Brochure

Keep your data safe

How HP DesignJet printers can protect your business

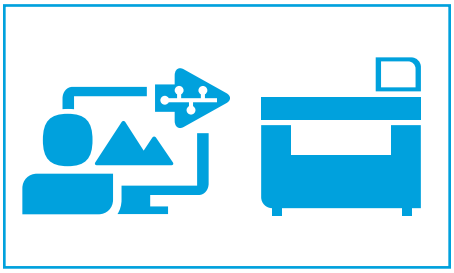
More than ever, it's critical for institutions to protect their most important, confidential, and sensitive data on their networks. That includes the information on their printers, which can store an enormous amount of data. In fact, for most companies, it's a luxury to have a large-format printer with security features manufactured in a trade-compliant country that can make the IT administrator's life easy.

HP DesignJet printers are designed with these needs in mind, featuring multiple security measures designed to keep data safe from harm and protected from incompatibility, tampering, theft, or disaster.

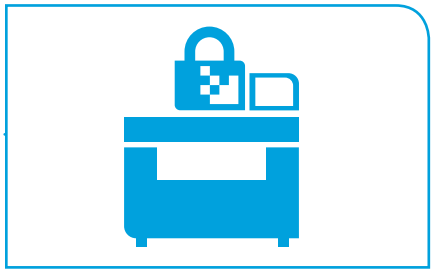
This document outlines the variety of features available on HP DesignJet printers designed to protect your data, and your business.

Security

The security features described in this document make HP DesignJet printers particularly well suited to deployment in environments where security features for network management, data transfer, controlled printer access, and data erasure are extremely important.

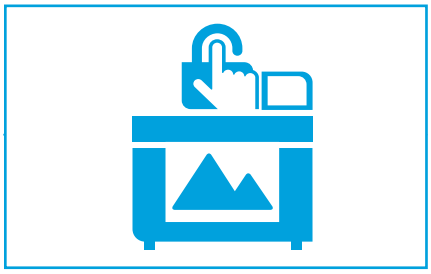


1. Data in transit
Help protect your data and user credentials from eavesdropping or from being tampered with while transferring through the company network or the Internet.



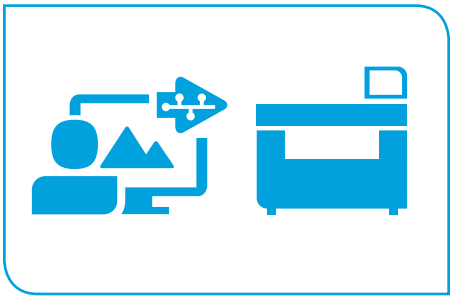
2. Data in storage
Protect your confidential data stored at the printer from being stolen or accidentally moved out of the department where it belongs, by encrypting or properly erasing the internal HDD (hard disk drive).

4. Help intrusion prevention
Keep hackers away and help prevent the printer from being hijacked and used against your network.



3. Authentication and authorization
Let users identify themselves so you keep control on the activities, features, expenses, and protocols each user is permitted to use.

1. Data in transit



Help protect your data and user credentials from eavesdropping or from being tampered with while transferring through the company network or the Internet.

Internet Protocol Security IPsec compatibility
IPsec is a standard that provides security at the IP (network) layer of TCP/IP-based communication. IPSec allows for private and secure communications over the public Internet. HP DesignJet printers are compatible with IPSec and provide the following benefits:

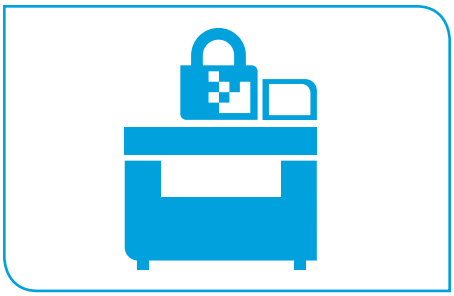
- Help ensure data confidentiality by making it difficult for anyone but the receiver to understand the data being communicated
- Allow each party in a communication session to reliably authenticate each other
- Help ensure that the data is not altered during transmission
- Protect against unauthorized resending of data

IPv6 and IPv4 compatibility
Easily transition from IPv4 to IPv6 with HP DesignJet printers. While IPv4 was a solid and long-lasting TCP/IP protocol version, the IPv6 protocol takes you to the next generation, solving the IP address limitation problem for an ever-increasing number of network devices.

CA/JD certificates
You can request, install, and manage digital certificates on the HP Jetdirect Embedded Print Server included in most HP DesignJet printers. Certificates are used to identify the HP Jetdirect Embedded Print Server both as a valid web server for network clients and as a valid client requesting access on a network with security features. By default, the HP Jetdirect Embedded Print Server contains a self-signed pre-installed certificate to provide optimal security from setup. It is possible to issue new certificates using this card.

TLS/SSL protocols
TLS/SSL are most widely recognized as the protocols that provide secure HTTP (HTTPS) for Internet transactions between web browsers and web servers. TLS/SSL can help to secure transmitted data using encryption. TLS/SSL also authenticates servers and, optionally, authenticates clients to prove the identities of parties engaged in secure communication. It also provides data integrity through an integrity check value. In addition to protecting against data disclosure, the TLS/SSL security protocol can be used to help protect against masquerade attacks, man-in-the-middle or bucket brigade attacks, rollback attacks, and replay attacks.

2. Data in storage



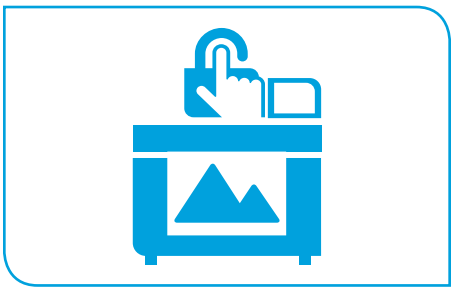
Protect your confidential data stored in the printer from being stolen or accidentally moved out of the department where it belongs, by encrypting or properly erasing the internal HDD (hard disk drive).

Secure File Erase
Secure File Erase is a feature that manages how files are deleted from the printer's hard disk, which can help ensure that no data is left behind in the printer. There are three security modes to the Secure File Erase feature, with the most secure meeting the United States Department of Defense (US DOD) 5220-22.M requirements for clearing and sanitization of disk media. When the Secure File Erase feature is enabled, all temporary files that might contain sensitive data are erased and no temporary files remain after a job has completed (scan, copy, or print). Secure File Erase is performed whenever the system is finished with a file and calls the delete procedure. If the Secure File Erase mode is never set to a secure mode, the system still deletes these files on a continuous basis, using an insecure manner. The printer performance can be affected while increasing the Secure File Erase level.

Secure Disk Erase
Secure Disk Erase allows the erasing of all information from the hard disk drive inside the printer in a secure manner, making it impossible to recover the information. It is possible to trigger a Secure Disk Erase using the US DOD 5220-22.M specification to erase all data from the hard disk partition that contains the user data.

The Advanced Encryption Standard (AES) reduces the risk of stolen data. AES technology provides trust that the printer's hard drive data is not readable if the hard disk is removed from the device. The SED supports AES256 encryption, following the FIPS 140-2 Level 2 (tamper evident sticker compliant) requirement.

There's no need to activate any settings or perform any action to encrypt the content. The SED is also protected with an ATA password, unique for each printer and changeable when required.



Let users identify themselves so you keep control on the activities, features, expenses, and protocols each user is permitted to use.

3. Authentication and authorization

HP native security capability

Control panel access lock

The control panel access is a feature intended for IT administrators, which allows them to lock the printer's control panel using either HP Web Jetadmin software, or the printer's HP Embedded Web Server. This feature prevents unauthorized users from accessing the control panel and changing the printer's settings. There are four levels of access that can be set:

- Minimum Lock—this option denies access to the Resets options, Enable/Disable connectivity options, and the Service Menu
- Moderate Lock—in addition to the Minimum Lock, this option also denies access to all printer settings, the job queue, information and service prints, and the printer log
- Intermediate Lock—in addition to the Moderate Lock, this option also denies access to the paper and ink supplies handling options, maintenance options, and demo prints; only viewing of printer and supplies information is allowed
- Maximum Lock—this option denies access to all options in the control panel

Disable interfaces

HP DesignJet printers are designed so that some ports can be disabled to help prevent unauthorized printing and scanning and possible data theft. For example, disabling the USB printing port prevents people from inserting a USB drive into the printer and printing or scanning to it.

Personal identification number (PIN) printing

Does your business need to print confidential or sensitive documents? Often, users need to print private documents to shared printers across a company's network. The HP DesignJet printer portfolio holds print jobs until a user enters a PIN to release the job to help ensure that confidential documents do not print until the user is physically present at the printer.

NTLMv2

NTLMv2 is used to authenticate the device to file servers, so it is allowed to put files from the scanner into a shared file folder. V2 is the latest version of this protocol, required by savvy administrators to make sure that authentication credentials are not captured in transit on the network.

Third-party security solutions

API Netgard® MFD Smartcard security appliance for CAC, PIV, and CIV cards

API Netgard® MFD is a drop-in, inline, multi-factor, user authentication solution for networked, special-purpose devices such as multifunction printers, scanners, and copiers. Netgard® protects a network by requiring users to authenticate themselves with a smartcard (CAC/PIV-personal identity verification, CIV commercial identity verification) and personal identification number (PIN), thereby preventing unauthorized users from accessing privileged materials or distributing unauthorized material. Without a card and PIN, Netgard® does not permit the user to print, scan, or send from the multifunction device to network resources.

- CAC/PIV/CIV authentication (HSPD-12 and DOD Compliant)
- Email encryption, secure print release, and scan-to-home
- Integrated with the HP DesignJet on-screen display

For more information, please visit
apitech.com/products/netgardmfd

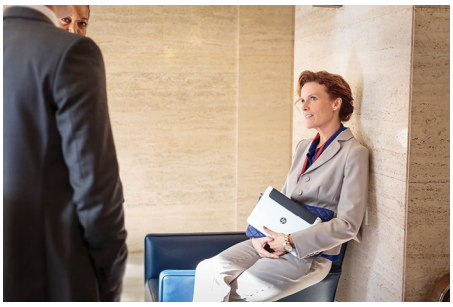
4. Intrusion prevention

Disabling unused protocols

In some cases, you may 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 through the FTP or connecting through telnet to 'manage protocols' the printer network settings. You can disable unused protocols through the Mgmt.protocols option in the HP Embedded Web Server or Network Enable features in HP Web Jetadmin.

Keep hackers away and help prevent the printer from being hijacked and used against your network.

To learn more about HP DesignJet printers and security features, visit
hp.com/go/designjetT120
hp.com/go/designjetT520
hp.com/go/designjetT730
hp.com/go/designjetT790
hp.com/go/designjetT795
hp.com/go/designjetT1300
hp.com/go/designjetT830
hp.com/go/designjetT930
hp.com/go/designjetT1530
hp.com/go/designjetT2530
hp.com/go/designjetT7200



Network management security features through SNMP v3
HP DesignJet printers can be managed through SNMP v1 and v2. In addition, most HP DesignJet printers can be managed via SNMP v3 which provides the following additional benefits:

- 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 Managed Device data that can be accessed by each Network Management System

802.1x compatibility
To provide additional security, a select number of HP DesignJet printers are 802.1x compatible out of the box. The 802.1x standard provides access control to the Ethernet network, and network devices that are unable to authenticate to the 802.1x authorization server are denied all network access. 802.1x can prevent unauthorized users from attaching devices to the network and can help ensure that only IT-deployed and trusted devices, such as those with virus protection software, are allowed access.

Supported 802.1x authentication protocols and configuration settings support the following protocols:

- **PEAP**—Protected Extensible Authentication Protocol (PEAP) is a mutual authentication protocol that uses digital certificates for network server authentication and passwords for client authentication.
- **EAP-TLS**—Extensible Authentication Protocol using Transport Layer Security (EAP-TLS) is a mutual authentication protocol based on digital certificates for authentication of both the client and the network authentication server.

Goverment

TAA Compliance
Select HP DesignJet printers (see table on page 6) are manufactured in TAA-compliant countries. TAA refers to the Trade Agreements Act (19 U.S.C. & 2501-2581), which is intended to foster fair and open international trade. TAA requires that the U.S. Government may acquire only “U.S.-made or designated country end products.” This act requires contractors to certify that each end product meets the applicable requirements. End products are “those articles, materials, and supplies to be acquired for public use.” This includes items that have been “substantially transformed” in the United States.

High-performance Self-encrypting Drive (SED)
The Self-encrypting Drive (SED) is designed to ensure your print data is automatically encrypted every time data is sent to the printer and written to the drive. It provides an additional layer of security for all of your printed files and reduces the risk of tampering or unauthorized access to the data. With an SED installed on select HP DesignJet printers, workgroups can safely store and print their most sensitive data over a network with security features.

FIPS certified Self-encrypting Drive (SED):
The Self-encrypting Drive (SED) is designed to ensure your print data is automatically encrypted every time data is sent to the printer and written to the drive. It provides an additional layer of security for all of your printed files and reduces the risk of tampering or unauthorized access to the data. With an SED installed on select HP DesignJet printers, workgroups can safely store and print their most sensitive data over a network with security features.
Certified military-strength encryption level.

Wi-fi removed
For products that have WiFi capabilities, there may be an orderable SKU that disables these capabilities to address security or health concerns.

Removable HDD
For high-security environments using confidential data, it is possible to disconnect and remove the printer HDD so that it can be kept in a safe place while the printer is not in use. Or to make it easier to destroy the HDD with any confidential data in case of need.

IT friendly

HP DesignJet printers are also designed for manageability in IT environments, with some additional solutions.

HP accounting solutions
HP DesignJet printers include advanced accounting features, enabling users to monitor usage, including statistics such as the amount of paper and ink used per job and per user. The user can retrieve this information directly from the printer, or instruct the printer to send it automatically by email at regular intervals.

Third-party accounting solutions
To track the usage of a wider variety of HP DesignJet printers, you can use HP certified third-party solutions that offer accounting or cost tracking. The HP certification program includes a comprehensive set of compatibility criteria, with certified software products taking advantage of the unique capabilities of HP DesignJet printers.

The third-party solutions that have been awarded HP Certified Accounting Solutions status have demonstrated compatibility with the HP DesignJet Accounting Software Development Kit (SDK) and use the advanced accounting features of the supported HP DesignJet printers. The following HP Certified Accounting Solutions are currently available:

- Sepialine Argos (sepialine.com)
- Capella MegaTrack (capellatech.com)
- Technesis (technesis.com)
- Printerpoint (printerpoint.com)
- Cloud4MPS (cloud4mps.com)
- Kothari KoJac™ (kothariinfotech.com)
- ARC Abacus (e-arc.com)

Note: HP does not warrant, and is not liable or responsible for, the accuracy of the information provided, the performance or compatibility, or the regulatory and/or legal compliance for any of the third-party products listed above.

HP Web Jetadmin access
HP Web Jetadmin is the user interface that manages the Secure File Erase and Secure Disk Erase functionality. This is the same functionality that is used in the HP Web Jetadmin device plug-ins for HP LaserJet printers, allowing you to set the same global options across your fleet of HP DesignJet printers.

To learn more visit
hp.com/go/webjetadmin

HP Embedded Web Server
The HP Embedded Web Server is a powerful remote access tool that can be used to manage the printer, check print jobs, and determine usage costs and is included with most HP DesignJet printers. The level of detail and functionality of the HP Embedded Web Server varies between printer models.

Accessing the HP Embedded Web Server of an HP DesignJet printer simply requires a TCP/IP connection and a standard web browser. Some of the powerful features offered by the HP Embedded Web Server include:

- Checking the status of the printer
- Checking the status of the printing supplies
- Updating the firmware
- Checking supply usage for each print job
- Managing the network settings

HP DesignJet Universal Print Driver (UPD)
The HP DesignJet Universal Print Driver (UPD) provides users and administrators with a standardized, one-driver solution for their printing needs. Instead of installing and managing individual drivers for each printer model, administrators can install the HP DesignJet UPD for use with a variety of HP large format printers. With only one package to manage, testing and internal certification of print drivers is simplified by the use of the HP DesignJet UPD packages. Time spent on installation, both on servers and workstations, is greatly reduced, and hard drive space formerly occupied by many product-specific drivers is now diminished significantly.

To learn more visit
hp.com/go/designjetupd

HP DesignJet printers—Security and manageability features

		HP DesignJet T120 Printer and HP DesignJet T520 Printer series	HP DesignJet T730 Printer	HP DesignJet T790 Printer series	HP DesingJet T795 Printer series and HP DesignJet T1300 PostScript Printer	HP DesignJet T830MFP	HP DesignJet T930 and HP DesignJet T1530 Printer series	HP DesignJet T2530 MFP and HP DesignJet T3500 Production MFP	HP DesignJet T7200 Production Printer
Data in transit	IPSec compatibility	-	-	✓	✓	-	✓	✓	✓
	IPv4 & IPv6 compatibility	-	✓	✓	✓	✓	✓	✓	✓
	CA/JD certificates	-	✓	✓	✓	✓	✓	✓	JD640
	TLS/SSL	-	✓	✓	✓	✓	✓	✓	JD640
Data in storage	No HDD	✓	✓	-	-	✓	-	-	-
	Secure File Erase (SFE)	-	-	✓	✓	-	✓	✓	✓
	Secure Disk Erase (SDE)	-	-	✓ / PS[1]	✓ / PS[1]	-	✓	✓	✓
Authentication and authorization	Control panel access lock	-	-	✓	✓	-	✓	✓	✓
	Disable interfaces	-	✓	✓	✓	✓	✓	✓	✓
	Personal identification number (PIN) printing	-	-	-	-	-	✓	✓	-
	NTLMv2	-	-	-	-	✓	-	✓	-
	API Netgard® MFD Smartcard security appliance for CAC, PIV, & CIV cards	-	-	✓	✓	-	✓	✓	-
	Disable USB drive	-	✓	✓	✓	✓	✓	✓	-
Intrusion prevention	Disable protocols	✓	✓	✓	✓	✓	✓	✓	✓
	SNMP v3 compatibility	-	✓	✓	✓	✓	✓	✓	✓
	802.1x compatiblitiy	-	✓	JD640	JD640	✓	✓	✓	JD640
Government only #BCB localizations	TAA-complaint country	✓	✓	✓	✓	✓	✓	✓	✓
	FIPS certified self-encrypting drive	-	-	✓	✓	-	✓	✓	✓
	Wi-Fi removed	✓	✓	-	-	✓	-	-	-
	Removable HDD	-	-	✓	✓	-	✓	✓	-
IT friendly	HP accounting solutions	-	-	✓	✓	-	✓	✓	✓
	Third-party accounting solutions	-	-	✓	✓	-	✓	✓	✓
	HP Web Jetadmin compatiblitiy	✓	✓	✓	✓	✓	✓	✓	✓
	HP Embedded Web Server	✓	✓	✓	✓	✓	✓	✓	✓
	HP DesignJet Universal Print Driver (UPD)	✓	✓	✓	✓	✓	✓	✓	✓

[1] Only in PostScript enabled devices

For more information, contact your HP representative today or visit
hp.com/go/designjet

4AA4-7458ENA, June 2016, Rev.3