exterro®
Data Risk Management

FTK ENTERPRISE 8.2 SP2

SYSTEM SPECIFICATION GUIDE

AUGUST 2025

Table of Contents

About Exterro

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. We deliver a fully integrated Data Risk Management platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world's largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

1 Infrastructure Overview

FTK Enterprise is comprised of a set of functional components that can be deployed as necessary to meet the specific needs of an organization. These components can either be installed on a single host or, more typically, distributed across multiple hosts to enhance scalability and extend functionality.

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

- **Database** – FTK Enterprise leverages a single database instance to manage multiple databases that store file metadata, user data, and other critical information. It supports the use of either Microsoft SQL Server or PostgreSQL, offering flexibility in database management.
- **FTK Enterprise Examiner** – The Examiner (Thick Client) is the primary user interface for FTK Enterprise, facilitating the forensic analysis of data by investigators and basic collection workflows. This component communicates with a centralized database and the FTK Web Service.
    - **FTK Enterprise Web Interface** – The Web Examiner (Smart View) is the secondary user interface of FTK Enterprise, facilitating both the forensic analysis of data and advanced remote collection workflows by investigators.

- **FTK Web Service (Self-Host)** – The FTK Web Service is a component that enables collaborative web-based data analysis and facilitates the collection of data from off-network agents and cloud-based sources using Smart View.
- **Processing Engine** – The Processing Engine performs data processing tasks such as the expansion of archives, indexing, de-duplication analysis, file type identification, and more. It is designed for flexible and scalable deployment, offering two distinct configuration options to meet varying needs:
    - **Distributed Processing Manager and Distributed Processing Engine** – In collaborative FTK Enterprise environments, the Distributed Processing Manager (DPM) and Distributed Processing Engine (DPE) are typically used. The DPM manages the processing tasks requested by an Examiner, while one or more DPEs can be assigned to the DPM to execute the tasks under its management.
- **Agent** – The FTK Agent is a modular application that can be deployed to computers, and which facilitates the secure forensic-level collection, analysis, and preservation of the computer's static and ephemeral data.
    - **Remote Mobile Discovery** – Leveraging the FTK Agent, the application supports consent-based collection of iOS Devices whether on/off-network without deploying any policies or applications on a targeted mobile device.
- **Site Server** – The Site Server is a component that facilitates data collection from Agents and Network Shares on behalf of the Examiner. Multiple Site Servers can be deployed in one of four distinct configurations, tailored to meet the necessary scale and specific data collection needs of customers:
    - **Root Site Server** – When deploying Site Servers, a single Root Site Server is configured to manage the distribution of collection jobs across the environment and to relay collected data back to the central system. They can also be configured to collect from on-network computers and network shares. Additional Site Servers can be deployed beneath the Root Site Server to support scalability and enable active Agent-based data collection from both on-network and off-network computers.
    - **Private Site Server** – Private Site Servers can be deployed under a Root Site Server to assist with active data collection from on-network computers and network shares. Although they can be used to scale collection capabilities, they are most commonly deployed in remote locations to enable low-latency collection from targeted systems.

- **Private (Protected) Site Server** – Private (Protected) Site Servers operate similarly to Private Site Servers, with one key difference: instead of bi-directional communication with the parent Site Server, they initiate all communication. This configuration is particularly useful when deploying a Site Server in locations that are outside the direct visibility of the primary environment.
- **Public Site Server** – Public Site Servers can be deployed beneath a Root Site Server to enable passive data collection from computers that are off-network or operating in a zero-trust environment. For scalability, multiple Public Site Servers can be deployed behind a load balancer or reverse proxy.

- **CodeMeter/Network License Server** – CodeMeter is the licensing service used by the FTK Enterprise. The Network License Server is an optional component that enables multiple Examiners to share a CodeMeter license.
- **Monitoring Tool** - The Monitoring Tool can assist with system monitoring, log collection, and service management within FTK Enterprise. **This is an optional component.**
- **Exterro AI Server -** The AI Server component utilizes a range of machine learning models and algorithms to support advanced features such as natural language multimedia search, text summarization of emails, documents, and chat conversations. **This is an optional component.**
- **Known-File Filter (KFF)** - The Known File Filter component, built on the Cassandra database engine, compares file hash values of known files against those in a case. Hash values, such as MD5, are derived from the file's content rather than its name or extension, enabling the identification of files with duplicate content even when the filename or other metadata has changed. **This is an optional component.**
- **Connectors** - The Connectors component manages data collection from certain structured data repositories supported by FTK Enterprise. **This is an optional component.**

2 Deployment Examples

The components of FTK Enterprise offer flexible deployment options to meet the specific needs of various organizations and workflows. The following section presents a series of broadly generalized configurations, highlighting some of the most common deployment methods. **Please contact Exterro Technical Support for further information and assistance.**

2.1 Shared Components

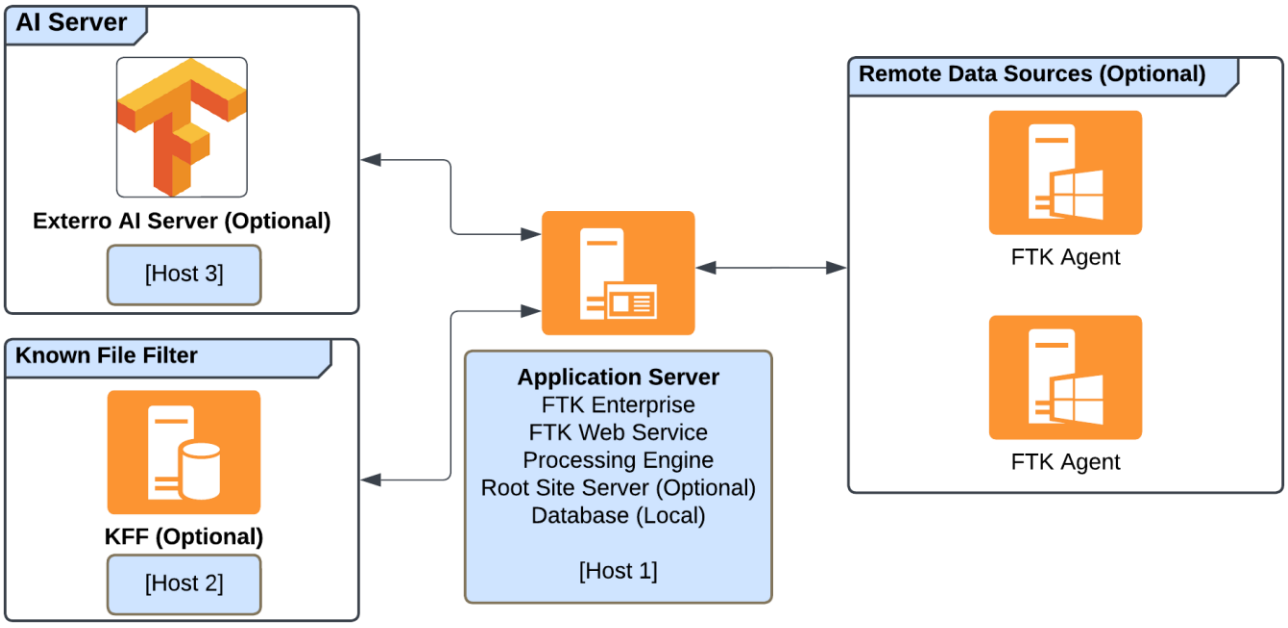
FTK Enterprise offers flexible deployment models, each built around a shared core of components designed to address diverse organizational needs. These components can include:

- **FTK Web Service**
- **FTK Enterprise Examiner (Thick Client)**
- **Application Database**
- **Processing Engines/Managers**
- **Exterro AI Server**
- **Known File Filter (KFF) Server**
- **Site Server**
- **Licensed Functionality**: Includes advanced features such as **ABBYY OCR** (Optical Character Recognition) for document processing and **RWS Offline Translations** for multilingual content analysis.

2.2 All-In-One Deployment

FTK Enterprise offers a flexible deployment model to accommodate a wide range of organizational needs. One such option is deploying all essential components on a single host (Application Server), which provides a streamlined setup for smaller environments or specific use cases. In this configuration, FTK Enterprise supports the complete suite of processing and review workflows, ensuring comprehensive functionality. Additionally, it can optionally facilitate direct data collection from on-network Agents and off-network Agents.

While it is possible to store the application database on the same host, Exterro strongly recommends deploying the database on a dedicated host. This approach enhances performance, scalability, and reliability, particularly in environments with high data throughput or complex workflows.



Note: Components labeled as (Optional) are not mandatory and can be excluded from deployments if their functionality is not necessary for an organizations specific use case.

2.3 Distributed Deployment (Collaboration with Remote Collections)

FTK Enterprise also supports a fully distributed deployment model, tailored for larger, more complex environments or organizations with higher performance and scalability requirements. In this configuration, all components are installed on dedicated hosts, ensuring optimal resource allocation and improved operational efficiency.

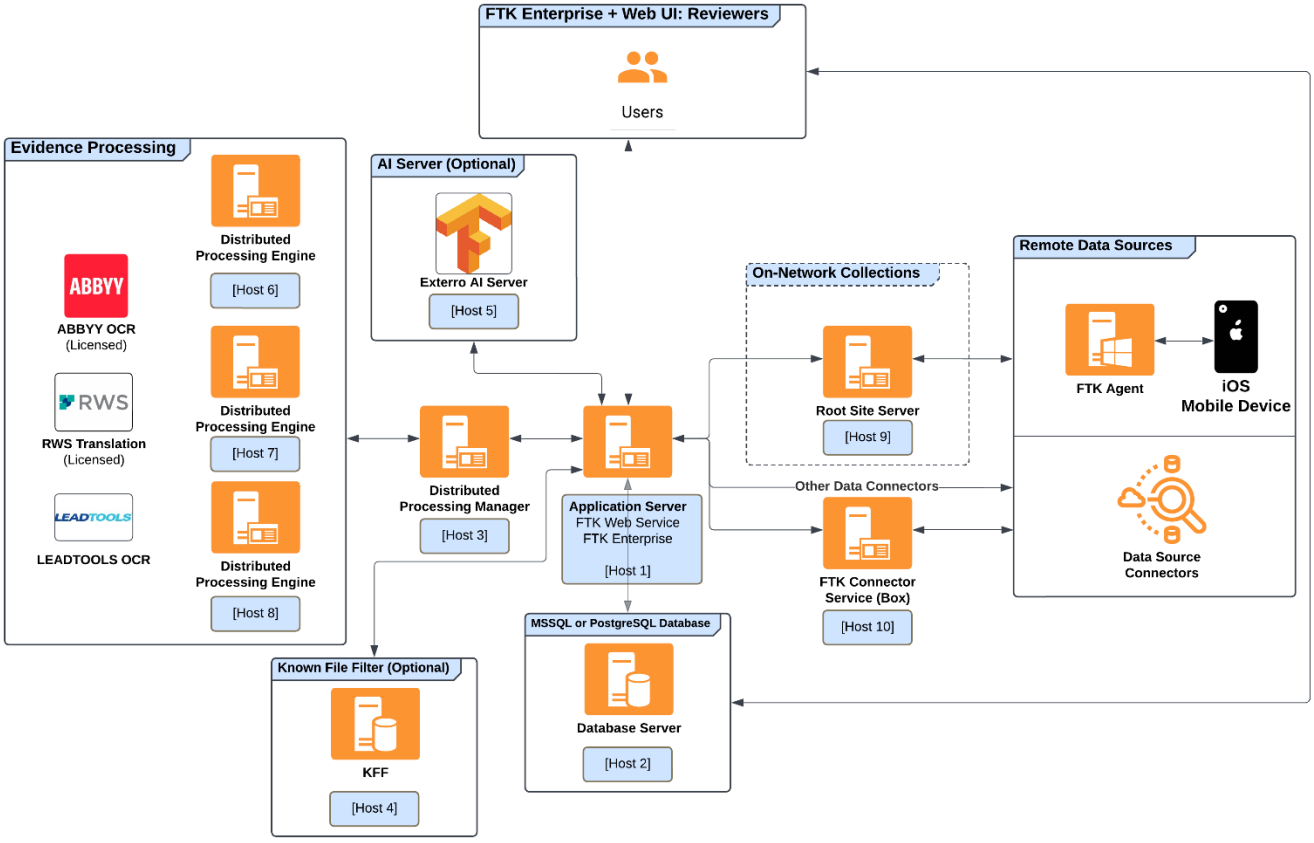
This deployment model leverages a Distributed Processing Manager (DPM) to efficiently orchestrate and delegate tasks across multiple Distributed Processing Engines (DPEs). By distributing processing jobs, it maximizes resource utilization and accelerates evidence processing, delivering faster and more efficient workflows.

With the addition of Site Servers and the FTK Connector Service, offering advanced data collection capabilities alongside its robust processing and review features. This configuration is designed to streamline evidence collection from both on-network and off-network. Agents as well as external data sources, including enterprise platforms like Slack, Microsoft Teams, Exchange and many more.

The Site Servers operate as a secure gateways, enabling reliable connectivity with remote systems and data sources while maintaining network integrity. The FTK Connector Service works in tandem with the FTK Web Service to facilitate seamless integration with modern communication and collaboration tools - a requirement only for Box Connector collections.

This architecture is ideal for organizations requiring large-scale investigative capabilities and advanced data collection from diverse sources. It supports growing teams, scales to meet evolving needs, and delivers the flexibility needed to handle today's complex forensic challenges.

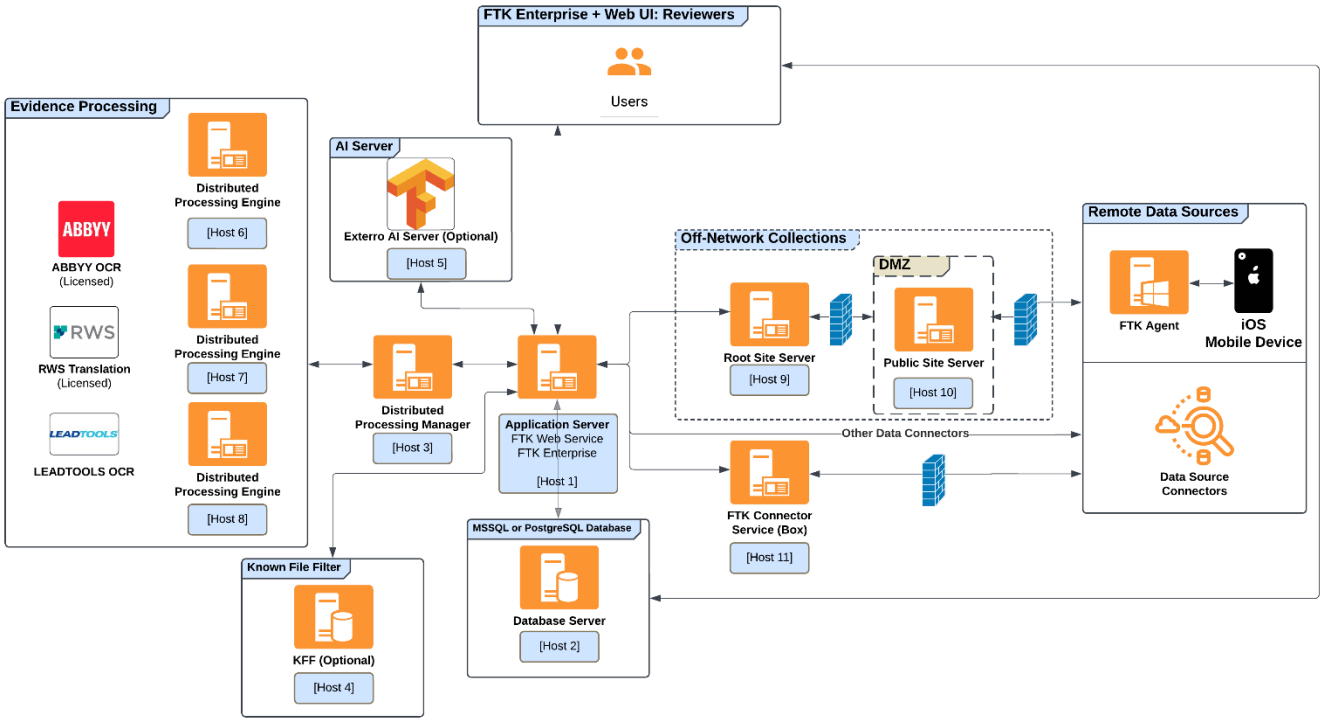
2.3.1 Distributed Deployment (On-Network Remote Collections)



Note: Components labeled as (Optional) are not mandatory and can be excluded from deployments if their functionality is not necessary for an organizations specific use case.

The FTK Connector Service is a requirement for environments collecting from Box data sources.

2.3.2 Distributed Deployment (Off-Network Remote Collections)



Note: Components labeled as (Optional) are not mandatory and can be excluded from deployments if their functionality is not necessary for an organizations specific use case.

The FTK Connector Service is a requirement for environments collecting from Box data sources.

3 General Requirements

Exterro strongly advises deploying all FTK Enterprise components on dedicated hosts to ensure optimal performance, security, and reliability. Configurations where FTK Enterprise components share a host with other enterprise applications are supported only at Exterro's discretion and may require additional review.

Exterro strictly prohibits the installation or operation of any FTK Enterprise component—other than the Agent—on systems functioning as Microsoft Domain Controllers. If the Agent is deployed on a system hosting a Domain Controller, it is critical to closely monitor the system's performance to maintain stability and mitigate any potential risks or disruptions.

3.1 Virtualization

Exterro permits the use of virtual machines or virtual hosts for all FTK Enterprise components. However, Exterro reserves the right to limit or withdraw support for any issues determined to arise from the virtualized environment or its configuration.

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

Note: The recommended instance size, virtual drive type, and other specifications depend on the client's case loads and user requirements. The sizing example provided by Exterro is intended for reference only. Clients should consult directly with Exterro to assess their specific sizing needs.

3.2 Service Account

FTK Enterprise deployments require a dedicated service account for reliable operation. In environments with multiple hosts, a domain-level service account is mandatory. To ensure seamless installation, upgrades, and functionality, the service account must meet the following criteria:

Permissions:

- Granted both **Logon as a Service** and **Interactive Logon** permissions.
- Added to the local Administrators group on each host in the environment or provided equivalent administrative privileges.

Database-Specific Requirements (if applicable):

If the Database component is hosted in Microsoft SQL Server, the service account must be added to the SQL Server instance's Logins.

During installation and upgrades, the account must temporarily be assigned the SysAdmin role to facilitate database schema initialization and updates.

Password Management:

- Should the service account password expire or be changed, the customer is responsible for updating all FTK Enterprise services configured to use this account.

Please contact Exterro Technical Support for further information and assistance.

3.3 Certificates

Depending on its configuration and usage, FTK Enterprise may require digital certificates to secure and facilitate communication between specific components.

Web Certificates:

Secure HTTPS communications between the FTK Web Service (Self-Host) and end-users through its browser-based user interface require the use of an SSL/TLS server certificate that meets the following requirements:

- The certificate format must follow the X.509 standard and be RFC 5280 compliant.
- The signature algorithm used for the certificate must be sha256RSA (SHA-256).
- The X509v3 KeyUsage section of the certificate must contain the Digital Signature and Key Encipherment attributes.
- The X509v3 ExtendedKeyUsages section of the certificate must contain the serverAuth attribute.
- The Subject Alternative Name ("SAN") must include the fully-qualified domain name ("FQDN") of the host where the certificate will be used, as well as any aliases that might be necessary.
- The Private certificate must be provided in a password-protected PKCS #12 format (.PFX).

Note: Some implementations may require the purchase of a properly configured certificate from a commercial Certificate Authority.

For Windows and Linux Agent Certificates:

Communications between the Examiner, FTK Web Service, Site Server, and Windows Agent components require the use of a dedicated Public/Private certificate pair that meets the following requirements:

- The certificate format must follow the X.509 standard and be RFC 5280 compliant.
- The signature algorithm used for the certificate must be sha256RSA (SHA-256).
- The Private certificate must be provided in a PKCS #12 format (.P12 or .PFX).
- The Public certificate must be provided in a binary DER-encoded .P7B or .CRT format and include the complete chain of trust (i.e., the Root CA and all intermediate CAs).

Note: Exterro provides a utility for Windows agents, Certman that can be used to generate valid self-signed Agent certificates.

For macOS:

- The certificate format must follow the X.509 standard and be RFC 5280 compliant.
- The signature algorithm used for the certificate must be sha256RSA (SHA-256).
- The certificate must be issued by a Certificate Authority that is trusted by all of the systems involved (i.e., the system hosting the FTK Web Service and the systems hosting the Mac Agents).
- The Subject Alternative Name ("SAN") must include the fully-qualified domain name ("FQDN") of the host where the certificate will be used, as well as any aliases that might be necessary.
- The Private certificate must be provided in a PKCS #12 format (.P12 or .PFX).
- The Public certificate must be provided in a binary DER-encoded .P7B or .CRT format and include the complete chain of trust (i.e., the Root CA and all intermediate CAs).

3.4 Anti-Virus

Most antivirus programs perform real-time scanning, which checks every file as it is accessed. This process can delay or block access to files needed by the program, potentially causing errors during normal operation. To minimize interference and enhance performance, Exterro strongly recommends configuring any antivirus or anti-malware software on servers hosting FTK Enterprise components to exclude specific folders—rather than individual files—from real-time scanning. This ensures that new or modified files generated by the components, particularly those containing case data, evidence, or temporary application files, are also excluded.

Regularly scheduled scans for these excluded locations are encouraged, but they should be monitored to ensure they do not impact the solution's overall performance.

Note: Full functionality of the Agent component may require explicit whitelisting of executables, .DLL files, or other associated files in some environments. A list of these files, along with their corresponding hash values, is provided with the installation media for each specific build of the Agent component.

Please contact Exterro Technical Support for further information and assistance.

4 Software Requirements

FTK Enterprise supports installation on Microsoft Windows, which must be licensed through Microsoft or an approved reseller. Each host's operating system should be kept up to date with the latest service packs and patches.

Supported operating systems:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

For tasks involving email processing, collection, or export, a licensed copy of Microsoft Outlook may be required on each host running a Processing Engine. This license must also be obtained through Microsoft or an approved reseller. The following table outlines the software prerequisites for each component. These prerequisites are included within the component installers, so manual installation before implementation is not necessary. It is important to note that compatibility with higher versions of these libraries and dependencies is not guaranteed, and installing versions newer than those listed below is not recommended.

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 Enterprise	• Python 3.10.11 (x64) • Microsoft Visual C++ 2015 - 2022 Redistributable Package (x64) • Microsoft .NET Framework 4.8 Full • Microsoft Visual C++ 2015 Update 3 Redistributable Package (x64) • Access Database Engine 2016 (x64) • Microsoft Distributed Transaction Coordinator (“MSDTC”)
Processing Engine *(Local or Distributed)*	• Microsoft .NET Framework 4.8 Full • Microsoft Visual C++ 2022 Redistributable Package (x64)

Component	Prerequisites
	• BlackIce Print Driver 14.8 MultiInstance (x64) • Microsoft Distributed Transaction Coordinator ("MSDTC")
Distributed Processing Manager	• Microsoft .NET Framework 4.8 Full • Microsoft Visual C++ 2022 Redistributable Package (x64)
FTK Web Service (Self-Host)	• Python 3.10.11 (x64) • Microsoft Visual C++ 2022 Redistributable Package (x64) • Microsoft .NET Framework 4.8 Full • Microsoft Visual C++ 2015 Update 3 Redistributable Package (x64)
Site Server	• PostgreSQL 14.17 • Microsoft .NET Framework 4.8 Full • Microsoft Visual C++ 2022 Redistributable Package (x64)
Exterro AI Server	• PostgreSQL 14.17 • PostgreSQL Vector Extension • Ollama 0.6.8 • Python 3.12.9 (x64) • Microsoft Visual C++ 2015 - 2022 Redistributable Package (x64) ***Note:*** *Refer to the* ***Exterro AI Server Installation Guide*** *for more details on the software requirements.*
Connectors	None
Monitoring Service	None

4.1 Third-Party Licensing

FTK Enterprise requires Microsoft Windows, and Microsoft SQL Server (optional), 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 Hardware Requirements

The performance of FTK Enterprise is dependent on the hardware used to host its various components. While the ideal setup would involve the latest processors, abundant memory, and large-scale RAID (Redundant Array of Independent Disks) servers, most environments are limited by budget constraints. To address this, the following guidelines have been developed to help create cost-effective environments that meet the diverse needs of a wide range of customers.

Minimum hardware recommendations for each component, when deployed on a dedicated host, are provided below. **Please contact Exterro Technical Support for further information and assistance.**

Component	Processor	Memory
FTK Enterprise (Web UI for Reviewers)	4 Logical Cores	8 GB RAM
FTK Enterprise Examiner (Thick Client)	4 Logical Cores	8 GB RAM
Processing Engine (Local or Distributed)	8 Logical Cores	16 GB RAM
Distributed Processing Manager	4 Logical Cores	16 GB RAM
FTK Web Service (Self-Host)	8 Logical Cores	16 GB RAM
Site Server	4 Logical Cores	8 GB RAM
Exterro AI Server ***Note**: Only NVIDIA GPUs are supported.* **Enterprise Grade GPU Recommendations:** • **Minimum**: NVIDIA V100 (16 GB) • **Recommended**: NVIDIA A100 (40 GB) **Consumer Grade GPU Recommendations:** • **Minimum**: GeForce RTX 5060 Ti • **Recommended**: GeForce RTX 4090 or higher	8 Logical Cores	16 GB RAM

Note: The Processing Engine component, whether deployed in either its “Local” or “Distributed” configuration, calculates the number of worker threads available for specific tasks based on the number of logical processor cores present on its host. Certain operations can be expected to utilize all available CPU and memory resources on the host system.

Systems with insufficient memory may experience performance bottlenecks as certain operations can trigger paging. Paging is a memory management technique that allows processes to use more memory than physically available by utilizing disk space as virtual memory. When an application requests data that isn't in memory, a page fault occurs, causing the operating system to load the data from disk. While paging helps optimize memory usage for larger programs, it introduces overhead that can negatively affect the solution's performance. Prolonged periods of excessive paging—commonly referred to as 'thrashing'—can severely degrade performance, potentially leading to operational failure.

To mitigate the risk of critical paging issues, it is strongly recommended that systems in the implementation environment have at least 2GB of RAM per logical processor core (e.g., an 8-core system should have a minimum of 16GB of RAM). For systems hosting the MSSQL Database, it is recommended to allocate at least 4GB of RAM per logical processor core (e.g., an 8-core system should have a minimum of 32GB of RAM).

6 Storage

The storage needs for FTK Enterprise are fluid, depending on variables like the number of case, the volume and types of data, and the specific workflows employed within the application.

To ensure optimal performance, prioritize key storage factors like seek time, latency, and data transfer rates. While high disk activity during certain operations is normal and usually not a concern, consistently high disk queues may indicate bottlenecks, leading to degraded performance or even operational failures.

The following sections outline descriptions, characteristics, and recommendations for the various types of storage utilized by FTK Enterprise.

6.1 Operating System and Applications

- **Relevant Components: All**

All systems hosting components of FTK Enterprise require dedicated space for the operating system and installed applications. Exterro recommends a minimum of 60GB for the operating system and associated applications. Additional storage may be necessary for systems with more than 16GB of RAM to accommodate increased pagefile sizes and dump files. Ensuring adequate space will help optimize system performance and facilitate smooth operation during deployment and upgrades.

6.2 Ephemeral Processing Data

- **Relevant Components: Processing Engine**

Systems hosting the Processing Engine component require local storage designated for ephemeral files—temporary files created during data processing. A minimum of 50GB is required for this storage, though 500GB or more is recommended for optimal performance, especially in larger environments. The critical consideration for this storage is speed; fault tolerance is not necessary, as the data is temporary and can be recreated if needed.

6.3 Ephemeral Collection Data

- **Relevant Components: Site Server**

Any system hosting the Site Server component, in any configuration, requires local storage to handle ephemeral files generated during data collection. While there is no strict minimum, Exterro recommends at least 100GB of storage. Environments involving multiple concurrent data collections may require additional storage space. While fault tolerance is generally not required, ensuring sufficient speed for efficient collections is important.

6.4 Collected Evidence

- **Relevant Components: Web Examiner, FTK Web Service, Processing Engine, Site Server**

A UNC (Universal Naming Convention) file share, accessible by all relevant components, is essential for storing collected evidence. While local storage can be used, network-attached storage (NAS) is recommended for better scalability and management. Initial space requirements will vary depending on the volume of data collected, but they can be substantial. This storage should be fault-tolerant and offer low latency to ensure efficient access by all components involved in the processing and review workflows.

6.5 Staged Evidence

- **Relevant Components: Web Examiner, FTK Web Service (Self-Host), Processing Engine**

A UNC file share, accessible by all relevant components, is required to store evidence that is acquired through methods other than direct collection (e.g., ingestion of external data). Like collected evidence, local storage is an option, but network-attached storage (NAS) is highly recommended for better performance and management. The space required will depend on the specific data ingestion needs of the organization, and it is expected to grow over time. This storage should be fault-tolerant and low-latency to ensure seamless access for all components involved in processing and review.

6.6 Case Data

- **Relevant Components: Web Examiner, FTK Web Service (Self-Host), Processing Engine**

UNC file share that provides storage for case-specific data, application-generated files, and internally-maintained copies of specific types of ingested data. Actual space requirements will vary considerably depending on for ingested evidence are roughly 33% of the space of the associated staged evidence. Over time, additional space may be required to support ongoing workflow operations. This storage should be fault tolerant with low latency to all relevant components.

Note: Collected Evidence, Staged Evidence, and Case Data storage may all share the same physical storage, though logical isolation (i.e., separate subfolders) is recommended.

7 Network Requirements

The following sections detail the default **inbound ports** utilized by each component of FTK Enterprise. These ports are primarily intended to handle **incoming connections**, as opposed to initiating outbound communications. Outbound connections are typically established using a dynamically assigned port from the **Windows Dynamic Port Range** (default: **49152–65535**) to communicate with the designated **listener port** on the target host. Accurate configuration and management of these ports are critical to ensuring reliable and secure communication between system components. **Please contact Exterro Technical Support for further information and assistance.**

7.1 Database

The database component can be deployed using either PostgreSQL or Microsoft SQL Server, based on the needs of your environment.

7.1.1 Microsoft SQL Server

Inbound Port	Protocol	Usage	Comments
135	TCP	RPC Endpoint Mapper	Microsoft Distributed Transaction Coordinator (“MSDTC”) uses this port to establish communication.
1433	TCP	Database Engine (Default)	This is the default port used for SQL Server instances if no named instances are specified.
1434	UDP	SQL Server Browser Service	This port is essential for client applications that need to find the port number for named instances of SQL Server. It’s particularly important when multiple SQL Server instances are running on the same machine.
49152-65535	TCP	Dynamic Port Range	Microsoft Distributed Transaction Coordinator (“MSDTC”) dynamically allocates a port for communication once the initial connection is made through port 135. This dynamic port range can be restricted through the operating system if needed.

7.1.2 PostgreSQL

Inbound Port	Protocol	Usage	Comments
5432	TCP	Database Engine (Default)	This is the default port for PostgreSQL instances.

7.2 Web Examiner

The Examiner does not have any inbound port requirements.

7.3 FTK Web Service (Self-Host)

Inbound Port	Protocol	Usage	Comments
4443	HTTPS	Web Services (Default)	This is the default port for the web-based data analysis and data collection interface. ***Note:*** *This port is commonly reconfigured to use port 443.*
4444	HTTP	Token Auth Web App Port	Used by the Desktop Viewer to stream live video content over HTTP using token-based authentication. This port enables secure access to video streams via the web application interface.
4446	HTTP	Mac Agent	Enables Offline Mac agent collections.
4442	HTTP	HTTP Listener and Redirector	HTTP port at which we will be listening to and automatically redirecting to HTTPS.

7.4 Processing Engine

Inbound Port	Protocol	Usage	Comments
34096	TCP	Processing Management (Default)	Used by the processing job management and engine event services. **Note:** This port is only active if the Processing Engine is deployed in its "Local" configuration.
34097	TCP	Processing Engine (Default)	Used by the processing engine services.
34099	TCP	Remote Format Converter (Default)	Used by the Remote Format Converter service for converting files.

7.5 Distributed Processing Manager

Inbound Port	Protocol	Usage	Comments
34096	TCP	Processing Management (Default)	Used by the processing job management and engine event services.

7.6 Site Server

Inbound Port	Protocol	Usage	Comments
443 *(For Windows)*	HTTPS	Managed Agent Check-In *(Default)*	Used to receive and manage check-in communication from Windows Agents (version 8.0 SP2 or later).
443 *(For Mac)*	HTTPS	Mac Agent (Site Server configured as a Reverse Proxy)	Default URL for Mac Agent, with Site Server acting as a reverse proxy.
54321	TCP	Client Communication *(Default)*	Used to receive job communication from the FTK Web Service (Self-Host) component. ***Note:*** *This port is only active if the Site Server is deployed in its "Root" and "Public" configurations.*
54545	TCP	Legacy Agent Check-In and Agent Collection *(Default)*	Used to receive and manage check-in communication from Legacy Windows Agents (version 8.0 SP1 or earlier) and collection-related communications from Windows and Linux Agents.
54555	TCP	Agent Heartbeat *(Default)*	Used to receive and manage "heartbeat" communication from Windows and Linux Agents. ***Note:*** *This port is only active if the Site Server is deployed in its "Root", "Private", or "Private (Protected)" configurations.* **Additional Information:** • Windows Agent **version 8.2.0.174 and above** will **not** use this port. • Linux Agent (latest version: **8.1.1.3**) **will continue** to use port **54555**.
54548	TCP	Data Replication *(Default)*	Used to receive job and contact information from associated (i.e., "parent" and "child") Site Servers.
3999	TCP	On-network agent job collection (default)	Used for data transfer between the Site Server (SS) and the agent over port 3999 in on-network scenarios.

7.7 Agent

7.7.1 Windows Agent

Inbound Port	Protocol	Usage	Comments
3999	TLS	Active Job and Collection Communication (Default)	Used to receive job- and collection-related communication from Web Examiners and Site Servers in active “on-network” collections.
5353	UDP	Remote Mobile Discovery: Receiving Jobs on Mobile Device Remote Mobile Discovery: Sending Jobs Back to Agent	Remote Mobile collections rely on dependencies such as Bonjour when collecting wirelessly. These dependencies automatically find available ports available for use during both; • jobs being sent to a mobile device • jobs being received from a mobile device

7.7.2 Mac Agent

Inbound Port	Protocol	Usage	Comments
3999	HTTPS	Active Job and Collection Communication (Default)	Used to receive job- and collection-related communication from Web Examiners and Site Servers in active “on-network” collections.

7.7.3 Linux Agent

Inbound Port	Protocol	Usage	Comments
3999	TLS	Active Job and Collection Communication (Default)	Used to receive job- and collection-related communication from Web Examiners and Site Servers in active “on-network” collections.

7.8 Desktop Viewer

Inbound Port	Protocol	Usage	Comments
9000 - 9010	HTTP	To view files in Desktop Viewer	The default URL for Desktop Viewer, used with the FTK Plus Lite executable.

7.9 KFF

Inbound Port	Protocol	Usage	Comments
9042	HTTP	To connect to the KFF service	Default URL for accessing the KFF service.

7.10 Additional Components

Inbound Port	Protocol	Usage	Comments
3210	HTTP	Reporting Service	To generate reports of documents and PDFs.
5000	HTTP	AI Server Service	To perform object detection, image recognition, multimedia search, and summarization.
6921	TCP	Network License Service	To receive Network License queries from Examiners.
7035	HTTP	Monitoring Service	To monitor the application components and perform corrective actions.
9042	HTTP	KFF Service (Cassandra)	To flag known hashes as either ignore/alert to help expedite the review.
22350	UDP	CodeMeter	Helps with licensing of the product.
8080	HTTP	Connector API Port	Enables box and other e-discovery collections.
5001	HTTP	Exterro AWS Service	Help with Upload and download of Files & folders from AWS S3.
22352	HTTP	CmWebadmin	Used to access the CodeMeter WebAdmin user interface.

8 Database Requirements

FTK Enterprise requires a dedicated database instance. While this instance can coexist with other instances on the same host, hosting the Database component within the same instance as another enterprise application is not supported.

The Database component can be hosted using either PostgreSQL or Microsoft SQL Server, with the latter requiring a license from Microsoft or an authorized reseller. This 'shared' instance stores file metadata, user data, and other application-related information. Additionally, each case created within the application is stored in a separate database within the instance.

Notes:

- In addition to the shared database instance, a local PostgreSQL database will be deployed on any system hosting a Site Server component. This local database is used by the Site Server to manage ephemeral information related to Agent interactions, job data, and other associated functions.
- A **dedicated PostgreSQL database** is also recommended for systems hosting the **AI Server** component. While it is technically possible to use the existing ADG or Site Server PostgreSQL instance by installing the **pgvector** extension (required for vector embeddings), deploying a dedicated PostgreSQL instance for AI workloads is strongly recommended. This ensures optimal performance and isolation for AI-related operations, such as natural language processing, multimedia search indexing, and embedding generation.

8.1 Microsoft SQL Server

Supported Versions: Microsoft SQL Server 2016, Microsoft SQL Server 2017, Microsoft SQL Server 2019, Microsoft SQL Server 2022.

When using Microsoft SQL Server to host the Database component, the instance must meet the following requirements:

- The instance must be configured to use the default US collation, 'SQL_Latin1_General_CP1_CI_AS'.
- TCP/IP and Named Pipes protocols be enabled in the Network Configuration settings of the instance.
- The instance must have Mixed Mode Authentication enabled.
- The Service Account created for FTK Enterprise must be added to the application database instance as a Login.
- This Login must be provided with the SysAdmin role during the database installation process. Elevated privileges may also be required during upgrades.

8.2 PostgreSQL

Supported Versions: PostgreSQL 14.17

FTK Enterprise includes installation media for the supported version of PostgreSQL. No additional configuration is typically required.

9 Appendix A: Pre-implementation Checklist

The following checklist should be used to document the prerequisites necessary to ensure the successful implementation of FTK Enterprise 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.
3. Service Account
   - 3.1. A dedicated Service Account named _____ 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.
7. Certificates
   7.1. (Optional) A valid certificate pair has been created for use with Agents.
   - *Refer to the How To Create Self-Signed Certificates with Certman (KB Article) for more information.*
   - *Refer to the Use a CA-signed certificate with Windows and Linux Agents (KB Article) for more information.*

   7.2. (Optional) A valid certificate is available for use with the FTK Web Service (Self-Host).

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 110

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