

PrintFleet Software Security

PrintFleet Data Collector Agent

Overview

The PrintFleet Data Collector Agent (DCA) is a software application that is installed on a networked server running Windows® 2000/XP, or Windows® Server 2003 to collect printer and copier metrics to be used in the PrintFleet Optimizer application. It does not require a dedicated system.

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

- IP address (IPs can be masked as a DCA configuration)
- Device description
- Serial number
- Meter reads (life, color life, copy mono life, copy color life, print mono life, print color life, fax)
- Monochrome / 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

Windows Service

The PrintFleet DCA runs as a Windows service, allowing it to operate 24 hours a day, 7 days a week. You can customize the transmission interval to determine how often the DCA will perform a device discovery.

After each discovery, the collected data will be sent to the hosting web server.

Alternatively, you can uninstall the Windows Service and run the DCA as a Windows Task Schedule.

Data Collection Protocols

The PrintFleet DCA collects device data using SNMP (Simple Network Management Protocol), ICMP (Internet Control Message Protocol), and HTTP (Hypertext Transfer Protocol).

Transmission Options

There are 3 methods by which you can transmit the data collected from the PrintFleet DCA, as listed below:

HTTPS, Port 443

Secure Hypertext Transfer Protocol. Data is transferred using the HTTP protocol, but instead of using plain text socket communication, the data is 128-bit encrypted using Secure Socket Layer (SSL) protocol during transit between the user's computer and the server itself. To prepare a web server for accepting HTTPS connections the administrator is required to create a public key certificate for the web server. This certificate must be signed by a certificate authority of one form or another, ensuring the user that the certificate holder is who they say they are.

HTTP, Port 80

Hypertext Transfer Protocol. A protocol used to transfer information over the World Wide Web.

FTP, Port 21 and/or Port 20

File Transfer Protocol. The standard protocol used to transfer files over the internet between computers.

Network Traffic

The network traffic created by a DCA network scan is minimal, and will vary on the number of IP addresses being scanned. The network traffic created by the DCA when scanning a single subnet (254 IP addresses) is approximately equal to the network traffic created by visiting a single standard webpage.

Optional Remote Updates

You can optionally enable the DCA Health Check and Intelligent Update features. Health Check will periodically check to ensure the DCA service is operating, 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 PrintFleet Administrator on the PrintFleet Optimizer host server.

The enabling and disabling of the Health Check and Intelligent Update features is entirely controlled at the end user site, and is not mandatory.

No User Data Collected

No personal or user data is collected with the DCA. Only printer metrics that do not identify users or documents are collected, such as page counts, device description, device status, and so on.

PrintFleet Suite PRO

Overview

PrintFleet Suite PRO is a secure program that in itself cannot harm a computer system or network, or endanger any private information.

No software to install

PrintFleet Suite PRO resides on a USB key that is plugged into an available USB port on the network, and does not need to be installed on the host computer.

Standard network protocols.

PrintFleet Suite PRO uses SNMP, ICMP, and HTTP to collect data.

Communicates with internal network only

All scan activities take place within the client's network. There is no communication with the internet, except under the following circumstances:

- Options under the Help menu connect to the internet so users can receive product updates and online help.
- A user performs a MIB Walk using PrintFleet MIB Walker and chooses to email the results to PrintFleet at the end of the scan

Collected information is retained by default on the USB key

The collected information is saved by default onto the USB key, in folders segregated by company.

Discovery process

PrintFleet Auditor sends a request out to the network, and applicable printing devices send the requested information back to the program. The amount of bandwidth that this scan takes is approximately equal to that used when viewing a single website.

PrintFleet Suite PRO does not send information out to the network or to any devices except under the following circumstances:

- The Send Print Job function within Auditor will send a requested print job to a specified device.
- PrintFleet Auditor has a selection to Restart Device, which will remotely restart a device, but requires the appropriate Community String if applicable.
- PrintFleet Asset Tracker can write the department, location, serial number, and asset number to the non-volatile memory of a device but requires the appropriate Community String if applicable.