FMAudit, LLC. By: Kevin Tetu,
VP Technology
FMA_Tech_White_Paper.doc
February 2013

FMAudit Technical White Paper
Product Line Overview

Overview

The FMAudit suite of products delivers 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 is a website that houses all the data received from the FMAudit data collection tools. It is a “Central Repository” that allows us to view data using a browser, generate reports, configure alert notifications, and synchronizes with ERP systems.

FMAudit Onsite is 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.

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 MFPs 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. Reconfiguration of antivirus or software firewalls may be required if blocking the SNMP port 161.

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, is 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 that is sent 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

Do FMAudit products work with Internet proxies?

Yes. The FMAudit Onsite service as well as the configuration file can be configured to work with various firewalls, proxy servers, and web filters. Occasionally, depending on the configuration of the proxy / web filter, exceptions may need to be entered in order to ensure proper communication with the central server.

What are the FMAudit Central and Onsite minimum requirements?

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

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 IPs so that when adding new devices to the network, they will be discovered and included in the audit results, limiting manual intervention.

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.