exterro®
Legal GRC Software

FTK LAB

SYSTEM SPECIFICATION GUIDE

September 2023

Table of Contents

Overview 4

1 Infrastructure Overview 5

2 Common Deployment Examples 7

2.1 Stand-Alone Examiner 7

2.2 Multi-Examiner Lab 8

3 General Configuration 9

3.1 Virtualization 9

3.2 Shared Hosts 9

3.3 Service Account 10

3.4 Certificates 11

3.5 Anti-Virus Software 11

4 Software Requirements 12

4.1 Third-Party Licensing 13

5 General Hardware Requirements 14

6 Storage 15

6.1 Estimating Storage Requirements 18

7 Network 19

7.1 Database 19

7.1.1 Microsoft SQL Server 19

7.1.2 PostgreSQL (When Used In Place of Microsoft SQL Server) 20

7.2 Processing Engine 20

7.2.1 Local Processing Engine 20

7.2.2 Distributed Processing Engine 21
7.3 Distributed Processing Manager 21
7.4 FTK Self-Host Service 21
7.5 Network License Service 22
8 Database Requirements 23
8.1 Microsoft SQL Server 24
8.2 PostgreSQL 24
Appendix A: Pre-implementation Checklist 25
Contact Exterro 27

Overview

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today, providing software solutions that help some of the world's largest corporations, law enforcement departments, and government agencies work smarter, more efficiently, and support the Rule of Law.

Exterro FTK Lab is the most trusted digital forensics software in the world. Exterro FTK Lab provides law enforcement officials, corporate security, and IT professionals with deep visibility into static data through its forensic analysis and review functionality. With Exterro FTK Lab investigators can perform focused forensic analysis efficiently, all while maintaining integrity of all ingested data. In addition Exterro FTK Lab allows for secure collaborative analysis amongst the various evidence reviewers both internal or external, real-time task and case management, and a massive increase in evidence processing speed by leveraging a processing farm of DPE's.

This document contains detailed information about the software and hardware leveraged by the FTK solution. In addition to the specific requirements for each component of the solution, this guide includes recommendations on its various configurations and workflows.

1 Infrastructure Overview

FTK Lab is comprised of a series of functional components which allow the solution to be tailored to the unique needs of an organization. Components may be installed to a single host or distributed across multiple hosts to provide both scalability and additional functionality.

The following section contains a brief description of each component and its role within the solution:

- **Database** – The FTK solution utilizes a single database instance, in which it maintains multiple databases containing file metadata, user data, and other information. FTK supports the use of either Microsoft SQL Server or PostgreSQL.
- **FTK Lab Examiner** – The Examiner is the primary user interface of the FTK solution, facilitating the analysis of data for the investigator.
- **Processing Engine** – The Processing Engine performs data processing tasks such as the expansion of archives, indexing, de-duplication analysis, file identification, secondary culling and filtering, and the creation of work product. It has been designed to be deployed in one of two ways to provide maximum flexibility and scalability:
    - **Local Processing Engine** – A Local Processing Engine ("EP") is commonly employed in stand-alone Examiner environments as it is capable of both managing and performing processing tasks requested by the Examiner.
    - **Distributed Processing Manager / Distributed Processing Engine** – The Distributed Processing Manager ("DPM") and Distributed Processing Engine ("DPE") are commonly employed in multi-Examiner environments. The DPM is responsible for managing processing tasks requested by the Examiner. One or more DPEs may be assigned to a DPM to perform the processing tasks being managed by the DPM.

- **FTK Self-Host Service** – The FTK Self-Host Service is an optional component that allows users to take advantage of Smart Review.
- **CodeMeter/Network License Server** – CodeMeter is the licensing service used by FTK. The Network License Server is an optional component that allows multiple FTK Examiners to share a CodeMeter license.

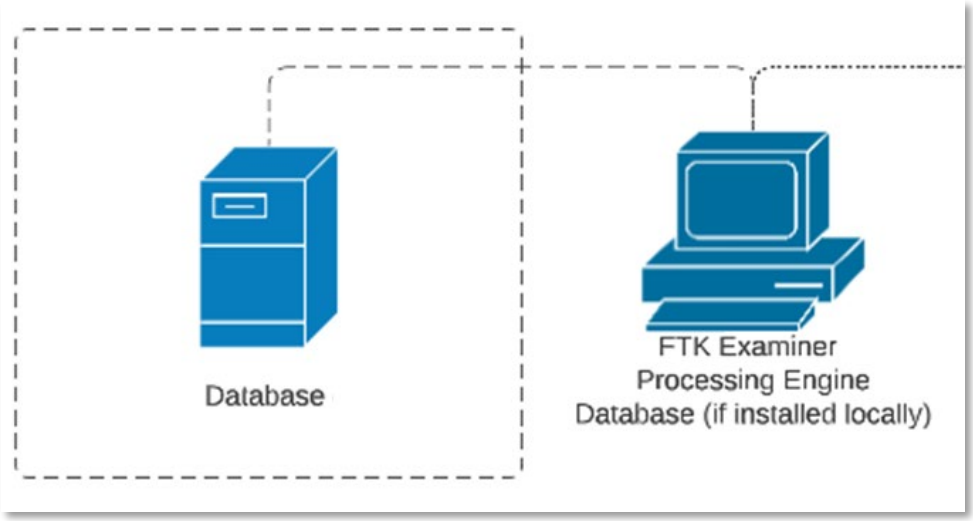
2 Common Deployment Examples

The majority of FTK Lab environments fall into one of the generalized implementation models included in the sections below.

Note: *The figures below are overly simplified diagrams meant to illustrate the basic infrastructure of each example. Please contact your Exterro technical support representative for further information and assistance*.

2.1 Stand-Alone Examiner

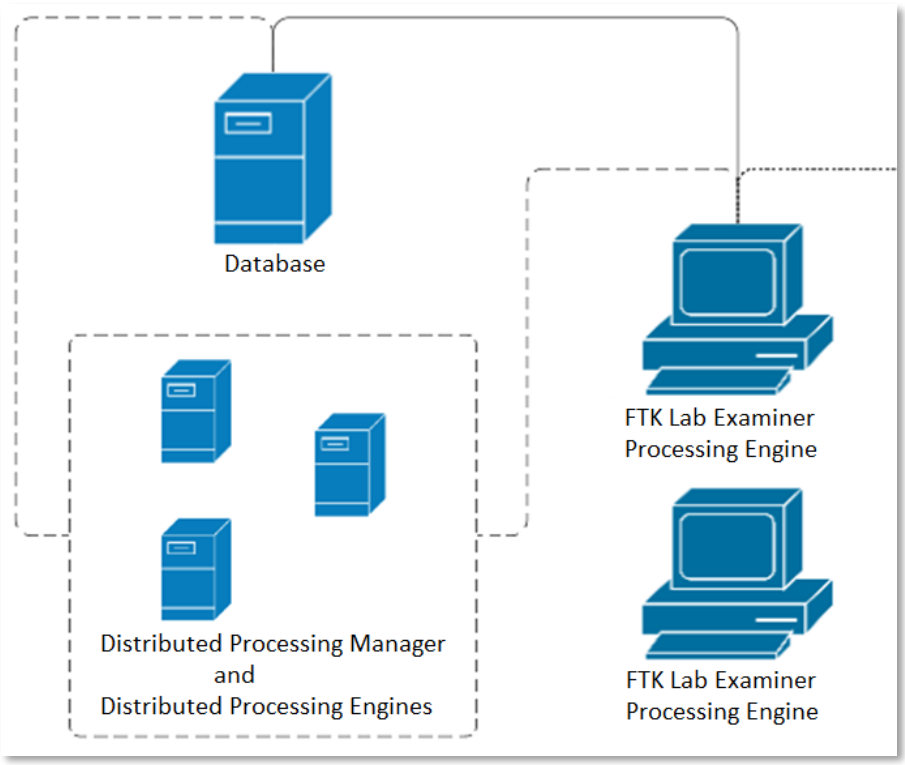
The fundamental FTK Lab deployment model is the Stand-Alone Examiner, in which each of the solution's essential components is installed to a single host. In this configuration, FTK is fully capable of all processing and review workflows.



In this model, the Database component may be installed to the same host as the other components or to its own dedicated host for the purpose of both simplifying the process of any future scaling of the environment and improving overall performance by eliminating resource contention between the Database and the solution's other components. Similarly, evidence and project data can either be maintained locally or on dedicated file shares.

2.2 Multi-Examiner Lab

The most common type of FTK Lab deployment is the Multi-Examiner Lab model. Effectively a scaled version of the Stand-Alone Examiner model, the Multi-Examiner Lab allows the solution to be scaled to accommodate additional concurrent users.



In this model, the Database component is shared by multiple Examiners and is typically installed to a dedicated host to ensure reliable access and file shares are established for evidence and project data.

This model frequently leverages distributed processing, which allows multiple Examiners to share use of one or more Distributed Processing Engines for additional processing power.

3 General Configuration

3.1 Virtualization

Exterro supports the use of VM hosts for all components. Exterro reserves the right to withdraw support on any specific support issue if during troubleshooting the issue is found to be induced by virtualization.

Supported hypervisor platforms include VMWare, Microsoft Hyper-V, Microsoft Azure, and AWS.

3.2 Shared Hosts

Support of an environment in which any component of the FTK solution shares a host with another application is subject to the discretion of Exterro.

The FTK solution requires a dedicated database instance. Attempts to host the Database component in the same instance as other enterprise applications will not be supported.

Exterro forbids the installation or operation of any FTK component on any system that hosts a Microsoft Domain Controller.

3.3 Service Account

The FTK solution requires a single, dedicated administrative/service account. In a multi-host environment, a domain-level service account is required.

To facilitate implementations and upgrades, the service account must be provided with “Logon as Service” and “Interactive Logon” system permissions and should be added to the local Administrator group (or possess privileges equivalent to membership in the local Administrator group) on each host in the environment.

If the Database component is hosted in Microsoft SQL Server, the service account must be added to the instance’s Logins. To facilitate the initialization and upgrade of the database schema, this Login will require membership in the SysAdmin role during implementation and upgrades.

If the service account password is configured to expire or is otherwise changed, it is the responsibility of the customer to update all component services running under the service account credentials. Please contact your Exterro technical support representative for further information and assistance.

3.4 Certificates

Depending on its use and configuration, the FTK solution may require certificates to protect communication between certain components.

3.5 Anti-Virus Software

Exterro strongly recommends that any anti-virus or anti-malware software located on a server hosting any component of the FTK solution be configured to disable on-access scanning of the drives or directories containing project data, evidence, database files, or application-specific temporary files.

Any manual or scheduled anti-virus or anti-malware scans should be monitored to ensure they are not interfering with the overall performance of the solution.

Please contact your Exterro technical support representative for further information and assistance.

4 Software Requirements

The FTK solution has been designed and developed to leverage Microsoft technologies. Each host's operating system should be patched to the latest service pack and updates.

The following table contains the software prerequisites for each component.

Note: *The italicized runtime libraries and dependencies are provided within the component installers and do not need to be manually installed prior to implementation. Compatibility for higher versions of these runtime libraries and dependencies are not guaranteed and installing higher versions than those listed below is not recommended.*

Component	Prerequisites
FTK Lab Examiner	**Windows 10, Windows Server 2016, Windows Server 2019** *.NET 4.8* *Microsoft Visual C++ 2015-2022 Redistributable (x64)*
Processing Engine (*Local or Distributed*)	**Windows 10, Windows Server 2016, Windows Server 2019** *.NET 4.8* *Microsoft Visual C++ 2015-2022 Redistributable (x64)*
Distributed Processing Manager	**Windows 10, Windows Server 2016, Windows Server 2019** *.NET 4.8* *Microsoft Visual C++ 2015-2022 Redistributable (x64)*
FTK Self-Host Service	**Windows Server 2016, Windows Server 2019** *.NET 4.8* *Microsoft Visual C++ 2015-2022 Redistributable (x64)*

4.1 Third-Party Licensing

The FTK Lab solution requires Microsoft Windows and, optionally, Microsoft SQL Server, both of which must be licensed through Microsoft or an approved reseller. If performing processing, collection, or export of email, you may need a licensed copy of Microsoft Outlook on each host with a Processing Engine which must be licensed through Microsoft or an approved reseller.

5 General Hardware Requirements

The overall performance of the FTK Lab solution is dependent on the hardware employed to host its various components. Ideally, all implementations would employ the latest processors, large amounts of memory, and massive redundant arrays storage. However, as most environments will be constrained by budgets, the following guidelines have been developed to assist in the creation of cost-effective environments that conform to the various needs of a diverse client base.

Minimum hardware recommendations for each component when deployed on its own host can be found below. Please contact your Exterro technical support representative for further information and assistance.

Component	Processor	Memory
FTK Lab Examiner	8 Logical Cores	16GB RAM
Processing Engine (Local or Distributed)	8 Logical Cores	16GB RAM
Distributed Processing Manager	4 Logical Cores	8GB RAM
FTK Self-Host Service	8 Logical Cores	16GB RAM

The Processing Engine (regardless of whether installed in a “local” or “distributed” configuration) calculates the total number of worker threads available to perform certain operations using the number of logical processor cores on a system. Certain operations can be expected to leverage all available processor and memory resources available to the host system.

Systems with insufficient memory resources can experience bottlenecks as certain operations may cause the system to start paging. The presence of any paging on a system will result in an associated reduction in the performance of the solution and severe paging—also known as “thrashing”—can lead to operational failure.

It is strongly recommended that any system involved in the implementation environment possesses at least 2GB of RAM for each logical processor core (e.g., an 8-core system should have at least 16GB of RAM) to reduce the likelihood of paging. Additionally, it is recommended that any system hosting the MSSQL Database possess at least 4GB of RAM for each logical processor core (e.g., an 8-core system should have at least 32GB of RAM).

6 Storage

The storage requirements of the FTK Lab solution are dependent on a number of variables, including the number of active projects, the volume of data involved in the projects, and the workflows employed within the tool.

The table below contains descriptions, characteristics, and recommendations on the various types of storage leveraged by the FTK Lab solution.

	Description	Comments
Operating System	Local disk volume on any system hosting one or more components that provides storage for the operating system.	The initial space requirements should include 40GB for the operating system. Systems with more than 16GB of RAM will require additional space to accommodate the system pagefile. This storage should be fault tolerant.
Applications	Local disk volume on any system hosting one or more components that provides storage for the installed application components.	The initial space requirements should include space sufficient to accommodate the components being installed. This storage may share the same disk volume as the Operating System, if desired.
Staged Evidence	UNC file share on a local disk volume or network-attached storage that provides storage for data acquired through means other than collection that will be ingested into the solution.	The initial space requirements are dependent on the needs of organization but can be significant. This storage should be fault-tolerant with low latency.
Collected Evidence	UNC file share on a local disk volume or network-attached storage that provides storage for data acquired using the solution's collection	The initial space requirements are dependent on the needs of organization but can be significant. This storage should be fault-tolerant with low latency.

	Description	Comments
	capabilities and may be ingested into the solution.	
Project Data	UNC file share on a local disk volume or network-attached storage that provides storage for project-specific data, application-generated files, and internally maintained copies of specific types of ingested data.	The initial space requirements for ingested evidence are roughly 33% of the space of the associated staged evidence. Additional space will be required to support ongoing workflow operations. This storage should be fault tolerant with low latency.
Exported Data	UNC file share on a local disk volume or network-attached storage that is used as a target for exported work product.	Exported data is separate from the associated records in a case and can be periodically purged to reduce the requirements of this storage space. The space requirements and fault tolerance are entirely dependent on the organization's workflow.
Processing Temp	Local disk volume on any system hosting the Processing Engine component that provides storage for ephemeral files generated by the Processing Engine during processing.	At least 50GB of space is required, but a minimum of 500GB is recommended. The most important characteristic of this space is its speed. This storage requires no fault tolerance.

For optimal performance, initial consideration should be given to the seek time, latency, and data transfer rates of the storage. High disk activity can be expected during certain operations and is not necessarily indicative of a problem. Sustained rates of disk activity above 85% or persistent disk queues over 2 during operations will result in a bottleneck effect and a corresponding reduction in the overall performance of the solution.

Note: *Sustained periods of high disk use and persistent disk queues can be a symptom of insufficient memory resources. Please see the recommendations found in the General Hardware Requirements section.*

Ongoing attention should also be paid to the space utilization and fragmentation of the storage which if neglected can also lead to a decrease in overall solution performance.

6.1 Estimating Storage Requirements

Projecting the storage space requirements for the FTK Lab solution begins with an initial estimation of the volume of Evidence that will be collected and processed into the platform.

Data Type	Description	Necessary Space	Performance
Evidence Files	The original staged or collected data to process into the solution.	Requirements are dictated by the needs of the organization.	Ideally, at least 3000 IOPS.
Project Data	Extracted files, generated SWF images, generated thumbnails, index files, etc.	Requirements can be estimated to be approximately 30% of the size of processed Evidence files.	Ideally, at least 7000 IOPS.
Processed Metadata	Extracted file metadata and associated information stored in the Application Databases.	Requirements can be estimated to be approximately 4-5GB of space in the Application Databases for every 1 million objects resulting from processing.	-

Please contact your Exterro technical support representative for further information and assistance.

7 Network

The following sections describe the relevant inbound "listener" TCP ports used by each component of the FTK Lab solution. **It is critically important to note that the ports listed in the sections below are often used only to establish a connection with the "listening" component.** Once a connection has been established, the actual communication taking place between the components will bind to a negotiate ephemeral port in the in the Dynamic Port Ranges of the "listening" host. The default Dynamic Port Range used by Windows is 49152 through 65535. Where applicable, this range has been included in the sections below for the sake of clarity.

Please contact your Exterro technical support representative for further information and assistance.

7.1 Database

7.1.1 Microsoft SQL Server

Port	Components	Comments
1433	FTK Lab Examiner Processing Engine FTK Self-Host Service	The default port used for routine connections to the default installation of the Database Engine. Named instances use dynamic ports. If the named instance is the only instance of the Database Engine installed, it will probably use TCP port 1433. If other instances of the Database Engine are installed, it will probably use a different TCP port. Because the port selected might change every time that the Database Engine is started, it's difficult to configure the firewall to enable access to the correct port number. If a firewall is used, we recommend reconfiguring the Database Engine to use the same port number every time. A fixed port or a static port is recommended.
MSDTC	FTK Lab Examiner Processing Engine FTK Self-Host Service	MSDTC uses RPC dynamic port allocation to randomly select a port number ranging from 1024 to 65535 for communication.

7.1.2 PostgreSQL (When Used In Place of Microsoft SQL Server)

Port	Components	Comments
5432	FTK Lab Examiner Processing Engine FTK Self-Host Service	The default PostgreSQL port. Connections to the PostgreSQL service use the localhost loopback interface, which is not generally blocked by system firewalls, but pre-existing port reservations have been known to prevent the PostgreSQL service from binding to the port.
49152 - 65535	FTK Lab Examiner Processing Engine FTK Self-Host Service	Negotiated TCP communication.

7.2 Processing Engine

7.2.1 Local Processing Engine

Port	Components	Comments
34096	FTK Lab Examiner FTK Self-Host Service	Default port used by the processing management, job, and processing engine event services.
34097	FTK Lab Examiner FTK Self-Host Service	Default port used by the processing engine services.
34099	FTK Lab Examiner FTK Self-Host Service	Default port used by the remote format converter service.
49152 - 65535	FTK Lab Examiner FTK Self-Host Service	Negotiated TCP communication.

7.2.2 Distributed Processing Engine

Port	Components	Comments
34097	Distributed Processing Manager	Default port used by the processing engine services.
34099	FTK Lab Examiner FTK Self-Host Service	Default port used by the remote format converter service.
49152 - 65535	Distributed Processing Manager FTK Lab Examiner FTK Self-Host Service	Negotiated TCP communication.

7.3 Distributed Processing Manager

Port	Components	Comments
34096	FTK Lab Examiner FTK Self-Host Service	Default port used by the processing management, job, and processing engine event services.
49152 - 65535	Distributed Processing Manager FTK Lab Examiner FTK Self-Host Service	Negotiated TCP communication.

7.4 FTK Self-Host Service

Port	Components	Comments
4443	End-Users FTK Lab Examiner	This port is customizable and is frequently changed to use port 443.
49152 - 65535	End-Users Distributed Processing Manager Distributed Processing Engine FTK Lab Examiner FTK Self-Host Service	Negotiated TCP communication.

7.5 Network License Service

Port	Components	Comments
6921	FTK Lab Examiner FTK Self-Host Service	Default port used by clients to query the Network License Service.
49152 - 65535	FTK Lab Examiner FTK Self-Host Service	Negotiated TCP communication.

8 Database Requirements

The FTK Lab solution utilizes a single database instance, in which it maintains multiple databases containing file metadata, user data, and other information. FTK Lab supports the use of either Microsoft SQL Server or PostgreSQL as its application database.

The following sections describe the general requirements for both database platforms with respect to their use with the FTK Lab solution.

Supported Databases:

- Microsoft SQL Server 2016 or 2017 or 2019
- PostgreSQL 14.0

8.1 Microsoft SQL Server

The FTK Lab solution requires a dedicated database instance. Attempts to host the Database component in the same instance as other applications will not be supported. Additionally, the support of any implementation which attempts to host the SQL Database component on the same hardware platform as other applications is subject to the discretion of Exterro.

The FTK Lab solution will create a separate database for each project within the application database instance, as well as associated SQL Logins which are used to facilitate and regulate access to the application databases. To ensure the proper operation of the platform, no modifications should be made to any of the Logins created and maintained by the application.

Exterro requires that the SQL instance hosting the application databases is created using the Default US Collation, "SQL_Latin1_General_CP1_CI_AS".

Exterro requires that the SQL Instance being used to host the SQL Database component must have Mixed Mode Authentication enabled.

Exterro requires that the Service Account that has been created for the FTK Lab solution be added to the application database instance as a Login. To facilitate the initialization and upgrade of the database schema, this Login will require membership in the SysAdmin role during implementation and upgrades.

Exterro requires the TCP/IP and Named Pipes Protocols to be enabled in the Network Configuration settings of the application database instance.

8.2 PostgreSQL

The FTK Lab solution includes installation files for its supported version of PostgreSQL. No additional configuration should be necessary in most situations.

Appendix A: Pre-implementation Checklist

The following checklist should be used to document the prerequisites necessary to ensure the successful implementation of FTK Lab and should be completed prior to product implementation by an Exterro engineer.

1. Hardware Information
   1.1. The hosts that have been designated for component installation and configuration are available.
   1.2. The hosts operating systems have been installed and are fully-patched.
   1.3. Any additional storage volumes or file shares have been properly provisioned and made available.
   1.4. SysPrep (or an equivalent operation) has been run on any host with a cloned or ghosted operating system (i.e., ensure each host has a unique SID).
2. Network Configuration
   2.1. The appropriate ports are open on each host (see Section 8).
3. Service Account *(If Applicable)*
   3.1. A dedicated Service Account name _____ has been created.
   3.2. The Service Account has been added to the local Administrators group on all hosts or provided with equivalent privileges.
   3.3. The Service Account has been given the “Interactive Logon” permission.
   3.4. The Service Account has been given the “Logon As Service” permission.
4. Microsoft SQL Server Configuration (*if applicable*)
   4.1. Microsoft SQL server has been installed and fully patched.
   4.2. The SQL instance name is _____ (default: “Default”).
   4.3. The SQL instance is configured to use port _____ (default: 1443).
   4.4. The SQL instance is configured to use “SQL_Latin1_General_CP1_CI_AS” coalition.
   4.5. The SQL instance has Mixed Mode authentication enabled.
   4.6. The Service Account has been added to the SQL instance as a Login and has been added to the SysAdmin role.
   4.7. Microsoft DTC is enabled.
   4.8. Named Pipes have been enabled for the instance.

5. Software Licensing
   5.1. A physical or virtual license dongle is accessible and has been properly stocked with the appropriate licensing.
6. Software Installation Media
   6.1. The Exterro engineer has provided a link to retrieve the latest software installers.
   6.2. The latest software installers have been downloaded and copied to all of the hosts or a location accessible from all of the hosts.

Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization's internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:

Exterro, Inc.

2175 NW Raleigh St., Suite 400

Portland, OR 97210.

Telephone: 503-501-5100

Toll Free: 1-877-EXTERRO (1-877-398-3776)

Fax: 1-866-408-7310

General E-mail:info@exterro.com

Website: www.exterro.com