Multilayered Print Protection:

How Dell empowers organizations to take control of printer security

Abstract

Organizations are looking for ways to maximize the security of their IT environments. An important part of IT security is protecting network printers. These essential devices are subject to both physical and network-based threats from internal and external sources. To guard against these threats, Dell printers and multifunction print devices are equipped with a variety of security features.

This paper provides a comprehensive survey of the printer security features provided by Dell to help organizations minimize the risk of unauthorized access to documents, guard against hacking and other network-based security threats, and audit user activity. Taken together, these features provide deep, multilayered protection and empower IT administrators to take control of printer security.

Multilayered Print Protection

How Dell empowers organizations to take control of printer security

Printers are easy to overlook when evaluating IT security and risk management. Advanced multifunction printers (MFPs) that provide printing, fax, and scan to e-mail capabilities are often considered simple output devices. However, network printers and MFPs are subject to security threats from both internal and external sources. These threats can be categorized as physical or network-based.

IT organizations are familiar with the need to guard against network-based threats to servers. Printers operating in a networked environment should be treated the same way. Today's printers have powerful processors running embedded Web servers (EWSs) that enable key services but can also be used as a conduit to launch an attack on the network. Some of the potential threats in a network environment include:

- Unauthorized access to the printer or MFP
- Denial-of-service attacks—tampering with device administrator settings or even changing the network location of the printer
- Using the printer or MFP to start an external hacking attack through an unused or open port

Physical security threats are no less important. In a workplace where many users share common printers, physical security breaches at the device are always a possibility. A user with unrestricted access to the printer may take a confidential document printed by someone else. Vulnerable documents include printed or copied items left inadvertently on the printer output trays and received faxes sitting unattended on a multifunction printer.

Unauthorized access to these documents can lead to an information leak or breach of confidential data such as an organization's financial information or intellectual property. It may increase the risk of identity theft, and can even pose regulatory risks if documents such as health records are involved. In today's digital world, minimizing security risk and protecting confidential information has become a top priority, and protecting network printers is a critical part of the data security equation.

Network Security	Device Security	
	Data	Physical
Confidentiality **Integrity** **Non-repudiation** • HTTPS (SSL/TLS) • IPSec • Secure IPP • SNMPv3	**Authenticate** **Authorize** **Identification** **Data erase** • Password/PIN access • Disk Erase (M5220.22) • AES encryption • Initiate/scheduled sanitization	**Access** • Slot for locking device, formatter, and trays
Monitor and Manage		
Configuration and management **Usage logs and audit trails** **Monitoring of availability of services** • Ability to disable unused ports, protocols • PIN/Password setup upon power on		

Figure 1. Dell laser printers are protected by multilayered security to safeguard information assets

Taking control of printer security

As a technology company familiar with enterprise security requirements from desktops to data centers, Dell gives document security the priority it deserves—and empowers IT administrators to adapt security measures to the needs of their organizations. Dell laser printers not only deliver excellent printing performance at a low cost per page, but also ship with standard security technology that helps to safeguard an organization's information assets by providing layered printer protection.

Dell's layered protection covers multiple points from the physical device to the print content to the network (Figure 1). The following are some of the key security features widely supported by Dell printers. For a complete table of features supported by the various Dell laser printer models, see page 6 of this document.

Print job security features

These Dell printer and MFP features are designed to help minimize the risk of unauthorized access to printed documents.

Secure Printing

Dell Secure Printing helps to minimize risk by securely storing the print job in a password-protected location. Users can control the timing of their output by providing a four-digit password when sending the print job to the printer. The printer then stores the print job either in RAM or on the hard disk drive; the job is released only when the originator enters the four-digit password on the printer's front panel.

Stored print

Users can store print jobs in the printer and securely release the print job with a four-digit password. This feature is helpful for storing frequently printed documents such as forms. Instead of walking to the printer multiple times to collect printouts, users can securely release multiple print jobs at once.

Secure Printing and stored print can be accessed by opening the print driver window, clicking the Properties button, pulling down the Job Type menu, and selecting the Secure Print option (Figure 2). The print job is released by selecting the user name and keying in the password on the printer's operator panel.

Jam Recovery

Administrators have the option of turning off the Jam Recovery feature on a printer to keep it from automatically reprinting jobs after a paper jam is cleared. If a printer jams, the originator of the print job is often not the person who clears the jam. This situation is a potential security risk because the reprinted copies may end up with an unauthorized person. With Jam Recovery turned off, pages will not reprint until the originator resends the job.

Physical locking

Dell printers and MFPs offer slots for locking the device and trays. Optional printer trays are protected with built-in locks on many printer models.

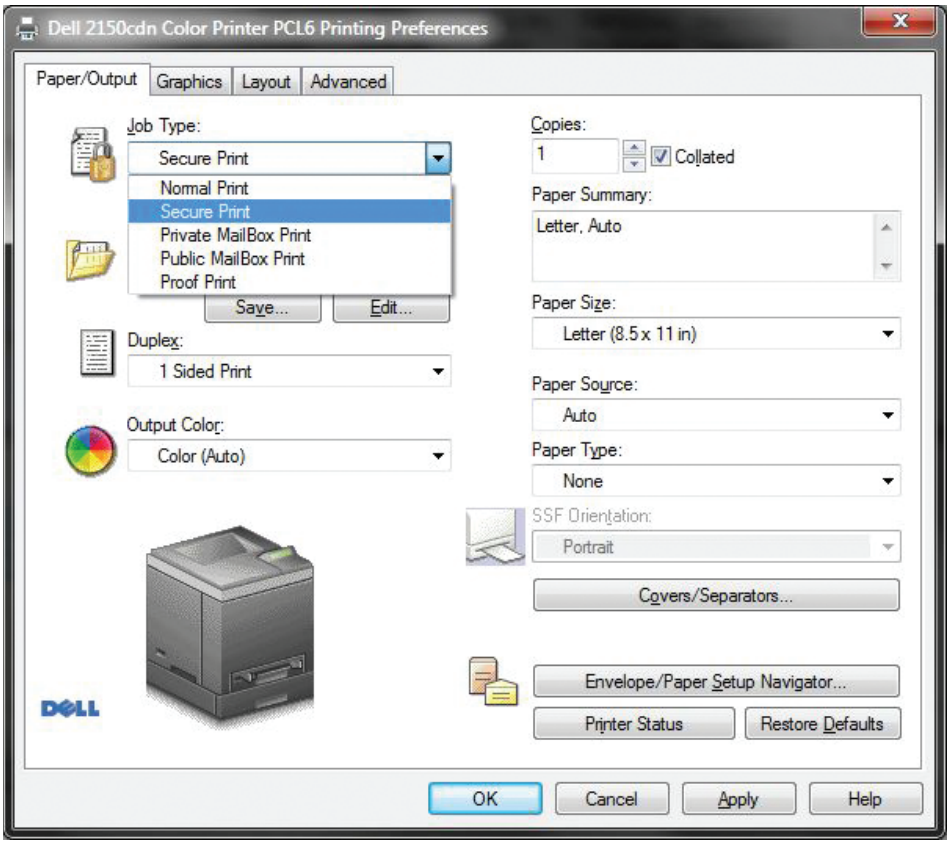

Figure 2. Users can access Secure Print from the Paper/Output tab under Properties in the print driver window

Disk Erase

The hard drive in a printer device automatically stores all print jobs. Disk Erase capability lets administrators clean the drive, which helps to eliminate the risk of an unauthorized person reading the hard drive and taking the data out of the printer. This feature also enables the device to be wiped clean for security if it is recycled or resold.

Network security features

These features are designed to protect against hacking and other network-based security threats.

Securing the Dell Web Tool

Dell network printers and MFPs are designed so that authorized persons can control the devices remotely using an EWS called the Dell Web Tool. To protect against unauthorized access, administrators can secure the Dell Web Tool by setting a password. Each printer ships with a default password of null (no password); administrators can change the default password during setup, preventing hackers from gaining access to the EWS and changing the printer settings.

IP filter (Access Control List)

The Dell Web Tool can be accessed by typing a device's IP address into an Internet browser. Administrators can use an IP filter called the Access Control List to prevent an unauthorized host from accessing the printing device. The IP filter consists of a list of IP addresses of PCs and notebooks that are allowed

to access the printer. If a computer's IP address is not on the Access Control List, it will be blocked from using the printer or configuring the printer through the Dell Web Tool.

Administrators can set up the IP filter using the Dell Web Tool. The process has a built-in safeguard: if the IP addresses in the IP filter list are entered incorrectly, access to the printer is lost and the device must be reset to its factory default in order to recover.

Secure access by HTTPS

Dell printers also support the HTTP over SSL (HTTPS) protocol to securely access the Dell Web Tool using an entry such as https://169.XX.XX.XX. HTTPS connections are often used for payment transactions on the Web and for sensitive transactions in corporate information systems. Using HTTPS can ensure that passwords and all administrator communications to the device are encrypted.

IPSec protection

IP Security (IPSec) is a suite of protocols for securing IP communications by authenticating and encrypting each IP packet. This suite supports both IPv4 and IPv6 networking. For printers and MFPs, IPSec is used to protect print job data sent between a host and the printing device. The print data is transported securely from the host to the printer by encrypting the data packets in the network transport layer. Because the data is encrypted, any sniffing of the data during the transport stage is ineffective. IPSec can be enabled through the print server using the Dell Web Tool.

Secure management through network (SNMPv3 and HTTPS)

IT administrators may use printer management tools such as Dell™ OpenManage™ Printer Manager to manage and monitor the printer fleet. These network printer management tools often employ industry-standard network protocols such as Simple Network Management Protocol (SNMP) and Hypertext Transfer Protocol (HTTP). Dell printers are equipped with the necessary security protocols, including HTTPS and SNMPv3, to permit management of the device over a secure network connection.

SNMPv3 employs an authentication mechanism and privacy password to help secure a management session over the network with the device. The privacy password is used to encrypt the data transmitted over the network between the device and the host that initiated the secure session.

Disabling unused network ports and protocols

Keeping unused ports and protocols open invites unauthorized access and threats from hackers. For this reason, it is advisable to keep unused ports and protocols closed. For example, in a network using only TCP/IP, you should close protocols such as Ethertalk, Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), and so on.

Similarly, unused ports such as ftp or Telnet should be closed. Dell printers allow administrators to disable unused ports and protocols using the Dell Web Tool. When closing unused ports, administrators should take care not to close Port 9100, as most print data goes through this port.

Access control and authentication

User authentication and access control features help to secure user access and also audit user activity.

Operator panel lock

Printer or MFP device configuration settings can be accessed from the front panel of the device by pressing the Menu button. This ease of use can lead to non-administrators accessing configuration settings and making unwanted changes. To minimize the risk of non-administrators gaining access to the configuration settings, administrators can lock the control panel using a four-digit password. The operator panel can also be locked remotely with the Dell Web Tool.

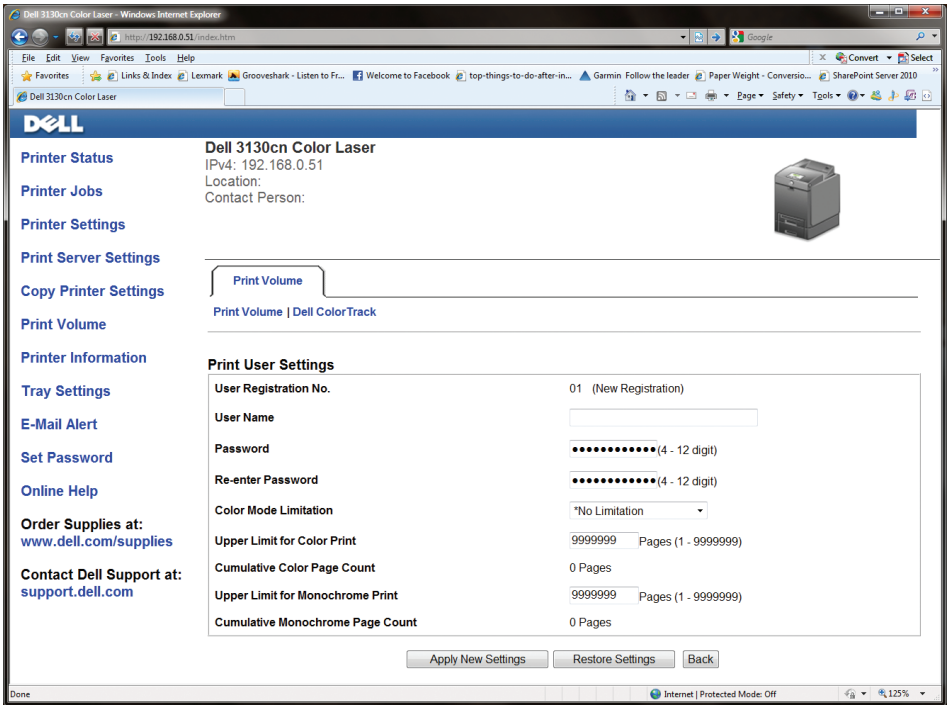

Figure 3. Administrators can access and set ColorTrack through the printer Embedded Web Browser

Multilayered Print Protection

How Dell empowers organizations to take control of printer security

Color control

Determining who should have access to color printing, and in what volume, is a key to managing print costs effectively. With Dell ColorTrack technology, administrators can assign levels of access that are appropriate for different individuals or groups (Figure 3). For example, graphic designers may require unlimited access to color printing to be productive, while finance departments may need only black and white printing. Other groups such as sales departments may require access to color printing, but within limits.

Administrators can open the Dell Web Tool of the desired printer by putting the printer's IP address in a Web browser. Clicking Print Volume and then clicking the Dell Color Track link brings up the Dell Color Track settings.

Usage auditing

Print History and Job Meter reports available in Dell printers and MFPs help IT administrators to track all printing activity in their devices. This capability helps prevent unauthorized use by detecting overuse and anomalies. It also helps ensure that printers are physically located to make the best use of printer assets. If a printer is underused, it can be moved to a better location within the work environment.

MFP user authentication

Multifunction devices in a highly classified environment can lead to security threats. An unauthorized person could scan to e-mail or photocopy sensitive documents, leading to a breach of security. The Dell MFP 2145cn color laser printer supports user authentication via Kerberos, SMB, or a local user access list, making it a good choice for highly classified environments.

		Color Single Function						Color Multifunction		
AREAS	**SECURITY ATTRIBUTES**	**Dell 1250c**	**Dell 1350cnw**	**Dell 2150cn/ 2150cdn**	**Dell 3130cn**	**Dell 7130cdn**	**Dell 5130cdn**	**Dell 1355cn/ 1355cnw**	**Dell 2155cn/ 2155cdn**	**Dell 3115cn**
Secure output (Print Job)	Confidential print	No	No	Yes[1]	Yes[1]	Yes[1]	Yes[1]	No	Yes[1]	Yes[1]
	Confidential stored print	No	No	No	No	Yes[1]	Yes[1]	No	No	No
	Print job encryption	No	No	No	No	Yes[6]	No	No	No	No
	Jam recovery (On/Off)	No	No	No	No	Yes	No	No	No	No
Print Data Security	Hard disk encryption	No	No	No	No	No	Yes	No	No	No
	Hard disk secure erase	No	No	No	No	Yes	Yes	No	No	No
Network Security (Wired)	HTTPS / SSL/TLS	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes[3]
	IP filter (access control list)	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
	SNMPv3	No	No	Yes	Yes	Yes	Yes	No	Yes	No
	IPSec	No	No	Yes	Yes	Yes	Yes	No	Yes	No
	802.1x wired security	No	No	Yes	No	Yes	Yes	No	Yes	No
	Port management (disable ports)	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Securing User Access	Secure Dell web tool (EWS) access	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[3]
	Operator panel lock	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Color printing access control	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
	Copy control (for MFP)	NA	NA	NA	NA	NA	NA	No	Yes	Yes
	Network authentication (Kerberos/SMB)	No	No	No	No	No	Yes	No	Yes	No
Fax	Confidential fax receive	NA	NA	NA	NA	NA	NA	No	Yes	Yes
	Junk fax barrier	NA	NA	NA	NA	NA	NA	Yes	Yes	Yes
	LAN – fax circuit isolation	NA	NA	NA	NA	NA	NA	Yes	Yes	Yes
Physical Security	Kensington lock slot on printer	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
	Kensington slot on tray	No	No	Yes	Yes	No	Yes	NA	Yes	Yes

Table 1. Current Dell product support, color laser printers

Fax security features

Fax functionality in today's multifunction devices requires protection against physical and network-based attacks.

LAN—Analog fax bridge

There is a risk with MFP devices when the fax circuit and LAN have a firmware or hardware bridging. If there is a bridge, a hacker can gain access to the network through the analog fax. During the design stage, Dell MFPs are careful to separate the analog fax and LAN circuitry to provide fax security.

Secure fax receiving

Unattended fax printouts in the output tray of a multifunction printer create a risk of unauthorized persons acquiring sensitive information. With Secure Fax, administrators can eliminate unattended printing of fax jobs. The administrator configures the MFP to release received fax jobs only after the user enters a four-digit PIN code in the MFP operator panel. In Secure Fax mode, received faxes are stored in the printer memory. Once the memory is full, the device will stop receiving faxes until the jobs are released.

[1] Feature is supported with optional 512 MB/1 GB memory DIMM
[2] Feature is supported with optional Hard disk drive
[3] Feature supported with optional multi protocol card (MPC) or Network Protocol Adaptor
[4] Feature supported with optional Gigabit card
[5] Feature supported with optional Print Encryption card
[6] Feature supported through IPP/SSL
[7] Feature supported with optional 256 MB RAM on-board
[8] HTTPS supported

Multilayered Print Protection

How Dell empowers organizations to take control of printer security

		Mono Single Function Printers											Mono Multifunction Printers				
AREAS	**SECURITY ATTRIBUTES**	**Dell 1130**	**Dell 1130n**	**Dell 1135n**	**Dell 2230d**	**Dell 2350d/ dn**	**Dell 3330dn**	**Dell 5330dn**	**Dell 7330dn**	**Dell 5230n/ dn**	**Dell 5350dn**	**Dell 5530dn**	**Dell 2335dn**	**Dell 2355dn**	**Dell 3333dn**	**Dell 3335dn**	**Dell 5535dn**
Secure output (Print Job)	Confidential print	NA	NA	NA	No	No	Yes	Yes	Yes[1]	Yes	Yes	Yes	Yes[7]	Yes	Yes	Yes	Yes
	Confidential stored print	No	No	No	No	No	No	Yes	Yes[1]	No	No	No	No	No	No	No	No
	Print job encryption	No	No	No	No	No	Yes[5]	No	Yes[6]	Yes[5]	Yes[5]	Yes[5]	No	No	Yes[5]	Yes[5]	Yes[5]
	Jam recovery (On/Off)	No	No	No	No	Yes	Yes	Yes	Yes[1]	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Print Data Security	Hard disk encryption	NA	NA	NA	No	No	NA	Yes	No	Yes[2]	Yes[2]	Yes[2]	No	No	Yes[2]	Yes[2]	Yes[2]
	Hard disk secure erase	NA	NA	NA	No	No	NA	Yes	Yes	Yes[2]	Yes[2]	Yes[2]	No	No	Yes[2]	Yes[2]	Yes[2]
Network Security (Wired)	HTTPS / SSL/TLS	NA	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes[8]	Yes	Yes	Yes	Yes
	IP filter (access control list)	NA	Yes	Yes	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	SNMPv3	NA	Yes	Yes	NA	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	IPSec	NA	Yes	Yes	NA	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Port management (disable unused Ports)	NA	No	No	NA	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
	802.1x wired security	NA	No	No	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Securing User Access	Secure Dell web tool (EWS) access	NA	No	No	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Operator panel lock	No	No	No	NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Copy control (for MFP)	NA	NA	No	NA	NA	NA	NA	NA	NA	NA	NA	Yes	Yes	Yes	Yes	Yes
	Network authentication (Kerberos/SMB)	NA	No	No	No	No	Yes	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Fax	Confidential fax receive	NA	NA	Yes	NA	NA	NA	NA	NA	NA	NA	NA	Yes	Yes	NA	Yes	Yes
	Junk fax barrier	NA	NA	Yes[9]	NA	NA	NA	NA	NA	NA	NA	NA	Yes	Yes	NA	Yes	Yes
	LAN – fax circuit isolation	NA	NA	Yes	NA	NA	NA	NA	NA	NA	NA	NA	Yes	Yes	NA	Yes	Yes
Physical Security	Kensington lock slot on printer	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	Kensington slot on tray	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No

Table 2. Current Dell product support, monochrome (black and white) printers

Junk fax restriction

Administrators may want to restrict MFPs to receiving faxes only from certain numbers or block certain phone numbers from sending faxes. The Junk Fax feature in the MFP control panel allows administrators to configure those settings.

Security feature matrix

Tables 1 and 2 show the security features supported by specific Dell laser printer models. In both tables, Yes means a feature is supported, No means it is not supported, and NA means that the feature is not applicable for this class of product.

[1] Feature is supported with optional 512 MB/1 GB memory DIMM
[2] Feature is supported with optional Hard disk drive
[3] Feature supported with optional multi protocol card (MPC) or Network Protocol Adaptor
[4] Feature supported with optional Gigabit card
[5] Feature supported with optional Print Encryption card
[6] Feature supported through IPP/SSL
[7] Feature supported with optional 256 MB RAM on-board
[8] HTTPS supported

For more information

For more details on Dell printers and printer security, visit **DELL.COM**/printers.

If you are interested in upgrading your Dell printer security capabilities, or if you have questions about security and Dell printers, contact your Dell sales team and ask for a print management consultant. For complete information on using Dell printers and security features, see the operating manual for your Dell printer product.

To learn more visit dell.com/Printers