PrintMIBUK
Management Information Based Meter Read Solutions

PrintMIBUK Security and Technology Disclosure

Technology has helped businesses work harder, faster and more efficiently than ever before. The downside is that computers and more specifically, sensitive data are more vulnerable than ever before. Recognizing this, PrintMIBUK continues to engineer and design all of our products to ensure the highest level of security possible. PrintMIBUK develops a suite of software designed to automate the management of printers, copiers, and multi-function printers (MFPs) using a combination of common protocols – mainly Simple Network Management Protocol (SNMP), Printer Job Language (PJL) and Hyper Text Transfer Protocol (HTTP). Our end user products are the PrintMIBUK Meter Read Key and the PrintMIB UK Server Client. The following briefly describes the main functionality of each program.

The PrintMIBUK Meter Read Key is a USB flash drive based application which collects imaging data and saves it to a database located on the USB key itself. The program is designed to be completely self contained and installs no files or software on the computer on which the program is being run. The first time the program is run on any particular computer it must be run with sufficient rights to create Windows registry entries for several files, but these files remain on the key. Other than the network address the Key collects no information from the workstation on which it is running.

The Server Client is very similar to the PrintMIBUK Meter Read Key, but it is designed to be permanently installed on a Windows workstation/server at a client location. At set intervals, it performs regular scans of the networked printers, copiers, and MFPs and reports the results directly to the PrintMIBUK Server. These data transmissions are done using standard HTTP (port 80) posts to a Secure Scan Archive Server. Other than the information entered into the Server Client database when the program is installed and the network address, it collects no data from the workstation/server on which it is running.

Both the PrintMIBUK Meter Read Key and the CPP Client track the following device information:

- Manufacturer Name
- Serial Number
- TCP/IP Address
- Supply Levels
- Alerts
- System Contact *
- Model
- MAC Address
- Page Counts
- Console Messages
- System Location *
- System Name *

* Optional values which may or may not be set on the print device by individual users, organizations, or leasing companies.

At no time does either program track or attempt to track any information other than that which is listed above.

The Server Client can be remotely managed from the PrintMIBUK Server. Management changes would include things like changing the scanning frequency, changes to IP Address ranges that the client uses or updating the scan engine database. With security in mind, these management changes are never “pushed” to the server Client. Instead, they “pulled” utilizing the same mechanism for posting scan data and “check in” to the PRINTMIBUK Server to find out if there are any changes that need to be “picked up”. All communications with the Secure Scan Archive Server are initiated on the client side. Specifically, the Server Client will “check in” once per hour to the PrintMIBUK Server to see if there are any changes for it. If there are changes, it picks them up, makes the changes and then confirms back to the Server that the changes were successfully made. All communication between the client and server is HTTP protocol.

PrintMIBUK has adopted the "Pull" only philosophy to avoid having to compromise network security by opening access to the outside world. By restricting communications to known and commonly used ports the Server Client does not require special exceptions or security rules. All communications are initiated by the Server Client and at no time does any outside system attempt to contact the Server Client.

In summary, PrintMIBUK is sensitive to the security concerns of both our clients and their clients, and we have attempted to design our products in such a way as to address the needed functionality without compromising vital security. We hope that this document is helpful in answering any questions regarding our products and the possible security concerns that using them might create. We strongly encourage that client network administration always be consulted when using any of our products at a client location, and will be happy to provide any additional information which may be needed.