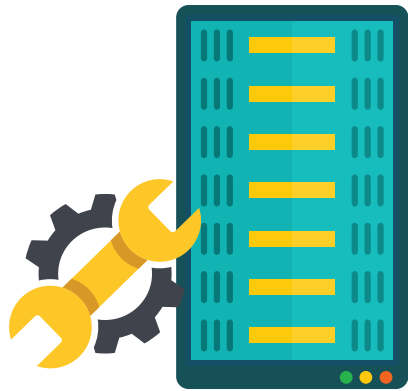
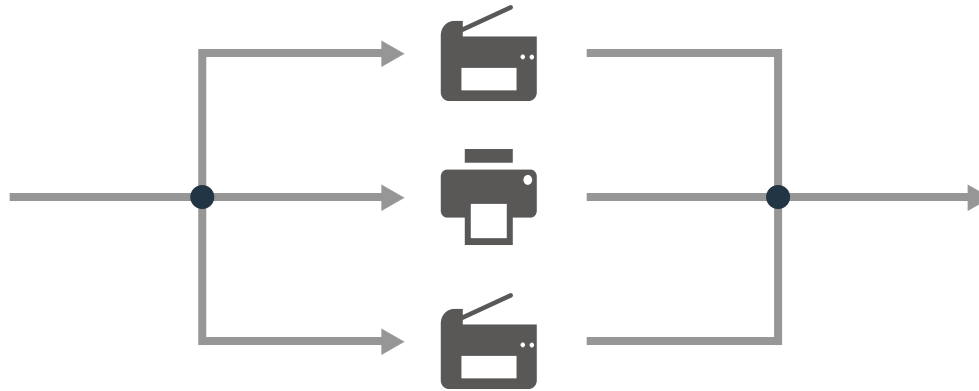


Data Collection Agent (DCA)

DCA Software
Installed on Customer Server



MFPs & Printers Connected to Customer Server
Transmits SNMP Data



RJY Secure Server Receives
Customer SNMP Data



RJY Downloads Encrypted Customer Data
for Usage Reporting, Monitoring Supply Levels & Receiving Alerts



Enterprise Security Overview

RJ YOUNG DATA COLLECTOR AGENT SOFTWARE

RJ Young provides a Data Collector Agent (DCA) 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 RJ Young DCA attempts to collect the following information from printing devices during a network scan:

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

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	Approx. 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

RJ YOUNG OPTIMIZER WEB CONSOLE

RJ Young Optimizer is the online interface used to access the collected information.

PERMISSIONS BASED USER MANAGEMENT

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

HTTPS ACCESS

The website can be accessed using HTTPS provided that the web server is installed with an SSL security certificate. Optionally, RJ Young administrators can force user to access the RJ Young Optimizer 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.

Enterprise Security Overview

SECURITY OVERVIEW

RJ Young software applications will not impact compliance with: Health Insurance Portability & Accountability Act (HIPAA), Sarbanes-Oxley, Gramm-Leach-Bliley Act (GLBA) or Federal Information Security Management Act (FISMA).

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

The use of RJ Young software applications will not have an impact on compliance with the Health Insurance Portability & Accountability Act (HIPAA) for covered entities. This is because RJ Young 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 RJ Young Software Applications

RJ Young 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. RJ Young 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 RJ Young software applications

The use of RJ Young software applications will not have an impact on compliance with the Gramm-Leach-Bliley Act (GLBA) for covered entities. This is because RJ Young 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 RJ Young 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 RJ Young software applications

RJ Young 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 RJ Young software applications will not have an impact on compliance with the Federal Information Security Management Act (FISMA) for covered entities. This is because RJ Young 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 RJ Young software applications.

For more information about the Federal Information Security Management Act, visit <http://lscrc.nist.gov/groups/SMA/fismalindex.html>