FMAudit Product Line: Security White Paper

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.