FMAudit Technical Whitepaper

Version 4.0

Table of Contents

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 so 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 and backend system 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 workflows and notifications, and synchronize data with ERP systems for billing or supply fulfillment.

ECI DCA: This newest DCA which brings about major advantages over FMAudit Onsite without losing any features, including full native cross-platform support of Windows, macOS, Linux, and Raspberry Pi, each with unique installation steps, support documentation, and trained support staff on these platforms. Also brings ongoing discovery and scanning of devices, improved MIBWalk and Log collection capability, and many more meter types are collected now.

FMAudit Onsite: A data collection tool that automatically performs print assessments and monitors consumable levels, printer status, and error logs. 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.

FMAudit Viewer: A data collection tool embedded on a USB key to perform fleet assessments without the need to install software. The data is retained on the USB key for additional analysis and reporting.

FMAudit WebAudit: A data collection tool that is a part of the Central application. Fleet assessments are performed directly from a browser without installing any software. The data captured is sent directly to FMAudit Central.

FMAudit Local Agent: A data collection tool used to discover devices that are connected locally via a USB port or Parallel port. This application is installed at the workstation where the locally connected printer resides. The data captured is sent to one of the other data collection tools (WebAudit, Onsite, or Viewer).

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.

How FMAudit 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.

FMAudit System Requirements

1.1 System 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.

PC/Server requirements for ECI DCA:

Microsoft Windows (x86/64)

Requirements:

- Windows 7, 8, 10, Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, and Server 2019
- .NET 4.5.2 or higher

Linux (x86/64 or ARM)

Requirements:

- Ubuntu 14.04, 16.04 or 18.04, Debian 9.5+, Raspbian Jessie or Stretch, RedHat Enterprise 7.5+, CentOS 7.5+, Fedora 28+
- Mono 5.4 or higher

macOS (x64)

Requirements:

- Sierra (10.12) or higher
- Mono 5.4 or higher

Raspberry Pi 2 Model B, Raspberry P 3 Model B, Raspberry Pi 3 Model B+, and Raspberry Pi 4 model

Requirements:

- Blank 8GB or larger microSD card
- PC capable of writing to microSD card

Firewall Considerations for ECI DCA:

Inbound Connections

There are no inbound connections from the internet to ECI DCA.

Outbound Connections

The below listed ports must be whitelisted to ensure connectivity of ECI DCA.

- Data Upload
    - Through **Port 443/tcp (HTTPS)** with a connection to FMAudit Central Server
- Software Updates

    - Through **Port 443/tcp (HTTPS)** with a connection to FMAudit Central Server
- Registration (fallback)
    - Through **Port 53/udp (DNS)** with a connection to Local Network DNS server (primary) and FMAudit Central (fallback)

PC/Server requirements for FMAudit Onsite:

- 1GB RAM
- 400 MB Disk Space
- Microsoft .NET Framework 4.7.1 or newer
- Windows 7 SP1, 8.1, 10, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019
- Internet Explorer 11.0 or newer, Chrome, Firefox
- 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_Central_FQDN)/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/Server requirements for FMAudit Java Onsite on Linux and MAC OS Systems (Optional installation): Linux OS System Requirements

- Administrator (Root) level permissions
- PC or Server with a 1 GHz Intel or AMD processor and 512MB of RAM
- Linux (CentOS, Raspbian, Debian, Fedora, Ubuntu, RHEL, SuSE)
- Java Runtime Environment 1.7 or later
- 400MB of available disk space
- Broadband Internet connection to contact the Central Server

MAC OS System Requirements:

- Administrator (Root) level permissions
- MAC with a 1 GHz Intel processor and 512MB of RAM
- MAC OS X 10.X or macOS Sierra or higher
- Java Runtime Environment 1.7 or later
- 400MB of available disk space
- Broadband Internet connection to contact the Central Server

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

- Windows XP, Windows Vista, Windows 7, Windows 2003, Windows 2008
- Microsoft .NET Framework 2.0
- 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 161/33333 inbound/outbound for both TCP and UDP

Note that for recent OS versions using driver model 4 (e.g. Windows 10), only Kyocera and Ricoh OEMs, and their variations, are supported currently.

Data Collected and Encryption

1.2 Data Encryption

All data packages from ECI DCA and FMAudit Onsite are encoded and obfuscated. FMAudit recommends utilizing HTTPS for communication Onsite and FMAudit Central. ECI DCA **must** be utilized with HTTPS to function correctly. Additionally, all sensitive settings and jobs between ECI DCA and Central are encrypted using AES256 standard symmetric encryption algorithm, using a protected shared key. This ensures end-to-end encryption, so data is protected from being read if intercepted by a third party, a competitive or otherwise non-authorized FMAudit instance.

1.3 Security Concerns

ECI DCA and FMAudit Onsite communicates with FMAudit Central by sending an encoded and obfuscated XML stream using the SOAP over HTTPS 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 ECI DCA or FMAudit Onsite, with the exception of IP Address, MAC Address, and HostName, which could be excluded from the data submitted if the user chooses to exclude these details.

ECI DCA and FMAudit Onsite does not collect or process any personal data and the only way the system will collect this type of information is if you or your customers input them into FMAudit within a field or label such as location or customer name. ECI DCA and Onsite enables you to monitor network devices using Simple Network Management Protocol (SNMP). It exists inside the customer's network and from there, it communicates with devices to gather operational information about the device that is made available via the device firmware and an SNMP Management Information Base (MIB). The data exposed by the device varies by manufacturer and model, but it is always technical or operational in nature and specific to the device itself. At the most basic level the data exposed by a printer MIB is documented in the IETF RFC 3805 (https:// tools.ietf.org/html/rfc3805). Additional device information may be exposed by the manufacturer through extensions and private MIBs, but the information is fundamentally technical and device-specific.

1.4 Types of Information Collected

ECI DCA and FMAudit Onsite attempts to collect the following information from networked printing devices during a network scan:

Device Attributes

- IP address (can be masked)
- Manufacturer
- Serial number
- Asset number
- MAC address
- Device description
- Location
- Miscellaneous (machine specific)

Coverage and Meters

- Meter reads
- Meter type
- Coverage level
- Monochrome or color identification

Supplies

- Toner cartridge serial number
- Toner cartridge supply level
- Drum levels
- Maintenance kit levels
- Non-toner supply levels
- Miscellaneous levels

Service

- LCD reading
- Device status
- Error codes
- Firmware

FMAudit Agent, explained further below, attempts to collect the following information from local devices:

- Manufacturer
- Asset number
- Device description
- Location
- Serial number
- Meter reads
- Supply levels (vendor dependent)
- Service codes (vendor dependent)
- Miscellaneous (machine specific)
- IP address of the machine the Agent is installed on (FMAudit Agent Host)

Network Discovery and Meter and Supply Collection (ECI DCA)

To add to the efficiency of the DCA, only when there is new or changed data from the devices will this information be sent into the FMAudit Central Server. This will ensure minimal network load and remove the frequency of any backlogs of device data submissions. Also, discovery and scanning of devices are now independent to ensure that only the IP addresses (or hostname) of devices that have been previously discovered are being scanned on the periodically set basis versus a full network scan (this is completed initially, periodically, or when determined by an admin user).

This will ensure that the speed of device data submissions is as up to date as possible. This will allow for users to be notified of troublesome devices within minutes or even seconds in many situations. ECI DCA separates device discovery from other scan types, enabling you to set custom scan intervals for retrieving meters, supplies attributes and errors. The minimum and maximum values for the scan intervals are:

Scan Function	Default	Minimum	Maximum
Discovery	30 minutes	10 minutes	720 minutes
Meters	120 minutes	10 minutes	720 minutes
Supplies	60 minutes	10 minutes	720 minutes
Errors	60 seconds	30 seconds	600 seconds
Attributes	360 minutes	10 minutes	720 minutes
Device W/out MDF	60 minutes	10 minutes	24 hours

Please note that scan intervals (meters, supplies, errors and attributes) are only available if a device has a model definition file (MDF). If this is not present, a full scan will be done on the device in question on a predefined interval.

FMAudit Central administrators can remotely manage ECI DCA that have been activated on the server as well as remotely trigger the ECI DCA to execute predefined commands such as data collection tasks, providing ECI DCA logs, running remote MIBWalks, installing HP JAMC, or updating ECI DCA and Onsite settings.

Note: ECI DCA always initiates this communication to the Central server, and not the other way around.

Note: Only when meter or supply information has updated or changed does communication occur, to reduce bandwidth usage.

Network Discovery and Meter and Supply Collection (FMAudit Onsite)

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

FMAudit Central administrators can remotely manage FMAudit Onsites that have been activated on the server as well as remotely trigger the Onsite to execute predefined commands such as data collection tasks, providing Onsite logs, running remote MIBWalks, installing HP JAMC, or updating Onsite settings. These are explained in further detail below:

Function	**Location**	**Description**
Tasks	Onsite Settings	Can remotely configure tasks to run on a preset schedule but can select tasks (Cache, Meters, Supplies, Service) to run immediately and collect device data on command.
MIB Walks	Onsite Settings	Can indicate certain IPv4/IPv6/Hostnames of devices and trigger the Onsite to Start the Collection of the MIB Walks immediately.
Logs (Detailed)	Onsite Settings	Can instruct the Onsite to collect the Logs (Critical, Error, Warning, Details, Debug) from a certain date.

None of these commands lead to data collection beyond the types of information collected as described above. Data exchanged between FMAudit Onsite and FMAudit Central is encrypted using strong encryption protocols that are FIPS compliant. Onsite receives secured software updates from the FMAudit Updates servers.

The Onsite communicates with Central at a predefined interval to determine if there are any queued actions which are not already executed, thus ensuring actions are executed in a timely manner.

Note: FMAudit Onsite always initiates this communication to the Central server, and not the other way around.

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, FMAudit 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 under one hour.

Local Printers

1.5 Local (USB) Device Support

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 and parallel. 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.

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.

FMAudit Central Application

FMAudit Central functionality is accessible via a web-based user interface.

Permissions based User Management

Access to the FMAudit Central web console is controlled with permissions-based user management. Users must log in to Central using a designated username and password. Users are assigned one or more roles which specify permissions and are granted access to one or more groups of devices. Administrators will full permissions can specify exactly which screens each user can view and/or interact with.

HTTPS access

The website can be accessed using HTTPS via port 443 provided that the web server is installed with a valid SSL security certificate. Optionally, FMAudit Central Administrators can require users that access the website using HTTPS by redirecting the HTTP version of the website. We recommended all sites to use HTTPS as it ensures encryption of data being transferred over the Internet.

FMAudit Side-By-Side

FMAudit Central utilizes a Model Attributes Database termed as Side-by-Side, which contains various model attributes as printing speeds, when was introduced on the market or OEM Part Numbers compatibilities, which is periodically updated as future models and versions are released by OEMs. FMAudit Central will communicate with Side-by-Side to check for new updates as well as retrieve device attributes to cache them locally on each FMAudit Central system.

1.6 Hosting

FMAudit Central is able to be hosted by ECi Software Solutions within secure and protected datacenters within the US and the UK as well as hosted on premise based upon the needs of the dealer or reseller. ECi Software Solutions understands that the confidentiality, integrity, and availability of our customers' information is vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes, to meet the growing demands and challenges of security.

1.7 Secure Data Centers

Our service is collocated in dedicated spaces at top-tier data centers. These facilities provide carrier-level support, including:

Access control and physical security

- 24-hour manned security, including foot patrols and perimeter inspections
- Biometric scanning for access
- Dedicated concrete-walled Data Center rooms
- Computing equipment in access-controlled steel cages
- Video surveillance throughout facility and perimeter
- Building engineered for local seismic, storm, and flood risks
- Tracking of asset removal

Environmental controls

- Humidity and temperature control
- Redundant (N+1) cooling system

Power

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems
- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage

Network

- Concrete vaults for fiber entry
- Redundant internal networks
- Network neutral; connects to all major carriers and located near major Internet hubs
- High bandwidth capacity

Fire detection and suppression

- VESDA (very early smoke detection apparatus)
- Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

Network protection

- Perimeter firewalls and edge routers block unused protocols
- Internal firewalls segregate traffic between the application and database tiers
- Intrusion detection sensors throughout the internal network report events to a security event management system for logging, alerts, and reports
- A third-party service provider continuously scans the network externally and alerts changes in baseline configuration

Backups

- All data are backed up to tape at each data center, on a rotating schedule of incremental and full backups
- Tapes are not transported offsite and are securely destroyed when retired

1.8 Version Management

Testing and Release Process

Each major and minor release of the software goes through a quality control process, in which multiple FMAudit personnel will regression test altered portions of the system to ensure there has not been a downgrade in security or functionality of the system, as well as validate the new functional aspects. Major releases go through a beta release process where select clients run the new and old systems in parallel.

Source Code Security

FMAudit source code is kept in a secured revision control system, accessible only to authorized persons. Every change to the source code is tracked, which includes which developer made the change and why. Products are encrypted and digitally signed with a code-signing certificate before shipping. An escrow deposit can be made available based on request.

Data Privacy and Legislation

General Data Protection Regulations (GDPR)

As of May 2018, the European Union's General Data Protection Regulations (GDPR) came into full effect. The GDPR replaces the Data Protection Directive 95/46/EC and is designed to strengthen and unify data privacy laws across Europe.

FMAudit has implemented a structured and comprehensive GDPR compliance program to help ensure readiness for the regulation when it took place and has on-going compliance post-implementation. The program consists of, among other things, training of staff, audit and risk assessment across the business, policies and procedures, governance and ongoing compliance. We encourage our customers to take similar steps to ensure their own businesses are prepared for the GDPR when it takes effect and also for the years to come.

For more information on GDPR, visit https://eugdpr.org/

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 range. 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.

For more information about HIPAA, visit http://www.hhs.gov/ocr/privacy/

Federal Information Processing Standard (FIPS)

The Federal Information Processing Standard Publication 140-2, (FIPS PUB 140-2), is a United States government computer security standard used to approve cryptographic modules. The standards describe document processing, encryption algorithms, and other information technology standards.

The FMAudit Onsite and ECI DCA data collection tool and FMAudit Central is fully compliant with FIPS regulations and standards.

Sarbanes-Oxley Regulations

Sarbanes-Oxley compliance is not affected by usage of FMAudit Central, ECI DCA, or FMAudit Onsite software applications as FMAudit software is not intended to be used as part of an internal control structure as outlined in Section 404: Management

Assessment of Internal Controls but will not interfere with these controls. Information Technology controls are an important part of complying with Sarbanes-Oxley. Under this Act, corporate executives become responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. There are IT systems in the market that are designed specifically for meeting these objectives.

FMAudit software is not designed as an IT control system but will not interfere or put at risk other systems that are intended for that purpose.

For more information about Sarbanes-Oxley, visit http://www.sec.gov/about/laws/soa2002.pdf

Gramm-Leach-Bliley Act (GLBA) Regulations

Gramm-Leach-Bliley Act (GLBA) compliance is not affected by usage of FMAudit Central, ECI DCA, or FMAudit Onsite software applications as the use of FMAudit software applications are not seen to have an impact on compliance with the Gramm-Leach- Bliley Act (GLBA) for covered entities. This is because FMAudit software applications do not collect, house or transmit any information regarding the content of print jobs, so have no way of accessing, housing or transmitting customers' personal financial information, even if this information is printed or otherwise sent to print devices monitored by FMAudit software applications.

For more information about the Gramm-Leach-Bliley Act, visit http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

Federal Information Security Management Act (FISMA) Regulations

Federal Information Security Management Act (FISMA) compliance is not affected by usage of FMAudit Central, ECI DCA, or FMAudit Onsite software applications as FMAudit software applications are not intended to be part of an internal control system for FISMA but will not interfere with these controls. The use of FMAudit software applications are not seen to have an impact on compliance with FISMA for covered entities. This is because FMAudit software applications do not collect, house or transmit any information regarding the content of print jobs, so have no way of accessing, housing or transmitting high risk information, even if this information is printed or otherwise sent to print devices monitored by FMAudit software applications.

For more information about the FISMA, visit http://csrc.nist.gov/groups/SMA/fisma/index.html

Payment Card Industry Data Security Standards (PCI DSS) Regulations

PCI DSS (Payment Card Industry Data Security Standards) compliance is not required for FMAudit Central, ECI DCA, or FMAudit Onsite software applications as the PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The PCI DSS standards apply to all organizations that store, process or transmit cardholder data. These organizations must be PCI DSS compliant.

The use of FMAudit solutions does not have an impact on PCI DSS compliance. FMAudit software applications do not store, process or transmit cardholder data or personal information. FMAudit solutions also does not collect, house or transmit any information regarding the content of print jobs, so has no way of accessing, housing or transmitting customers' personal financial information, even if this information is printed or otherwise sent to print devices monitored by FMAudit software.

For more information about PCI DSS compliance, visit https://www.pcisecuritystandards.org/security_standards/index.php

Transport Layer Security (TLS) Updated Protocol Compliance

Transport Layer Security (TLS) is a protocol that secures data communicated between clients/servers via the internet. It is a more secure version of its predecessor, Secure Sockets Layer (SSL). TLS provides data privacy and integrity, encrypting data to ensure no third-party can read or tamper with it while transmitted to a client/server.

A connection with potential weaknesses, such as TLS 1.0, could expose sensitive data such as usernames, passwords and credit card numbers. As a result, security standards like the Payment Card Industry Data Security Standard (PCI DSS) have been updated to require the use of newer TLS versions that address these weaknesses and use stronger encryption. As of July 1st, 2018, TLS 1.0 will no longer be compliant by PCI security standards and so merchants must update to TLS 1.1 or higher prior to this date to continue processing card payments. Again, it is important to note that PCI security standards do not apply to FMAudit solutions as the software does not store, process or transmit cardholder data. However, recommendations in the PCI security standards, specifically the use of TLS 1.1 and higher, may indirectly affect applications like the ECI DCA and FMAudit Onsite data collection agent that communicates via the internet.

ECI DCA and FMAudit Onsite was built on Microsoft .NET Framework 2.0, which originally did not support TLS 1.1 and TLS 1.2 because these protocols were released after it was created. Onsite v3.7.4 or newer supports TLS 1.1 and 1.2 if the latest Windows Updates and some OS-specific Hotfixes are installed. TLS 1.1 and TLS 1.2 are not available for Windows XP, Server 2003, Vista and Server 2008, so if TLS 1.0 is disabled on the Central server then these systems will not be able to communicate with Central. FMAudit Central v4.5 and newer include ECI DCA 1.4.0 and FMAudit Onsite v3.7.4 that will automatically attempt to install the required Hotfixes for each host OS version where the application is installed.

Frequently Asked Questions (FAQs)

Do FMAudit products work with Internet proxies?

Yes, ECI DCA and FMAudit Onsite are able to work with most proxies. In the user interface of the Onsite there are options to configure different proxy settings. This is also possible from the ECI DCA or Onsite Settings within the FMAudit Central UI under the 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, ECI DCA, 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 7 SP1, 8.1, 10, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019.

Detailed hardware and software requirements can be found at the following URL:
ftp://ftp.fmaudit.com/customer/documents/Software-Requirements.pdf

Is FMAudit Products compatible with Mac, Linux, or Raspberry Pi environments?

This ECI DCA brings about major advantages over FMAudit Onsite without losing any features, including full native cross-platform support of Windows, macOS, Linux, and Raspberry Pi, each with unique installation steps, support documentation, and trained support staff on these platforms. The installation process has also greatly improved and is much more intuitive for all types of users.

Does the FMAudit Viewer require Internet access?

Generally no, except for Licensing and some of the Dynamic Reports that need to connect to FMAudit Side- by-Side services. 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. ECI DCA and 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. However, the below listed ports must be whitelisted to ensure connectivity of ECI DCA.

- Data Upload
  - Through **Port 443/tcp (HTTPS)** with a connection to FMAudit Central Server
- Software Updates
  - Through **Port 443/tcp (HTTPS)** with a connection to FMAudit Central Server

- Registration (fallback)
    - Through **Port 53/udp (DNS)** with a connection to Local Network DNS server (primary) and FMAudit Central (fallback)

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?

ECI DCA and 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.

How does the FMAudit WebAudit process work?

From FMAudit Central, the dealer specifies the end-user's (customers) applicable billing cycle. At this time, an email is automatically generated and sent to the appropriate contact informing them it is time to collect their meters. The instructions include a URL whereby when the end-user clicks the link, it automatically launches their web browser, ready to perform the action. The end-user then clicks "'start" and "'save"'. Done. No software is installed at any time. A link to the WebAudit page may also be posted on the dealers existing website, i.e. Enter Meter Readings web page. This allows the user to automate the collection, rather than having to manually walk from device to device, print the configuration page and transcribe the meters.

How do I get additional information for FMAudit Central, ECI DCA, FMAudit Onsite, etc?

Additional information can be found on the FMAudit website: http://www.fmaudit.com/