Managed Print Services Learning Series

FMAudit Suite

FMAudit suite queries your network print devices for information through SNMP protocol.

How It Works

The core engine, which is the heart of every FMAudit product, 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). 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 basically an internal database that all 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.

FM Audit Installation Requirements

Printers, copiers and MFPs must have 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.

Virus Concerns

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 anti-virus software on your network.

Security Concerns

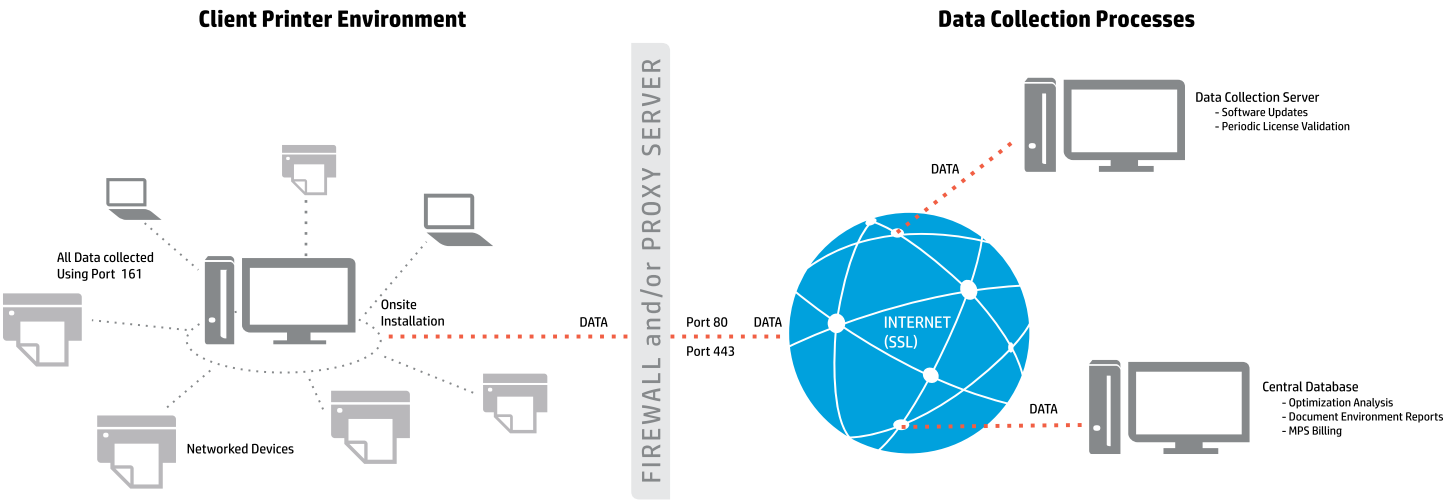
FMAudit applications only read from networked devices and do not write to devices. FMAudit Onsite communicates with FMAudit Central by sending an encoded XML stream over port 80 or 443. Confidential data is not collected, viewed or saved by any FMAudit application. Only printer-related data is collected and viewed by HP. No other network data can be identified or collected by FMAudit.

Network Discovery

As an additional option, the 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 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, 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



Remote monitoring process

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 vs. Network Devices

The FMAudit product suite includes an application that provides the capability to capture locally connected equipment information, labeled as the FMAudit Agent. This part of the FMAudit product suite is meant to be used for an inventory purpose only and should not be utilized to manage continuous reports from locally connected devices.

While the capability exists, HP does not actively support the FMAudit Agent product. This policy is primarily due to it being extremely vulnerable to external factors that cause the data to be inconsistent, duplicated, and inaccurate. All of the benefits and challenges are listed below in comparison with network attached equipment. It is always optimal to have FMAudit Onsite engaged to work with network attached devices.

Network Connected Equipment Benefits

- Secure
- Optimized
- Accurate
- Consistent
- Additional automation features available (Toner Replenishment, etc.)
- Low IT interaction required for deployment
- Significantly more intelligent MIB's

Network Connected Equipment Challenges

- None. These 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).

Locally Connected Equipment Challenges

- MIB sophistication level is often very low due to being forced to communicate via USB through the print driver.

- Data is often inconsistent, inaccurate or duplicated
- Increased vulnerability to external factors:
  - Device moves physically, once reconnected creates a duplicate record
  - Driver change results in duplicate record in most cases
  - Host PC turned off/asleep results in no report
  - Extensive IT involvement to deploy
  - Must be installed to every workstation with a locally connected device

HIPAA Regulations

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.

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 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 patient related information ever leaves the network via FMAudit products.

If you have questions about FMAudit Suite, please contact your MPS Consultant or email: cmps-us-fmaudit@hp.com

Excerpts taken from FMAudit Technical White Paper located at **help.fmaudit.com**

Share with colleagues