SmartPrint Security Overview

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

System requirements

- Hardware: Non-dedicated server powered on 24 hours a day, 7 days a week. If a server is not available, the Data Collector Agent can be installed on a desktop computer system powered on 24 hours a day, 7 days a week, but this method carries a risk of transmission difficulties.
- Operating System: Windows XP, Windows Server 2003, Windows Server 2008 or Windows Vista*
- Network Card: 100mbit or higher (system must have only one active network card)
- RAM: 512MB or higher
- CPU: 1GHz or higher
- Microsoft .NET Framework 2.0 installed
- Internet connected browser

Virtualization software support

If you want to install the DCA on a virtual machine, the following virtualization software will support the installation:

- Microsoft Virtual Server 2005 or VMWare GSX

Important: Do not install the DCA on a laptop. If you plan to use the DCA to collect data via VPN, please be aware that due to the extended transmission, there is a risk of data loss.

SmartPrint Data Collector Agent Software

The SmartPrint 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 SmartPrint DCA attempts to collect the following information from printing devices during a network scan:

IP address (can be masked)	Monochrome/color identification	Toner levels	Asset number
Device Description	LCD reading	Toner cartridge serial number	Location
Serial Number	Device status	Maintenance kit levels	MAC address
Meter Reads	Error codes	Non-toner supply levels	Firmware

No print job or user data is collected.

Data collection and transmission methods

The DCS collects imaging device metrics at a specified interval using SNMP, ICMP, and HTTP; it then transmits the data to the centralized database via HTTPS (port 443 – recommended), HTTP (port 80), FTP (port 21/port 20), or SMTP (port 25, sends via e-mail).

It is recommended that users transmit data using HTTPS, because this provides SSL 128-bit encryption of the data during transmission. HTTP, FTP, and SNMP 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 operation, and if not, it will restart the DCA service. Intelligent Update allows the DCA to check for and receive software updates and DCA configuration changes posted by your SmartPrint 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 web page.

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

HTTPS access

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