# *FMAudit Product Line: Technical White Paper*

## Overview

What may seem like magic is the result of years of hard work by veterans of the imaging industry. Keeping in mind that a meter collection system is only as good as the information and accuracy of the information it provides, the FMAudit product line is architected and designed to take advantage of the advanced features and benefits of the Microsoft .NET platform. What wasn't possible just a few years ago is delivered by FMAudit in a compact and user friendly interface. The result is it no longer takes a skilled technician to install software and then spend time to configure and maintain the system as with similar products. FMAudit Viewer USB may be used by a typical sales person for the purposes of a print assessment, FMAudit Onsite deployed by a technician with minimal software and networking experience and FMAudit WebAudit may be initiated by the sales person or even the end-user.

## How It Works

The core engine, which is the heart of every FMAudit product, identifies networked printers, copiers and MFP's using the ***S***imple ***N***etwork ***M***anagement ***P***rotocol (SNMP). SNMP is an application layer protocol that facilitates the exchange of ***M***anagement ***I***nformation ***B***ase (MIB) between network devices. A Management Information Base (MIB) is a collection of hierarchically organized characteristics of a managed device, comprised of one or more object instances, which are essentially values. An object identifier (or object ID) uniquely identifies a managed object in the MIB hierarchy. Using patent pending ***I***dentity ***M***apping ***T***echnology (IMT), FMAudit correctly identifies re-branded models. Once identified, information is extracted using a combination of SNMP and FMAudit's patent pending ***H***yper-***M***eter ***T***echnology (HMT) that combines a mixture of multiple protocols, communicating and extracting information from a multitude of different areas within a device depending on its architectural design.

## Requirements

Printers, copiers and MFP's must have the SNMP protocol enabled for discovery and extraction of information. The SNMP protocol is part of the ***T***ransmission ***C***ontrol ***P***rotocol/***I***nternet ***P***rotocol (TCP/IP) protocol suite; therefore a network using the TCP/IP protocol which allows communication over the SNMP port 161 are base requirements. By default the "public" SNMP community name is used, but may be modified in the FMAudit applications to support custom environment settings. The target devices must reply to a "ping". This indicates that communication won't be blocked during an audit.

## Security Concerns

FMAudit Viewer and WebAudit may be launched from a Windows 2000/XP/2003 workstation or server with restricted user permissions to the target network.

Although SNMP commands support both read and write operations, FMAudit applications only read networked devices and do not modify any default or custom device settings.

FMAudit Onsite allows audit information to be sent from the target network to a remote destination as an attachment to an email (default port 25) or an XML stream (default port 80). By default, this information is encrypted, and requires a user and pass combination for authentication.

Only the information which is extracted during an audit may be saved or transferred to the FMAudit applications. The end-users' confidential data files are not viewed or saved by any FMAudit applications.

The FMAudit Viewer pages display the main user interface in a web page fashion. It does not communicate over the internet except for obtaining a license, or during use of the included dynamic reports. For the action of performing audits on end-users' networks, you do not require internet access.

## Virus Concerns

The FMAudit application files have been digitally signed to prevent execution if a virus has infected the file integrity. This method ensures the virus is not activated, and prevents spreading the virus from one network to another. For additional assurance, we recommend using antivirus software to scan the contents of the USB key in between visits to the end-users network.

## Network Discovery

The patent pending FMAudit ***A***utomatic ***N***etwork ***D***iscovery ***S***ettings (ANDS) 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.

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 ***L***ocal ***A***rea ***N***etwork (LAN) and the public internet that connects these locations via a ***W***ide ***A***rea ***N***etwork (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.

## WAN's and Network Traffic

FMAudit applications use default timeout settings of 1000ms. Using unicast settings, each IP within the configured ranges will be queried and if no response is received within 1 second, a timeout will occur. 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.

The audits use an intelligent system that extracts minimal information for each printer, copier or MFP's. 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 identified device supports, with each device query being no more than a few kb of data. To further reduce the amount of network bandwidth used during a discovery, the FMAudit core engine communicates with no more than 20 devices at a single time, with the capability to extract information from up to 5 devices per second in an optimized environment. The amount of network traffic at any given time is minimal as a result.

## Manufacturer Support

FMAudit products are manufacturer engine neutral. They support all of the major manufacturers and model families. Manufacturer architectural design limitations may prevent extraction of all identification and meter values. This typically occurs on older models, prior to the year 2000.

## Locally Connected Printers

The patent pending FMAudit Agent is the only solution of its kind to extract information from one or multiple local printers attached to any Windows port type, such as USB, parallel, blue tooth or infrared. The Agent service contains a proprietary multi-tier MIB which accompanies its own SNMP server, thereby

creating a bridge over the computer that is otherwise a road-block. During an SNMP query on the network, the Agent service wakes up and communicates direct over the port with the printer. The Agent then extracts the hardware reported life-time meters, serial number, toner coverage's, toner levels, service alerts and more.

The Agent does not interrupt the job flow. It is a passive service that sits dormant in the background. It is invoked only when called upon by one of FMAudit's collection applications; Viewer, Onsite or WebAudit, and then shuts back down. 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, and/or the alternative Agent fallback port 33333.

## JetDirect's and 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.