WJA	EWS//WJA

Model	HP PageWide XL 8000/5000/4500/4000 Printer	HP PageWide XL 5000/4500/4000 Multifunction Printer	HP PageWide XL 4500 Printer and Multifunction Printer TAA Compliant (US Only)
Data security - Encrypted communications			
IPSec	EWS/WJA	EWS/WJA	EWS/WJA
TLS/SSL	Yes	Yes	Yes
Encrypt web comms	EWS//WJA	EWS//WJA	EWS//WJA
FIPS-140	Yes, only using SED	Yes, only using SED	Yes, only using SED
Data security – Authentication			
802.1X Authentication	Yes	Yes	Yes
NTLM	EWS/WJA	EWS/WJA	EWS/WJA
Data security - Protected data in storage			
External HDD	No	No	No
Removable HDD	No	No	Yes
Self-encrypted hard disk	Yes	Yes	Yes
Secure file erase	EWS/WJA	EWS/WJA	EWS/WJA
Secure disk erase	EWS/WJA	EWS/WJA	EWS/WJA
Disable internet connection	No	No	No
Exclude personal info. from accounting	Yes	Yes	Yes
Disable ePrint Center connectivity	FP/EWS	FP/EWS	FP/EWS
Document security – PIN printing			
Job Storage Mode and PIN printing	Yes	Yes	Yes

4. Large Format scanners: security features summary

Multi-function printers (MFPs) consist of two main parts: the printer and the scanner. For the scanner, refer to the table below.

Model	DJ 4500 MFP/T1100 MFP, HD-MFP Series DJ 4520 Scanner DJ 4500 Scanner DJ HD Scanner	HP DesignJet HD/SD Pro Scanner HP HD/SD Pro Scanner	PageWide XL MFP series	T1120 SD-MFP	T2300 MFP	T2500 MFP	T2530 MFP	T3500 MFP	T830 MFP
Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Disable FTP & Web Access	Yes	Yes	Yes	N/A	Yes	Yes	Yes	Yes	Yes
Access to images in scanner through network	Yes, by default (FTP & EWS - Read only)	Yes, by default (FTP & EWS - Read only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Security patches	Through scanner S/W update		Through FW update						
Install scanner software into a separate PC	Possible but not official process	Possible but not official process	N/A	N/A	N/A	N/A	N/A	N/A	N/A

5. Ports used in HP printers

Below you can find a list with the ports used by HP printers. Some connection problems are caused by a firewall blocking the needed port. They are ordered by protocol or function.

NOTE: Ports may change as HP products develop and evolve; these changes will be communicated to the official channel and the documentation will be updated.

Protocol/function	Use	Port used	Consequences of disabling it	Used for
9100 printing	Yes	9100 TCP in	It will become impossible to print RAW documents (plain text/JPEG/PNG) on remote devices in local network or internet, using port 9100. This is one of the main printing ports for Windows & Mac	Printing
9101 printing	Yes	9101 TCP in	It will become impossible to print using RIP application based on LFP SDK.	Printing
9102 printing	Yes	9102 TCP in	It will become impossible to print using HP Smart Stream	Printing
LDP (Line Printer Daemon protocol/Line Printer Remote protocol) printing	Yes	515 TCP in	It will disable LDP printing from Windows or OS X, which is almost never used by end users as is a legacy protocol	Printing
WS-Print	Yes	3910 TCP in	Together with 9100, this is one of the two default Windows printing paths. If you disable this, 9100 will be the only printing path from Windows. Partially depends on WS-Discovery being also available	Printing
IPP (Internet Printing Protocol) printing	Yes	631 TCP in	It will disable printing over IPP protocol. So, AirPrint and HP ePrint would not work either. In HP DesignJet T790/795/T1300, this feature is only available with Jetdirect accessory. It can be manually used from Windows or Mac	Printing and sharing
FTP printing	Yes	20, 21 TCP in	It will be impossible to upload documents to the device via FTP protocol. Rarely used. It depends on connection tracking (firewall feature)	Printing

Protocol/function	Use	Port used	Consequences of disabling it	Used for
SLP (Service Location Protocol) config	Yes	427 UDP Multicast in & out	The device will not be discoverable over SLP from DMF - impact is minimal if Bonjour is enabled (SLP treated as legacy technology)	Finding a device. Service Location Protocol - allows computers and other devices to find services in a local area network
Bonjour	Yes	5353 UDP Multicast and Unicast in & out	It will disable advertising of services supported by the device including 9100 printing, LPD printing and IPP/IPPS printing used on OS X for device discovery (i.e. OS X will not discover device in Add Printer dialog). AirPrint, Printing from Android and HP Smart App will not work	Finding a device
WS-Discovery: enabled or disabled	Yes	3702 TCP/UDP Multicast in & out	The Windows HP Installer will not work and Windows will not choose automatically WS-Print as path to print	Finding a device. Multicast discovery protocol to locate services on a local network
Telnet	Yes	23 TCP in	It will become impossible the remote configuration of the HP Jetdirect device when there are no other configuration methods	Device management. It gives remote access to printer FS and configs
IPsec/Firewall	Yes	50/51 TCP, 500 UDP	It will become impossible to use encrypted secure connection to the device over Internet or LAN. It would also become impossible to setup ports/services mapping/forwarding.	
LLMNR	Yes	5355 UDP in Multicast	The device will not be able to introduce itself in local network, when DNS name resolving is inaccessible. It should have no impact for OS X. Mostly used in Windows.	Resolving device name
HP Jetdirect XML services	Yes	HTTP/HTTPS ports (80, 8080) in	The printer Embedded Web Server would not be reachable. HP WJA fleet management tool might not work.	Device management
Certificate management service	Yes	829 TCP in	The HP WJA fleet management tool might not work.	

Protocol/function	Use	Port used	Consequences of disabling it	Used for
Enable WINS port	Yes	-	The printer will not be discoverable through WINS when DNS is not available	Turning on/off WINS registration
WINS registration	Yes	137 UDP. Works over NetBIOS. in	The printer will not be discoverable through WINS	Resolving device name (find device)
TFTP (Trivial File Transfer Protocol) configuration file	Yes	69 in	Only if Jetdirect card is used: configuration through this protocol could not be used. Rarely used.	Used to device management
IPPS printing	Yes	631 TCP - for printing. 631 - UDP for discovery. in	The device will not be able to print over secure IPP protocol. Used almost only from OS X/iOS	Printing
SDK (Paper management)	Yes	8085 TCP in	RIP applications using the HP LFP SDK will not work	Device management
SDK (Remote management)	Yes	8086 TCP in	RIP applications using the HP LFP SDK will not work	Device management
SDK (XDM status)	Yes	8090 TCP in	Some RIP applications using the HP LFP SDK could not work. For HP DesignJet T790/795/T1300, the HP DesignJet Utility will not work neither	Device management
SDK (SNMP)	Yes	161 UDP in	External applications will not be able to get printer information (status, etc.) using SNMP objects	Device management

Protocol/function	Use	Port used	Consequences of disabling it	Used for
Email sending (alerts & job scanned)	Yes	25, 465, 587 TCP out	The printer will not be able to send alerts or jobs through e-maill	Device management
Scan to network	Yes	445, 139 TCP out	MFPs will not be able to send scanned data to networks folders	Sending scanned data out of the MFP
Scan to ftp	Yes	21 TCP out	MFPs will not be able to send scanned date to an ftp server	Sending scanned data out of the MFP
Scanner SDK	Yes	8076 TCP in	Software applications getting data using the scanner SDK will not work.	Sending scanned data out of the MFP
ePrint	Yes	5222 TCP out	It will not be possible using HP Connected service	Printing
Fibonacci, RIO, ePrint	Yes	443 TCP out	It will not be possible using HP Connected service. It will not be possible to send usage data nor to HP usage server (Fibonacci) neither to supplies reordering service (RIO)	Printing and exporting usage information to HP servers

Security Glossary

HP DesignJet & PageWide XL printers

This glossary lists words and features you might hear or read in a security document.

Please note that the features and protocols listed are not all integrated into the HP DesignJet or PageWide XL printers.

Device protection related

BIOS

BIOS

The BIOS (basic input/output system) is the program used to get the printer system started after it is turned on.

HP Sure Start

It validates the integrity of the BIOS at every boot cycle. If a compromised version is discovered, the device reboots using a safe, “golden copy” of the BIOS.

UEFI Secure Boot

Method to prevent the loading of unauthorized operating systems during the system startup. Based on the UEFI Forum specification (www.uefi.org).

CONFIGURATION

Disable ports and protocols

It allows the administrator to select which protocols and services are enabled. Restricting the enabled protocols to only those that are actually needed means the administrator can reduce the risk of vulnerability.

Instant-On Security

Devices supporting **Instant-On Security** features can be automatically added into the Security Manager as soon as they are connected to the network or from reset without any intervention. Instant-On Security immediately configures the device to be compliant with the corporate security policy.

SNMPv3

SNMP is a protocol to get and configure printer information. SNMPv3 is the encrypted version. When enabled, only the client applications knowing the keys will be able to access the printer using this protocol.

FIRMWARE

HP signed firmware packages

Firmware packages are digitally signed by the HP Code Signing group. The printer uses the public key of this group to verify the signature before installing the new firmware, thus ensuring that only legitimate firmware from HP can be installed in the printer.

Only forward firmware security upgrades

Behavior of the firmware that prevents installation of older firmware releases that have known security vulnerabilities.

RD only file system

Solution to guarantee that the firmware cannot be altered. It is based on configuring the filesystem where the printer firmware is located as a read only partition.

Remote firmware upgrade

This service allows an administrator to configure the printer to check for availability of new firmware versions and prepare them to be installed. For the administration of large networks with several printers, HP recommends using the HP Web Jetadmin software to upgrade the printer or multi-function printer firmware.

Whitelisting

Feature that ensures integrity of all the code and data used to control the printer, guaranteeing that no malicious code can be executed

FRONT PANEL

Front Panel access lock

This feature allows the printer administrator to define which Front Panel menus and applications are available for non-administrator users.

Hide IP address from front panel

An option in the **Service Utilities** menu of the front panel to show/hide the Internet Protocol (IP) address of your printer. If the address is hidden, only registered users or network administrators will know the correct address to submit jobs to the printer.

PASSWORDS

File system password

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 configuration changes 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**.

Individual passwords

Each user that wants to interact with the printer must have a different password.

SECURITY EVENTS

Logging and auditing

System to monitor the security of the printers. It requires that the printer logs all the security events and uploads them to a server. It also requires a tool to generate reports using server data. This feature is part of the Common Criteria requirements.

Run-time intrusion detection

Detects anomalies during complex firmware and memory operations. In the event of an intrusion, the device provides information on the intrusion and automatically reboots.

Data protection related

AUTHENTICATION

802.1X

Protocol that the printer uses for its authentication in some networks.

Access control list

It allows the administrator to specify which IPv4 addresses on the network are allowed access to the device.

Authentication & authorization workflows with card readers

Users authenticate themselves using an ID card and a card reader before they can scan/copy/print.

Authentication & authorization walk-up workflows based on Argos OnBoard, ABC Imaging, HP Cost recovery

The users authenticate themselves by providing their identification and passwords through the printer Front Panel. The printer connects to the specific server to get authorization for the required workflow. The user information is then stored in the job accounting, thereby enabling cost recovery solutions.

HP Access Control

HP solution based on the OXP interface that offers secure workflows through authentication with LDAP, secure pull printing and job accounting/cost allocation.

LDAP

Protocol used to access directory services to get information about users, devices, printers, etc. The most used directory service is the Windows Active Directory.

LDAP authentication

The device requires a username and password from an LDAP directory. Currently using the LDAP directory as the authentication source through an **LDAP Bind**. If users have **LDAP Bind** rights, they will be able to authenticate via LDAP authentication.

Authenticated scan & copy w/ LDAP

Users identify themselves in the Front Panel and the MFP authenticates them against the LDAP server before proceeding with the scan or copy. The MFP can then access the folder required by the user from the LDAP server to store the scanned/copied file.

Authenticated scan & copy w/ Kerberos and LDAP

In some enterprise environments, devices can only copy files in a server using the ticket provided by Kerberos. In this workflow, the users identify themselves in the Front Panel and the MFP authenticates them against the Kerberos server before proceeding with the scan or copy. The MFP then gets the folder where the copied/scanned file needs to be stored from the LDAP server.

Active directory

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.

Kerberos

Authentication protocol that enables two devices in a network to demonstrate their identities in a secure way. Kerberos is the authentication service in Windows networks.

NTLMv2

The authentication protocol used, among other cases, to access to SMB servers. The multi-function printers use it to be allowed to write the scanned data into the network folders.

Role based access control

Different and dynamic roles can be defined in the printer and have different permissions about which functionalities they are allowed to run. Users can be linked to a role. In this way, administrators will have a better control over what they allow each user to do.

User authentication

The user is requested to authenticate at the device.

COMMUNICATIONS

Encrypted e-mail

It encrypts all e-mails sent by multi-function printers (i.e. scanned data) to protect the content from being read by anyone that is not the intended recipient.

HTTPS

The standard secure (with authentication and encryption) version of the HTTP protocol. Printers and multi-function printers can be configured to use HTTPS when accessing the printer through the Embedded Web Server, or printing through solutions that use HTTPS.

Protocol

A protocol is a set of rules and guidelines for communicating data. Rules are defined for each step and process during the communication between two or more devices. Networks must follow these rules to successfully transmit data.

SSL

A cryptographic protocol for internet secure communications. It is used, for example, by HTTPS.

X.509

A standard for certificates using public keys. The certificates are the base to encrypt data for secure data transmission between devices connected to the internet.

STORAGE

ATA password protected disks

The disk of the printer is functional only after the printer BIOS authenticates itself by providing a password. It protects information on the disk even if the disk is removed from the printer and installed in a PC.

Encrypted hard disk

Hard disk in which the data is stored applying an encryption method. This ensures that disk contents cannot be read if the disk is removed from the printer and connected to a computer.

Secure file erase and disk erase

Procedures to ensure that actual data in storage systems is removed, avoiding any possibility of data recovery. They are based on repeatedly writing multiple patterns in the areas were the original data was located.

Secure sanitizing erase

It conforms to the U.S. Department of Defense 5220-22.M specification for deleting magnetically stored data. Secure sanitizing erase uses multiple data overwrites to eliminate trace magnetic data and also prevents subsequent analysis of the hard disk drive's physical platters for the retrieval of data.

Secure storage

A solution to storage critical information encrypting it (using hardware such as TPM or a virtual TPM). It is a way to add another protection barrier to protect information, even if the HDD has been accessed.

IP

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.

Firewall

Provides a simple way to configure which IP addresses can be accessed to/from the printer.

IPsec

Suite of protocols for securing communications over Internet Protocol (IP). It authenticates and/or encrypts every IP package. It is a way to secure data transmission without using upper protocols such as SSL, TLS or SSH.

VULNERABILITIES

TLS

The successor of SSL, which solves some of its vulnerabilities. It is used, for example, by HTTPS.

Document protection related

On-demand document retrieval

It allows print jobs to be saved electronically in the device, or on an external server, until the authorized user is ready to print them. The user provides a simple PIN code, or uses an authentication method supported for other HP multi-function printers in walk-up operations, to release the print job.

Job held timeout

This feature is part of the Job retention feature. It limits a held job to the selected time, and then the printer deletes it. You 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

This feature provides job retention options such as private job and hold job. You will be able to make sure that they are present during printing to provide privacy for documents in the printer output bins.

Private job recovery

When configured in this mode, the printer holds the jobs in the queue with a user identifier. User must identify themselves in the FP. After the authentication, the users can see their jobs in the queue and trigger the printing. Users can only see their own jobs in the queue.

Private printing

The job is retrieved from a specific printer, which has been selected prior to sending the job.

Pull printing

Documents can be retrieved from a pool of printers.

Secure PIN printing

Method to protect user printout from others to access. It works by holding the job in the printer queue until the intended recipient of the printed output provides his/her PIN through the printer Front Panel.

Secure print

An end-to-end workflow in which the data is secured by encrypting it just from the submission point (i.e. in the driver).

Smart card

A smart card will be required by the device to access a certain function.

Authentication Manager (LJ feature)

This feature enables 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 Web Jetadmin: www.hp.com/go/webjetadmin

September 2017