

HP DesignJet and PageWide XL Printers

Security features

© 2014, 2016, 2021,2024 HP Development Company, L.P.

Reproduction, adaptation, or translation without prior permission is prohibited, except as allowed under the copyright laws.

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.

February 2024 Edition

Table of contents

1. Introduction & Overview ... 3
2. Security concepts explanation ... 3
2.1 Device security ... 3
2.2 Device configuration protection ... 4
2.2.1 Control Panel Access lock ... 9
2.2.2 Access control ... 12
How to configure Access Control ... 12
Front Panel log in ... 14
2.2.3 Deadlock: Front Panel locked + EWS password forgotten ... 15
SCL certificates ... 15
2.2.4 How to change my printer's default admin password ... 18
2.2.5 Reset admin password to default ... 18
2.2.6 Administrator password ... 20
2.2.7 Guest password ... 21
3. Advanced workflows ... 44
3.1 Printing using LPR protocol. ... 44
3.2 Printing using FTP protocol. ... 45
3.3 Printing with PJLs ... 47
4. Large Format printers: security features summary ... 51
4.1 GRAPHIC PRINTERS ... 51
4.2 TECHNICAL PRINTERS ... 54
4.3 Production machines, bigger offices (DesignJetXL and PageWideXL) ... 60
5. Large Format scanners: security features summary ... 63
6. Ports used in HP printers ... 65
Appendix 1 – Web Jetadmin ... 73
Appendix 2 – JetAdvantage Security Manager ... 76
Appendix 3 - Security Manager ... 78
Appendix 4 - Netgard overview ... 80
Appendix 5 – HP Designjet T850 and T950, & HP Designjet XL3800 ... 90
HP Wolf Security ... 90
Security features ... 91
Security Glossary ... 100
Device protection related ... 100
Data protection related ... 102
Document protection related ... 105

1. Introduction & Overview

This document provides an overview of the security and connectivity features supported by HP DesignJet and PageWide XL printers as of February 2024.

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).
- Description of the advanced printing workflows that can be used with the HP DesignJet (only T2600/Z6/Z9+/Z6 Pro/Z9+ Pro) and PageWide XL printers (Section 3, Advanced workflows).
- 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 4, 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 5, 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

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.

HP Secure Boot

HP Secure Boot is another security feature that further protects the printer during boot process by making the BIOS validate its own integrity at the very start before continues execution. Secure Boot ensures a clean bootup to avoid any usage of external software installed in the printer and blocking backdoors to prevent hacking of the BIOS of the device.

To achieve this, file whitelisting ensures that the firmware and datafiles are originals and not modified or replaced files by unknown sources.

Security Event Logging (Sysslog)

Security Event Logging ensures the device can register all the security-related events. It is achieved through integration with Splunk and McAfee's SIEMS.

All sensitive information, such as keys and passwords, are stored in an independent hardware item. To access this hardware, the system uses different keys, protecting the printer's identity when authenticating.

Integration with SIEM tools

SIEM tools are software products and services that result from the combination of Security Information Management and Security Event Management. They provide real-time analysis and recording of security alerts generated by applications and network hardware.

Connection Inspector

Connection Inspector monitors the printer connections to the internet, detecting patterns from malicious software connections and acts on them. It can display 3 different system errors, based on severity:

- Warning
- Severe Continuable
- Severe not Continuable (requires printer restart). By restarting the printer, during the disk check, traces and injected malware will be cleared.

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:

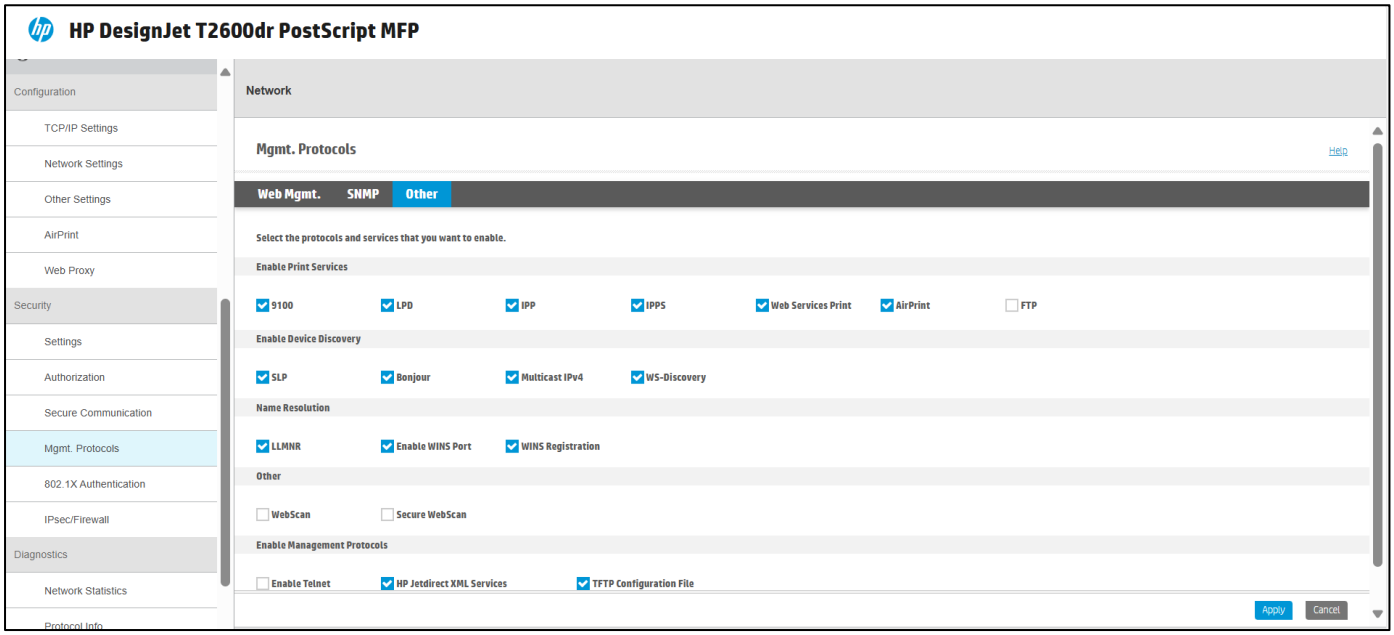
- Protect the EWS access with an admin account (see section 2.2.6, Embedded Web Server (EWS) access control).
- Disable the firmware upgrade from USB (see section 2.2.7, USB drive control)
- Use the Automatic Firmware Upgrade to download the firmware.

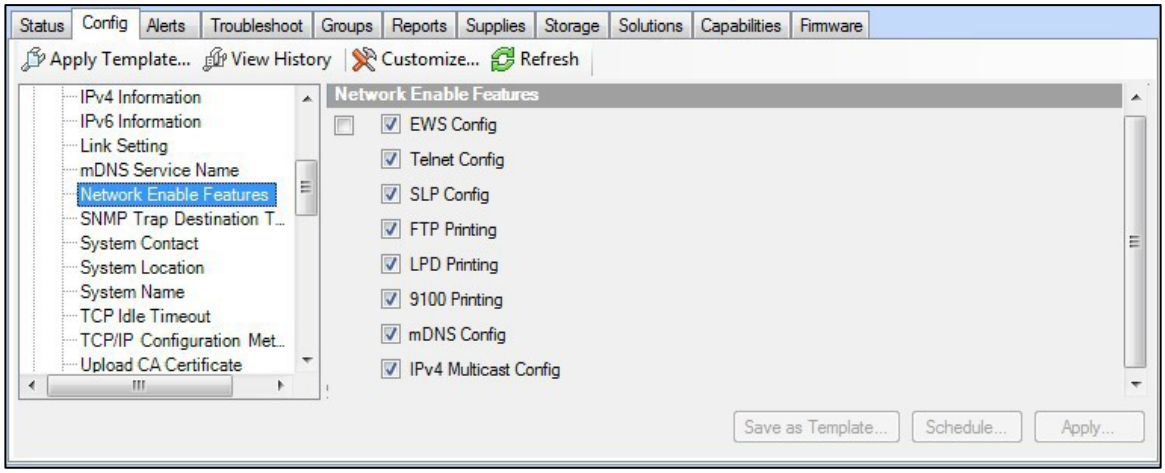
2.2 Device configuration protection

Disable protocols

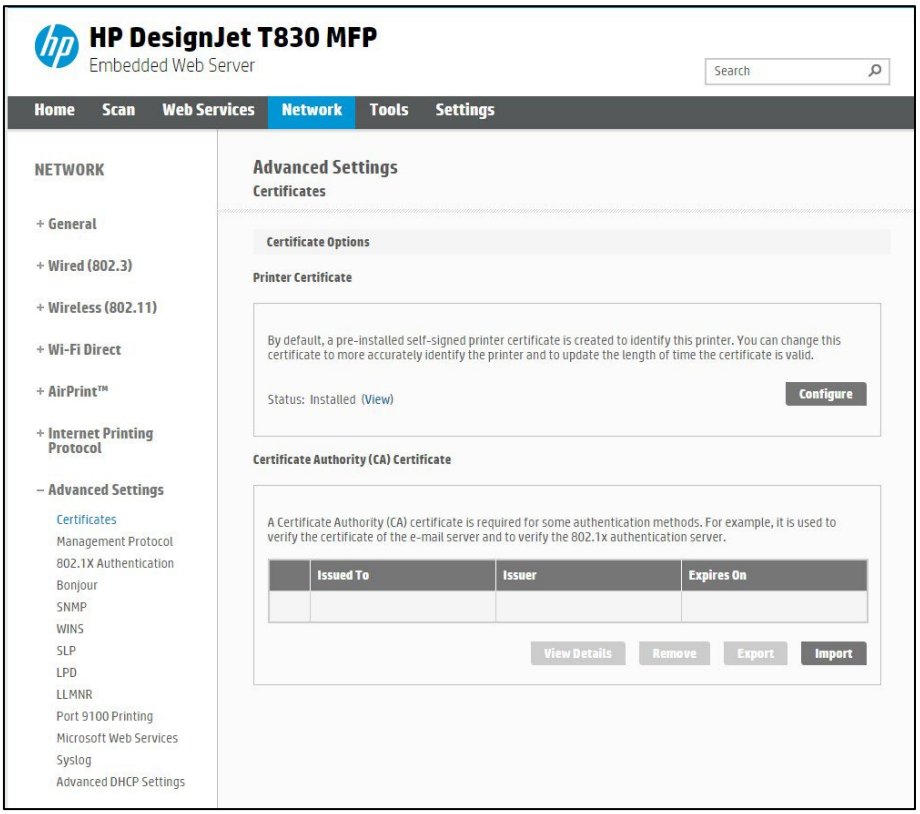
In some cases, you might want to disable all protocols that you do not plan to use to access your printer. For example, you might prevent users from sending files via ftp or connecting through telnet to manage the printer

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 and HP DesignJet T200/600/Studio Printer, the network Management Protocols can be configured from the Network > Advanced Settings menu.



SNMP compatibility

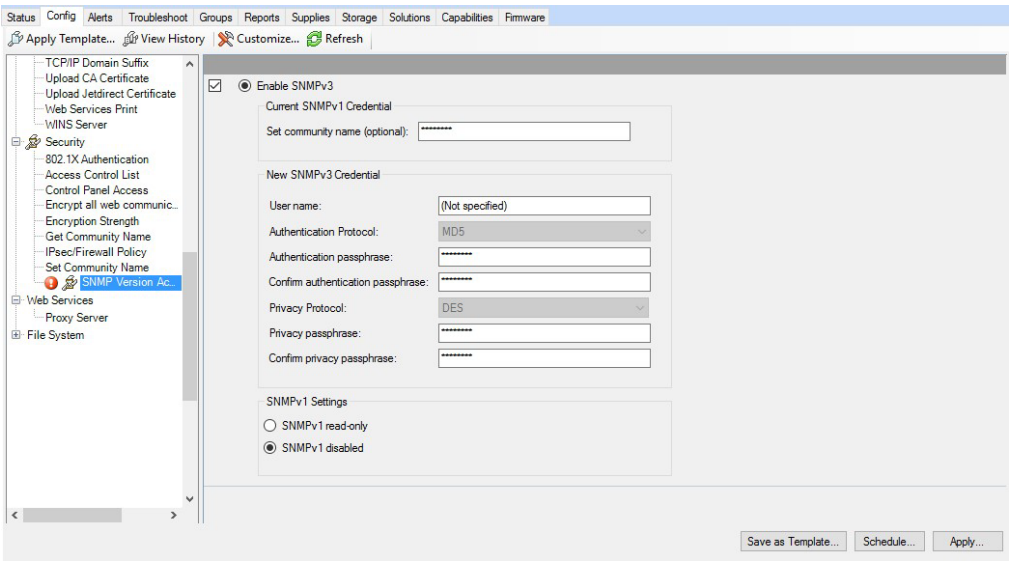
SNMP is a protocol to get printer information and to configure it. SNMPv3 is its encrypted version. Enabling it, only the client applications knowing the keys will be able to access the printer using this protocol.

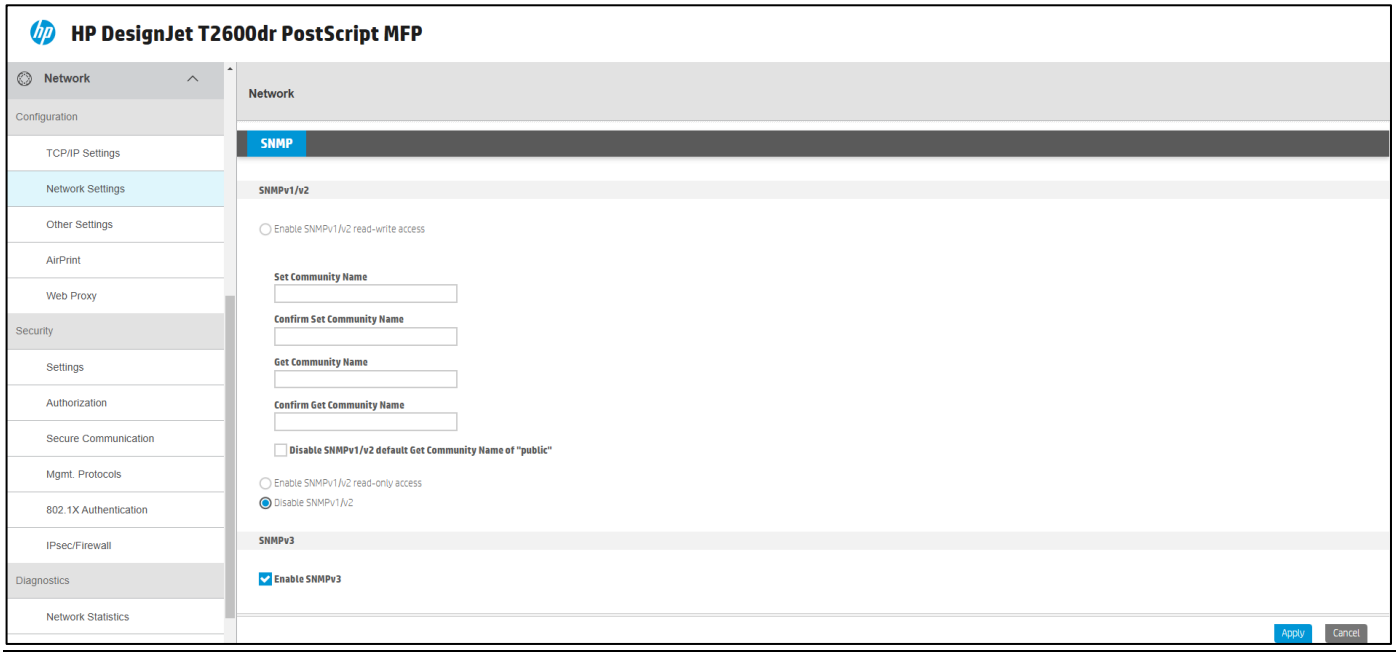
The main benefits of using SNMPv3 are:

- 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.





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.

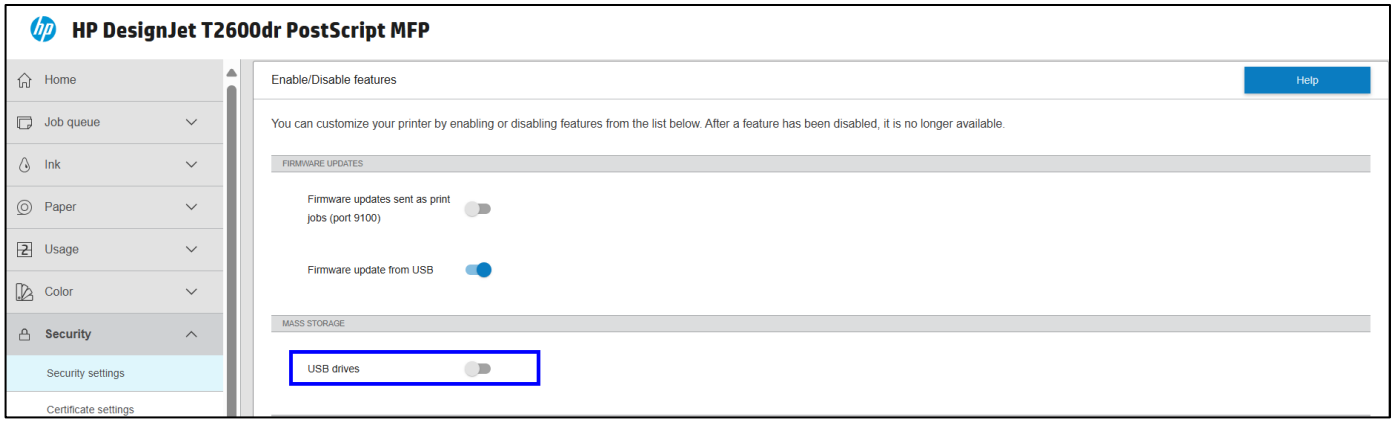
Ideal for enterprise and workgroup SMBs requiring full-featured, secure, and backward-compatible print management of printers and MFPs over shared, wired networks.

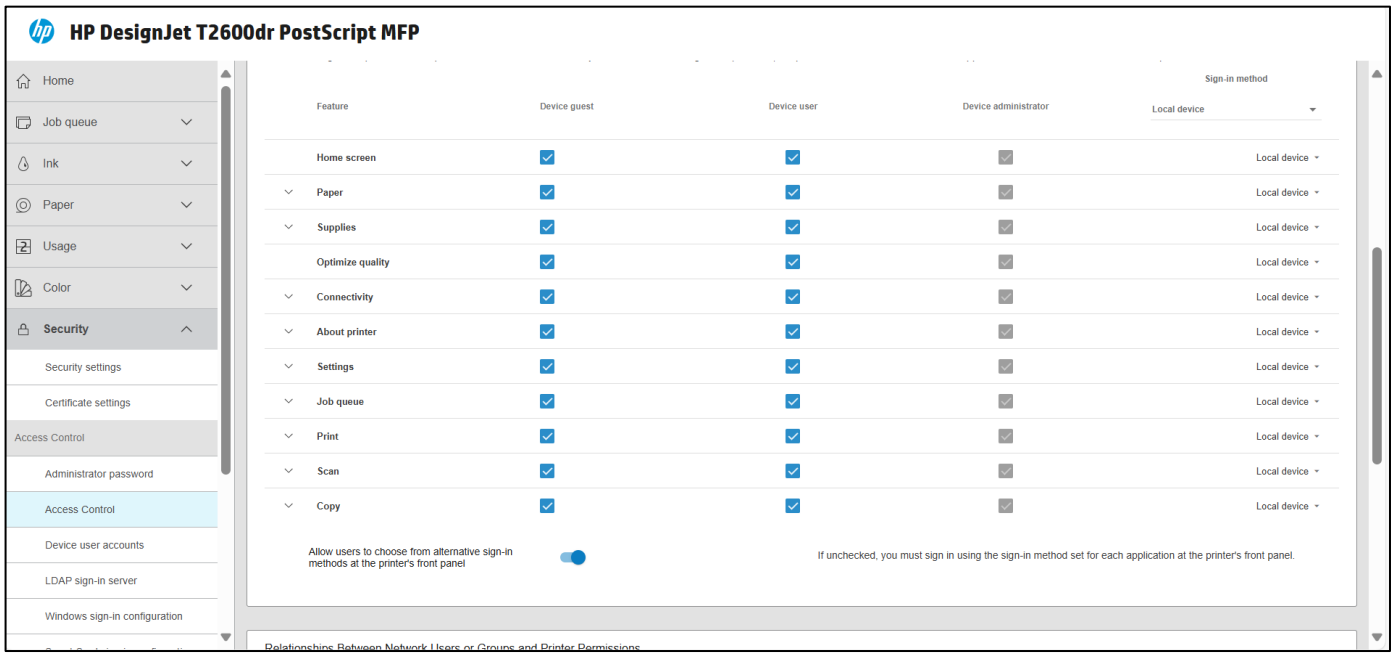
Features: Print at high speed over gigabit networks

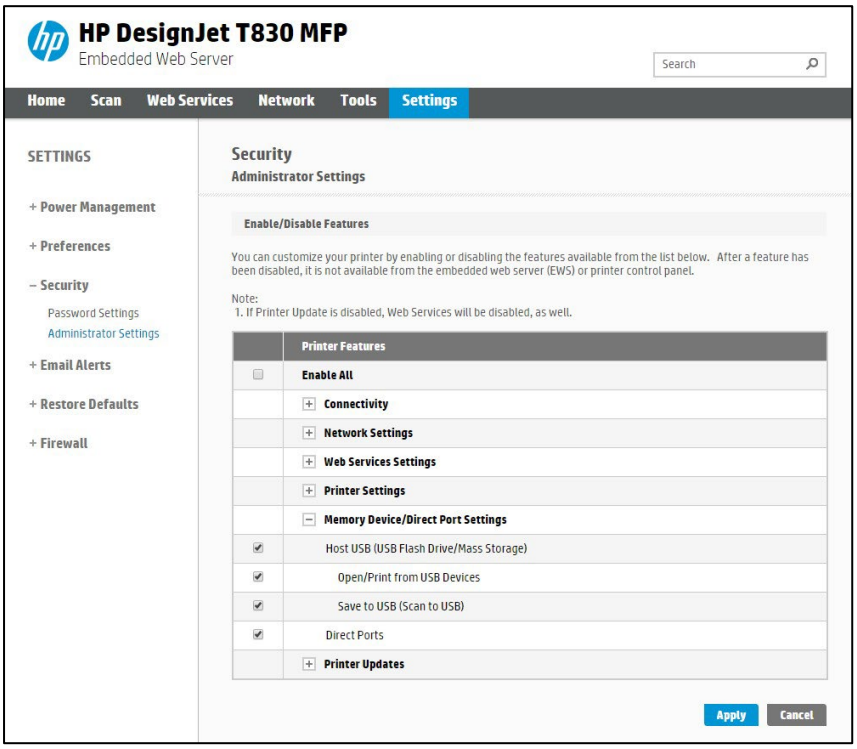
- Quickly connect to shared printers and MFPs throughout your office, over a gigabit network.
- Maintain rigorous standards through IPv6 network features: more IP addresses than IPv4 and IPsec security.
    - Help reduce administration and operation costs with off-the-shelf functionality and backward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







Control Panel Access

The DesignJet and PageWide technologies allow the printer administrator to lock 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:

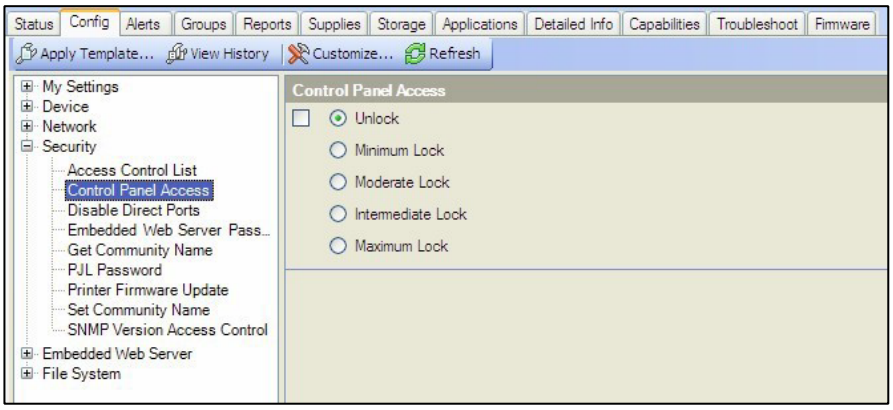
- Network connectivity & Internet connectivity
- Control firmware upgrades
- Reset factory defaults
- External hard disk connection
- Security

2.2.1 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:



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:

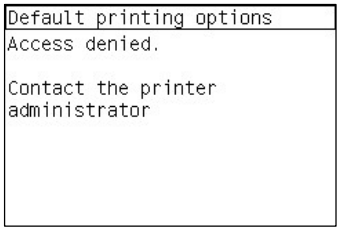
Actions	Permission denied if FP lock level is at least:
Settings App Access	4 - Maximum
Connectivity App Access	4 - Maximum
Connectivity App Details Access	2 - Moderate
Settings App Internet connectivity	2 - Moderate
Settings App Connectivity Troubleshooting	2 - Moderate
IDS App Access	4 - Maximum
IDS 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

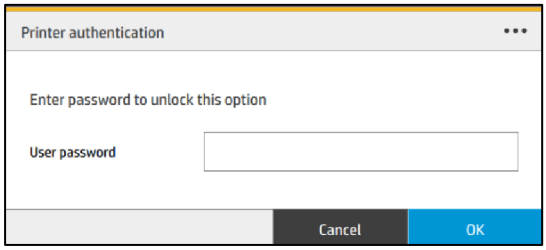
NOTE: When the Intermediate or Maximum locks are set, you will not able to load/unload paper or replace printheads/ink cartridges without first unlocking the front panel. These options should only be set in specific circumstances where the implications are known and understood.

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.



2.2.2 Access control

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

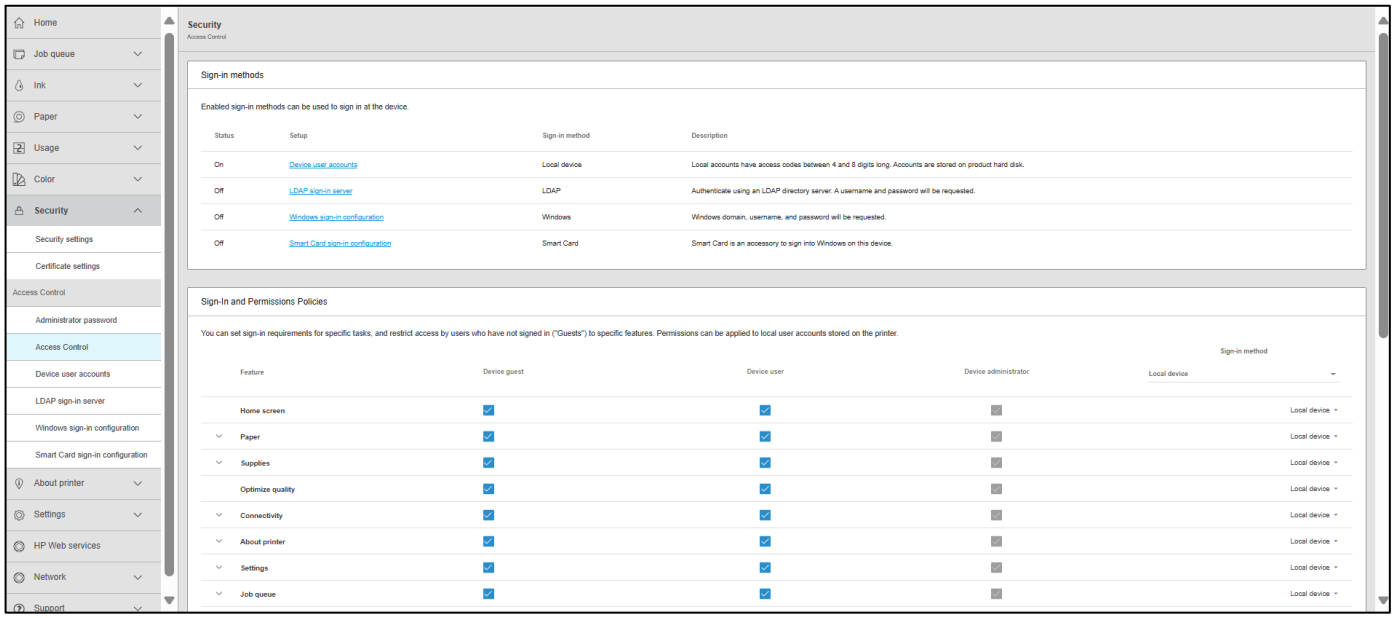
This function allows you to manage at least three roles of use (depending on the firmware version), defining which applications are available for each of them.

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.



a. Sign-in methods

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

Currently, sign-in methods are Local device, LDAP and Windows Sign-in (Kerberos).

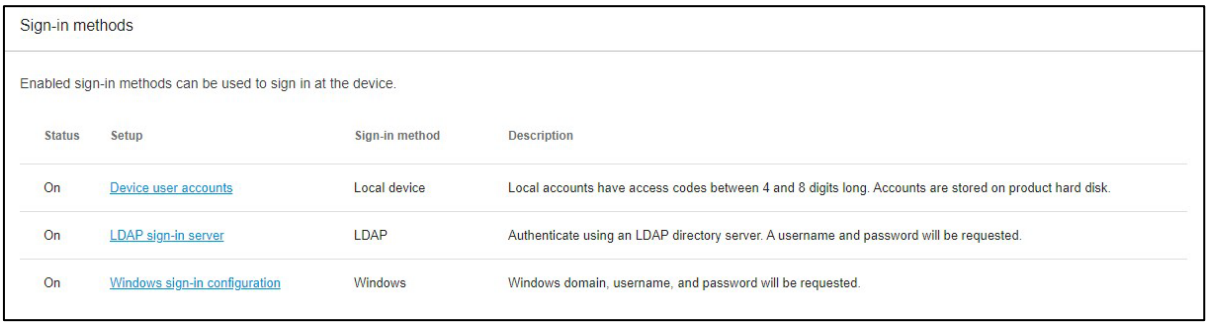


Figure 2 - Sign-in methods

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.

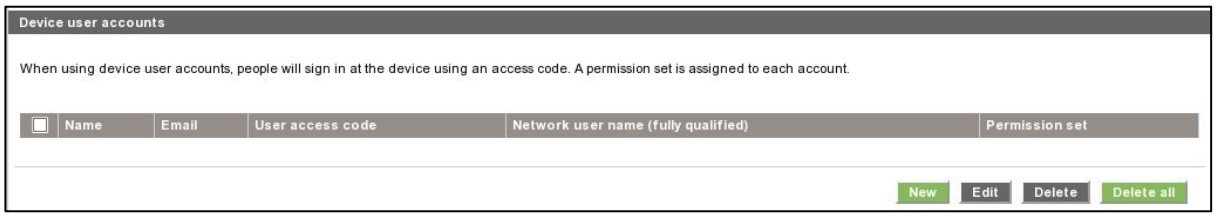


Figure 3 - Empty user accounts list

To add a new user:

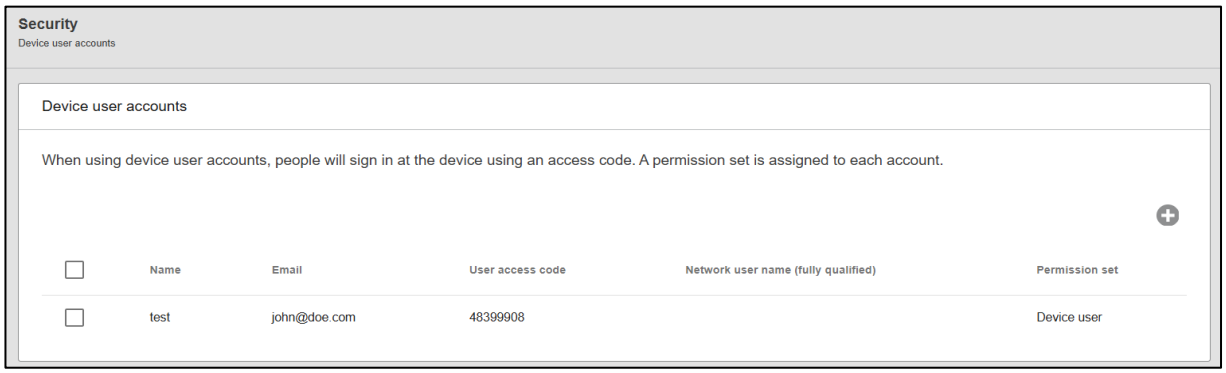
- Click the New button; a section is expanded. It is required to fill in the name and password fields.
- It is possible to change the User access code and the Permission that is set. You can select from the following permission roles.

User type	Role details
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.



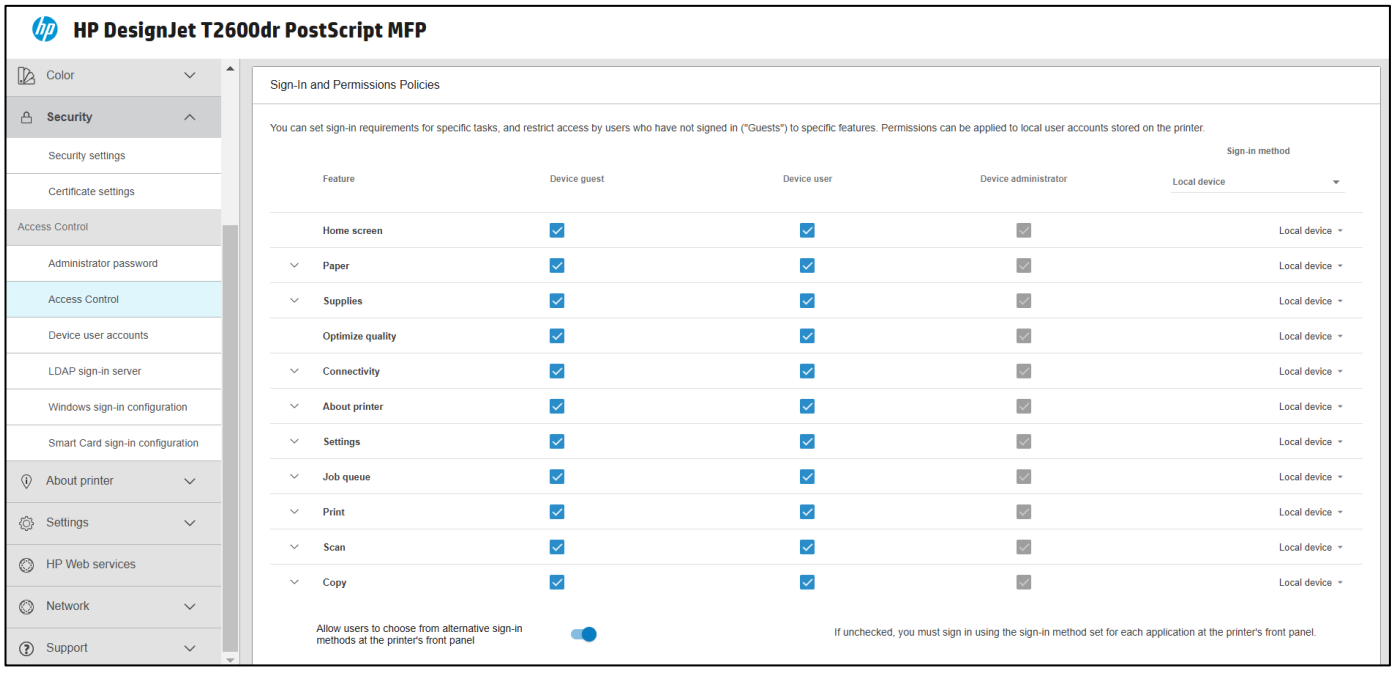
Figure 4 - Creating a user account

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



c. Sign-in and permissions policies

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



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.

2.2.3 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.

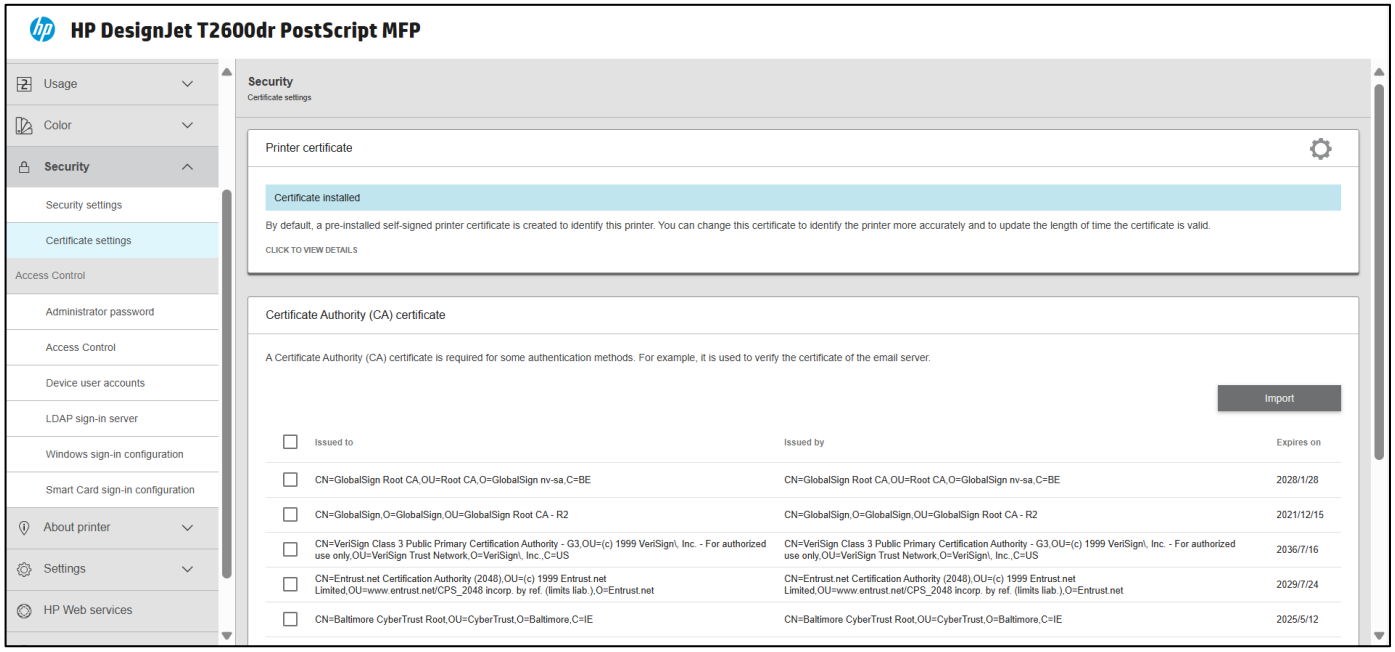
NOTE: If the printer's front panel becomes locked and you are unable to unlock it, then you should contact HP support as soon as possible.

SCL certificates

- Jetdirect identity certificate

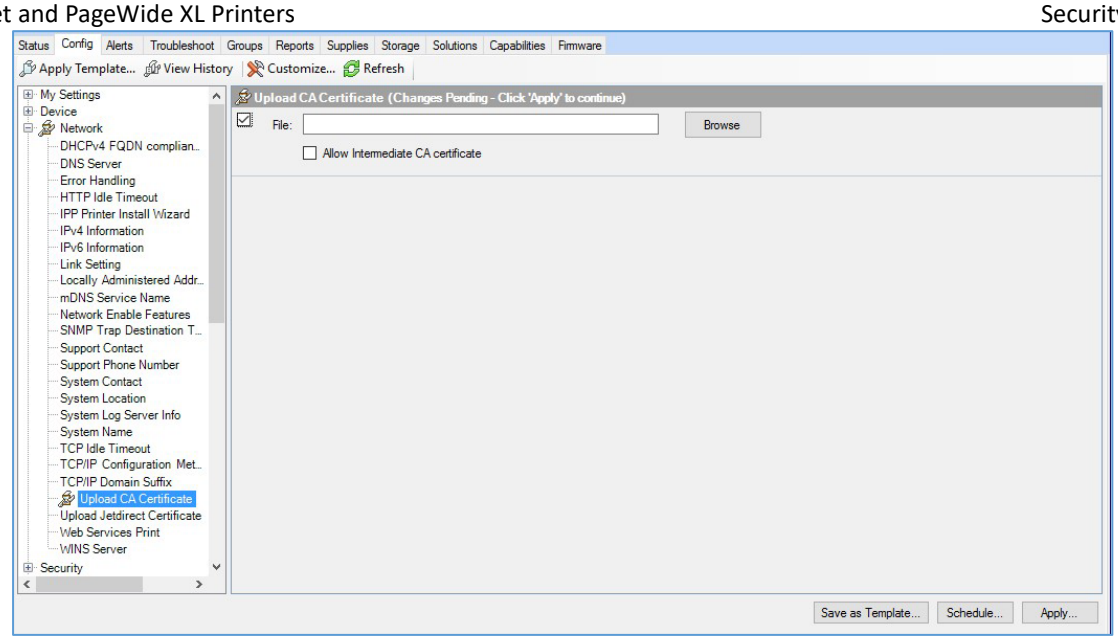
  You can request, install, and manage digital certificates on the HP Jetdirect print server. Certificates are used to identify the Jetdirect print server both as a valid web server for network clients, and as a valid client requesting access on a secure network. By default, the Jetdirect print server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

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



- 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 ker servers secured with SSL.



Unique Admin password for EWS access control

New regulatory policies in some states worldwide state that governmental devices should have a non-blank default administrative password and that all printer administration/configuration resources should be protected by an admin password.

For this reason and to increase HP LFP Printers default security level, HP DesignJet and PageWide Printer Series now come with a new Security feature, the default unique admin password. This feature is currently only present in DesignJet and PageWide printers listed in the below table but will be extended to further products. A default admin password will be assigned at manufacturing stage to all HP DesignJet and PageWide Printer Series printers going forwards that is unique for every printer.

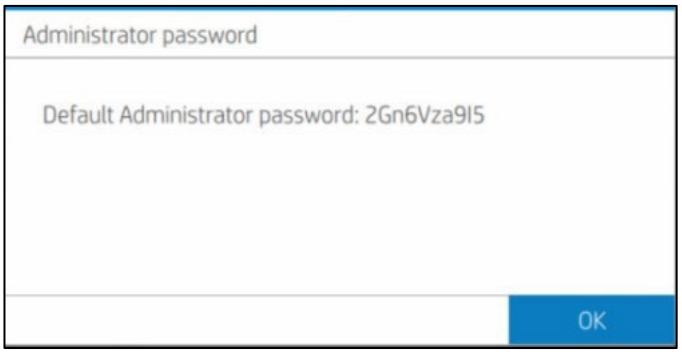
Similarly, to other technical devices, this default admin password is already set when the user purchases the product. Depending on the printer model the default admin password may be found in different places. In some models this password can be located on a sticker on the rear of the printer. In other models the user will have a front panel menu option to obtain this default admin password. By referencing the below table, you can see where to find your printer's unique default password and steps on how it can be changed/customized in each case.

DesignJet and PageWide Printer Series	Location of default Admin password

PageWide XL 3920 MFP PageWide XL 4200 Printer/MFP PageWide XL 4700 Printer/MFP PageWide XL 5200 Printer/MFP PageWide XL 5200 Printer PageWide XL Pro 5200 Printer/MFP PageWide XL 8200 Printer/MFP PageWide XL 8200 Printer PageWide XL Pro 8200 Printer/MFP PageWide XL Pro10000 Printer DesignJet Z6 Pro Printer DesignJet Z9+ Pro Printer	Front panel of the printer Settings Menu --> Security --> Administrator password:
HP DesignJet T200/600/Studio Printer	On the serial number label located on the back of printer

Using the Front Panel to discover the default admin password.

Using the Front Panel, navigate to Settings Menu > Security > Administrator password:



It can also be discovered from the Front Panel through Printer Information:



When the default admin password is modified, under these menu paths you will see: Administrator password "Your password has been modified by the administrator, in case you lost it and need to recover, please contact your HP Service Representative"

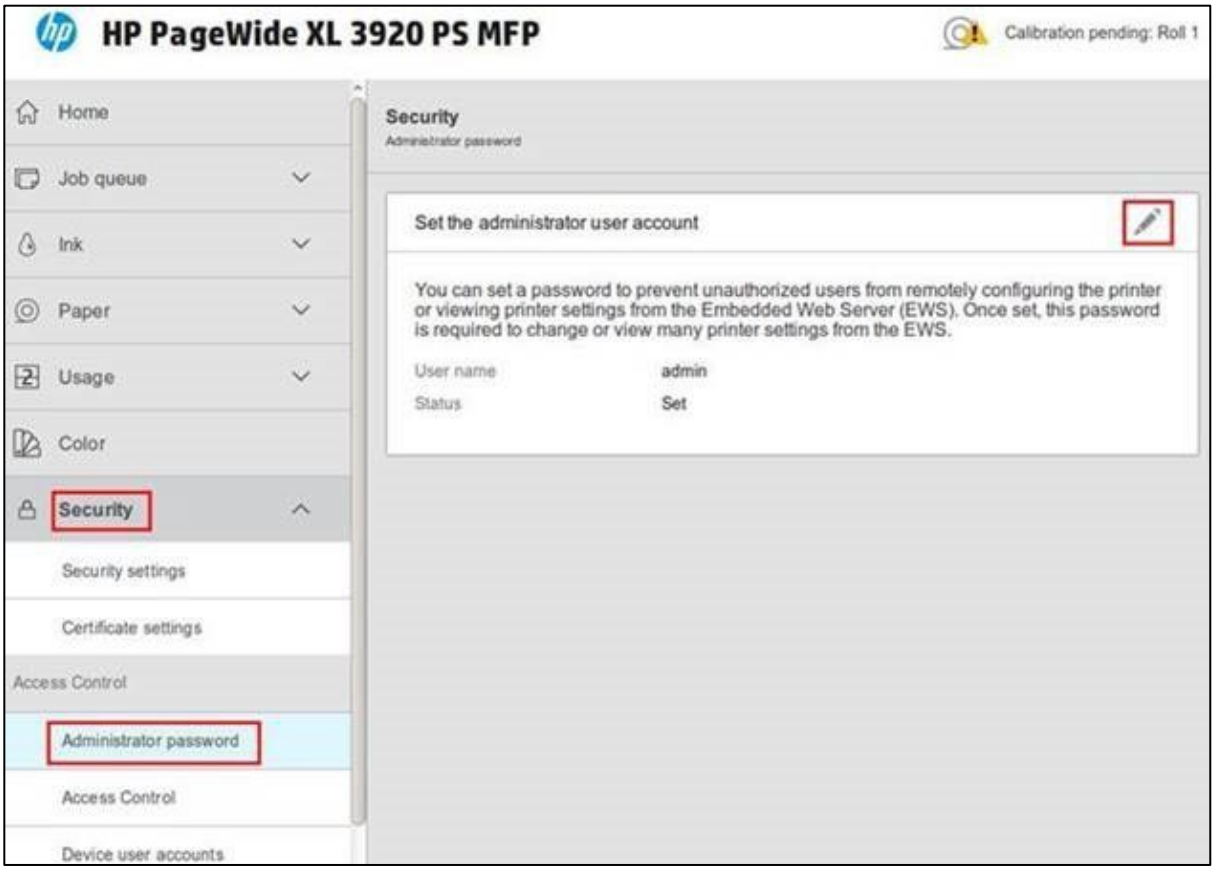
NOTE: This is only an example. In every LFP printer the default admin password will be different.

2.2.4 How to change my printer's default admin password

The printer's admin password can be changed for any of your own (except a blank password). The process to change admin password can be performed in different ways.

Printer users can change the admin password through the web browser going to:

Settings > Security > Administrator password > Click on the Pen Icon:



A new window will ask both the default admin password and the new admin password. Note that the new admin password will have no constraint except that blank passwords are not allowed.

The admin password will remain between reboots.

NOTE: Default User name: admin

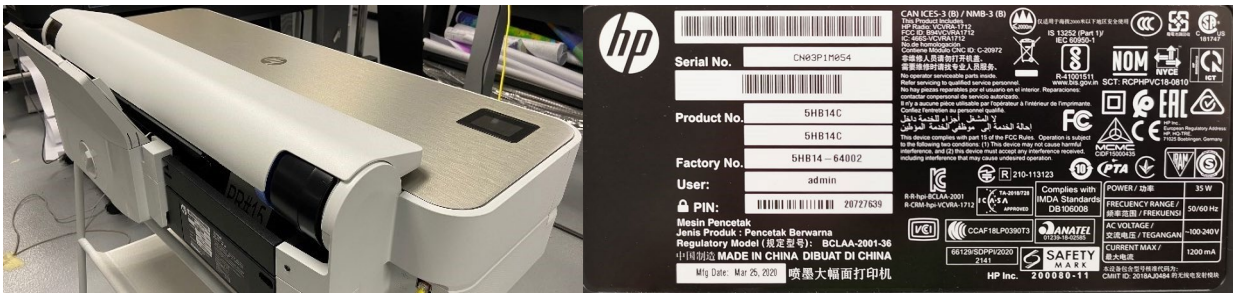
2.2.5 Reset admin password to default

In printers where the Unique Admin Password can be found on the printer front panel, users cannot reset the admin password to the default without assistance. If, for any reason, the customer admin password of the printer is not known, it is necessary to call a service representative to reset this password.

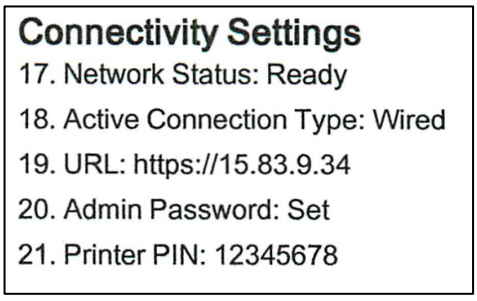
Only developers and servicing personnel will be allowed to reset admin password. *Unique Admin Password on printer label*

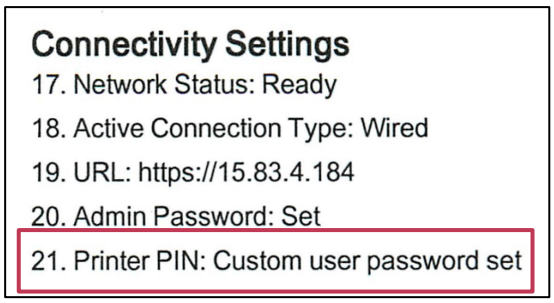
Some Printer models are not able to display the unique admin password on the printer front panel and are therefore shipped with the default unique admin password on the printer label. These models can be identified from the above table. In these printer models there are 2 ways to find the default EWS password:

1. A label on the back of printer.



2. "Printer PIN" on "Printer Status Report". Printable from front panel if it has not been changed from the default. If you change the PIN, the status report will no longer show it. It will show "Custom user password set" in the report instead.





NOTE: Default User name: admin

In printer models where the default admin password is found on the printer label it is possible to reset the admin password to its default through a factory rest of the printer.

Perform Setup > Printer Maintenance > Restore > Reset Factory Default

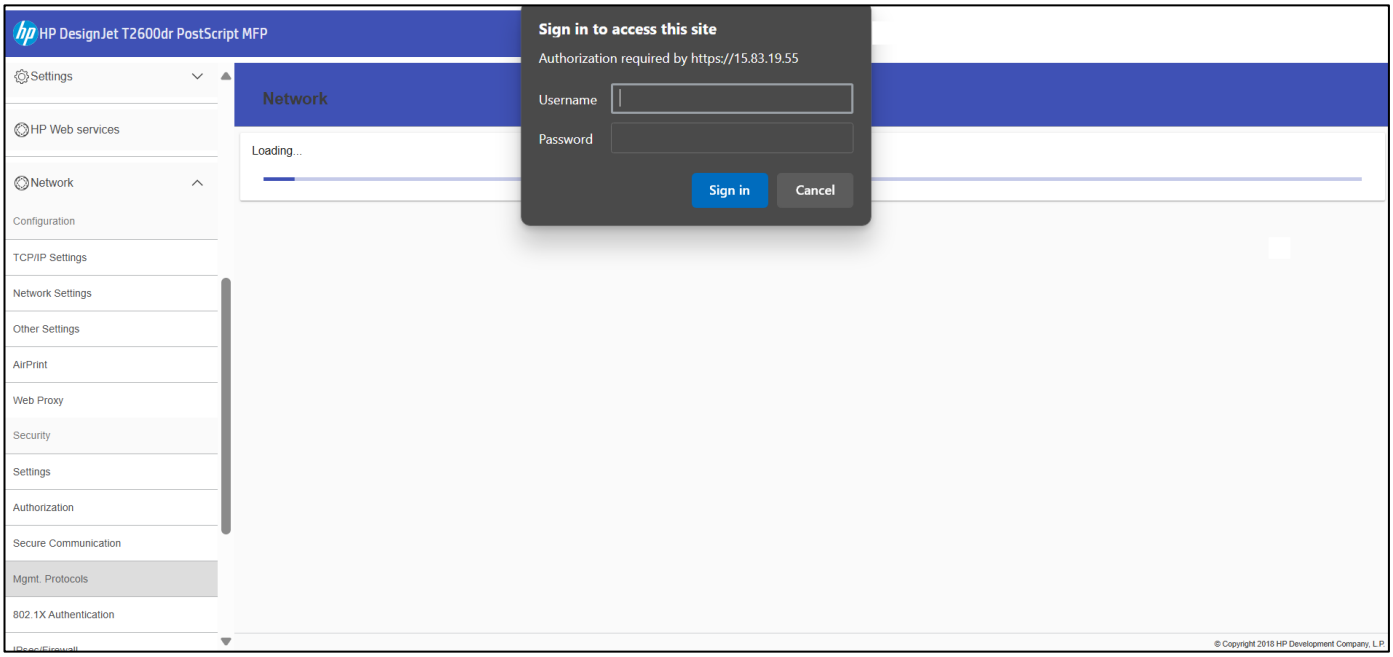
Embedded Web Server (EWS) access control

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).

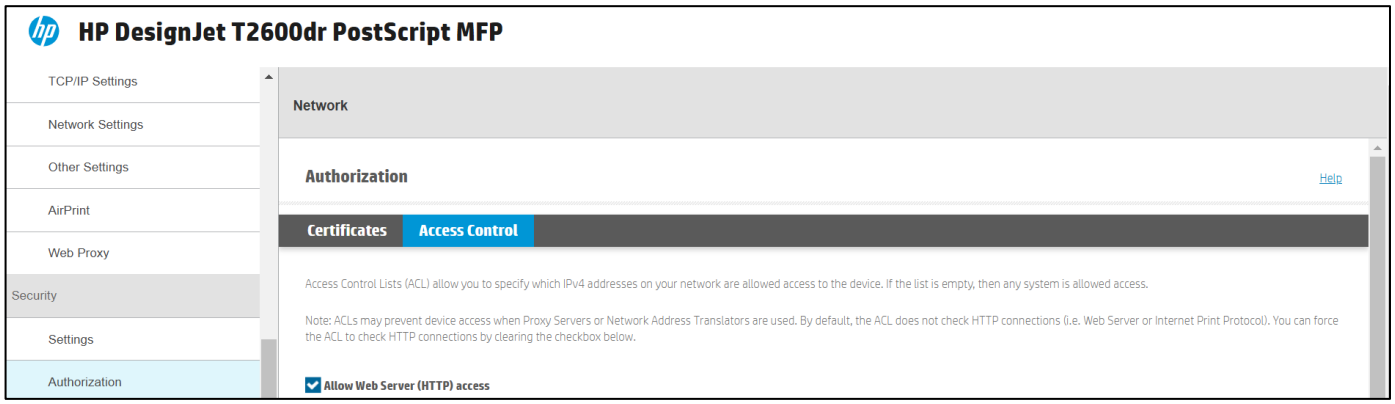
If the two levels of access have been set, and you have neither of the passwords, then you will not be able to gain access to the EWS information, as in the image below.

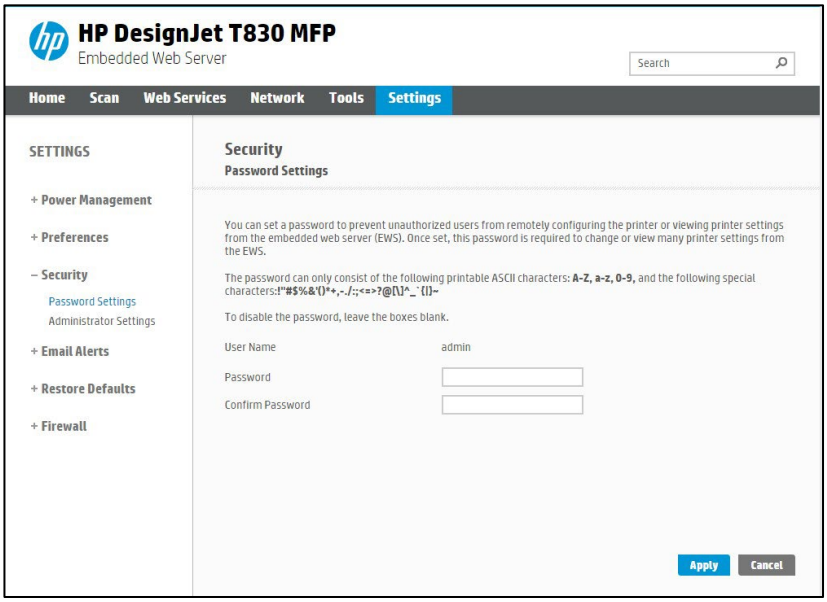


2.2.6 Administrator password

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.





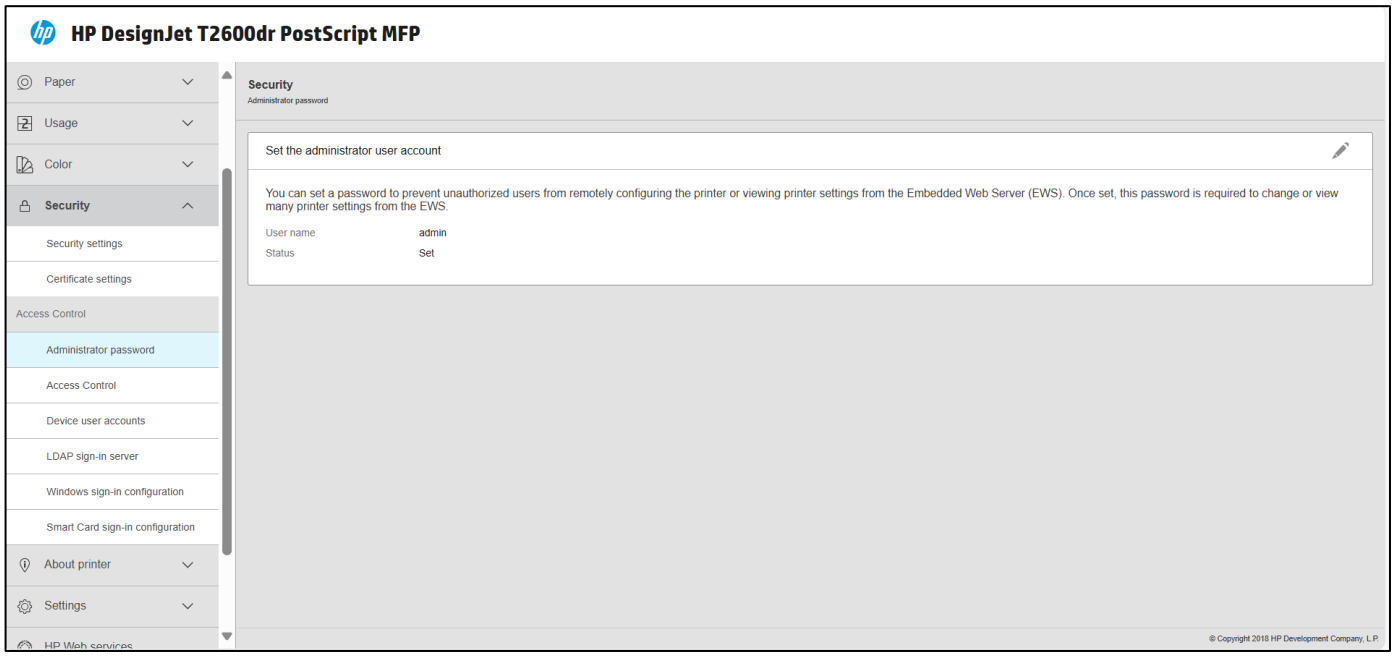
If there is no administrator account, then the restricted operations can be accessed without a password.

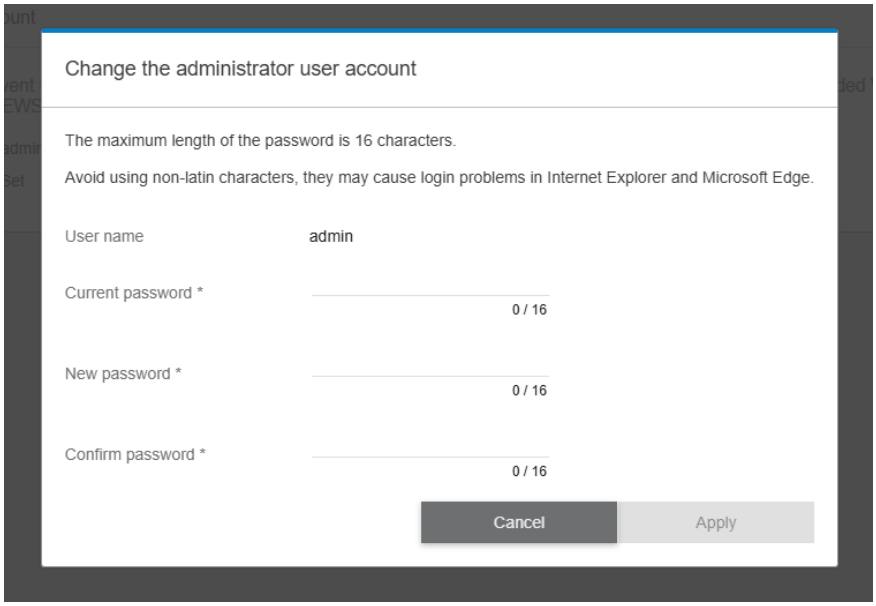
2.2.7 Guest password

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.

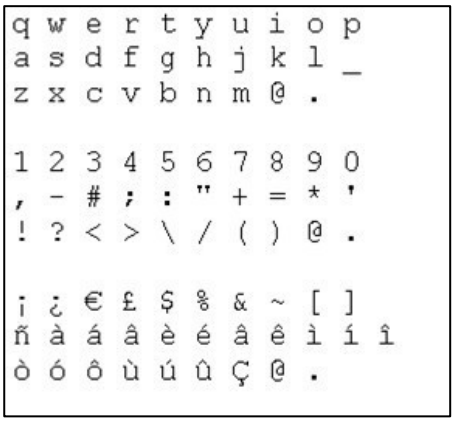
If the guest account is not set up, a username and password are not required for unrestricted operations.





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).



- 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.

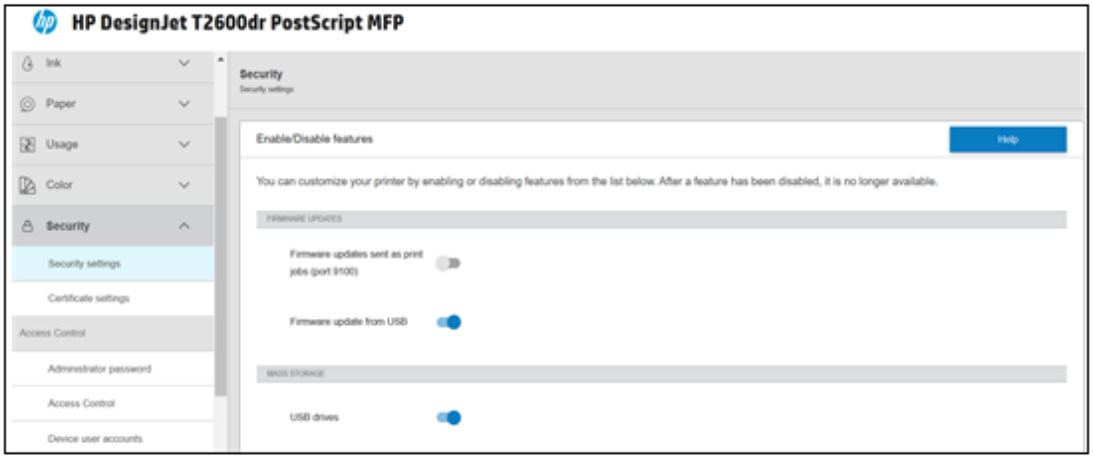
USB drive control

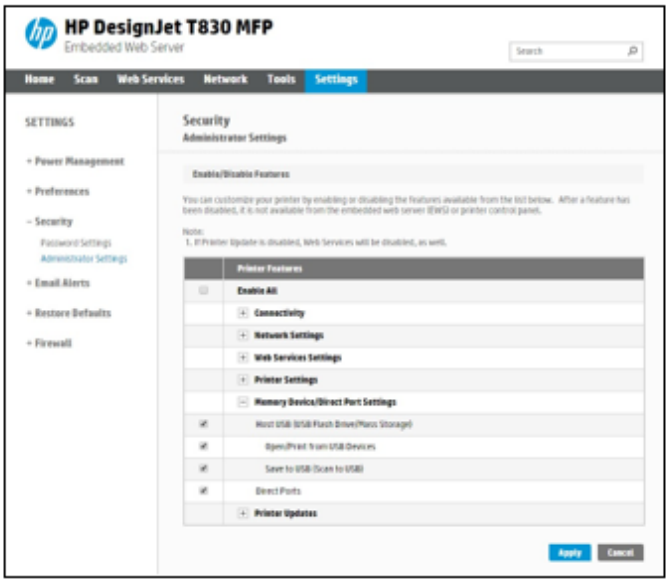
All printers allow you to control the USB use, in two ways:

- 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.



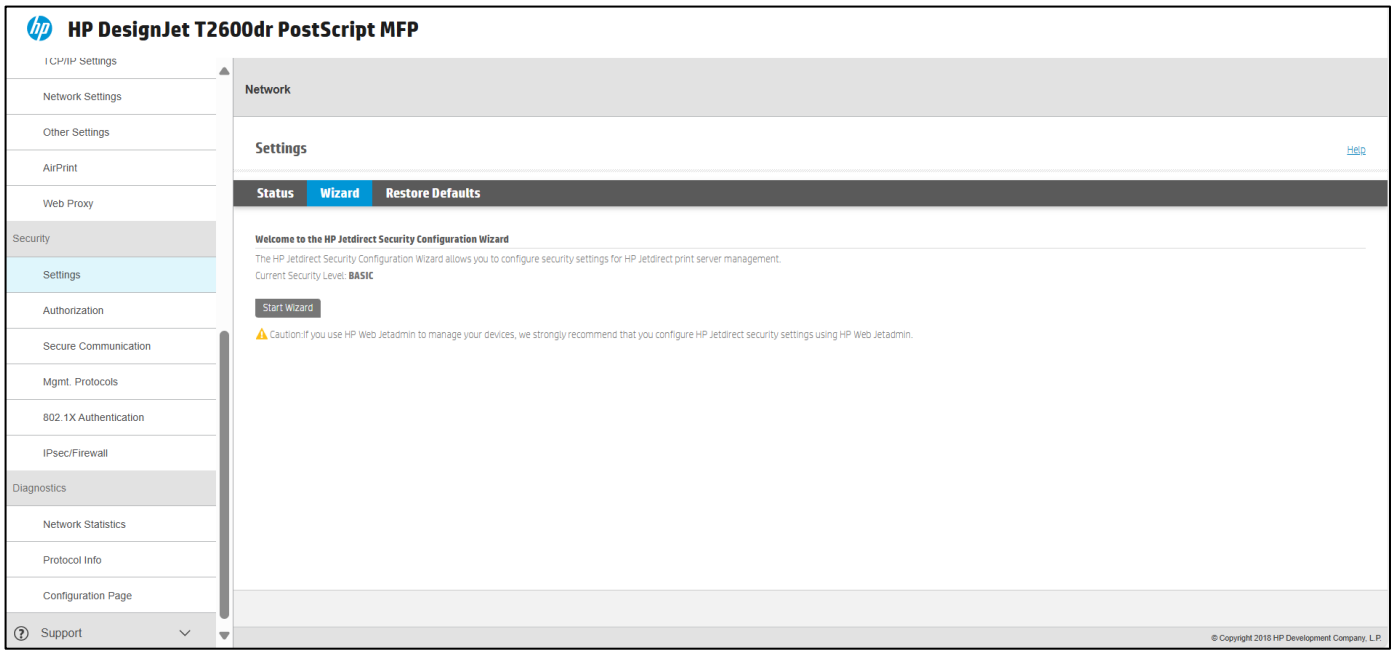




Jetdirect Security Wizard (HP T9x0-T15x0-T25x0-T3500-PageWide XL)

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:

Security level	Details
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.



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

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.

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.

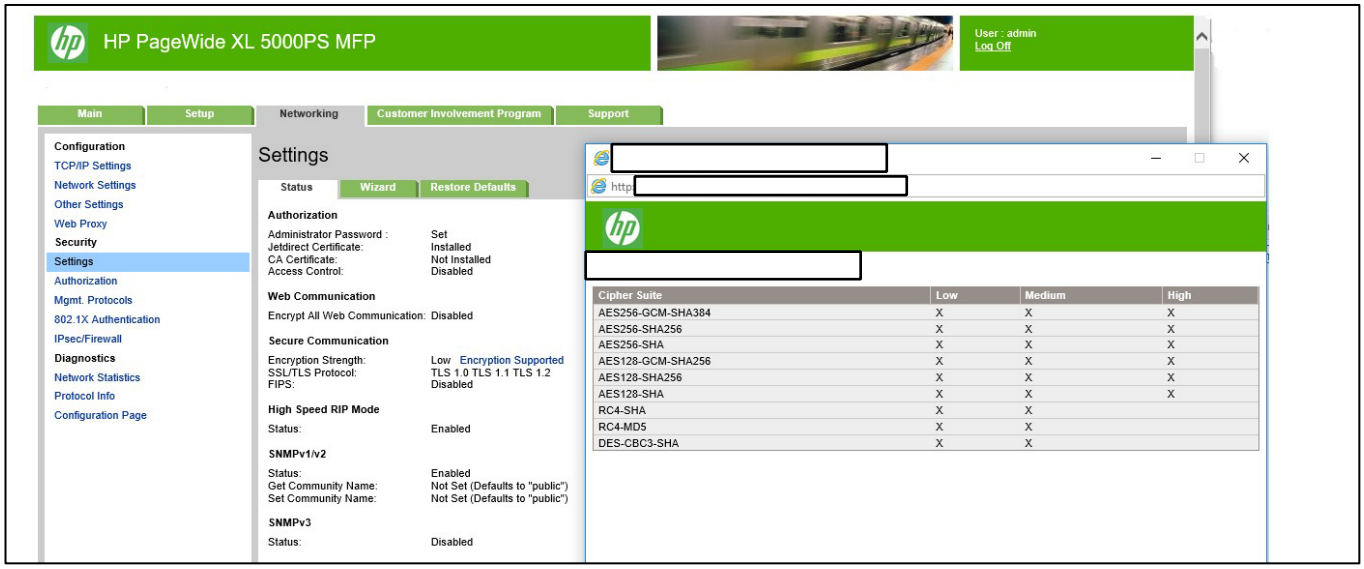
Firewall. Use this page to view or configure a firewall policy. A firewall policy consists of up to 10 rules, where each rule specifies the IP addresses and services that are allowed by the print server and device. To add a rule, click Add Rule. This setting runs a wizard that will help you to configure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

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. SSL/TLS Protocols used in the communications can be configured in the printer's EWS. Supported cipher suites can also 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.

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.

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

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.

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).

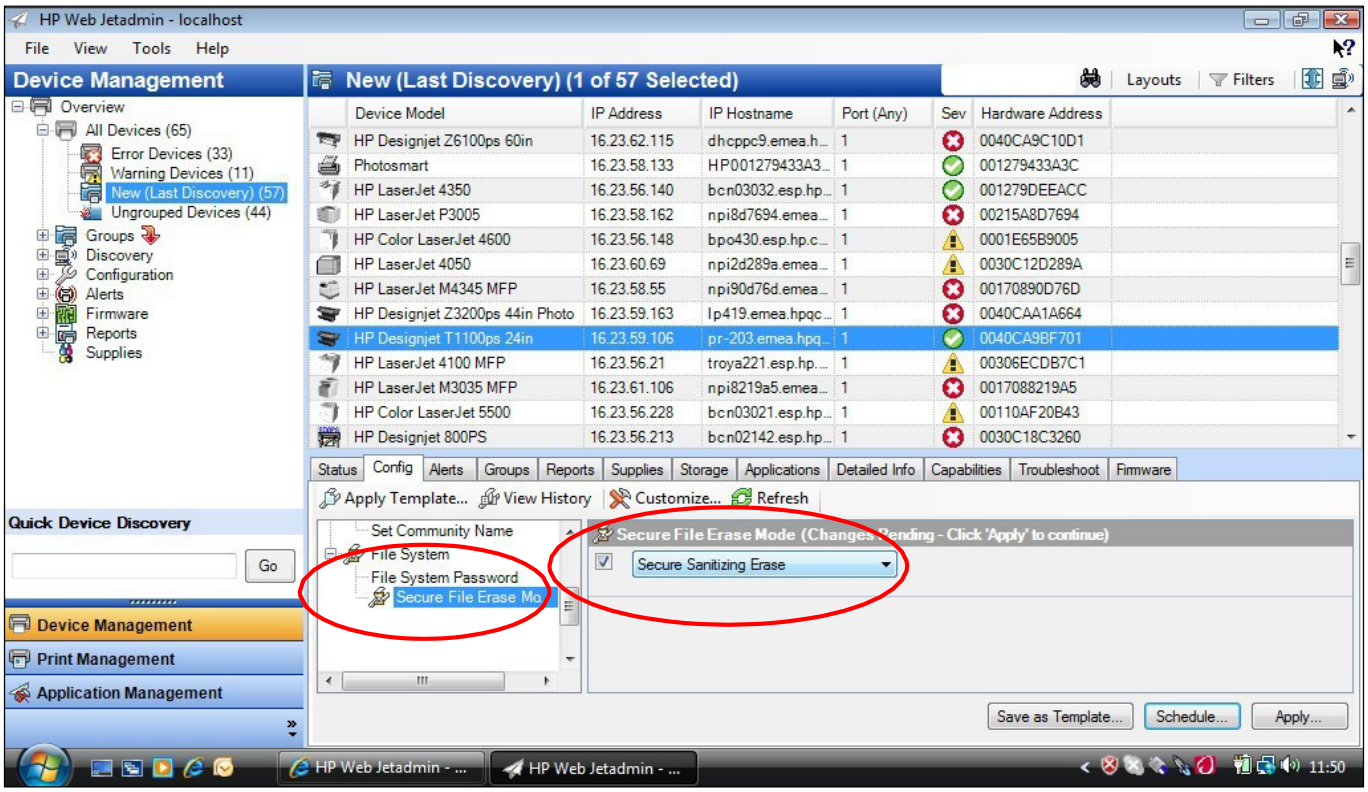
- Non-Secure Fast Erase: In this mode, all file pointers to the data (table indexes) are erased. Temporary data remains on the Hard Disk Drive until the disk space it occupies is needed for another purpose, and is then overwritten. This is the fastest mode of operation and is the default for all printers.
- 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.

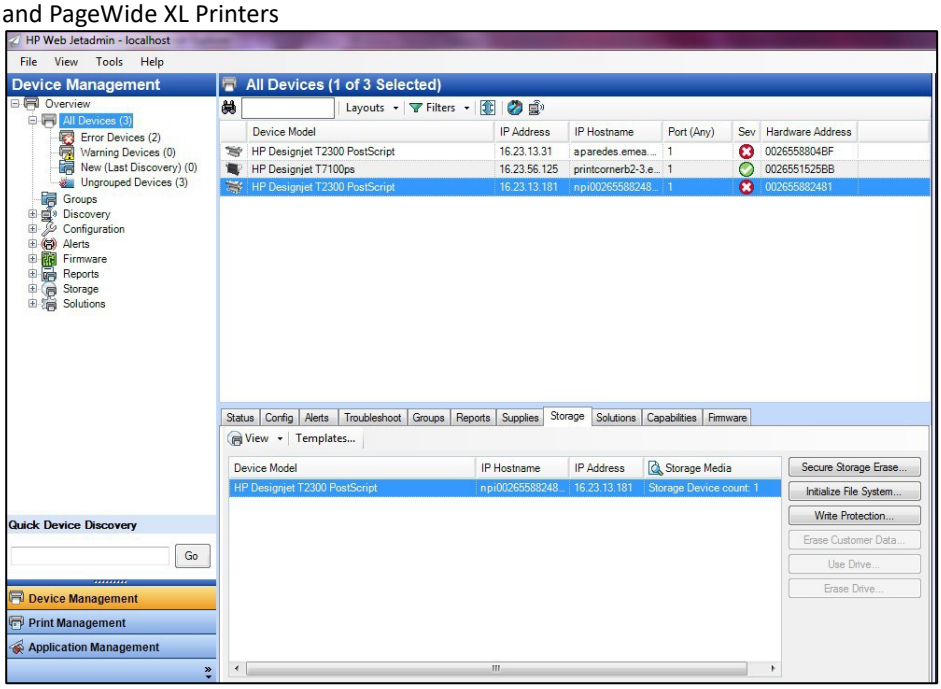


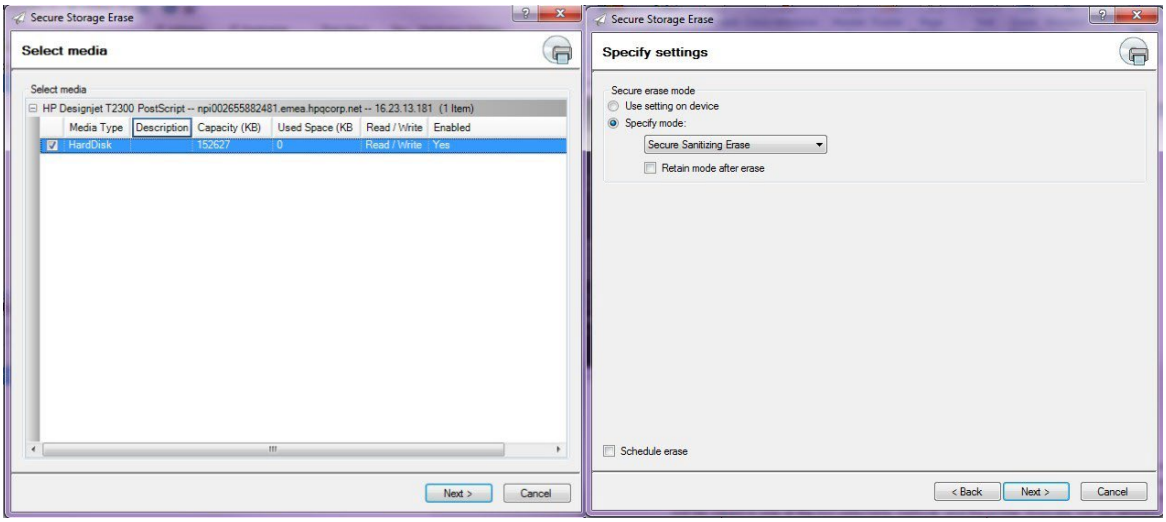
Secure Disk Erase (SDE)

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.





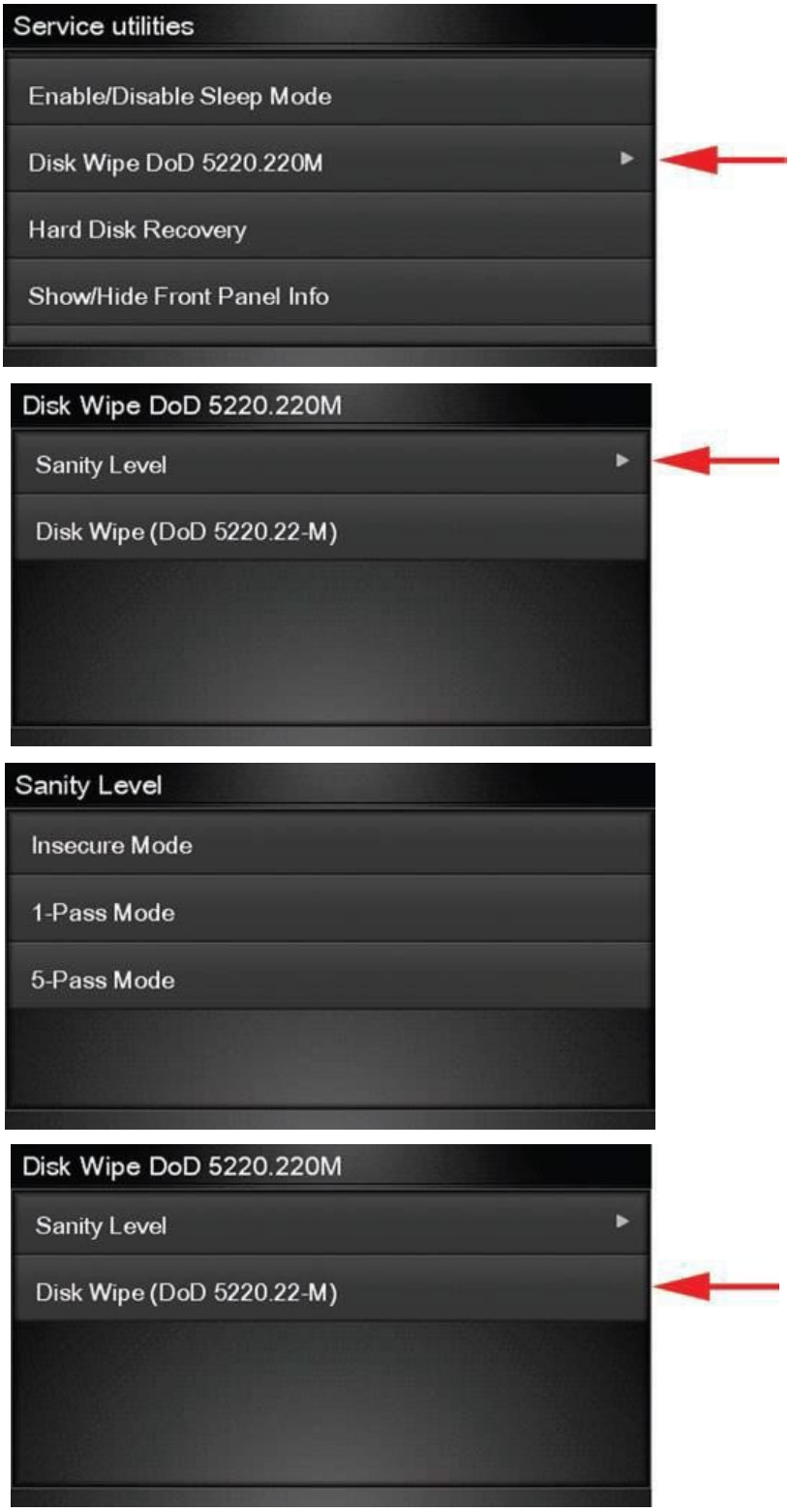
- Printer Front Panel access: Once you have entered the Service Menu with the help of an HP Support representative, you can perform the Secure Disk Erase using the same 3 options that you have in Web Jetadmin. Note that the name of the feature in the front panel is Disk Wipe DoD 5220.220M, and that the 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 time that this action will take depends on the amount of information stored on the HDD, the printer model and the option selected to perform it. The average time is:

Insecure Mode: 1 minute
1-pass mode: 2 days
5-pass mode: 2 weeks

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



Scan to network (HP DesignJet T2500, T2530, T3500, T2600, XL3600 eMFP Series)

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.

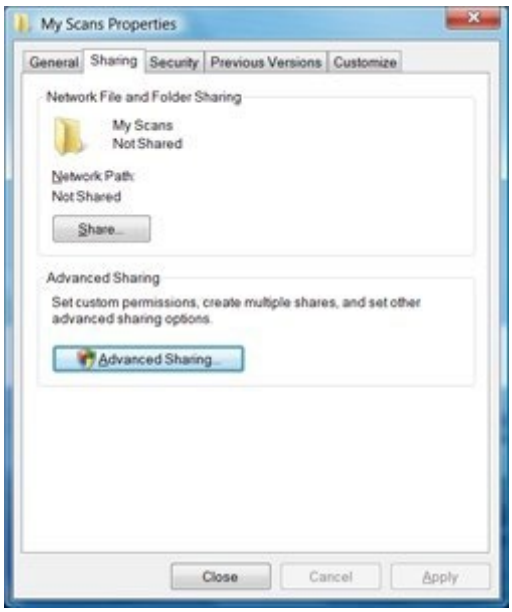
5. In the printer's Embedded Web Server, select Network folders inside the settings menu.
6. On the Scan to network page, click Add folder details, and fill in the various fields.
   - The Server name should contain the network name of the remote computer. This remote computer must be connected in the 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.

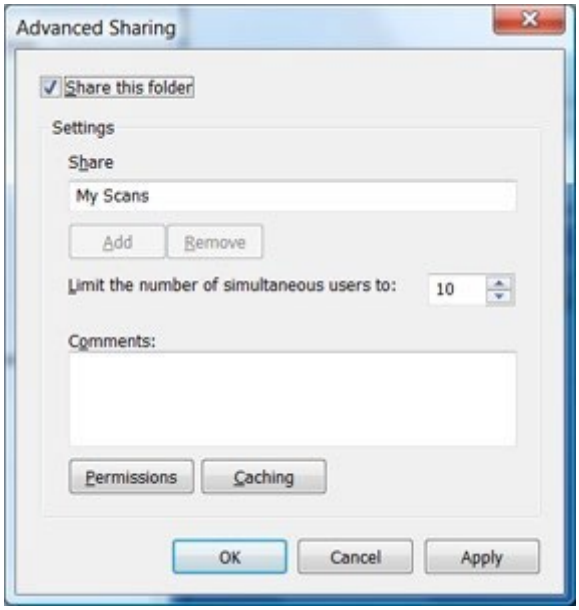
   The printer automatically checks that it can access the network folder.

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

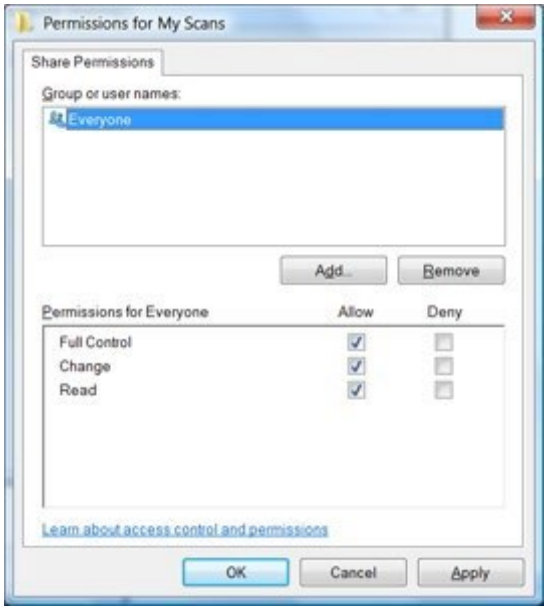
1. Create a new user account for the *scanner user* on the remote computer. You can use an existing user account for this purpose, but it is not recommended.
2. Create a new folder on the remote computer (unless you want to use an existing folder).
3. Right-click the folder and select Properties.
4.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



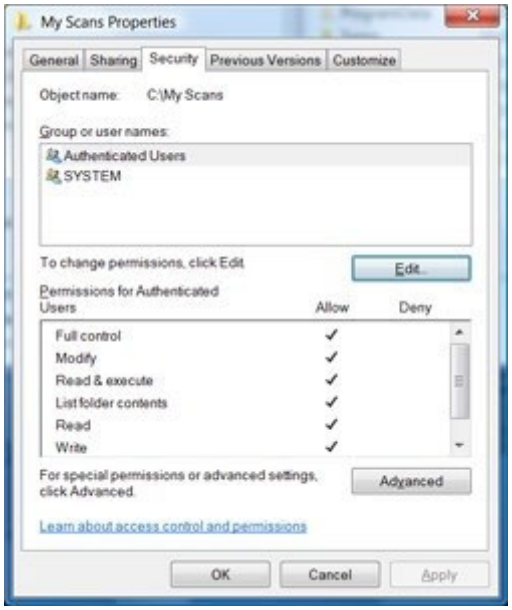
5. Check the Share this folder box.



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 Security tab. Only some file systems such as NTFS require this.



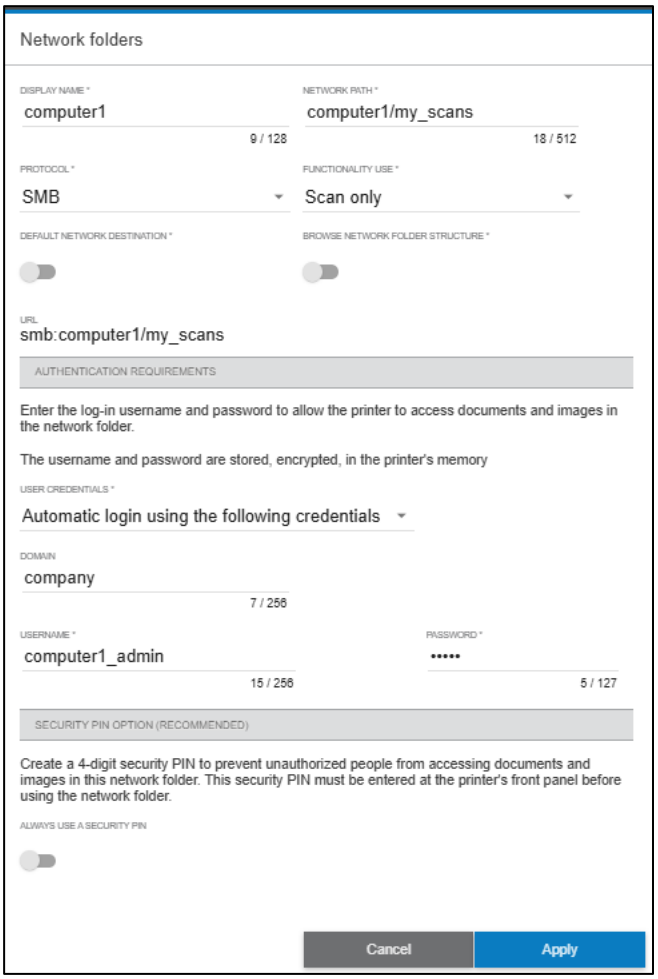
The *scanner user* can now access the folder and write files to it. Next, you must configure the printer to send scans to the folder.

8. In the Settings menu, select Network folders:



9. Click +:

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



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.

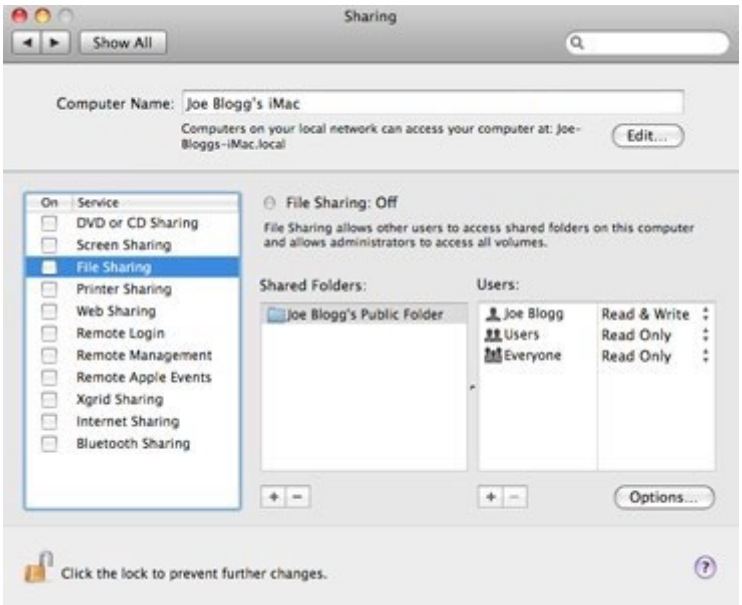
    You can check at any later time that the shared folder remains accessible by clicking Verify in the Embedded Web Server. A correctly configured shared folder can become inaccessible if the user's password is changed, or if the shared folder is moved or deleted.



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. In the Settings menu, select Network folders.
9. Click +.

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

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.

2.5.1.1 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.

Notes:

- 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, Kerberos, NFS and SSPI protocols.
- Scan to Cluster Server environment is supported in newer printers regardless if DFS is installed or not. Previous MFP series do not support scan to cluster server environment. You can check the current models that support this feature in the following table.

Printer model	Product Number	Scan to Cluster Server environment supported
HP DesignJet T2600 36-in Multifunction Printer	3XB77A	Yes
HP DesignJet T2600 36-in PostScript Multifunction Printer	3XB78A 3XB78F	Yes
HP DesignJet T2600dr 36-in Multifunction Printer	Y3T75A	Yes
HP DesignJet T2600dr 36-in PostScript Multifunction Printer	3EK15A 3EK15B 3EK15F	Yes

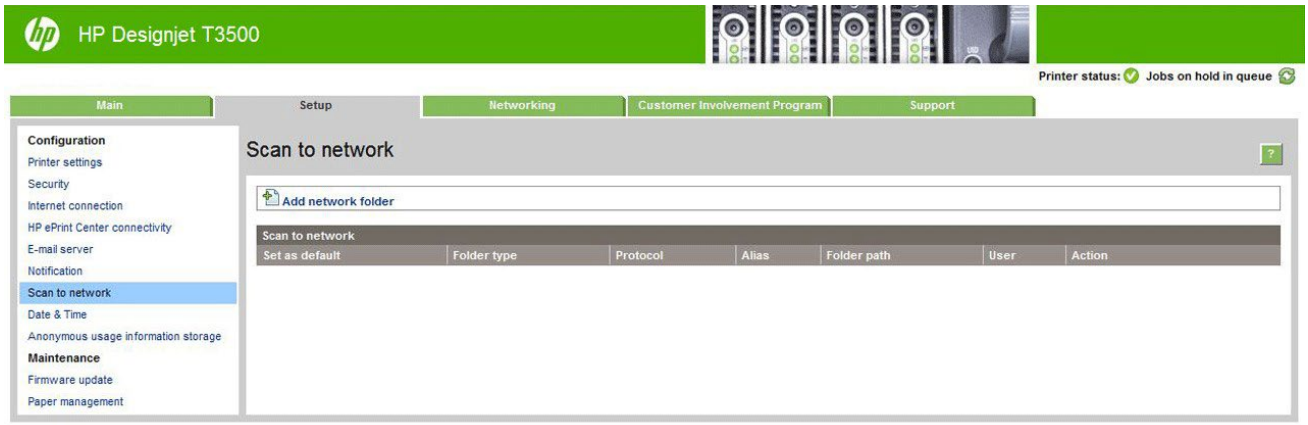
HP DesignJet XL 3600 36-in Multifunction Printer	6KD23A 6KD23G 6KD23H 6KD23F 6KD23L 6KD23M 6KD23N	Yes
HP DesignJet XL 3600 36-in Multifunction Printer PS	6KD24A 6KD24G 6KD24H 6KD24F 6KD24L 6KD24M 6KD24N	Yes
HP DesignJet XL 3600dr 36-in Multifunction Printer	6KD25A 6KD25G 6KD25H 6KD25F 6KD25L 6KD25M 6KD25N	Yes
HP DesignJet XL 3600dr 36-in Multifunction Printer PS	6KD26A 6KD26G 6KD26H 6KD26F 6KD26L 6KD26M 6KD26N	Yes
HP PageWide XL 3920 Multifunction Printer HP PageWide XL 4200 Multifunction Printer HP PageWide XL 4700 Multifunction Printer HP PageWide XL 5200 Multifunction Printer HP PageWide XL Pro 5200 MFP Printer HP PageWide XL Pro 8200 MFP Printer	4VW11A 4VW13A 4VW15A 4VW17A 4VW19A 4VW20A	Yes

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.

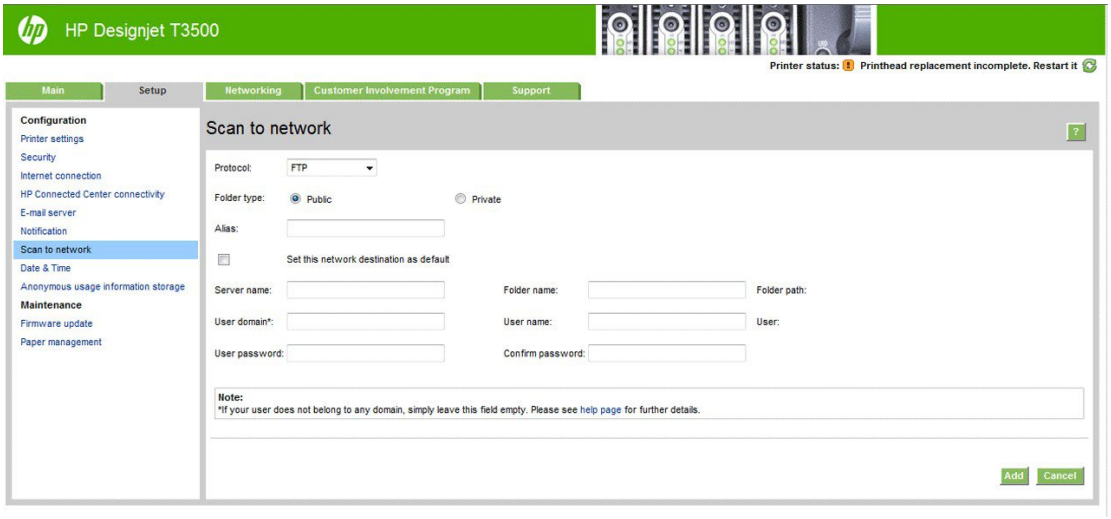
NOTE: You must complete the above steps for one option or the other before starting the remaining steps below.

3. In the printer's Embedded Web Server, select the Setup tab and then Scan to network. See *Access the Embedded Web Server*.



Alternatively, in the HP Utility, select the Settings tab and then Scan to network. See *Access the HP Utility*.

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. For more information, see *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 User Guide of the printer.

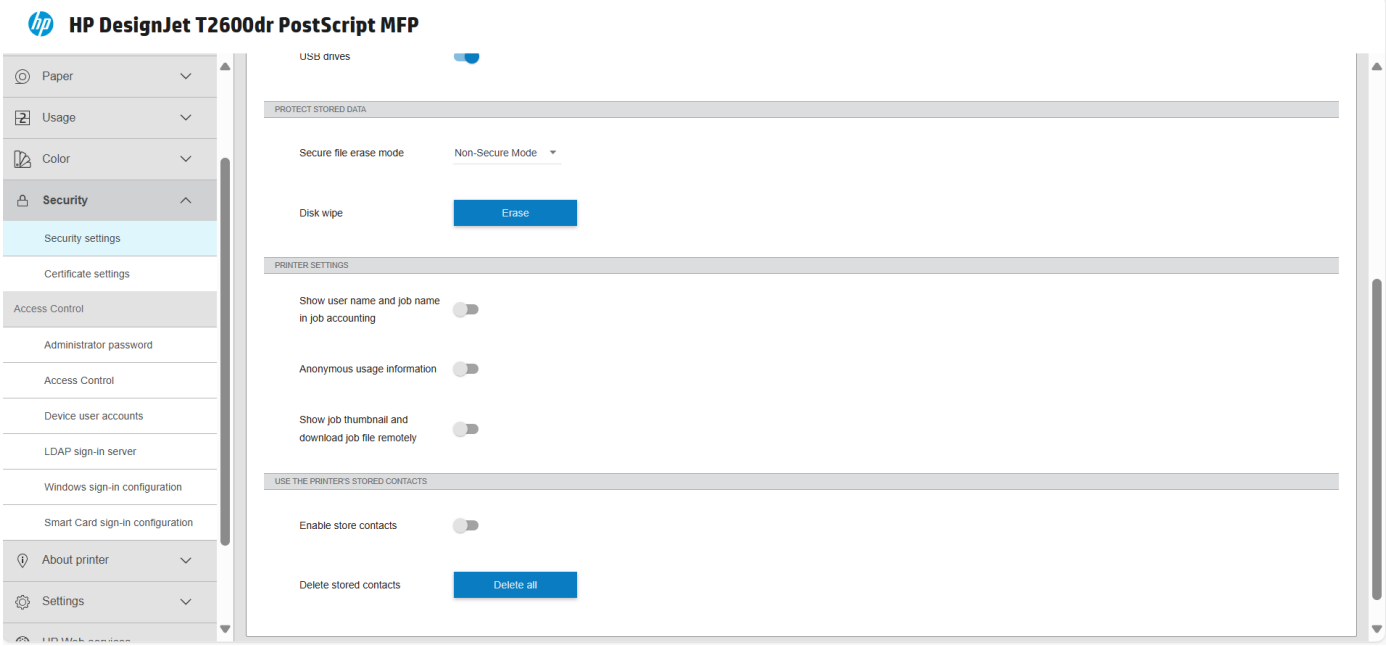
You can check at any later time that the shared folder remains accessible by clicking Verify in the Embedded Web Server. A correctly configured shared folder can become inaccessible if the user's password is changed, or if the shared folder is moved or deleted.

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.



Disable internet connection

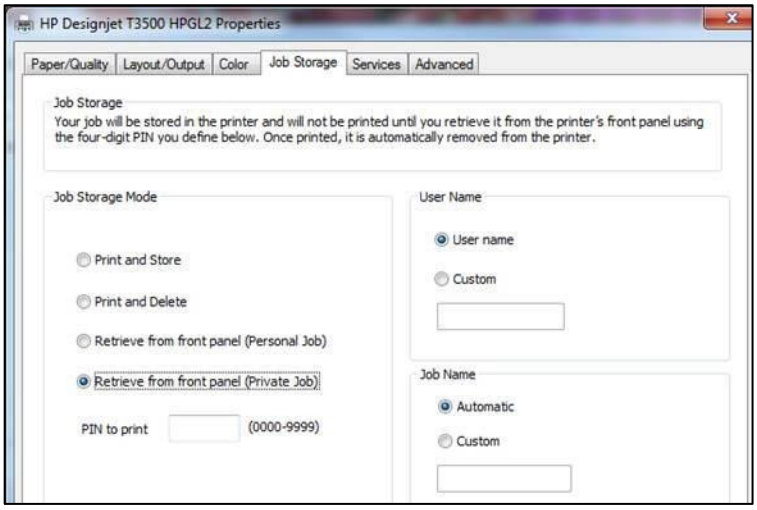
Disable the direct connection of the printer to the internet. This option also prevents the printer from automatically performing firmware upgrades.

2.6 Document security

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).

---

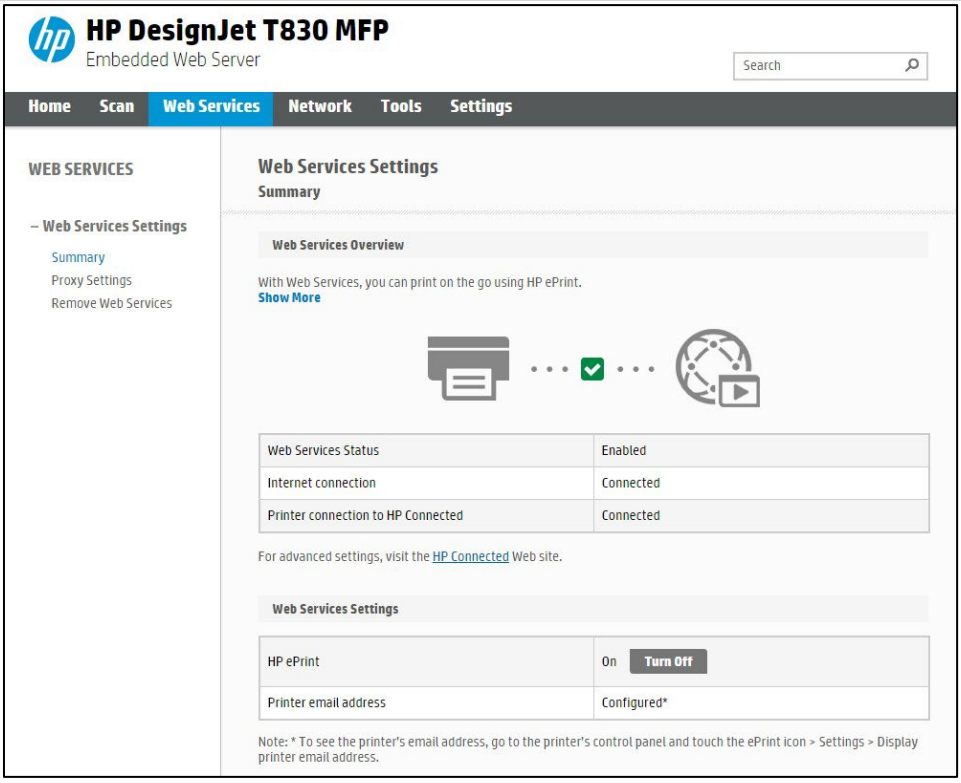
ePrint center connection

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.

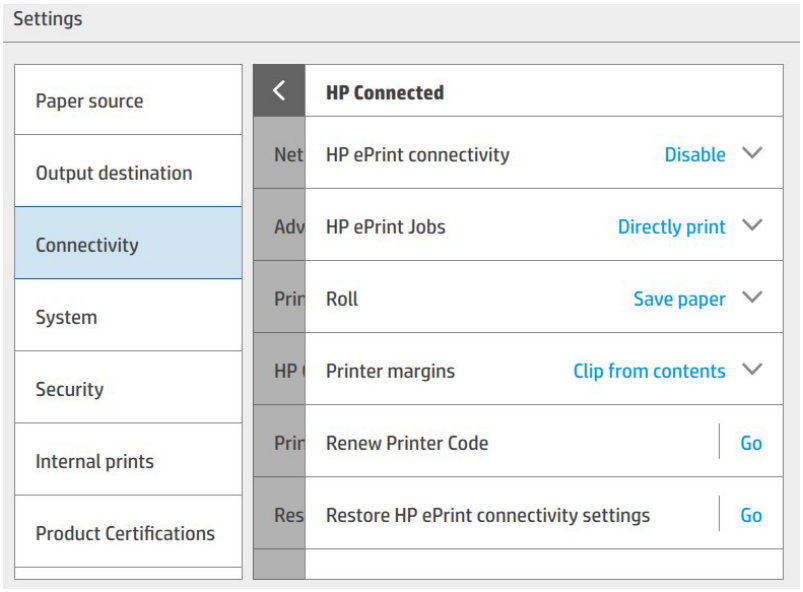






This functionality is disabled by default.

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. Advanced workflows

This section describes some advanced printing workflows that can be used to interact with the HP PageWide XL, DesignJet T1700, DesignJet Z6, Z6 Pro and DesignJet Z9+ and Z9+Pro printers.

3.1 Printing using LPR protocol.

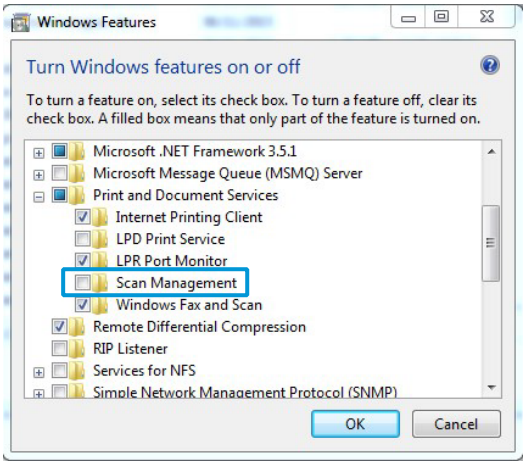
This feature allows you to print any supported file without drivers or other programs.

It can be useful to develop internal programs to manage production or to develop programs for operating systems without a driver.

The job sent using this method will be printed with the default settings, some options can be managed using PJLs. (See section 3.3, Print with PJLs)

This protocol must be enabled in the EWS or Web Jetadmin. If you do not use it, keep it disabled for security.

How to use the LPR command in Windows.



- Turn on the windows feature
    a. Go to Control Panel > Programs > Programs and Features > Turn Windows features on or off.
    b. Select the LPR Port Monitor from the list.
- Open a command window (search cmd in the Start menu).
- Use the command: Lpr -S *IP* –P *printer File name*
    a. IP Format: *xx.xxx.xx.xxx*
    b. Printer: any name you want to use.
    c. File name: including complete route.



*In this example, the file is located in C:\.

3.2 Printing using FTP protocol.

This feature allows you to print any supported file without drivers or other programs. It can be used through command line or as a drag and drop system, combined with any FTP client program.

As with the LPR command, it can be used for developing specific tools to simplify your workflow.

The job sent using this method will be printed with the default settings, some options could be managed using PJLs. (See section 3.3, Print with PJLs)

This protocol must be enabled in the EWS or Web Jetadmin. If you do not use it, keep it disabled for security.

How to use FTP in Windows

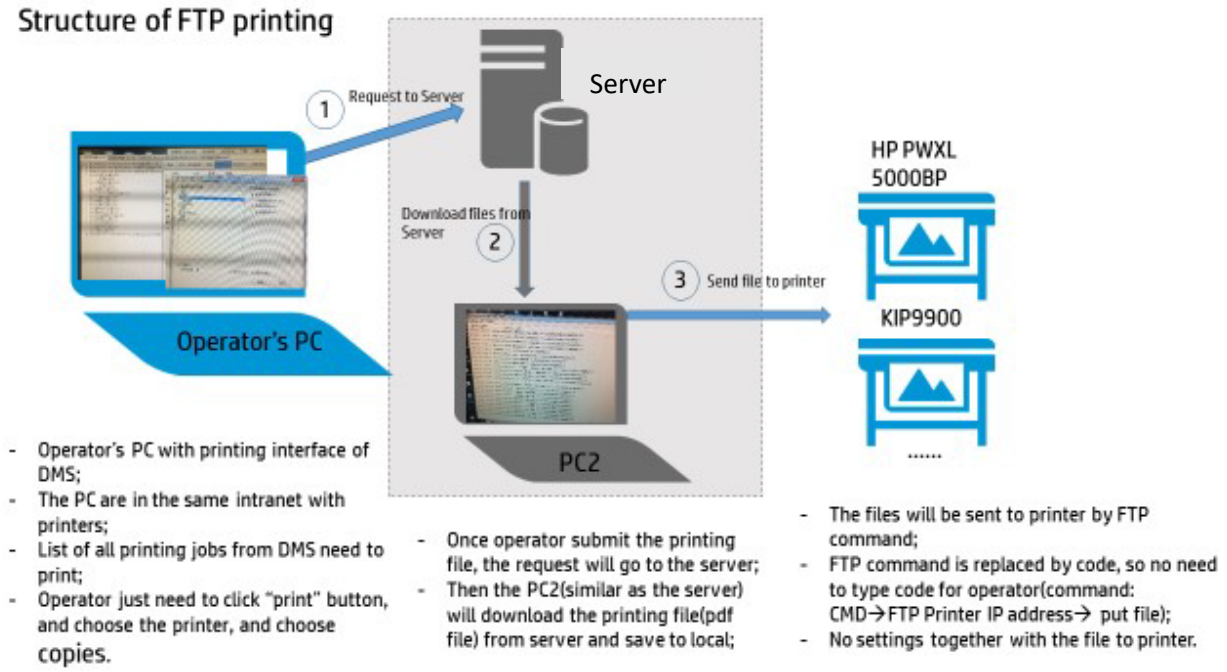
1. Open the Windows Explorer.
2. Write in the route box: “ftp:*IP*”.
3. Now you have a window with one folder (Port).
4. Open the folder.
5. Use Drag and Drop. (Any file added to this folder will be printed.)

How to use FTP from DOS command

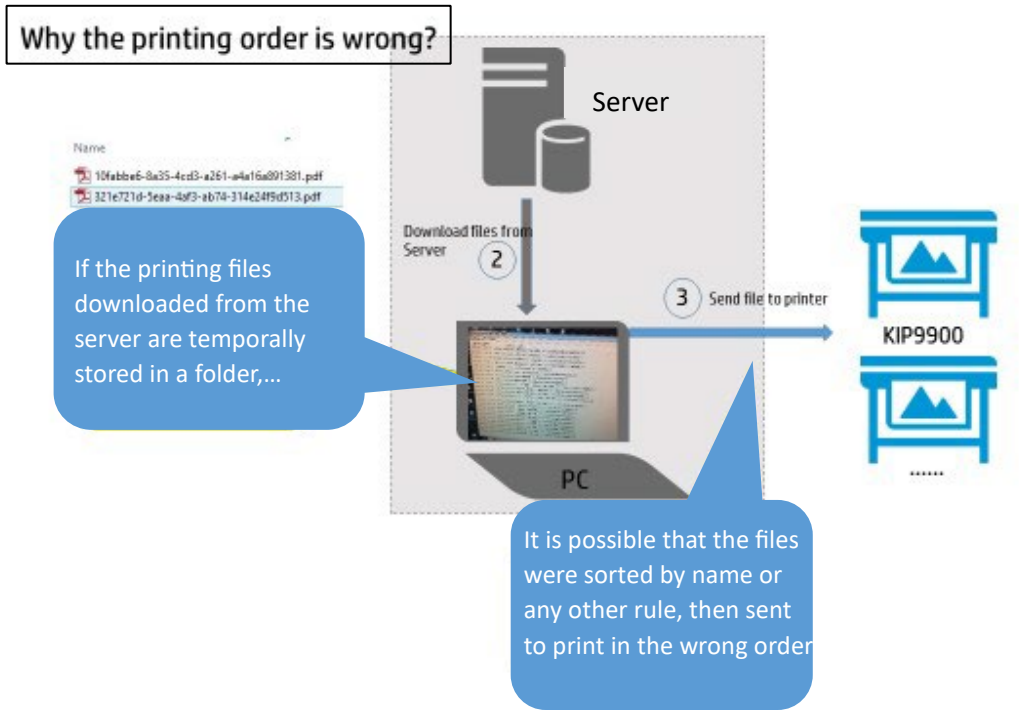
This example uses the ftp command in a similar way to that of LPR. You only have to connect the Printer with the FTP command and use any command, such as “put” or “send” (see the FTP help for the command format), to add the files to the printer FTP.

If you have an admin password defined, the printer will ask for it to approve the connection.

How to use FTP combined with DMS server



Possible issue



3.3 Printing with PJLs

PJL commands allow you to add print settings to a PDF file (not compatible with other files). This means that you can use a direct print mode (send the file directly to the printer without a driver or software) modifying some properties.

The following table contains the list of PJLs that are currently supported in the supported printers.

This list is still in development, more commands could be added in future releases.

PJL Name	Description	Accepted values	Example
STRINGCODESET	Indicates the string's codification type used for the "@PJL JOB NAME, @PJL SET JOBNAME and @PJL SET USERNAME" commands (therefore, it comes before them).	UTF8 UTF8URL ROMAN8 KAN8	@PJL SET STRINGCODESET=UTF8
JOBNAME (also set via @PJL JOB NAME)	Sets the localized version of the job name. It requires specification of the string's codification type. This value has precedence over the "@PJL JOB NAME=jobname". Maximum length is 128 bytes.	<String>	@PJL SET JOBNAME="My Job" @PJL JOB NAME="My Job"
USERNAME	Sets the localized version of the user name. It requires specification of the string's codification type.	<String>	@PJL SET USERNAME="wintest"
MARGINLAYOUT	Selects how the margins will be applied.	STANDARD OVERSIZE CLIPINSIDE	@PJL SET MARGINLAYOUT=CLIPINSIDE
PRINTQUALITY	Specifies the desired print quality for a page. This command affects the entire page. Once data has been sent to the printer, any subsequent print quality change will not take effect until the following page. NOTE: HP PageWide XL Print Quality mapping: * Lines/Fast = DRAFT * Uniform areas = NORMAL * High Detail = HIGH	DRAFT NORMAL HIGH	@PJL SET PRINTQUALITY=DRAFT

RENDERINTENT	Indicates which color properties must be kept and which can be modified.	PERCEPTUAL COLORIMETRIC SATURATION	@PJL SET RENDERINTENT=PERCEPTUAL
RENDERMODE	Sets the printing mode for your plot to color or grayscale.	COLOR GRAYSCALE	@PJL SET RENDERMODE=COLOR
RESOLUTION	The value depends on the data format and print quality.	<Integer 75 ... 2400>	@PJL SET RESOLUTION=300
MEDIASOURCE	Selects the input media source.	ROLL1 ROLL2 … ROLL6 AUTO	@PJL SET MEDIASOURCE=ROLL4
MEDIADESTINATION	Chooses the output destination for the job.	DEFAULT BIN STACKER FOLDER ACCESSORY_STACKER	@PJL SET MEDIADESTINATION=BIN
FOLDINGMETHODTYPE	Specifies the folding method type.	USER STANDARD	@PJL FOLDINGMETHODTYPE=USER
FOLDINGMETHODENUM	Specifies the folding method value: 0: Do not fold 1: User Defined 2: Folder Selected 3: Stack 4 - 255: Reserved, Do Not Use	<Positive Integer>	@PJL SET FOLDINGMETHODENUM=0
	256 - 65535: Use freely		
FOLDEROUTPUTBIN	Specifies the folder output bin number for the job.	<Positive Integer>	@PJL FOLDEROUTPUTBIN=0
AUTOROTATE	Specifies whether Autorotate is enabled or not.	ON OFF	@PJL SET AUTOROTATE = ON
SCALE	Specifies scaling of the job.	<Positive Integer [25..400]>	@PJL SET SCALE = 50
COPIES	Specifies the number of copies of the job.	<Positive Integer>	@PJL SET COPIES =2
ENTER LANGUAGE	Specifies the language of the job encapsulated.	PDF TIFF JPEG HPGL2	@PJL ENTER LANGUAGE="PDF"

How to use PJLs

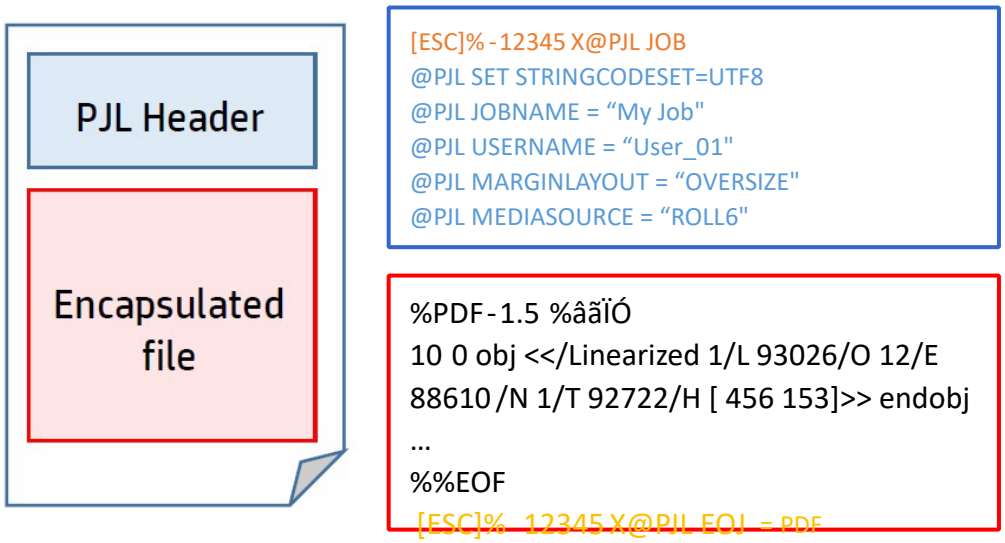
In order for PJL values to be applied to a job when sending it to the HP PageWide XL, the submitted file needs to be modified.

The first line [ESC]%-12345X@PJL JOB is pointing out that a PJL Job is beginning. Please note that [ESC] references to the ASCII escape character.

The following lines contain the PJLs supported by HP PageWide XL, as shown in the example. The

last line in the header references the language of the file encapsulated, for instance PDF.

Finally, a last line closing the job is needed.



4. Large Format printers: security features summary

4.1 GRAPHIC PRINTERS

Device Protection				
Security Feature	Z6/Z9	Z6200/Z6600/Z6800	Z6+pro, Z9+pro	Z2600/Z5600
Secure boot with HW root of trust	Yes	No	Yes	No
Firmware Code Signature Validation	Yes	-	Yes	-
Automatic FW Updates	Yes	No	Yes	Yes
HTTPS Redirect enabled by default	Yes	-	Yes	-
SNMPv1/2 read-only by default	FY24	-	FY24	-
SNMPv3 disabled by default	Yes	Yes	Yes	Yes
Write memory protection	Yes	-	Yes	-
HP Cartridge Security	Yes	-	Yes	-
Unique password	FY24	No	Yes	-
Sure start (with self healing)	No		No	-
Whitelisting (with self healing)	Yes	No	Yes	-
Runtime intrusion detection (with self healing)	No	-	No	-
Connection inspector (with self healing)	No	No	Yes	No
Security event logging	yes	No	yes	-
Disable USB ports	Yes	Yes	Yes	Yes

Data Protection				
Security Feature	Z6/Z9	Z6200/Z6600/Z6800	Z6+pro, Z9+pro	Z2600/Z5600
Front panel access lock	Yes	Yes	No	-
Role-based access control	Yes	No	Yes	-
LDAP authentication	Yes	No	Yes	-
Kerberos authentication	No	No	Yes	-
Self-encrypted disks (FIPS 140-2)	Yes	Yes	Yes	-
Removable HDD	No	No	No	Yes
Swappable HDD	No	-	No	-
TLS 1.2	Yes	Yes	Yes	No
TLS 1.3	No	No	No	No
IPsec	Yes	Yes	Yes	Yes
802.1x	Yes	Yes	Yes	Only JD640
NTLMv2	Yes	No	Yes	
Secure file erase	Yes	Yes	Yes	Yes
Secure disk erase	Yes	Yes	Yes	Yes
Trusted Platform Module (TPM)	No	No	Yes	-
IPv4 & IPv6 Compatibilty	Yes	Yes	Yes	-
CA/JD Compatibility	Yes	Yes	Yes	Yes
Encrypted PIN Printing	Yes	No	Yes	-

Document Protection				
Security Feature	Z6/Z9	Z6200/Z6600/Z6800	Z6+pro, Z9+pro	Z2600/Z5600
HP SmartCard Solution (HP CAC)	No	-	No	-
Celiveo	Yes	No	No	-
PIN Printing	Yes	Yes	Yes	-
Environment Protection				
HP Web JetAdmin	Yes	Yes	Yes	-
HP Security Manager	Yes	Yes	Yes	-
HP Command Center	No	No	No	No
SIEM Integration	yes	No	yes	-
Security Certifications				
Common criteria certification	No	No	No	No
ISO 20243	Yes	Yes	Yes	Yes
NISPOM	No	No	No	No
FIPS 140-2 - Data in transit	No	No	No	No
FIPS 140-2 - Data at rest	No	-	No	-

4.2 TECHNICAL PRINTERS

Device Protection												
Security Feature	T918/T908	T858	T850/950 SF	T850/950 MFP	Studio Series	T200/T600 T730/830	T3500	T1600/T2600	T1700	727 (T series)	72, 726 (T Series)	T120/T520
Secure boot with HW root of trust	Yes	Yes	Yes	Yes	-	FY24	No	Yes	Yes	-	-	-
Firmware Code Signature Validation	Yes	Yes	Yes	Yes	-	FY24	No	Yes	Yes	-	-	-
Automatic FW Updates	Yes	Yes	Yes	Yes	-	Yes	Yes	Yes	Yes	-	-	-
HTTPS Redirect enabled by default	Yes	Yes	Yes	Yes	-	FY24	No	Yes	Yes	-	-	-
SNMPv1/2 read-only by default	Yes	Yes	Yes	Yes	-	FY24	No	FY24	FY24	-	-	-
SNMPv3 disabled by default	Yes	Yes	Yes	Yes	-	FY24	Yes	Yes	Yes	-	-	-
Write memory protection	Yes	Yes	Yes	Yes	-	FY24	No	Yes	Yes	-	-	-
HP Cartridge Security	Yes	Yes	Yes	Yes	-	FY24	Yes	Yes	Yes	-	-	-

Unique password	Yes	Yes	Yes	Yes	-	Yes	No	FY24	FY24	-	-	-
Sure start (with self healing)	No	No	No	No	-	No	No	No	No	-	-	-
Whitelisting (with self healing)	Yes	Yes	Yes	Yes	-	No	No	Yes	Yes	-	-	-
Runtime intrusion detection (with self healing)	No	No	No	No	-	No	No	No	No	-	-	-
Connection inspector (with self healing)	No	No	No	No	-	No	No	No	No	-	-	-
Security event logging	Yes	Yes	Yes	Yes	-	No	No	Yes	No	-	-	-
Disable USB ports	Yes	Yes	Yes	Yes	-	Yes	Yes	Yes	Yes	-	-	-

Data Protection												
Security Feature	T918/T908	T858	T850/950 SF	T850/950 MFP	Studio Series	T200/T600 T730/830	T3500	T1600/T2600	T1700	727 (T series)	72, 726 (T Series)	T120/T520
Front panel access lock	No	No	No	No	-	No	No	Yes	Yes	-	-	-
Role-based access control	No	No	No	No	-	No	Yes	Yes	Yes	-	-	-
LDAP authentication	No	No	No	No	-	No	No	Yes	No	-	-	-
Kerberos authentication	No	No	No	No	-	No	No	Yes	No	-	-	-
Self-encrypted disks (FIPS 140-2)	No	No	No	No	-	No	No	Yes	Yes	-	-	-
Removable HDD	No	No	No	No	-	No	Yes	Yes US Gov SKUs	No	-	-	-
Swappable HDD	No	No	No	No	-	No	No	No	No	-	-	-
TLS 1.2	Yes	Yes	Yes	Yes	-	No	Yes	Yes	Yes	-	-	-
TLS 1.3	Yes at intro+3	Yes at intro+3	Yes at intro+3	Yes at intro+3	-	No	No	No	No	-	-	-
IPsec	No	No	No	No	-	No	Yes	Yes	Yes	-	-	-
802.1x	Yes	Yes	Yes	Yes	-	Yes	Yes	Yes	Yes	-	-	-
NTLMv2	No	No	No	Yes	-	No	Yes	Yes	Yes	-	-	-

Secure file erase	No	No	No	No	-	No	Yes	Yes	Yes	-	-	-
Secure disk erase	Not applicable	Not applicable	Not applicable	Job queue erase	-	No	Yes	Yes	Yes	-	-	-
Trusted Platform Module (TPM)	No	No	No	No	-	No	No	Yes	No	-	-	-
IPv4 & IPv6 Compatibilty	Yes	Yes	Yes	Yes	-	No	Yes	Yes	Yes	-	-	-
CA/JD Compatibility	Yes	Yes	Yes	Yes	-	Yes	No	Yes	Yes	-	-	-
Encrypted PIN Printing	No	No	No	No	-	No	Yes	Yes	Yes	-	-	-

Document Protection												
Security Feature	T918/T908	T858	T850/950 SF	T850/950 MFP	Studio Series	T200/T600 T730/830	T3500	T1600/T2600	T1700	727 (T series)	72, 726 (T Series)	T120/T520
HP SmartCard Solution (HP CAC)	No	No	No	No	-	No	No	Coming 24	No	-	-	-
Celiveo	No	No	No	No	-	No	No	Yes	Yes	-	-	-
PIN Printing	Yes (via HP Smart)	Yes (via HP Smart)	Yes (via HP Smart)	Yes (via HP Smart)	-	No	Yes	Yes	Yes	-	-	-
Environment Protection												
HP Web JetAdmin	Yes	Yes	Yes	Yes	-	No	No	Yes	Yes	-	-	-
HP Security Manager	Yes	Yes	Yes	Yes	-	No	No	Yes	Yes	-	-	-
HP Command Center	Yes	Yes	Yes	Yes	-	No	No	No	No	-	-	-
SIEM Integration	Yes	Yes	Yes	Yes	-	No	No	Yes	No	-	-	-
Security Certifications												
Common criteria certification	No	No	No	No	No	No	No	No	No	No	No	No
ISO 20243	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	-	-
NISPOM	No	No	No	No	No	No	No	No	No	No	No	No

FIPS 140-2 - Data in transit	No	No	No	No	No	No	No	No	No	No	No	No
FIPS 140-2 - Data at rest	No	No	No	No	No	No	Yes	Yes	Yes	-	-	-

4.3 Production machines, bigger offices (DesignJetXL and PageWideXL)

Device Protection						
Security Feature	XL3800		766 (XL3600)	4000, 5200, 8200	5200 pro, 8200 pro, 10000 pro	4000, 4500, 5000, 8000
Secure boot with HW root of trust	Yes	Yes	Yes	Yes	Yes	No
Firmware Code Signature Validation	Yes	Yes	Yes	Yes	Yes	Yes
Automatic FW Updates	Yes	Yes	Yes	Yes	Yes	Yes
HTTPS Redirect enabled by default	Yes	Yes	Yes	Yes	Yes	Yes
SNMPv1/2 read-only by default	Yes	Yes	FY24	FY24	FY24	No
SNMPv3 disabled by default	Yes	Yes	Yes	Yes	Yes	Yes
Write memory protection	Yes	Yes	Yes	Yes	Yes	No
HP Cartridge Security	Yes	Yes	Yes	Yes	Yes	Yes
Unique password	Yes	Yes	FY24	Yes	Yes	No
Sure start (with self healing)	Yes	Yes	No	No	No	No
Whitelisting (with self healing)	Yes	Yes	Yes	Yes	Yes	No
Runtime intrusion detection (with self healing)	Yes	Yes	No	No	No	No

Connection inspector (with self healing)	Yes	Yes	No	Yes	Yes	No
Security event logging	Yes	Yes	Yes	Yes	Yes	No
Disable USB ports	Yes	Yes	Yes	Yes	Yes	No

Data Protection						
Security Feature	XL3800		766 (XL3600)	4000, 5200, 8200	5200 pro, 8200 pro, 10000 pro	4000, 4500, 5000, 8000
Front panel access lock	Yes	Yes	Yes	Yes	Yes	Yes
Role-based access control	Yes	Yes	Yes	Yes	Yes	No
LDAP authentication	Yes	Yes	Yes	Yes	Yes	No
Kerberos authentication	Yes	Yes	Yes	Yes	Yes	No
Self-encrypted disks (FIPS 140-2)	Yes for US Gov SKU	Yes	Yes	Yes	Yes	Yes
Removable HDD	Yes for US Gov SKU	Yes	Yes US Gov SKUs	Yes US Gov SKUs	Yes US Gov SKUs	Yes US Gov SKUs
Swappable HDD	FY24	Yes	No	No	No	No
TLS 1.2	Yes	Yes	Yes	Yes	Yes	Yes
TLS 1.3	Yes at intro+3	Yes	No	No	No	No
IPsec	Yes	Yes	Yes	Yes	Yes	Yes
802.1x	Yes	Yes	Yes	Yes	Yes	Yes
NTLMv2	Yes	Yes	Yes	Yes	Yes	Yes
Secure file erase	Yes	Yes	Yes	Yes	Yes	Yes
Secure disk erase	Yes	Yes	Yes	Yes	Yes	Yes

Trusted Platform Module (TPM)	Yes	Yes	Yes	Yes	Yes	No
IPv4 & IPv6 Compatibilty	Yes	Yes	Yes	Yes	Yes	Yes
CA/JD Compatibility	Yes	Yes	Yes	Yes	Yes	No
Encrypted PIN Printing	Yes	Yes	Yes	Yes	Yes	Yes

Document Protection						
Security Feature	XL3800		766 (XL3600)	4000, 5200, 8200	5200 pro, 8200 pro, 10000 pro	4000, 4500, 5000, 8000
HP SmartCard Solution (HP CAC)	Yes at intro+6	Yes	Coming 24	Coming 24	No	No
Celiveo	No	No	Yes	No	No	Yes
PIN Printing	Yes	Yes	Yes	Yes	Yes	Yes
Environment Protection						
HP Web JetAdmin	Yes	Yes	Yes	Yes	Yes	Yes
HP Security Manager	Yes	Yes	Yes	Yes	Yes	No
HP Command Center	Yes	Yes	No	No	No	No
SIEM Integration	Yes	Yes	Yes	Yes	Yes	No
Security Certifications						
Common criteria certification	At intro +12	No	No	No	No	No
ISO 20243	Yes	Yes	Yes	Yes	Yes	Yes
NISPOM	No	No	No	No	No	No
FIPS 140-2 - Data in transit	At intro +6	Yes?	No	No	No	No
FIPS 140-2 - Data at rest	Yes	Yes	Yes	Yes	Yes	Yes

5. 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 HD/SD Pro Scanner* HP HD Pro 2 Scanner*	PageWide XL MFP series	T1120 SDMFP	T2300 MFP	T2500 MFP	T2530 MFP	T3500 MFP	T830 MFP	T2600 MFP	XL3600 MFP
Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Disable FTP & Web Access	Yes	Yes	Yes	N/A	Yes	Yes	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	N/A	N/A
Security patches	Through scanner SW 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	N/A	N/A
NTLM	N/A	V2	V2	N/A	V1	V2	V2	V2	V2	V2	V2

* HD/SD Pro Scanners are standalone scanners, meaning they are not attached to a printer by default. They include a Panel PC to operate them, which is running a custom version of Windows IoT. This is a closed operating system that prevents software installations and settings changes that can affect system performance or security. This also implies that it is not possible to install third-party software or third-party printer drivers. Different Windows OS are used depending on the model:

- Windows 10 IoT Enterprise LTSC®
    - Includes a firewall that cannot be disabled.
    - The scanner cannot be pinged from the network to increase security.

- Windows 7 Embedded Standard®
    - The scanner can be pinged from the network.

6. 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	Port	In/ Out	Purpose and consequences of disabling it	Configuration	DesignJet & PageWide XL SFP	DesignJet & PageWide XL MFP
FTP Printing	TCP 20,21	In/Out	Printing. It will be impossible to send documents to the device via FTP protocol. Rarely used. It depends on connection tracking (firewall feature).	[EWS] > Network > Other Settings > FTP Printing	Yes	Yes
Scan to Network (FTP)	TCP 21	Out	Scan to network folder. MFPs will not be able to send scanned date to an ftp server.	[EWS] > Setup > Scan to network	No	Yes
Telnet	TCP 23	In	This port can be used for remote configuration of the HP Jetdirect device when there is no other configuration method, or it can be used to check the current configuration.	[EWS] > Network > Other Settings > Telnet Config	Yes	Yes
Email sending (alerts & job scanned)	TCP 25, 465, 587	Out	Email. Newer HP Printers and Multi-Function Devices have the capability of sending e-mail alerts directly from the device. The port is configurable, and others could be selected instead.	[EWS] > Settings > Email Server	Yes	Yes
IPsec/Firewall	TCP 50/51, UDP 500	In/Out	It will become impossible to use encrypted secure connection to the device over the Internet or LAN. It would also become impossible to set up ports/services mapping/forwarding.	[EWS] > Network > TCP/IP Settings	Yes	Yes

Printers

LLMNR	UDP 5355	In	Resolving device name. 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.	[EWS] > Network > Other Settings	Yes	Yes

Protocol/Function	Port	In/ Out	Purpose and consequences of disabling it	Configuration	DesignJet & PageWide XL SFP	DesignJet & PageWide XL MFP
DNS	TCP, UDP 53	Out	DNS. Allows devices to resolve hostnames used by any feature that requires outgoing connections.	[EWS] > Network > TCP/IP Settings > Network Identification	Yes	Yes
DHCPv4 and BOOTP	UDP 67, 68	In/Out	DHCPv4 and BOOTP.	[EWS] > Network > TCP/IP Settings > TCP/IP(v4)	Yes	Yes
TFTP (Trivial File Transfer Protocol) configuration file	UDP 69	In/Out	This port is used for configuration and upgrading of the Jetdirect firmware. Only in the case that the Jetdirect card is used: configuration through this protocol cannot be used. Rarely used.	[EWS] > Network > Other Settings > TFTP Configuration File	Yes	Yes
HP Jetdirect XML services	TCP 80, 8080	In	Some HP software utilities may perform web service requests to this port to retrieve device status information. If disabled, the printer EWS would not be reachable, and HP Web Jetadmin and other utilities might not work.	[telnet] > TCP/IP Menu > Other Settings > EWS Config [Control Panel] > Settings > Security > Embedded Web Server [Control Panel] > Settings > Security > Web Services Printing & Management	Yes	Yes
AFU, Connectivity Test	TCP 80	Out	Access to the Automatic Firmware Upgrade host (under hp.com), performing connectivity tests. If disabled, the printer will not be able to automatically receive the latest FW upgrades and the connectivity test will always fail.	[EWS] > About printer > Firmware Update [EWS] > Connectivity > Services > Settings > Services > Printer Data Sharing Agreement	Yes	Yes
Kerberos	TCP, UDP 88	In/Out	Used by HP Large Format devices for Kerberos authentication.	[EWS] > Security > Access Control > Windows Sign In Configuration [EWS] > Network > Security > IPsec/Firewall	Yes	Yes

NetBIOS, SMB (Scan to network)	TCP 139, 445	Out	Scan to network folder (to SMB destination). If disabled, MFPs will not be able to send scanned data to networks folders.	[EWS] > Setup > Scan to network	No	Yes

Protocol/Function	Port	In/ Out	Purpose and consequences of disabling it	Configuration	DesignJet & PageWide XL SFP	DesignJet & PageWide XL MFP
SDK (SNMP)	UDP 161	In	This port can be accessed by any SNMP Management utility. HP Web Jetadmin use SNMP to configure and query the status of a printer.	[EWS] > Network > Security > Mgmt. Protocols > SNMP	Yes	Yes
SDK (SNMP traps)	UDP 162	In/Out	This port can be used when the network is configured to capture trap information. Many SNMP Management utilities can be configured to capture traps.	[EWS] > Network > Security > Mgmt. Protocols > SNMP	Yes	Yes
LDAP	TCP 389	Out	LDAP client. Allows Large Format devices to perform address lookups and authentication. Host and Port can be configured.	[EWS] > Security > Access Control > LDAP Sign in server [EWS] > Setup > Address Book	Yes	Yes
SLP (Service Location Protocol)	UDP 427	In/Out	Devices use SLP for advertising their services. Some HP software utilities use SLP to automatically discover and automatically install a printer on the network. The device will not be discoverable over SLP from DMF - impact is minimal if Bonjour is enabled (SLP is treated as legacy technology).	[EWS] > Network > Other Settings > SLP	Yes	Yes

EWS, Web Services (Fibonacci, RIO, ePrint)	TCP 443	In/Out	The printer connects through HTTP over TLS/SSL to several cloud services. IPP Jobs that include HTTPS references may also require downloading the print job using HTTPS. If disabled, it will not be possible to use the HP Connected service or to send usage data to the HP usage server (Fibonacci) or to the supplies reordering service (RIO).	[EWS] > Network > Mgmt. Protocols > Web Mgmt. [telnet] > TCP/IP Menu > Other Settings > EWS Config [Control Panel] > Settings > Security > Embedded Web Server [Control Panel] > Settings > Security > Web Services Printing & Management	Yes	Yes
Syslog	UDP 514	Out	Allows the device to send syslog events to a syslog server. Host and Port can be configured.	[EWS] > Network > TCP/IP Settings > Advanced	Yes	Yes

Protocol/Function	Port	In/ Out	Purpose and consequences of disabling it	Configuration	DesignJet & PageWide XL SFP	DesignJet & PageWide XL MFP
LPD (Line Printer Daemon protocol/Line Printer Remote protocol) printing	TCP 515	In	LPD Print Protocol. It will disable LPD printing from Windows or OS X, which is almost never used by end users as it is a legacy protocol.	[EWS] > Network > Other Settings > LPD [EWS] > Network > Other Settings > LPD Queues	Yes	Yes
DHCPv6	UDP 547	In/Out	DHCPv6	[EWS] > Network > TCP/IP Settings > TCP/IP(v6)	Yes	Yes
IPP (Internet Printing Protocol) printing	TCP 631	In	IPP Printing Protocol. This protocol is used by AirPrint and some HP Software utilities. In the HP DesignJet T790/795/T1300, this feature is only available with the Jetdirect accessory. It can be manually used from Windows or Mac.	[EWS] > Network > Other Settings > IPP Printing	Yes	Yes

LDAP over TLS	TCP 636	Out	LDAP over TLS client. Allows Large Format devices to perform address lookups and authentication. Host and Port can be configured.	[EWS] > Security > Access Control > LDAP Sign in server [EWS] > Setup > Address Book	Yes	Yes
Certificate management service	TCP 829	In	Used for certificate management. If disabled, the HP WJA fleet management tool might not work.	[EWS] > Networking > Security > Mgmt. Protocols	Yes	Yes
WS-Discovery	UDP 3702	In/Out	Multicast discovery protocol to locate services on a local network. If disabled, the Windows HP Installer will not work, and Windows will not automatically choose WS-Print as path to print. Usually for Windows hosts.	[EWS] > Network > Other Settings > WS-Discovery	Yes	Yes
Web Services for Devices	TCP, UDP 3910, 3911	In	Web Services for Devices, Usually for Windows hosts.	[EWS] > Network > Other Settings > WS-Print	Yes	Yes
HP ePrint	TCP 5222	Out	Used by HP ePrint to connect to HP cloud services (email printing).	[Control Panel] > Connectivity > Services > Settings > Services > HP Connected	Yes	Yes

Protocol/Function	Port	In/ Out	Purpose and consequences of disabling it	Configuration	DesignJet & PageWide XL SFP	DesignJet & PageWide XL MFP
				[EWS] > Setup > HP ePrint Connectivity		
Bonjour	UDP 5353	In/Out	Used for IP address and name resolution. 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. AirPrint, printing from Android and HP Smart App will not work.	[EWS] > Network > Other Settings > Bonjour	Yes	Yes

Web Services	TCP 7627	In	HP Web Jetadmin software may perform web service requests to this port to retrieve device status information and manage the device.	[Control Panel] > Settings> Security > Web Services Printing & Management	Yes	Yes
SDK (Scanner)	TCP 8076	In	Sending scanned data out of the MFP. If disabled, software applications getting data using the scanner SDK will not work.	[Control Panel] > Settings> Security > Web Services Printing & Management	No	Yes
SDK (Paper management)	TCP 8085	In	Some HP software utilities and HP SDK for RIPs may perform web service requests to this port to retrieve and configure paper preset information.	[Control Panel] > Settings> Security > Web Services Printing & Management	Yes	Yes
SDK (Remote management)	TCP 8086	In	Some HP software utilities and HP SDK for RIPs may perform web service requests to this port to monitor and calibrate the device.	[Control Panel] > Settings > Security > Web Services Printing & Management	Yes	Yes
SDK (XDM status)	TCP 8090	In	Some HP software utilities may perform web service requests to this port to retrieve device status.	[EWS] > Network > Other Settings > XDM	Old devices	Old devices
9100 printing	TCP 9100	In	Default printing port for HP driver and HP SDK. If disabled, it will become impossible to print RAW documents (plain text/JPEG/PNG) on remote devices in the local network or internet, using port	[EWS] > Network > Other Settings > 9100 Printing	Yes	Yes
Protocol/Function	Port	In/ Out	Purpose and consequences of disabling it	Configuration	DesignJet & PageWide XL SFP	DesignJet & PageWide XL MFP
			9100. This is one of the main printing ports for Windows & Mac.			

9101 printing	TCP 9101	In	Alternative printing port for HP SDK. If disabled, it will become impossible to print using RIP applications based on LFP SDK.	[EWS] > Network > Other Settings > 9100 Printing [EWS] > Network > Other Settings > Enable High Speed Mode	PageWide XL only	PageWide XL only
9102 printing	TCP 9102	In	Alternative printing port for HP Smart Stream.	[EWS] > Network > Other Settings > 9100 Printing [EWS] > Network > Other Settings > Enable High Speed Mode	PageWide XL only	PageWide XL only

Appendix 1 – Web Jetadmin

HP Web Jetadmin is a printer management solution capable of performing different functions on a fleet of devices. This includes device configuration, alerts subscription, and printer status information. The tool allows the user to set up a configuration template and send it to a list of printers. For instance, HP Web Jetadmin can be used to carry out the following operations (assuming they are supported on the device):

- Disable protocols.
- Control panel access lock.
- Setup Admin password.
- USB drive control. (Enable or disable the use of the USB to print or scan, enable or disable the possibility of upgrading the firmware from a USB.) • Change the settings of Secure File Erase.
- Schedule a Secure Hard Disk Wipe.
- Remote firmware upgrade.

Please refer to Web Jetadmin documentation for updated information on supported features.

HP Web Jetadmin can be downloaded at the following link:

http://www8.hp.com/us/en/solutions/business-solutions/printingsolutions/wja.html

Manageability contract for Large Format Printers

Since the introduction of HP PageWide XL printers, the list of features supported by HP Web Jetadmin is included in a Manageability Contract (MC DJA) that is periodically updated. Each version of the Manageability Contract builds on the features of the previous version and adds support for additional functionalities. This means that MCA DJA 2.0 includes all the features of MC DJA 1.0, and some extra ones.

Currently, two versions of the MC DJA exist:

MC DJA Version	1.0	2.0
Products implementing it	PageWide XL	Z6, Z6 Pro, Z9+, Z9+ Pro and T1700
Configuration features	Basic device identification Basic device settings Basic security settings JD J8022E settings	Access control Permissions by role User role mappings Device user accounts Common email server settings Enable Scan to email Enable printer firmware update
Supply status	Yes	Yes
Device status & alerts	Yes	Yes
Firmware upgrade	Yes	Yes

MC DJA 1.0

Device identification	Device settings	Security settings	J8022E networking settings	J8022E security settings
System Contact	Control Panel Language	Color Copy Option	DNS Server	8021X
System Location	Printer Wakeup	Control Panel Access	HTTP Idle Timeout	Access Control List
Asset Number	Sleep Delay Time	EWS Password	IPv4 Information	Encrypt all web communication
Company Name		Enable Host USB	IPv6 Information	Encryption Strength
Contact Person		Enable Save to Network Folder	Link Setting mDNS	SNMP Community Name
Device Name		ePrint Settings	Service Name	SNMP Version Access Control
			Network Enable Feature	IPsec/Firewall Policy
			SNMP Trap Destination Table	
			TCP Idle Timeout	
			TCP/IP Configuration Method	
			WINS Server	
			DHCPv4FQDNCompliance	
			Error Handling	
			IPP Printer Install Wizard	
			mDNS Service Name	
			Locally Administered Address	
			System Log Server Info	
			Webservice Print	
			TCP\IP Domain Suffix	
			Upload CA Certificate	
			Upload JetDirect Certificate	
			Proxy Server	

MC DJA 2.0 - Only additions are shown

Device identification	Device settings & Digital sending	Security settings	J8022E networking settings	J8022E security settings
	Common email server Enable Scan to email ePrint settings	Enable firmware update File system password Erase all stored files Access control for device functions Device user accounts		

Appendix 2 – JetAdvantage Security Manager

The HP JetAdvantage Security Manager is a fleet security management tool, which allows the user to apply a security policy across a fleet of devices, monitor the security of these devices, and secure new devices as soon as they are added to the network. This tool can generate security reports to monitor compliance with user defined security policies.

HP JetAdvantage Security Manager can be downloaded at the following link:

http://www8.hp.com/us/en/solutions/business-solutions/printingsolutions/security_manager.html

Please refer to HP JetAdvantage Security Manager documentation for updated information on how to use the tool and supported features.

Policy compatibility features (HP DesignJet T1700/Z6/Z9+/ Z6 Pro/Z9+ Pro Printer Series)

Authentication			
	Authentication Services		
		802.1 x Authentication		Y
			802.1x EAP-TLS	Y
	Certific ate Management		
		Identity Certificate		Y
		CA Certificate		Y
	Credentials		
		Admin (EWS) Password		
			Minimum Password Length	N
			Admin (EWS) Password	Y
			Password Complexity	N
			Account lockout	N
		SNMPv1/v2		Read only enabled
			Read Community Name	Y
			Read/Write community Name	Y
			Default SNMPv1/v2 Credentials Access	Y
		SNMPv3		Y
			SNMPv3 User Name	Y
			Minimum Password Length	N
			Password Complexity	N
			Authentication Passphrase	Y
			Privacy Passphrase	Y
			Encryption algorithms	Y
			Account lockout	N
Device Control			
		I/O Timeout		N
	Control Panel			

	CP Lock	Y
Device Security Checks		
	Check for Latest Firmware	Y
	Check for Latest Jetdirect Firmware	N
External Connections		
	Host USB Plug and Play	N
Logging		
	System Logging	Y
Stored Data		
	File Erase Mode	Y
Devic e Discov ery		
	Service Location Protocol (SLP)	Y
	IPv4 Multicast	Y
	LLMNR	Y
	WS-Discovery	Y
	Bonjour	Y
Netw ork Secur ity		
	Internet Protocol Security (IPsec)/Firewall	Y
	FIPS 140 Compliance Library	N
	Windows	N
	Verify Certificate for IPP/IPPS Pull Printing	N
	Enable WINS Port	N
	WINS Registration	N
Access Control		
	Allow Web Access	Y
	Access control List	Y
Netw ork Servi ces		
	Novell Remote Config (RCFG)	N
	Telnet	Y
	TFTP Configuration File	N
	HP Jetdirect XML Services	Y
	Certificate Management Service	Y
	FTP Firmware Update	Y
Web		
	Require HTTPS redirect	Y
	HTTPS	Y
Web En cryption Settings		
	Web Encryption Strength	Y
	Ciphers	Y
	TLS 1.2	Y
	TLS 1.1	Y

	TLS 1.0	Y
	SSL 3.0 - Insecure Protocol	N
	Embedded Web Server Access	Y
Printing		
	Standard TCP/IP Printing (P9100)	Y
	AirPrint	Y
	LPD/LPR	Y
	Internet Print Protocol (IPP)	Y
	Secure Internet Print Protocol (IPPS)	Y
	Web Services Print (WS-Print)	Y
	File Transfer Protocol (FTP)	Y
	AppleTalk	N
	DLC/LLC	N
	Novell (IPX/SPX)	N

Appendix 3 - Security Manager

The HP ProtectTools Security Manager can be configured to prevent unauthorized access using Smart Cards, TPM Embedded security chips, USB tokens and other security technologies.

HP ProtectTools Security Manager is completely customizable, which gives business customers the flexibility to choose the level of security that best meets their needs. The optional integrated Smart Card Reader on select notebook families provides simple deployment and management of this solution. In addition, HP ProtectTools Security Manager is now available on a wide array of Business Notebooks and select Business Desktops and Workstations. Built on open standards and HP intellectual property.

Plug-in modules:

- Smart Card security for HP ProtectTools
- Initialization and configuration of the Smart Card
- Manage Smart Card accounts and security settings
- Integration with supporting notebook BIOS requiring Smart Card to continue pre-boot process
- Embedded Security for HP ProtectTools
- TPM Embedded Security Chip configuration and management
- Credential Manager for HP ProtectTools
- Multifactor Windows Authentication
- Single sign-on
- BIOS configuration for HP ProtectTools
- BIOS configuration and security settings from within the HP ProtectTools Security Manager console

Benefits:

- Smart Card-based solution is based on open standards, meaning easy implementation, integration, and maintenance.

- Same Smart Card can be used for multiple devices, including notebooks and handhelds, and multiple applications, such as user authentication and building access.
- HP ProtectTools Security Manager can complement other layers of authentications, such as TPM encrypted passwords, fingerprint ID, biometrics and USB Tokens.
- Console design can grow to incorporate new functionality from within the same user interface.

Find attached the links where you can find further information about it:

- User guide: http://h10032.www1.hp.com/ctg/Manual/c03564719
- Installation guide: http://h10032.www1.hp.com/ctg/Manual/c03564723
- Supported printers: http://h10032.www1.hp.com/ctg/Manual/c03601723
- Licensing: http://h10032.www1.hp.com/ctg/Manual/c04677865

NOTE: To obtain an update for your solution or to renew your license, send an email to e-sw-opssupport@hp.com with “Software Updates Portal” in the Subject line and include the name of the solution in the body of the email.

Appendix 4 - Netgard overview

Introduction

API's Netgard™ MFD product is a network access control device that is used for authenticating users who use multifunction devices (MFDs) and peripherals to access the network. Through the use of a Common Access Card (CAC) or Personal Identification Verification (PIV), this device prevents users from performing 'Scan', 'Copy' and 'Print from USB' operations without authenticating. Moreover, the 'Job queue' application is also protected.

When this feature is configured in the printer, the following "stand-up workflows" are restricted to unknown users:

- Scan ('Scan to USB', 'Scan to Email', 'Scan to HP Smart Stream' and 'Scan to Network folder').
- Copy
- Print from USB
- Job queue

A user must be authenticated by inserting a Smartcard into the API Netgard card reader to gain access to those workflows. A user who is not previously authenticated would not have access to those workflows.

The rest of the workflows such as "Print from Skylon" and "Print from Driver" are not protected (authentication is not required to launch them) and, therefore, they are supposed to work normally.

User account

The user account that will be used for testing purposes is the following one:

Smartcard:

- PIN: 123456

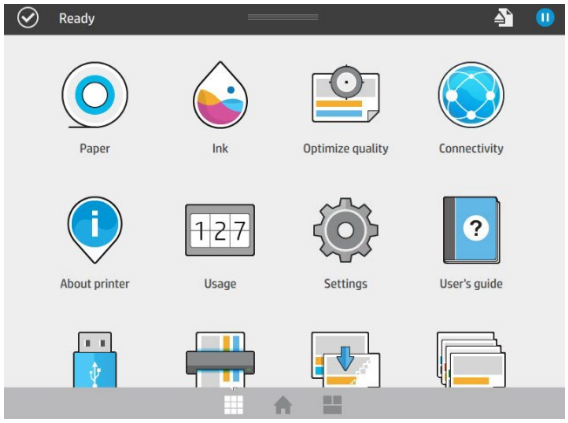
FP settings

To enable Netgard, it will be necessary to configure the following setting at the Front Panel:

Settings > Partner menu > (…) User password > Extended workflows > API Technologies > Enable Netgard MFD

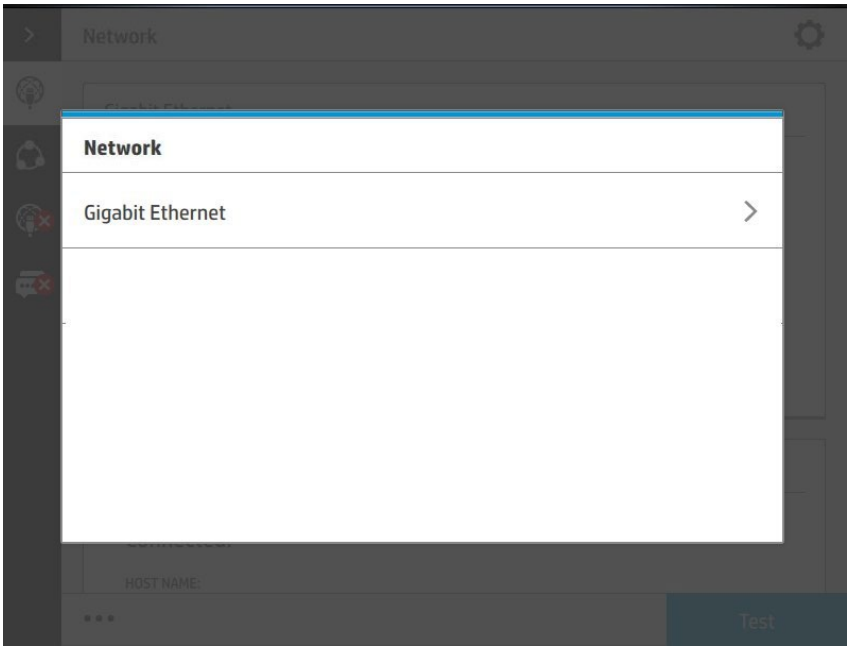
To configure the network and the Netgard appliance, it will be necessary to follow the next steps:

1. Select the "Connectivity" icon.

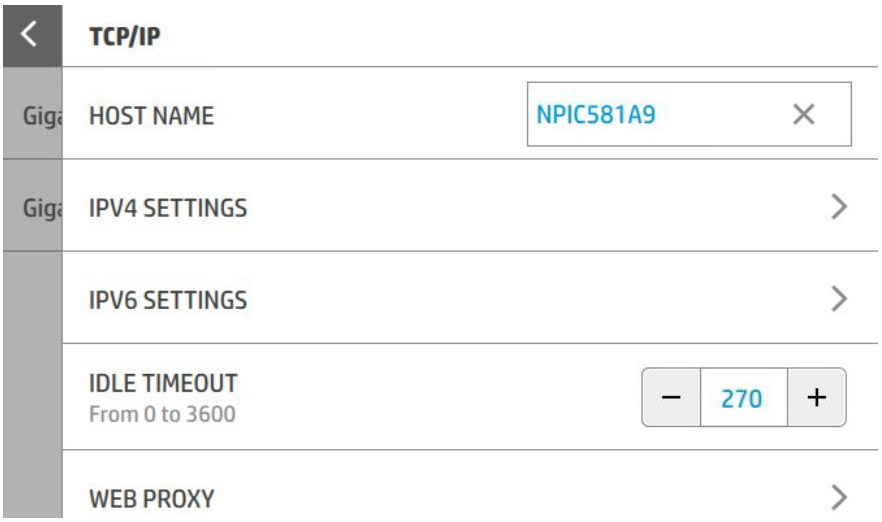


2. Select this icon: 



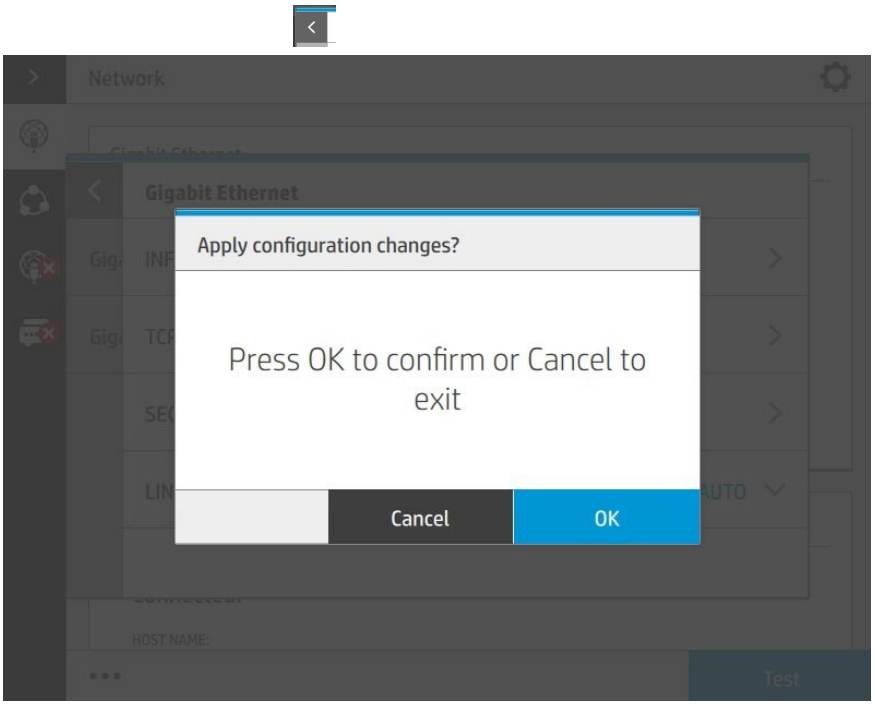


3. Select the IPV4 SETTINGS option and set the Config Method as DHCP.



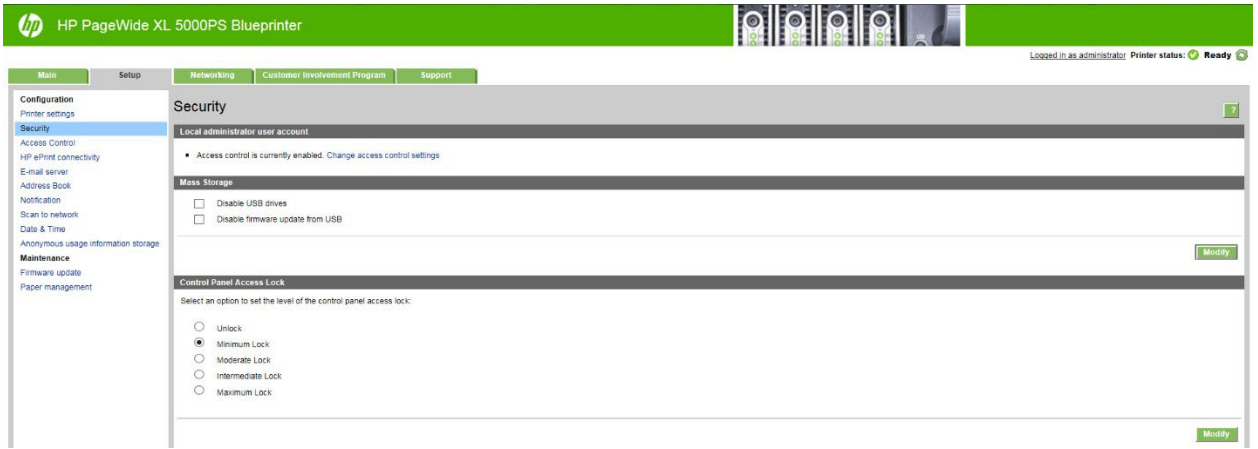
4. Afterwards, select this icon in the FP:

5. Finally, select OK to confirm the settings.

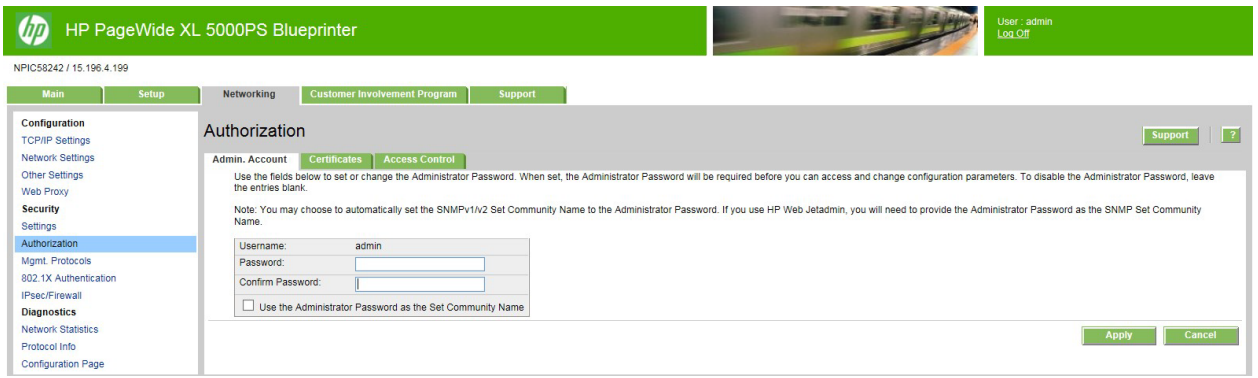


EWS settings

1. Access to the EWS through this IP @: 15.196.22.211
2. Go to Setup > Security and apply the following configuration:

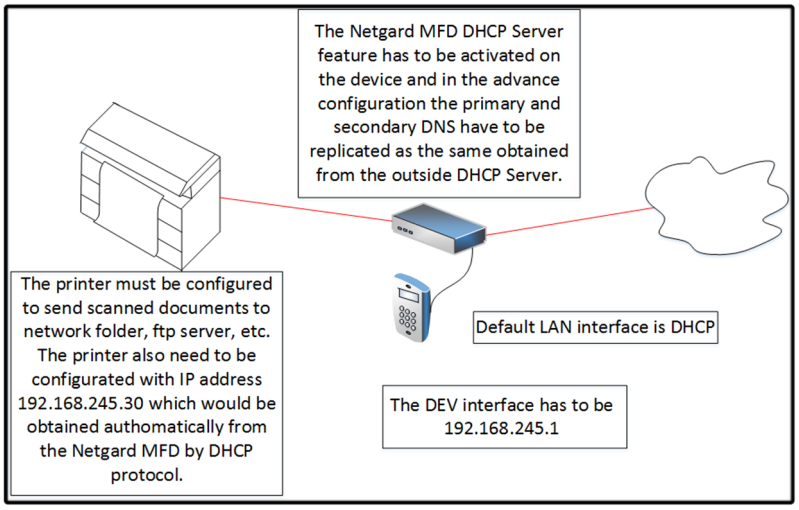


3. Go to Networking > Authorization and set a password for the ‘Administrator’ account.



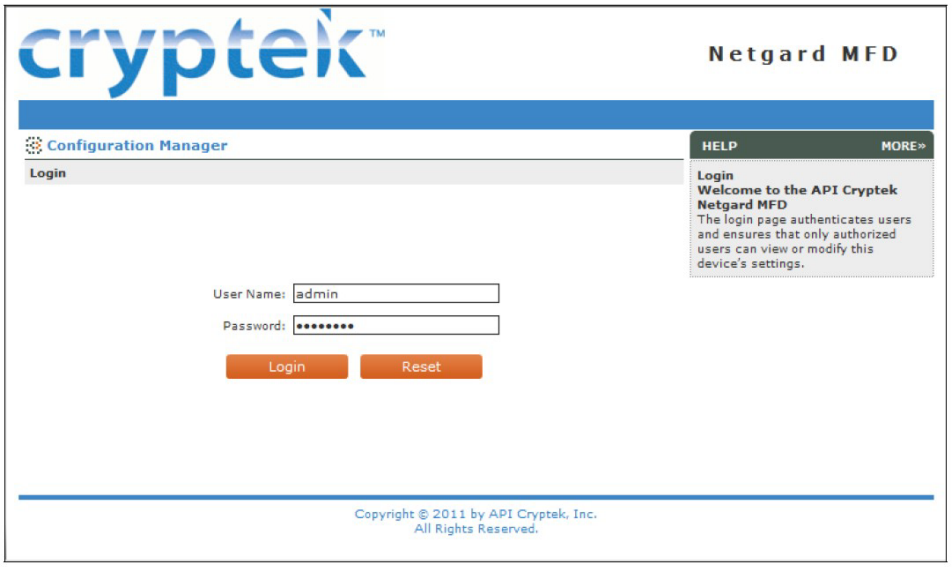
Netgard MFD configuration

Basic configuration of Netgard MFD for HP printers



Netgard MFD user interface access

1. Connect your computer to the MGMT port of the Netgard MFD and assign to your computer an IP address in the same subnet than the MGMT port. It is recommended to use the following details:
    - IP: 192.168.20.20
    - Subnet: 255.255.255.0
    - Gateway: 192.168.20.1
2. Open a Firefox window and enter the default address (https://192.168.20.1.8080/) of the Netgard MFD in the Firefox web browser address bar. After entering this address, the Netgard MFD will display the login screen. The login page authenticates users and ensures that only the ones who are authorized can view or modify the device settings.

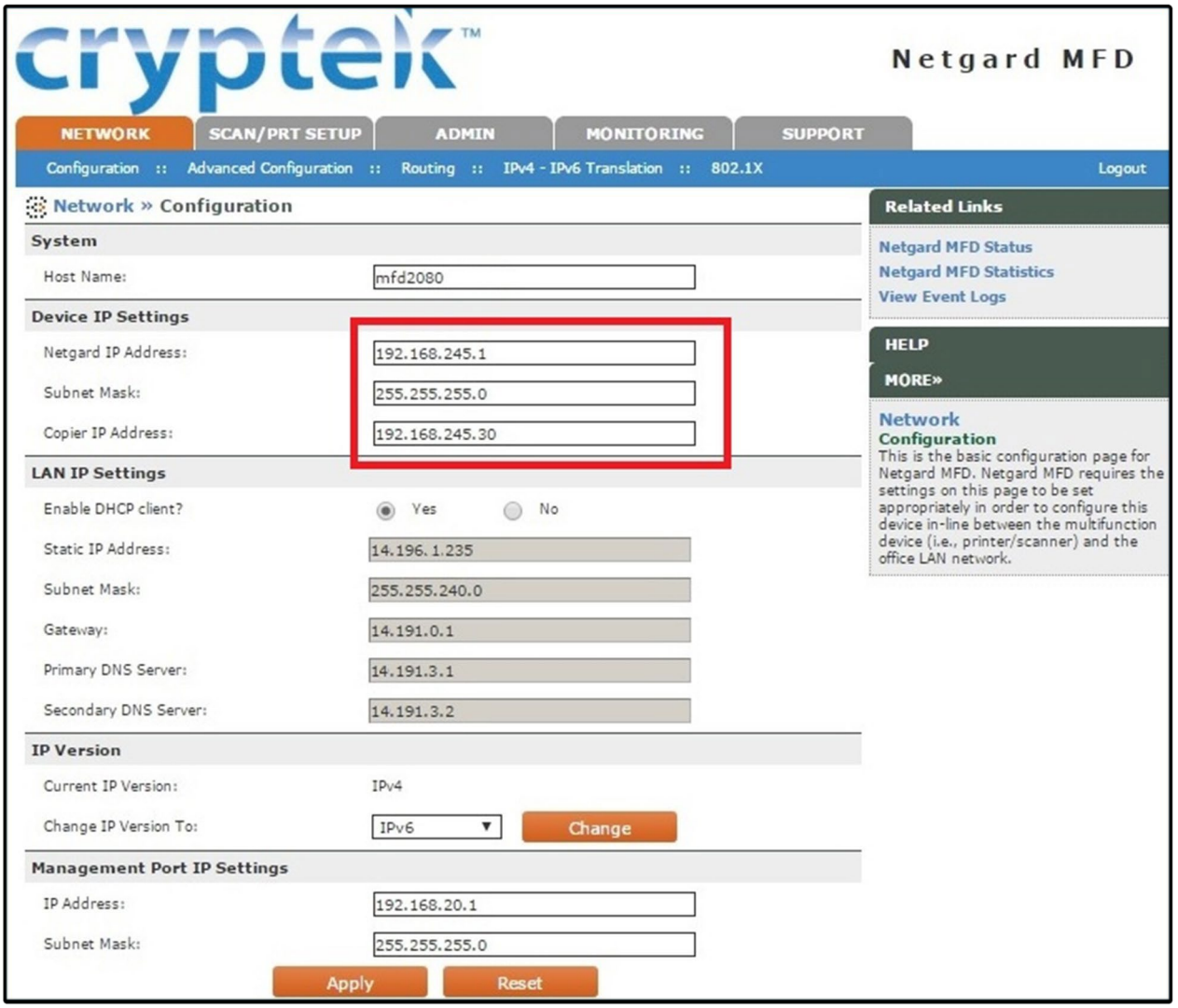


You have to insert the User Name and Password to log in:

User Name: admin

Password: password

3. When the user is logged in, select the Network tab.



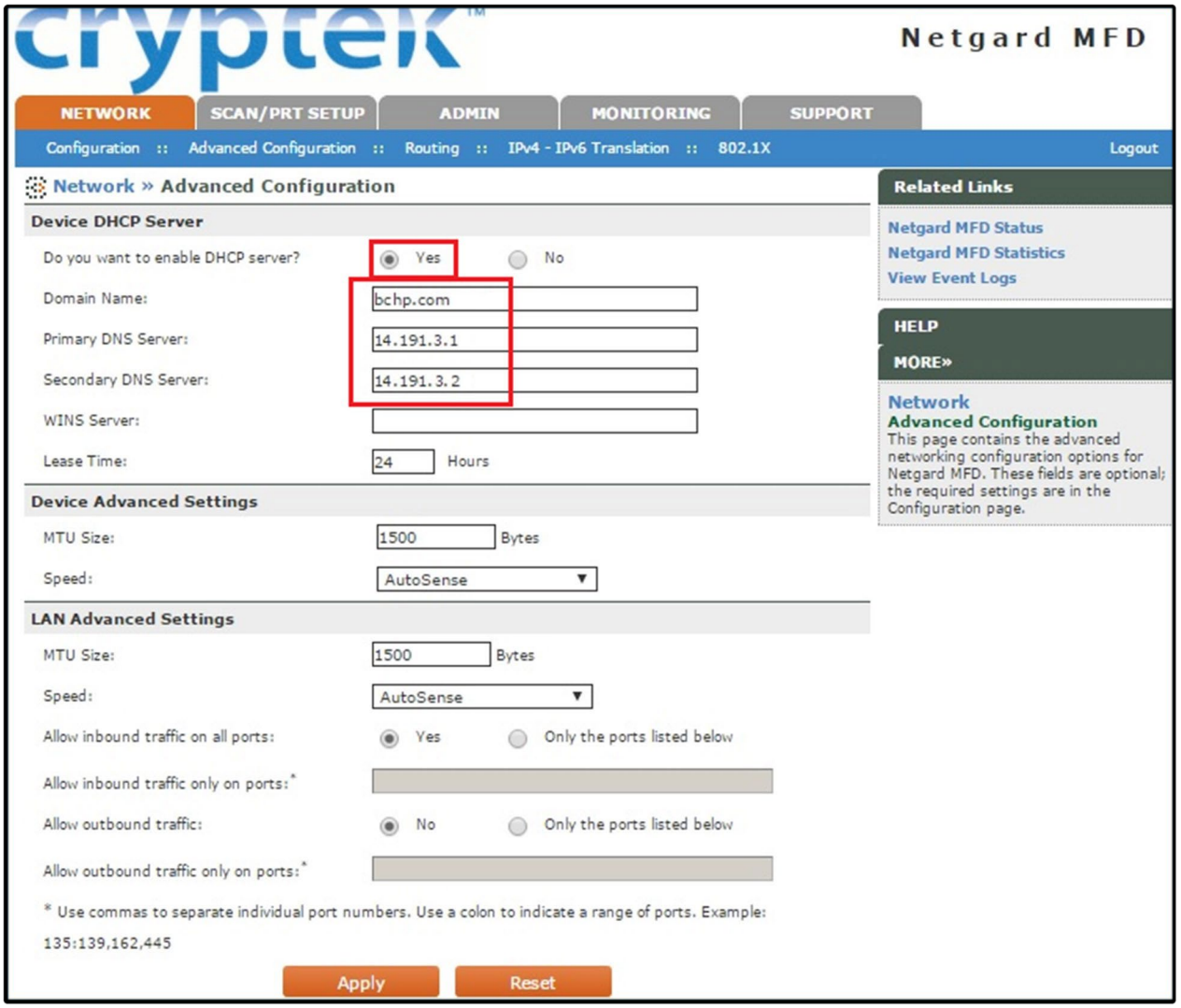
For HP printers the user has to apply some changes in the default Netgard MFD configuration:

Netgard IP Address: 192.168.245.1

Subnet Mask: 255.255.255.0

Copier IP Address: 192.168.245.30

4. Go to Advance Configuration and check that the DHCP server is enabled.



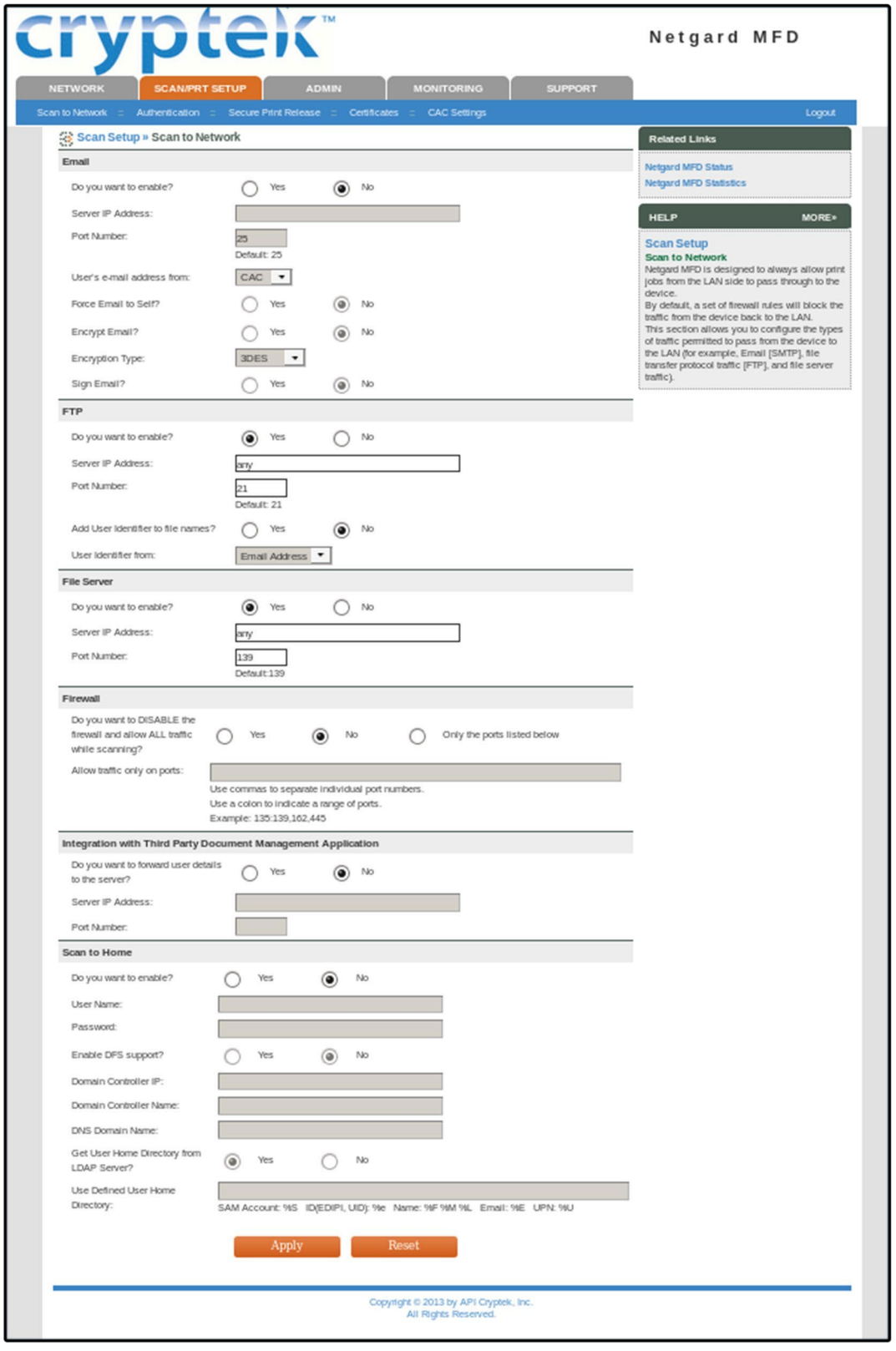
Set the following fields:

Domain Name: bchp.com

Primary DNS Server: This information is specified under the Network > Configuration section.

Secondary DNS Server: This information is specified under the Network > Configuration section.

5. Go to Scan/Prt Setup > Scan to Network.



Apply the following settings:

Scan Setup	Enabled/disabled	Port

Scan to Email	Enabled	Depending on the server: SMTP 25 or 465 IMAP 143 or 993
Scan to FTP	Enabled	21
Scan to File Server	Enabled	139
Scan to Home	Disabled	---

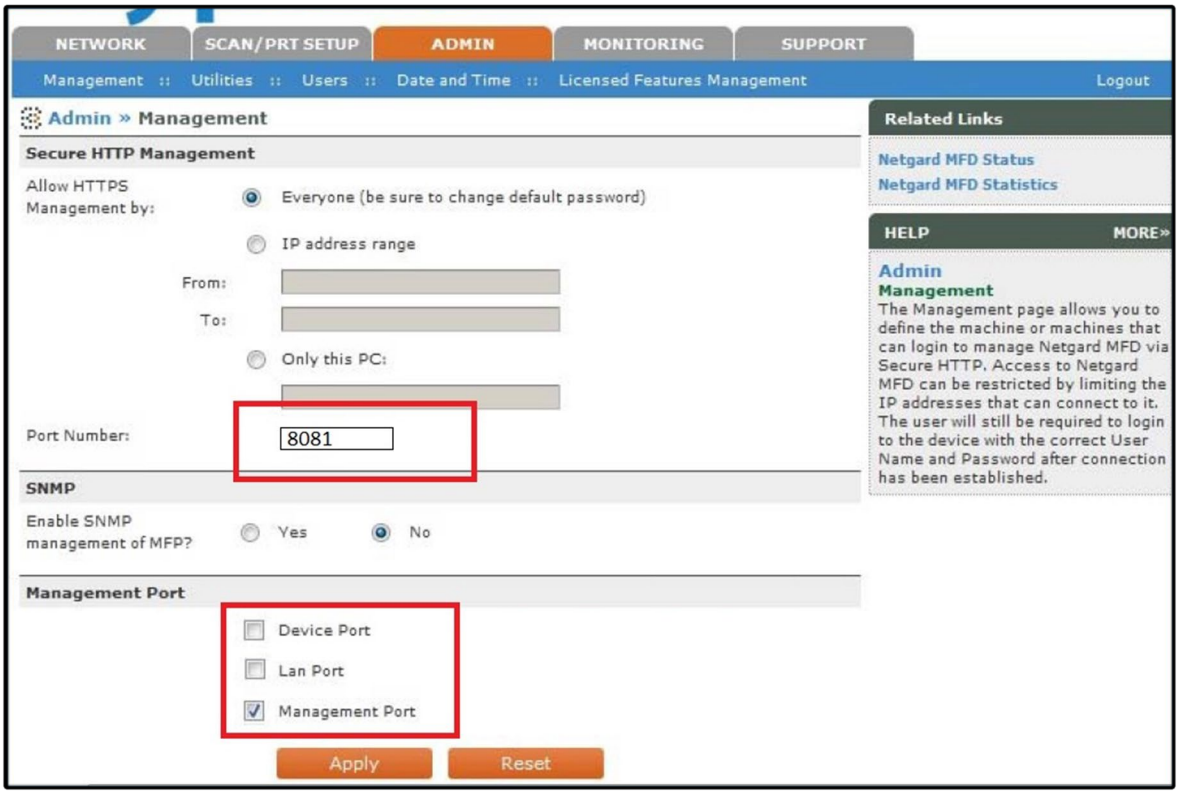
The Firewall has to be enabled while scanning (we have to make sure that the “No” option is selected at the Firewall section). Moreover, the Integration with Third Party Document Management Application section must be set as “No”.

6. Go to Scan/Prt Setup > CAC Settings.



In the Integration with MFP section, set the Use MFP LCD Panel for PIN Entry parameter to “Yes” and the Encrypt Data to/from MFP parameter to “No”.

7. Go to Admin > Management.



Change the Port Number field to “8081”. Then, the address to access to Netgard MFD Configuration will be “https://192.168.20.1:8081”.

Additional information

- When the Netgard feature is configured in a specific printer, in the case of changing the printer by a different one, it will be necessary to disconnect the appliance (unplug the power supply cable from the appliance) before connecting the Netgard HW to the new printer; otherwise, it will not be possible to configure the Netgard feature.
- Netgard is not compatible with other features such as “Abacus”, “Planwell”, etc. Therefore, it’s necessary to make sure that all those features are disabled in Front Panel.
- For further information, please, refer to the documents below:
    - CAC readers.pptx
    - APINETGARD with DHCP (Faltan logos y ultima revision).docx

DesignJet Printers supported:

- HP DesignJet T2500 and T3500 MFP
- HP DesignJet T795, T920, T930, T1530, T2530 and T1500 printer series

PageWide Printers supported:

- HP PageWide XL 8000 Printer series
- HP PageWide XL 5000 Printer series

- HP PageWide XL 4000/4500 Printer series

Appendix 5 – HP Designjet T850 and T950, & HP Designjet XL3800

HP Wolf Security

When your workplace is everywhere, endpoint security is everything.

HP Wolf Security now extends to large format HP DesignJet printers and plotters. HP Wolf Security strengthens your company's cyber-resilience:

1-**Effective**:

i. Full-stack security: Layered resiliency from hardware to cloud
ii. Endpoint isolation stops what NGAV and EDR can't even see
iii. Printers with advanced detection and self-healing capabilities

2-**Efficient**:

i. Integrated IT and security risk management
ii. Fewer alerts and false positives
iii. Reduced endpoint incident analysis and remediation

3-**Productive**:

i. Manage risk without disrupting user experience
ii. Enable work without worry, anywhere
iii. Rapid IT disaster recovery at scale

HP DesignJet printers with HP Wolf Security have varying degrees of protection already built into them. By purchasing an HP Wolf secure printer, you are sure to have the appropriate level of security for your needs.

HP Wolf Security provides 3 levels of security: **Essential**, **Pro** and **Enterprise**.

- HP Wolf Essential Security:
  Lay a secure foundation with hardware-powered protection.

- HP Wolf Pro Security:
  Safeguard your business with proactive protection against cyber threats.

- HP Wolf Enterprise Security:
  Stay ahead of evolving security threats while supporting hybrid work.

Recognize hidden risks	Understand potential costs	HP can help
Although many IT departments rigorously apply security measures to individual computers, printing and imaging devices are often overlooked and left exposed. When there are unsecured devices present, the entire	If private information is jeopardized due to unsecured printing and imaging, the ramifications could include identity theft, stolen business information, a tarnished brand image and reputation, litigation, and loss of business productivity	Defend your network with security features embedded into our large format printers. HP can help you automate device, data, document, and network protection with a broad portfolio of solutions.

network can be exposed to a cybersecurity attack.	and efficiency. Plus, regulatory and legal noncompliance can result in heavy fines.	

Security features

Defend Device, Data and Document - Protect, Detect and Recover

Firewalls alone can't withstand attacks from hackers. You need outstanding protection from HP to help protect your devices, data, documents, and network.

The new HP DesignJet T850, T850 MFP, T950, T950 and HP DesignJet XL 3800 printers and MFPs are designed to help reduce risk, improve compliance, and protect your network end-to-end. HP large format printers provide embedded features and add-on solutions that can help you defend against attacks.

HP Designjet and Page Wide XL strategy to protect our customers is based on 4 pillars: **Defend you Devices** , **Data** and **Documents**… and your **Network**. To be able to accomplish this strategy , first of all is recognize and detect the threats:

- Threats to your **Device**:
  - Control panel : Users can exploit device settings and functions.
  - Default password; Printers can come from the factory with simple default passwords that can be easily compromised.
  - BIOS and firmware: Compromised firmware can open a device and network to an attack.

- Threats to your Data:
  - Data at rest: Printers store sensitive data that can be at risk.
  - Capture: Unsecured MFPs can be used to send scans anywhere.
  - Data in transit :Jobs can be intercepted as they travel to/from a device.

- Threats to your documents:
  - Output tray: Abandoned documents can fall into the wrong hands.
  - Ports and protocols: Unsecured ports (USB or network) or protocols (FTP or Telnet) put devices at risk.
  - Management: Undetected security gaps put data at risk.

2.1- Protect your Device

Solutions, protocols and HW implemented in the printer and MFP to protect the device against malicious attacks

HP Secure Boot : The BIOS is a set of instructions used to load critical hardware components and initiate firmware during startup. Thanks to **HP Secure Boot**, the integrity of the code is validated at every boot cycle—helping safeguard your device from attacks.

Whitelisting: **Whitelisting** automatically checks the firmware during startup to determine if it is authentic and digitally signed by HP. If an anomaly is detected, the device shuts down and notifies IT.

HP Connection Inspector: The **HP Connection Inspector** inspects outbound network connections typically abused by malware, determines what is normal, and stops suspicious activity. If the printer is compromised, it will automatically trigger a system restart.

HP Trusted Platform Module (TPM): The **HP Trusted Platform Module** (TPM) strengthens the protection of encrypted credentials and data stored on your printer or MFP.

Unique admin Password: All printers have a unique admin password by default, so your printer is always password-protected even without setup.

HP SmartCard solution: Help protect confidential information and control printing access by requiring users to use two-factor authentication at the printer

LDAP/Kerberos user authentication: These protocols allow you to authenticate the printer user through the company directory to ensure that the user only accesses authorized options and information.

Role-based access control: Role-based access control allows the administrator to restrict user access to sensitive areas and printer settings by configuring different roles and assigning them to such users.

Security event logging: Provides full visibility to quickly detect malicious threats. The security log records each event as defined by the audit policies set on each object.

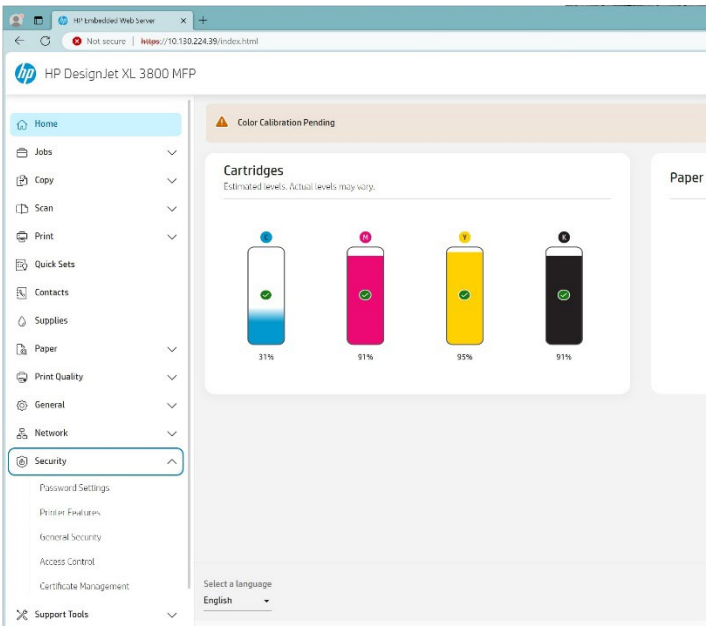
Run-time Intrusion Detection: Run-time Intrusion Detection continuously monitors the kernel memory and detects corruption or tampering attempts. Once detected, the device will self-heal by rebooting into a good state.

HP Sure Start: HP Sure Start is an advanced hardware-enforced solution providing comprehensive firmware and software settings that validates the digital signature of the BIOS

Secure access to devices by authenticating and encrypting: The SNMP Version 3 feature provides secure access to devices by authenticating and encrypting data packets over the network to provide protection against common threats to network management operations, namely Modification of Information, Masquerade, Disclosure, and Message Stream Modification.

Several of those features are not going to need to be configured, but some of them yes. To do the configuration the user can use a SIEM system connecting the printer to it, or access the printer thru the Embedded Web Server (EWS) and do the configuration.

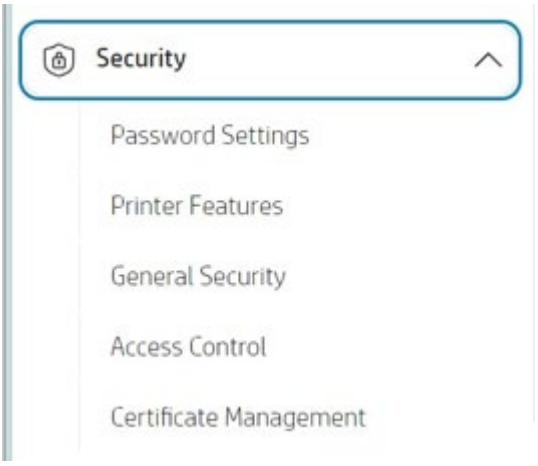
2.1.1- Embedded Web Server – portal to security



From EWS there are several places to access to the security configuration, being the ***Security*** and ***Network*** tabs the main ones.

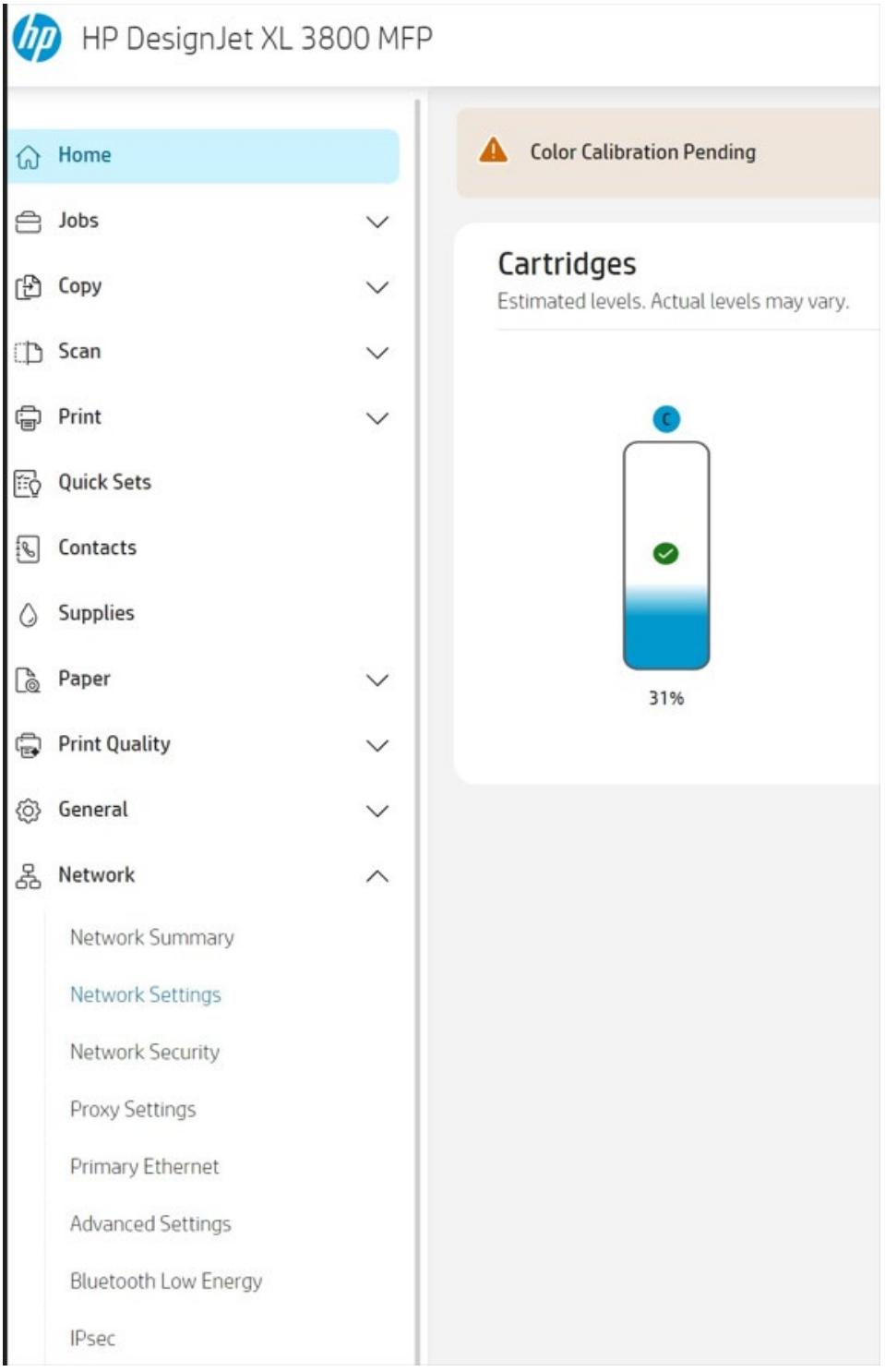
2.1.2- Security tab

On the Security tab the user will be able to perform several functions:



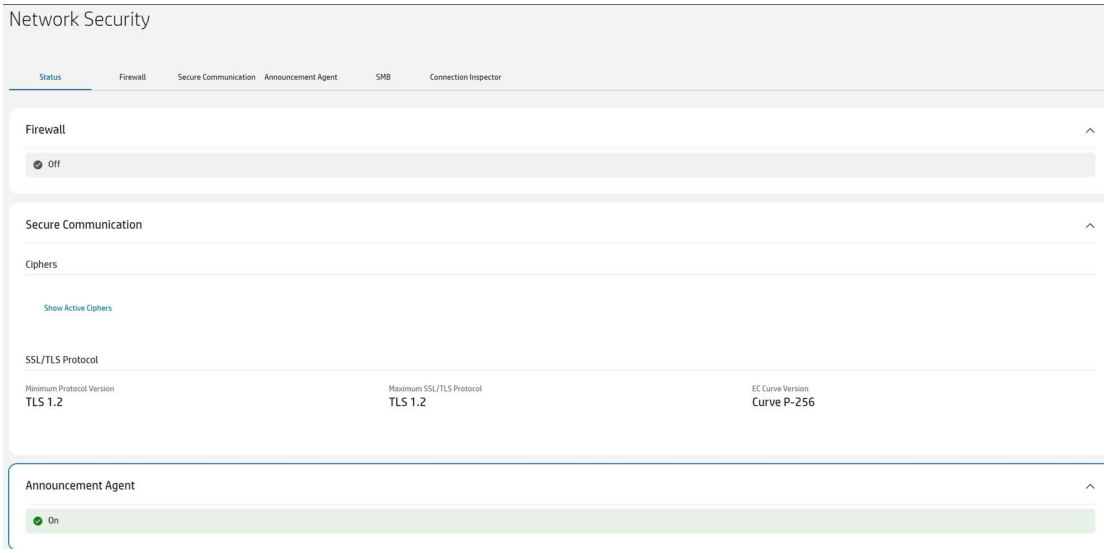
- *Password Settings*: The printer arrives to the customer site with an unique password setup from factory (no other printer will have the same password). From this tab in EWS the user will be able to change the password.
- *Printer Features*: From this tab in the Security tab, user will be able to enable / disable different functionalities in the printer, such as hardware ports (print from USB, Scan to USB), print from network folder or enable Copy functionality
- *General Security*: From here user will be able to check the status or configure settings such as EWS Session time-out and Control panel inactivity time out.
- *Access Control*: From this tab the user will be able to configure all the Access Control functionalities (permissions, printer user accounts, LDAP setup and Windows authentication)
- *Certificate Management*: From here user will be able to consult the certificates installed on the printer, and create new ones

2.1.3- Network tab



In the Network tab there are 2 tabs that are relevant for security: Network Security and IPsec

Network Security



From this tab, user will be able to:

- Enable and disable the firewall
- Select the ciphers that will be used by the different authentication protocols
- Select the SSL/TLS protocol version
- Select the EC Curbe version for the encryption

2.2- Protect your Data

Solutions, protocols and HW implemented in the printer and MFP to protect the data stored on your printer or MFP on memory hardware components, or in transit to your printer or from your printer from being intercepted or corrupted.

Self-encrypted non-volatile memory : Protects sensitive business information stored on the non-volatile (NVM) with built-in self encryption – On DesignJet XL3800, the printer comes with a 256 GB SSD with AES-256 GB self encrypted; on the BCB model, the printer comes with 500 GB HDD with AES-256 encrypted and FIPS-140-2 certification

Secure file erase: Ensures that no data is left behind in the printer after files have been deleted from the hard disk or non-volatile memory. On the Designjet XL3800 BCB model with a 500 GB self-encrypted hard drive, the deletion is done by rewriting the memory spaces several times with random data (0`s and 1`s) and after that, delete the reference to the direction of the data.

Due to the architecture of a SSD non-volatile memory, on the SSD 256GB NVM of the XL3800 model, the NVM has a ***wear-leveling mechanism*** where, when a change/write is made to a block, it actually copies the block with the change to a different block, so that the number of writes is evenly distributed across all blocks (because the spaces of memory on an NVM have a limited numbers of re-writes), and something similar happens on a delete of a file, and after that , it is deleted the reference to the direction.

Secure disk erase: Erases all information from the printer's hard disk, making it impossible to recover sensitive data (DoD 5220.22-M)

Encrypted communications: Standard encryption protocols 802.1x or IPSec use encrypted network standards to protect data traveling over the network when printing from drivers or submitters. Also the use of SNMPv3 to ensure the secure access to the device, or TLS1.3 to facilitate privacy and data security for communications over the Internet encrypting the communication between web applications and servers.

Removable HDD for security and confidentiality: Removable hard drives can be easily removed and stored securely when not in use, reducing the risk of unauthorized access to sensitive information stored on the printer. This is especially important in environments where confidentiality is paramount, such as in corporate or government settings (*only available on the XL3800 #BCB model for government*).

Swappable HDD for security and confidentiality: Swapping out the hard drive allows for secure storage of sensitive data. When handling confidential or proprietary information, such as customer files or business plans, being able to physically remove the hard drive and store it securely reduces the risk of unauthorized access or data breaches(*only available on the XL3800 #BCB model for government*).

2.3 Protect your Documents

While hackers are more commonly associated with exploiting digital vulnerabilities , stealing printed documents from a printer tray is a straightforward method of information theft.

Pull Printing : Pull printing is a function that provides end-to-end tracking and reporting to protect sensitive information and media, and reduce unclaimed print jobs. It helps boost productivity and keep abandoned documents from falling into the wrong hands. HP large format printers are also compatible with other third-party pull printing solutions.

HP Smart Card: Enhance security and improve productivity with unified printer authentication across your organization.

Encrypted Prin Printing: When users send confidential print jobs, they can assign a PIN to the document on the printer driver. The document will then be held in the printer until the user enters the PIN at the device. This way the user can be sure their confidential document won't be left unattended.

2.4 Protect your Network

Utilizing security monitoring and management solutions enables the identification of vulnerabilities and the implementation of a cohesive, policy-driven strategy to safeguard data, mitigate risks, and ensure regulatory compliance. By preventing security gaps, these solutions aid in averting potential financial penalties.

Protect your devices and network : HP Security Manager helps you reduce cost and resources to establish a fleet-wide security policy, automate device settings remediation, and install and renew unique certificates. **The Instant-on security feature** included with HP Security Manager automatically configures new devices when added to the network or after a reboot.

HP Command Center (HPCC) is a cloud solution that allows IT admins to create a security policy for onboarded devices. Using HPCC, they can assess and, if necessary, remediate device security settings to comply with pre-established company security policies.

Compliance audit reporting of print fleet security : Use HP Security Manager on premise and HPCC in the cloud to create proof-of-compliance reports that demonstrate the application of security policies to printers and the securing of customer data.

Non-compliant devices can hurt your business: Unprotected or under-protected endpoints create more opportunity for cybercrime. To help counter the growing threat, government bodies across the globe are implementing strict security regulations that require organizations to better protect customer information. It's crucial to deploy devices and solutions—like HP DesignJet printers and HP Security Manager—that can help you meet compliance requirements and protect your business information from security threats.

HP printer portfolio

		HP DesignJet T850/T950 Printer series	HP DesignJet XL 3800 Multifunction Printer
Device	HP Secure Boot	✓	✓
	HP Connection Inspector		✓
	Whitelisting	✓	✓
	Unique admin password	✓	✓
	TPM		✓
	Run-time intrusion detection		✓
	Sure start		✓
	LDAP/Kerberos user authentication		✓
	Role-based access control		✓
	Front panel access lock		✓
Data	Security event logging	✓	✓
	SNMP v3 compatibility	✓	✓
	Self-encrypted HDD		✓
	Removable HDD		✓
	No HDD	✓	
	IPSec compatibility		✓
	TLS/SSL[a]	✓	✓
	Secure file erase		✓
	Secure Disk erase	✓[a]	✓
	802.1x compatibility	✓	✓
	NTLM v2	✓	✓
Document	Encrypted PIN printing		✓
	IPv4a and IPv6 compatibility	✓	✓
	CA/JD certificates	✓	✓
	Disable network ports and protocols	✓	✓
	HP SmartCard Solution[1]		✓
	PIN printing	✓	✓
Fleet security management	HP Web JetAdmin	✓	✓
	HP Security Manager/HP Command Center	✓	✓
	SIEM integration	✓	✓

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 at startup integrity of all the code and data used to control the printer, guaranteeing that no malicious code is 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.



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 multifunction 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 as certificates even access to the HDD would have been done.

TPM

Hardware component used to securely store cryptographic keys and perform cryptographic operations. The TPM capabilities are used to add additional security protection to data stored in the system, such as certificates, and to enable secure cryptographic operations to identify and communicate with the printer. 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.

Encrypted PIN printing

The data sent to the printer when using the PIN printing feature is encrypted.

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

© 2014, 2016, 2021 HP Development Company, L.P. 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 constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Adobe™ and PostScript™ are trademarks of Adobe Systems Incorporated, which may be registered in certain jurisdictions.

January 2021