FMAudit Technical White Paper
Product Line Overview

Overview

The FMAudit suite of products deliver an “enterprise class” managed print solution that is very easy to use and deploy. It is architected and designed to take advantage of the advanced features and benefits of the Microsoft .NET platform. The result is it no longer takes a skilled technician to install software and then spend time to configure and maintain the system. The suite consists of the following components:

FMAudit Central: A website that houses all the data received from the FMAudit data collection tools. It is a “Central Repository” that allows you to view data using a browser, generate reports, configure alert notifications, and synchronizes with ERP systems.

FMAudit Onsite: A data collection tool that automatically performs print assessments, monitors consumable levels and printer status. This application is installed at the customer site and can perform print assessments automatically on a scheduled basis without human intervention. The data captured is sent to the Central website using HTTPS or HTTP. A technician with minimal software and networking experience can quickly deploy to a customer site.

FMAudit Viewer: A data collection tool installed on a USB key that can perform prints assessments without installing any software. The data captured is saved to the USB key. A typical sales person can perform print assessments.

FMAudit WebAudit: A data collection tool that is part of the Central website. You can perform a print assessment right from a browser without installing any software. The data captured is sent directly to FMAudit Central. An end user can initiate a print assessment themselves through the FMAudit Central.

FMAudit Local Agent: A data collection tool for printers that are connected locally via a USB port or Parallel port. This application is installed at the workstation where the locally connected printer resides. The data captured is sent to one of the other data collection tools (WebAudit, Onsite, or Viewer).

How It Works

The core engine, which is the heart of every FMAudit product, correctly identifies and extracts data from networked printers, copiers and MFPs utilizing the protocols the devices support such the Simple Network Management Protocol (SNMP). SNMP is a network protocol that facilitates the exchange of information between network devices; extracting data from the Management Information Base (MIB) and other locations within the print device. The MIB is basically an internal database that all network connected devices have, that contains information like the model name, toner levels and the current status of the device.

Requirements

Printers, copiers and MFP's must have the SNMP protocol (Port 161) enabled for discovery and extraction of information. The SNMP protocol is a standard part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. By default the "public" SNMP community name is used, but may be modified in the FMAudit applications to support custom environment settings.

Manufacturer Support

FMAudit products are manufacturer neutral. They support all of the major manufacturers and model families. Some devices have limitations that prevent extraction of certain information.

Virus Concerns

The FMAudit application files have been digitally signed to prevent execution if the file integrity is compromised. This ensures that any virus is not activated, and prevents spreading the virus from one network to another. For additional assurance, we recommend using antivirus software.

Security Concerns

FMAudit applications only read from networked devices and do not write to devices.

FMAudit Onsite communicates with FMAudit Central be sending an encoded XML stream over port 80 or 443.

Confidential data is not collected, viewed or saved by any FMAudit application.

Network Discovery

The optional, patent pending, FMAudit Automatic Network Discovery Settings feature uses a mixture of algorithms to discover and communicate with the different network elements such as the current workstation or server, routers, hubs switches and other network hardware to identify the network ranges where print devices may be located.

Network Traffic

Audits use an intelligent system that extracts 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, the FMAudit family of products 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, the FMAudit core engine 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 a little more than one hour.

Local Printers

The patent pending FMAudit Agent is the only solution of its kind to extract information from one or more local printers attached to any Windows port type, such as USB, parallel, Bluetooth or infrared. The Agent does not interrupt the print job flow, it only activates when called upon by one of FMAudit's collection applications; Viewer, Onsite or WebAudit, and then shuts back down. The Agent then extracts the hardware reported model, serial number, life-time meters, toner coverage's, toner levels and service information depending on what the specific device supports.

Unlike other solutions, it is not an application that runs intrusively on an ongoing basis. It does not invasively monitor the spooler to count pages as they are printed. In addition, solutions that interrupt the job to capture data are limited in their use. They only report a cumulative page count (not actual engine page counts) and result in inaccuracies, especially when jobs are cancelled and/or not printed successfully. They are also limited to a single page count and are not able to report serial numbers, toner coverage's, toner levels, service alerts and more.

FMAudit Agent may be deployed to the workstations using a solution such as Microsoft SMS. Reconfiguration of antivirus or software firewalls may be required if blocking the SNMP port 161 or the alternative Agent fallback port 33333.

HIPAA Regulations

HIPAA aims to protect all medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule.

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 engines 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 the is send using industry standard SSL over https.

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 patient records, FMAudit products do not and cannot determine anything about the information being printed. It only performs audits, on a scheduled basis, the meter readings of the device, or in the case of a device problem, 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 patient related information ever leaves the network via FMAudit products.

Frequently Asked Questions (FAQ's)

Do FMAudit products work with Internet proxies?

Yes. FMAudit Viewer and Onsite are local applications and use the Internet Explorer (IE) 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, and generate the Dynamic Reports included in Viewer. In Internet Explorer on the Tools menu -> Internet Options -> Connections TAB -> LAN Settings button -> Advanced button -> add the appropriate "Secure" value for "Proxy address to use" and "Port".

How does the FMAudit Viewer USB key work?

FMAudit Viewer USB is installed and licensed on an approved USB key. When plugged in to a recipient computer, this key will be seen as a removable drive. The FMAudit Viewer software is run directly from this key. No software is transferred to or installed onto the computer.

What are the FMAudit Central, Onsite and Viewer minimum requirements?

- The FMAudit Products, may be run on any modern Windows operating system (in 32 and 64 bit modes) including:
  - Windows 2000, XP, Vista, 7, Server 2003, 2008, 2008 R2
- Details hardware and software requirements can be found at the following URL
  - http://help.fmaudit.com/fmac/sysreq.html

Does the FMAudit Viewer require Internet access?

No. For the action of performing audits on end-users' networks, you do not require internet access. FMAudit Viewer does communicate over the Internet to verify licensing when running specific reports.

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 which 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 which runs in the background and performs audits and exports to configured destinations on predefined schedules. It's recommended to use subnets (IP ranges) instead of fixed IP's so that when adding new devices to the network, they will be discovered and included in the audit results, limiting manual intervention.

What hosting options are available for FMAudit Central?

There are a few hosting options available:

1. Hosted Internally

Dealer may install internally at their office and provide internal and/or external access to their employees and end users (customers).

2. Third Party

Outside hosting service such as Rackspace, 1and1 or GoDaddy.

How does the FMAudit WebAudit process work?

From FMAudit Central, the dealer specifies the end-users' (customers) applicable billing cycle. At this time, an email is automatically generated and sent to the appropriate contact informing them it is time to collect their meters. The instructions include a URL, whereby when the end- user clicks the link, it automatically launches their web browser, ready to perform the action. The end-user then clicks 'start' and 'save'. Done. No software is installed at any time. A link to the WebAudit page may also be posted on the dealers existing website, i.e. Enter Meter Readings web page. This allows the user to au-

tomate the collection, rather than having to manually walk from device to device, print configuration page and transcribe the meters.

What versions of SNMP are supported?

FMAudit supports SNMP versions v1 and v2c

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 adjusted. 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.

JetDirect’s & Compatibles

FMAudit’s core engine supports HP JetDirects 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 reported life-time meters, serial number, toner coverage’s, toner levels, service alerts and more.

How do I get additional informaiton

Additional information can be found on our website; http://www.fmaudit.com/