Brochure

The world's most preferred printers.

Help your customer improve print security

Many organizations have implemented a security strategy for their network and endpoints, including rigor around PC security. However, most do not include their imaging and printing devices in their overall security strategy. If not properly secured, printers and MFPs can also expose a network to security risk. Organizations should integrate imaging and printing security needs into their larger IT security strategy.

HP LaserJet printers and MFPs have approximately 200 unique security features that your customers can enable to secure their devices and data. With modern technology, there is a balance between usability and security. Since each organization is unique, HP printers and MFPs come from the factory to meet the needs of a broad range of users. Given the sheer number of settings, this can seem like a daunting task.

The purpose of this guide is to help you understand some of the basic device settings that all companies—regardless of size or industry—should implement to secure their network imaging and printing devices. By explaining what each setting is for and the risk associated with leaving a setting unsecure, you can help your customer get started on an imaging and printing security strategy.

Recommended device settings for an HP printing fleet

Customers might need help understanding which security settings should be considered to protect their data. We have narrowed down the possible device settings from over 200 configuration settings. These are basic security settings that all companies—regardless of size or industry—should consider setting. HP recommends these minimal security settings to address the most common security issues.

It is important to note that every customer environment is unique. Each customer must determine the balance between security and end-user productivity. Configuring an MFP for a network may require adjustments to this configuration—your customer will need to consider the right configurations for their network environment.

Potential outcomes of leaving a device unsecured...

- Loss of employee productivity because device settings have been changed and they are no longer able to print, copy, scan or fax
- Unauthorized access to sensitive data
- Potential exposure of device settings, including credentials
- Increased support calls taking valuable IT time

Before they get started, recommend that your customer...

- Upgrade the device to the latest firmware version to ensure the device has the most up-to-date capabilities.
- Ensure the printer or MFP is behind their firewall, to keep it secure. Some HP solutions require the device to have Internet access to work properly.

To avoid the risk that...	Security setting	Action	Purpose of setting
Anyone can change device settings or buttons on the control panel (e.g., to disable product features)	Admin password for HP Embedded Web Server (EWS)	Set up password	Controls access to the configuration parameters of the HP EWS.
Anyone can change the file system configuration and erase files on storage device	File System Password	Set up password	Controls access to the file system configuration and file storage device.
Anyone can change control panel settings	Printer Job Language (PJL) password	Set up password	PJL commands provide two-way communication with the printer; can use to change control panel settings.
Anyone can change settings on the printer, if SNMPv1/v2 "write" is allowed	SNMPv1 / v2 Simple Network Management Protocol	Set to "Read Only"	Provides support for older management tools that rely on SNMPv1/v2 for device discovery and status.
Anyone can discover a device on the network and change settings, if SNMPv3 is left open	SNMPv3	Enable; Create an account on the device	SNMPv3 employs a user-based security model that features authentication and data privacy through encryption. More secure method than SNMPv1/v2.
Anyone could update firmware that would revert to a less secure version and impact functionality of existing solutions, if left open	FTP firmware update	Disable	A method to remotely update firmware on a device.
Anyone could remotely update firmware that would revert to a less secure version and impact existing solutions, if left open	Remote firmware upgrade (RFU)	Disable Note: Turn on to remotely update firmware; turn off when finished.	A different method of remotely updating firmware on a device
Someone could sniff network traffic and view data, if data is unencrypted	Require HTTPS redirect	Enable	Encrypts data from device to your computer when browsing to your device's embedded web server.
Someone could access device and make changes to device configurations, if protocols are left on	Turn off unused protocols • Telnet • File Transfer Protocol (FTP) • Novell (IPX/SPX) • Appletalk	Disable	These protocols allow sending or receiving information from a network device. Typically, unused protocols are left in for legacy applications.
Users could access and manipulate files as if they were stored locally on their own hard drive	Prevent file access • Network File Systems • Printer Management Language • Printer Job Language • Postscript	Disable; Uncheck all boxes	Prevents network users from remotely accessing files stored on a printer's disk drive.

Easily apply security policies across a fleet of HP devices

Nearly 90%

of enterprises say they have suffered at least one data loss through unsecured printing[1]

65%

of breaches are accidental employee negligence or IT/ business process failures[2]

$3M overall

The cost of a single data breach averages $145-154 per record compromised, and $3 million overall[2]

Why security policies are important

Your customer is continuously creating confidential, valuable data that's crucial to running their business. And they may be using multiple security methods—including authentication, encryption, and monitoring—to protect this data on their networks, PCs, and servers. But is their printing and imaging environment as secure as the rest of their infrastructure?

Security gaps can leave sensitive data dangerously exposed:

- Imaging and printing devices store files on internal drives or hard disks, from which anyone can access sensitive information.
- Multifunction printers (MFP) can easily capture and route jobs to many destinations, potentially exposing sensitive data.

Security settings may be out of date or non-compliant with security regulations:

- In some countries, the company may be subject to penalties if their security settings are non-compliant.

With the basic security settings provided on page 2, you can help your customer get started on an imaging and printing security strategy.

Guiding questions

To qualify a customer's needs, begin by asking work environment-related questions, such as:

- What IT security policies do you currently have in place?
- Do your security policies include imaging and printing devices?
- Are you aware that your network printers are a point of vulnerability?
- Do you know how to set those security settings on your device?
- Did you know that HP has a solution that will allow you to create a security policy and apply it to all devices in your fleet?

HP JetAdvantage Security Manager

HP JetAdvantage Security Manager is a powerful tool for creating and editing security policies across a fleet of HP printing and imaging devices.[3] HP Security Manager offers top security without requiring administrators to be security experts.

Printing devices can be secured one at a time via the Embedded Web Server (EWS)—not very practical when securing a fleet of devices. Managing security settings across your entire fleet does not need to be confusing or time-consuming. The security settings provided on page 2 are the minimal security settings recommended by HP to address the most common security issues. They are a subset of the settings associated with the base policy included in HP Security Manager.

As your customer begins to secure their network, they can create their own policy with the minimal settings and add more over time. By using HP JetAdvantage Security Manager and Instant-On capable devices, your customer can enable important security settings as soon as a new printer is connected to the network.

HP Security Manager
Secure your HP printing fleet with the solution Buyers Laboratory (BLI) calls trailblazing.[4]

How HP JetAdvantage Security Manager secures your fleet

HP Security Manager helps streamline the process of applying customer-defined security policies across a fleet of HP printing and imaging devices, as well as monitoring and maintaining compliance. HP Security Manager easily identifies devices that are out of compliance and automatically reestablishes policy-based security settings. HP Instant-on Security makes it easy to secure new HP devices as soon as they are added to the network. Make it easier for IT administrators to manage the certificate process—and help save your business time and money.

Unlike traditional network device management utilities that are general use tools for monitoring and managing output devices on the network, HP JetAdvantage Security Manager is the most comprehensive printing security solution in the market, offering an effective, policy-based approach to securing HP printing and imaging devices.[5]

To get started today with a 60-day free trial, visit: software.hp.com/kiosk.

Username: HPSM_TRIAL60_KIOSK
Password: hpsm60020112

Learn more

To learn more about making HP Security Manager an integral part of your company's overall IT security strategy or to obtain a free trial, visit hp.com/go/securitymanager.

The world's most preferred printers (cover page): Worldwide printer marketshare, and HP printer brand awareness, consideration and preference study in 9 markets 2014.
[1] "Managed Print Services Landscape, 2014," Quocirca, June 2014.
[2] Ponemon Institute, "2015 Global Cost of a Data Breach Study", May 2015.
[3] HP JetAdvantage Security Manager must be purchased separately. To learn more or to obtain a free trial, please visit hp.com/go/securitymanager.
[4] Source: Solutions Report on HP JetAdvantage Security Manager 2.1 from Buyers Laboratory LLC, February 2015. For details, see hp.com/go/securitymanager or buyerslab.com.
[5] Based on HP Internal secured data (Device Security Comparison, January 2015), and Solutions Report on HP JetAdvantage Security Manager 2.1 from Buyers Laboratory LLC, February 2015.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA5-8727ENW, September 2015, Rev. 3