

Facilities Manager - Security Overview

Scanning

- SNMP scanning is done within the internal network only, via the standard SNMP port (UDP port 161).
- The Information Collection Engine (ICE) uses unicast transmission to communicate to each IP address in the configured scan range. No broadcast packets are sent.
- A community string can be specified in the ICE configuration if required.

Data Storage

- PrinterManagement's server is located in a physically secure environment.
- PrinterManagement's server is located behind a dedicated hardware firewall that blocks all external access except that which is required for PrinterManagement's Facilities Manager to function.
- The server is kept up to date with the latest operating system patches, security patches, and anti-virus updates.
- Server administration logins are restricted to a very limited number of authorized personnel who require access only for routine maintenance and backup purposes.
- PrinterManagement's Facilities Manager is the only application running on this server and therefore there is no security threat posed by other programs.

Data Collection

No personal or user data is collected with the ICE. Only the following information is gathered and transmitted to PrinterManagement's secure server:

- Printer name, make and model
- Location
- Serial number
- IP Address
- MAC Address
- Page Counts
- Toner levels
- Status / Alerts (e.g. out of paper, paper jam)

Data Transmission

- The ICE connects to PrinterManagement's server via an outbound connection only. There is no reverse connection made from PrinterManagement's server to the ICE.
- HTTPS is the default send method in the ICE configuration window. This ensures that the data is encrypted during transmission using standard internet security protocols (128 bit SSL on TCP port 443). If HTTPS is not available, the ICE will use HTTP (port 80) as the send method.
- HTTPS (128-bit SSL) is the same security as is used in Internet banking or purchasing goods online from a merchant such as Amazon.
- The server sends a simple acknowledgement that the data was received, but no other data is sent back to the ICE in response to the transmission. This response is also encrypted in the same manner as the transmission itself.