Infinite Device Management

IDM Security Overview

Version: 13

Date: 04-Dec-2018 15:17

Table of Contents

Scanning 2

Data Storage 3

Data Collection 4

Data Transmission 5

Web Interface 6

Scanning

- SNMP scanning is done within the internal network only, via the standard SNMP port (UDP port 161). SNMPv3 is supported for addtional security.
- 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

- Print Audit's server is located in a physically secure environment.
- Print Audit's server is located behind a dedicated hardware firewall that blocks all external access except that which is required for Infinite Device Management 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.
- Infinite Device Management 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 Print Audit'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 Print Audit's server via an outbound connection only. There is no reverse connection made from Print Audit's server to the ICE.
- HTTPS is the only send method used by the Print Audit Information Collection service. This ensures that the data is encrypted during transmission using standard internet security protocols (256 bit SSL on TCP port 443).
- HTTPS (256-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.
- ICE receives configuration changes, software updates, and acknowledgements of ICE data transmissions. No connections are made to ICE. All connections are generated via initiation by ICE.
- ICE configuration settings in IDM are retrieved when ICE requests the most recent configuration settings from IDM, prior to performing a scan. This is a simple SOAP call that returns XML to ICE. If desired, this can be disabled by configuring ICE to only use local configuration.
- ICE uses a Windows service (port 80) that sends the current installed version of the ICE to IDM. If a newer version is available, IDM provides a response and ICE will download and run the update. This occurs every 12 hours (and when the service starts) and may be disabled by turning off Automatic Updates on the ICE

Web Interface

- All external access is via secure login (username and password) and only through the secure web application at https://fm.printaudit.com
- Infinite Device Management logins can be restricted to either a set of customers for a single dealer (a "dealer level" account) or a single customer (a "customer level" account). Advanced privileges can also be assigned to users.
- Access to the secure web application at https://fm.printaudit.com uses 256-bit SSL encryption.