ECi® fmaudit®
Collect. Manage. Profit

FMAudit Technical Whitepaper: The purpose of this document is to provide a product line overview of the FMAudit Suite of Products from a technical perspective to help facilitate answers to the most common questions Information Technology teams will receive.

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 sp that it no longer requires a skilled technician to install software and configure and maintain the system. 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 is ever transmitted out of the network via FMAudit products. 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, and 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, HTTP, or if the customer prefers a propriety encrypted file.

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). FMAudit currently supports v1, v2c and v3 of the SNMP protocol. SNMP v3 provides increased packet protection to ensure information and communication is transmitted via reliable sources. Unlike SNMPv1 or v2, v3 is encrypted for increased security and requires both a username and a password. A benefit to using SNMP v3 is that network administrators can determine the encryption method as well as a strong username and password.

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 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 printer.

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 Application Layer of the TCP/IP suite.

To review a full list of FMAudit System Requirements please visit http://help.fmaudit.com/fmao/sysreq.html

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 80 or 443) Outbound:

Data transmission:

- https://(company name)/WebServices/Onsite2Service.asmx
- Application: fmaonsite.exe
- SOAP over HTTP(s) must be allowed past firewall

Network Requirements:

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

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

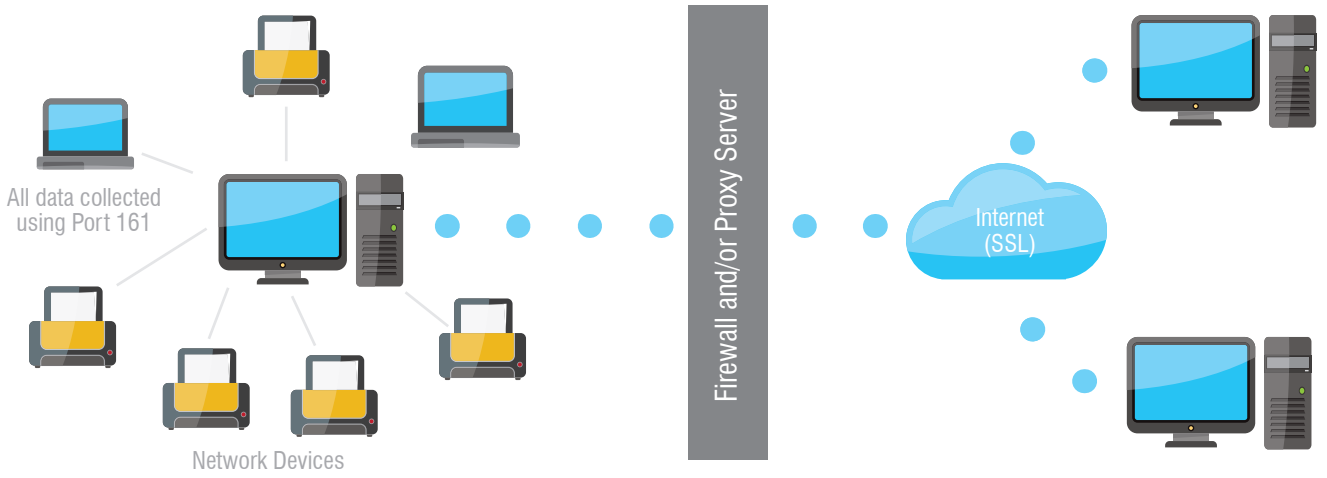
- Windows XP, Windows 2000, Vista, Windows 7, Windows 2003
- .Net Framework 2.0 or higher
- Current driver for the local printer (UPD is recommended for HP devices)
- Printer must support Printer Job Language (PJL) or Printer Management Language (PML)
- Remove any unused print drivers
- Driver's bi-directional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

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 that may be present is not activated, and prevents spreading the virus from one network to another. For additional assurance, we recommend using antivirus software on your network.

Security Concerns
FMAudit Onsite communicates with FMAudit Central by sending an encoded XML stream over port 80 or 443 using the SOAP over HTTP(s) protocol. 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.

Network Discovery
The FMAudit patented Automatic Network Discovery Settings use a mixture of algorithms to discover and communicate with the multiple network elements such as active workstations or servers, routers, hubs, switches and additional network hardware to identify the network ranges where print devices may be located.



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 PRINTERS

The 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 printing job flow, it only activates when called upon by one of FMAudit's collection application tools—Viewer, Onsite or WebAudit— and then closes. The Agent collects specific information dependent upon the intelligence levels of the device from the engine and not the print spooler. Most common attributes reported are model, serial number, life-time meters, consumable coverage, consumable level, and service. 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.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

(HIPAA) Regulations

Health Insurance Portability and Accountability Act (HIPAA) aims to protect all medical records and other individually identifiable health information that is 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 are 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.

FREQUENTLY ASKED QUESTIONS (FAQS)

Do FMAudit products work with Internet proxies?

Yes Onsite is able to work with most proxies. In the user interface there are options to configure different proxy settings.

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 , 2012, 2012 R2

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

Which versions of SNMP are supported?

FMAudit supports SNMP versions v1, v2c, and v3.

How do I get additional information?

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