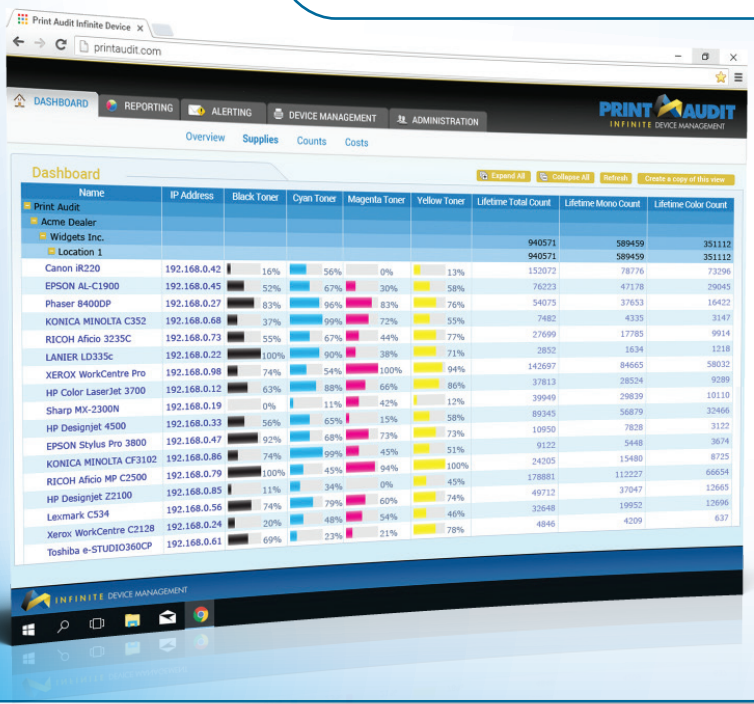
# The cutting-edge software that monitors your print devices during our Office Werks Study & Optimization Process

Office Werks App

Powered by Print Audit®




## Network Meter & Print Asset Tracking Software

We utilize the industry leading MPS Toolset and independently licensed version of Print Audit®. At no cost to you, the application is installed on a non-dedicated server or desktop at one of your locations. The software then collects critical printing data directly from each device and sends it encrypted to the central database server where it becomes easily accessible via a custom secure web portal allowing us to generate real time reports and analytics.

## Print Audit Infinite Device Management:

- Gives us real-time intelligence on your printing and copying device usage and TCO Analysis.
- Allows us to audit vendor usage billing and meter reading history.
- The application device data dashboard is easily accessed by the Office Werks Study team and your own internal IT staff.

BUYERS LABORATORY BLI SOLUTIONS

PRINT AUDIT INFINITE DEVICE MANAGEMENT

http://www.ecoOfficeWerks.com/PrintAudit

Infinite Device Management

# IDM 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 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.

## 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.

## 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 are restricted to Eco Office Werks certified consultants or a single customer (a "customer level" account). Advanced privileges can also be assigned to client IT users.

Access to the secure web application at https://fm.printaudit.com uses 256-bit SSL encryption.

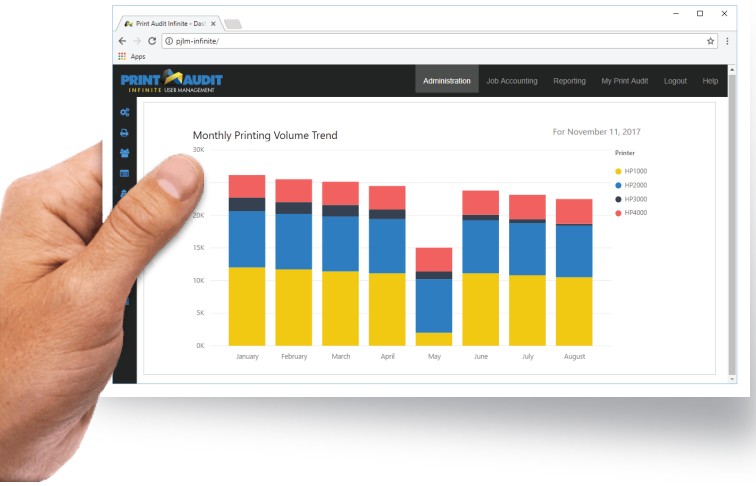
# Optional User Print Analysis

Office Werks App

Powered by Print Audit®

## INFINITE USER MANAGEMENT

Print Audit IUM empowers Eco Office Werks clients to understand the true usage patterns of up to 100 users in your environment during our Phase #1 Office Werks Study process.




- Automatically track 100% of your printing, including local, networked and direct-to-IP devices.
- Spot equipment abuses with powerful volume analysis reporting tools that detail who is printing the most, to what devices, what is being printed and more.
- Save money by revealing printing inefficiencies such as excessive printing to high cost personal printers.
- Installs silently to tens, hundreds or thousands of workstations.
- Powerful, fully web-based reporting tools.

## Technical Advantages

Workstation-based IUM tracks from the workstation which enables it to track every print job. This also allows it to retrieve more information about each print job, such as the name of the program or the web site address. Also, tracking from the workstation, rather than the print server, requires less network bandwidth since port monitoring is not required to capture all locally connected and direct to IP devices.

Simple installation and setup IUM does not require any modification of the local network or print servers to track 100% of the printing activity. It installs easily to each workstation from a central location on the network.

Tracks everything IUM is the only print tracking software solution that tracks all print devices out of the box. Whether a print job goes through a print server, directly to a printer with its own IP address or to a local printer, IUM captures it. It will creates an inventory of all print devices in use on the network, regardless of whether those devices are known to exist by the network administrator.

PRINT AUDIT
INFINITE USER MANAGEMENT

http://www.ecoOfficeWerks.com/PrintAudit

Optional Infinite User Management

# IUM Security Overview

## Technical Overview

IUM uses a client-based architecture. This has an important advantage over server-based tracking systems in that it allows tracking of all local as well as network printing by printer port and IP address identification, without utilizing valuable network bandwidth. Another equally important advantage is that IUM is safe and easy to install, without any alteration of the existing network whatsoever.

### Privacy

• No data is transmitted to third parties. The system can be configured to not track the document names and / or user names for each print job.

### Network

• Communication between Client and Client Web Services is always SSL encrypted. IUM uses a self-signed certificate by default, which the system administrator can can replace with their own certificate if desired
• All communication between the product components occurs on the local network, aside from licensing checks which are SSL secured.
• IUM supports secure SMTP when sending emails from the system

### Data

• All data is stored in the SQL database. The data is as secure as the network / server on which it resides.

### Database

• SQL databases are password protected by default and can utilize all of the security features of the Microsoft SQL Server platform if desired (including Windows/Integrated security).

### Applications

• Different user roles can be created to manage system access. Some users can be granted full access to the system, others read-only access (for reporting), and others can be denied access except the ability to track their printing.
• Users can be prompted to enter either a secure PIN code or their network password to gain access to the administrator and reporting tools.
• Users can be prompted to enter either a secure PIN code or their network password for validation in order to print.
• PIN codes are stored in the database in encrypted form, never in clear text.
• Users can be authenticated against Active Directory if desired.

### Internet-Based License Activation

• Normally, IUM licenses are activated via our secure licensing server using the HTTPS protocol. If it is not possible or desirable to activate over the Internet, the license can be activated manually.