FMAudit is the most powerful enterprise-class suite of print management products that is feature rich, easy to use and simple to deploy.

The suite consists of the following components:

- ***FMAudit Central:*** A cloud-based application that houses all of the data received from FMAudit data collection tools. It is a "central repository" that allows you to view data using a browser and to also generate reports.
- ***FMAudit Onsite:*** A data collection tool that automatically performs device analytics, monitors consumable levels and equipment status. This application is installed at the customer site and can perform print assessments manually or automatically on a scheduled basis without human intervention. The data captured is sent to your MPS provider's Central website using HTTPS, and information is automatically sync'd with your ERP billing systems.
- ***FMAudit Local Agent:*** A data collection tool for devices that are locally connected via a USB port or parallel port. The Agent Windows Service is installed at the workstation where the locally connected printer resides. The agent communicates directly with devices and relays the data captured to FMAudit Onsite.
- ***FMAudit Deployer:*** A tool that assists with the deployment of FMAudit Agent and other MPS related software packages. Deployer manages what build is needed by verifying the OS being utilized and installs the correct Agent build.

How FMAudit Works

The core engine, FMAudit Onsite, correctly identifies and extracts data from networked printers, copiers and multifunction printers (MFPs) utilizing the protocols the devices support, such as Simple Network Management Protocol (SNMP). FMAudit currently supports v1,v2c and v3 of the SNMP protocol. By default the "public" SNMP community name is used, but this may be modified in the FMAudit application to support custom environment settings. (See page 4 for more system requirements.) SNMP is a network protocol that facilitates the exchange of information between network devices, extracting data from the management information base (MIB) and other data collection locations within the print device. The MIB is an internal database that most network-connected devices have as part of their anatomy. The MIB holds data such as the model name, toner levels and the current status of the device.

How FMAudit Benefits You

Adaptive Supply Management (ASM) allows your MPS provider the opportunity to offer a customized program to control service and supply notifications. This system is developed by your MPS Provider to fit your specific business needs based on information delivered from FMAudit. ASM gives your MPS partner the ability to offer just-in-time automatic toner replenishment to ensure that your toner emergencies are relieved. Perhaps the most important function of a remote monitoring program is the ability to ensure your information is synchronizing efficiently with the Enterprise Resource Planning System (ERP) of your provider. Unlike other systems available, FMAudit offers Bi-Directional communication, allowing the application to push and pull data from your MPS providers' EPR systems. This system was developed to relieve the effects of human error associated with meter reconciliations and overall program management.

Virus Concerns? Not with FMAudit

The FMAudit application files have been digitally signed to prevent execution if the file integrity is compromised. This approach ensures the deactivation of any viruses and prevents spreading a virus from one network to another. For additional assurance, we recommend using antivirus software on your network. FMAudit applications only read from devices and do not write to devices. Many implementations currently use port 80, although port 443 is desired, IT Admin's may be upset later to find out that their provider is using port 80. FMAudit Onsite communicates with FMAudit Central by sending an encoded XML stream over port 443. Confidential data is not collected, viewed or saved by any FMAudit application. Only printer-related data is collected and viewed. No other network data can be identified or collected by FMAudit.

573-632-2461 • fmaudit@ECiSolutions.com • www.fmaudit.com

ECi Software Solutions | Inc. 500

Network

Network Traffic

Audits conducted by the software use an intelligent system to extract minimal information for each printer, copier or MFP. Unlike similar products that send a fixed set of queries (a superset of all possible queries) to every networked device, FMAudit Onsite only sends the relevant queries according to the fields the target device supports, with each device query being no more than a few kb of data. To further reduce the amount of network bandwidth used, Onsite communicates with no more than 20 devices at a single time. Each IP within the configured ranges will be queried and if no response is received within the configured timeout period it will move onto the next IP address. A rule-of-thumb is that FMAudit will gather information on 65,000 devices in just over one hour.

Local vs. Network Devices

The FMAudit product suite includes an application to provide information on locally connected devices. As with all technology applications, it is best to keep in mind that some external factors cause data from locally connected devices to be vulnerable and inconsistent. It is always optimal to have FMAudit Onsite engaged to work with network attached devices. Listed to the right are expectations for both network and locally connected devices.

Network-connected Equipment Benefits

- Secure
- Accurate
- Optimized
- Consistent
- Low IT interaction required for deployment
- Significantly more intelligent MIBs

Network-connected Equipment Expectations

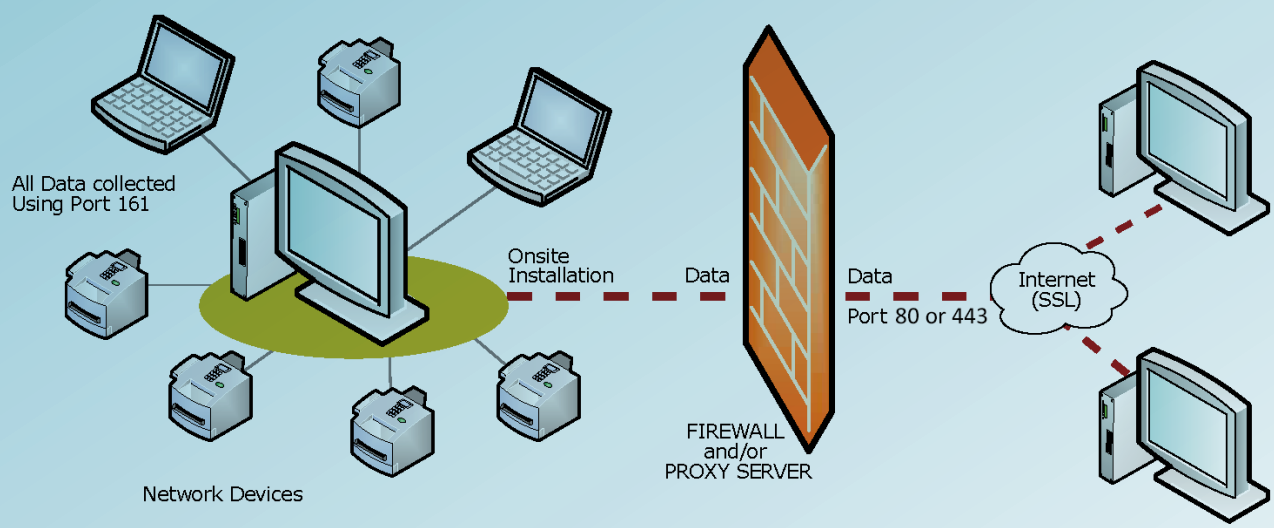
None. Network connected devices have all of the capability that is needed to engage with the FMAudit Onsite application to return accurate and consistent information.

Locally Connected Equipment Benefits

- Capability to capture locally attached equipment (USB)
- Easily deploy Agent to workstations with a locally connected printer

Locally Connected Equipment Expectations

- MIB sophistication is usually limited to the device specifications
- Installed on individual workstations with locally connected devices
- FMAudit recommends using OEM specific print drivers
- For additional information refer to FMAudit Knowledge Base articles



Client Printer Environment **Data Collection Processes**

573-632-2461 • fmaudit@ECiSolutions.com • www.fmaudit.com

ECI Software Solutions | Inc. 500

Health Insurance Portability and Accountability Act (HIPAA)

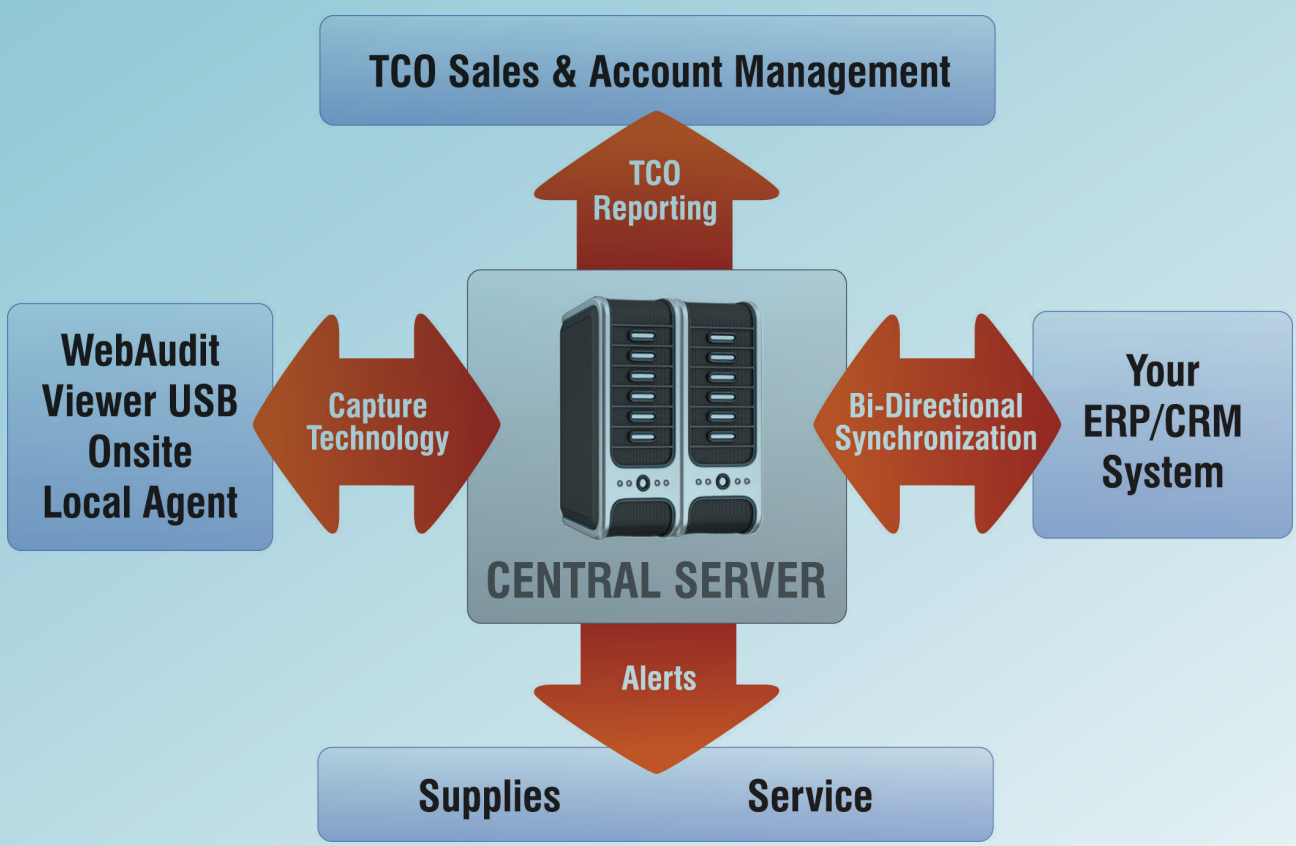
HIPAA aims to protect all medical records and other individually identifiable health information communicated, stored, or disclosed in any form. This goal prevails whether the information is being communicated electronically, in printed format or verbalized.

The FMAudit products are fully compliant with the HIPAA regulations as FMAudit products do not store, process, monitor or manage any patient records or any records or information that is specific to any one patient or group of patients. The product engine communications are controlled, using limited access to contact a specific IP address and/or ranges. All communications must originate from the FMAudit products, and there is no way to contact and access the products from outside the network. The communication outside of the network uses a proprietary, compressed data stream that is sent using industry-standard SSL over HTTPS.

Communication

The FMAudit products report the usage counts (meter readings) and status of print devices on the network. It does not communicate any information about any specific print jobs. While the devices might print out confidential information, FMAudit products do not and cannot determine anything about the information being printed. It only performs audits of the print devices on a scheduled basis and communicates the meter readings of the device or an alert.

The FMAudit products cannot in any way be configured to perform a task beyond the ones for which it was designed. The transmission of data from the products to outside sources is tightly restricted. The products do not report any other details except for information of the equipment being monitored (i.e., type of equipment). No confidential information ever leaves the network via FMAudit products.



573-632-2461 • fmaudit@ECiSolutions.com • www.fmaudit.com

ECi Software Solutions | Inc. 500

Requirements

Windows OS support for FMAudit Products

	Service Pack	Bit Support	Central	Onsite	Viewer	WebAudit	.NET Version	Agent
Windows XP	SP2	32	----	YES	YES	YES	2.0	YES
Windows Vista		32	----	YES	YES	YES	2.0	YES
Windows 7		32/64	----	YES	YES	YES	2.0	YES
Windows 8		32/64	----	YES	YES	NO	3.5	NO
Windows Server 2003		32/64	YES	YES	YES	YES	2.0	YES
Windows server 2008		32/64	YES	YES	YES	YES	3.5	YES
Windows Server 2012		32/64	YES	YES	YES	NO	3.5	NO

More FMAudit System Requirements
PC/Server requirements for FMAudit Onsite:

- 1GB RAM, 30 MB Disk Space
- .NET Framework 2.0 or higher
- Internet Explorer 7.0 or higher
- MDAC 2.8 or higher (normally included when Windows is installed)
- JET 4.0 or higher (normally included when Windows is installed)
- Loaded on a machine that is up 24/7 or at least the entire business day
- Must be logged on as a Local Administrator (or equivalent) during the installation

Firewall considerations (Port 443) Outbound:

- License activation site:
  - — https://www.gttechonline.com/secured/licensingex/LicenseActivator.asmx
  - — Application: fmaonsite.exe
- Data transmission:
  - — https://(company name)/WebServices/Onsite2Service.asmx
  - — Application: fmaonsite.exe

Network Requirements:

SNMP (Port 161) traffic must be routable across the LAN or WAN

PC/Printer requirements for using the Local Agent (Optional installation):

- Windows XP, Windows 2000, Vista, Windows 7, Windows 2003
- .Net Framework 2.0 or higher
- Current driver for the local printer (UPD is recommended for HP devices)
- Printer must support Printer Job Language (PJL) or Printer Management Language (PML)
- Remove any unused print drivers
- Driver's bi-directional support is enabled
- Windows Firewall modifications
  - — Port 161 inbound/outbound for both TCP and UDP

573-632-2461 • fmaudit@ECiSolutions.com • www.fmaudit.com

ECI Software Solutions | Inc. 500

Frequently Asked Questions

Do FMAudit products work with Internet proxies?
Yes. FMAudit Onsite applications use the Internet Explorer settings. In Internet Explorer on the Tools menu » Internet Options » Connections TAB » LAN Settings button » place a check mark in “Bypass proxy server for local addresses” box. The “Secure” settings must also be configured to license FMAudit products. In Internet Explorer on the Tools menu » Internet Options » Connections TAB » LAN Settings button » Proxy Server » Select ”Use a proxy server for your LAN...button » Advanced button » add the appropriate “Secure” value for “Proxy address to use” and “Port.”

Does FMAudit Onsite require Microsoft Internet Information Services (IIS)?
No. FMAudit Onsite includes its own server to display the Web pages and is set up automatically during the installation.

Can you install FMAudit Onsite on a computer that already hosts another IIS website?
Yes. FMAudit Onsite uses port 33330 by default, but this may also be configured to use a different port if required.

How much ongoing maintenance does FMAudit Onsite require?
FMAudit Onsite is a service that runs in the background and performs audits and exports to configured destinations on predefined schedules. It is recommended to use subnets (IP ranges) instead of fixed IPs so when adding new devices to the network, they will be discovered and included in the audit results, limiting manual intervention.

How do I get additional information?
Additional information can be found on the FMAudit website: www.fmaudit.com

What versions of SNMP are supported?
FMAudit supports SNMP versions v1, v2c and v3.

Why am I not seeing all of my networked print devices?
Firewalls and other network hardware may prevent or limit the discovery of the network configuration. Networks with multiple physical locations typically have firewalls in between each local area network (LAN) and the public Internet that connects these locations via a wide area network (WAN). The network IP ranges (segments) may be manually added to the FMAudit products, with the minimum requirement that the target devices can be “pinged” from the originating location. Depending on the amount of network traffic and the general network latency, the default timeout may need to be increased. Differences in the total number of devices from one audit to another within the same relative timeframe, is a good indicator the timeout setting needs to be increased.

HP Jetdirect and Compatible Devices?
FMAudit’s core engine supports HP Jetdirect and compatible devices. During an SNMP query on the network, the FMAudit core engine communicates with the Jetdirect or compatible device and extracts the hardware’s reported lifetime meters, serial number, toner coverage’s, toner levels, service alerts and more.

573-632-2461 • fmaudit@ECiSolutions.com • www.fmaudit.com

ECI Software Solutions | Inc. 500