OptiPrint Security Overview

OptiPrint 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:

- OptiPrint Data Collector Agent software
- OptiPrint.com web console

It is also explained why using OptiPrint software applications will not impact compliance of the following laws:

- Health Insurance Portability & Accountability Act (HIPAA)
- Sarbanes-Oxley
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)

OptiPrint Data Collector Agent Software

The OptiPrint 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 OptiPrint 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
- 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 Dealer or OptiPrint administrator. 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
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

OptiPrint.com Web Console

OptiPrint.com is the online interface used to access the collected information.

Permissions based user management

Access to the OptiPrint.com web console is controlled with permissions-based user management. Users must log in to OptiPrint.com using a designated username and password.

HTTPS access

Optiprint.com can be accessed using HTTPS. This can be done by visiting https://www.OptiPrint.com. This ensures 128-bit encryption of data being transferred over the Internet.

Health Insurance Portability & Accountability Act (HIPAA) compliance is not affected by usage of OptiPrint software applications

The use of OptiPrint software applications will not have an impact on compliance with the Health Insurance Portability & Accountability Act (HIPAA) for covered entities. This is because PrintFleet software applications do not collect, house, or transmit any information regarding the content of print jobs, and thus have no way of accessing, housing, or transmitting electronic protected health information (ePHI) as defined by HIPAA.

For more information about HIPAA, visit http://www.hhs.gov/ocr/hipaa/

Sarbanes-Oxley compliance is not affected by usage of OptiPrint Software Applications

OptiPrint software is not intended to be used as part of an internal control structure as outlined in Section 404: Management Assessment of Internal Controls, but will not interfere with these controls.

Information Technology controls are an important part of complying with Sarbanes- Oxley. Under this Act, corporate executives become responsible for establishing, evaluating, and monitoring the effectiveness of internal control over financial reporting. There are IT systems in the market that are designed specifically for meeting these objectives. OptiPrint software is not designed as an IT control system, but will not interfere or put at risk other systems that are intended for that purpose.

For more information about Sarbanes-Oxley, visit
http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/

Gramm-Leach-Bliley Act (GLBA) compliance is not affected by usage of OptiPrint software applications

The use of OptiPrint software applications will not have an impact on compliance with the Gramm-Leach-Bliley Act (GLBA) for covered entities. This is because OptiPrint software applications do not collect, house, or transmit any information regarding the content of print jobs, and thus have no way of accessing, housing, or transmitting customers' personal financial information, even if this information is printed or otherwise sent to print devices monitored by OptiPrint software applications.

For more information about the Gramm-Leach-Bliley Act, visit
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Federal Information Security Management Act (FISMA) compliance is not affected by usage of OptiPrint software applications

OptiPrint software applications are not intended to be part of an internal control system for FISMA, but will not interfere with these controls.

The use of OptiPrint software applications will not have an impact on compliance with the Federal Information Security Management Act (FISMA) for covered entities. This is because OptiPrint software applications do not collect, house, or transmit any information regarding the content of print jobs, and thus have no way of accessing, housing, or transmitting high risk information, even if this information is printed or otherwise sent to print devices monitored by OptiPrint software applications.

For more information about the Federal Information Security Management Act, visit
http://csrc.nist.gov/groups/SMA/fisma/index.html