

HP Pay For Print Security Overview

HP Pay For Print is committed to providing software products that are secure for use in all network environments. HP Pay For Print software products only collect the critical imaging device metrics necessary to manage a printing environment, and never collect any personal or user information.

This document discusses network and information security as it relates to:

- HP Pay For Print Data Collector Agent software
- HP Pay For Print Web Console

HP Pay For Print Data Collector Agent Software

The HP Pay For Print Data Collector Agent (DCA) is a software application that is installed on a non-dedicated networked server at each location where imaging device metrics are to be collected.

The DCA runs as a Windows® service (or, optionally, a scheduled task), allowing it to operate 24 hours a day, 7 days a week.

Types of information collected

The HP Pay For Print DCA attempts to collect the following information from printing devices during a network scan:

- IP address (can be masked)
- Device description
- Serial number
- Meter reads
- Monochrome or color identification
- LCD reading
- Device status
- Error codes
- Toner levels
- Hostname
- Toner cartridge serial number
- Maintenance kit levels
- Non-toner supply levels
- Asset number
- Location
- MAC address
- Manufacturer
- Firmware
- Miscellaneous (machine specific)

No print job or user data is collected.

Data collection and transmission methods

The DCA collects imaging device metrics at a specified interval using SNMP, ICMP, and HTTP; it then transmits the data to the centralized database via FTP (port 21/port 20), HTTP (port 80), or HTTPS (port 443).

It is recommended that users transmit data using HTTPS, because this provides SSL 128-bit encryption of the data during transmission. FTP and HTTP do not provide encryption. To transmit using HTTPS, the machine receiving the transmitted data must be installed with an SSL security certificate.

Optional remote updates

The DCA contains an optional remote update feature, which is activated by enabling the Health Check and Intelligent Update options. Health Check will periodically ensure that the DCA service is operating, and if not, it will restart the DCA service. Intelligent Update allows the DCA to check for a receive software updates and DCA configuration changes posted by your HP Pay For Print administrator on the hosting server. These features are enabled and disabled at the end user site, and are not required.

Network traffic

The network traffic created by the DCA is minimal, and will vary depending on the number of IP addresses being scanned. The table below outlines the network load associated with the DCA compared to the network load associated with loading a single standard webpage.

Network Byte Load Associated with the DCA

Event	Approximate Total Bytes
Loading a single standard webpage	60,860
DCA scan, blank IP	5,280
DCA scan, 1 printer	7,260
DCA scan, 1 printer, 1 subnet	96,300
DCA scan, network of 13 printers	111,530

HP Pay For Print Web Console

HP Pay For Print Web Console is the online interface used to access the collected information.

Permissions based user management

Access to the HP Pay For Print Web Console is controlled with permissions-based user management. Users must log in to HP Pay For Print Web Console using a designated username and password getting from the Service Provider.

HTTPS access

The website can be accessed using HTTPS provided that the web server is installed with an SSL security certificate. Optionally, HP Pay For Print administrators can force users to access the HP Pay For Print Web Console website using HTTPS, by redirecting the HTTP version of the website. This is recommended, as it ensures 128-bit encryption of data being transferred over the Internet.