SYSTEM SPECIFICATIONS GUIDE

AD Enterprise

NETWORK INVESTIGATION AND POST-BREACH ANALYSIS

v6.5 Revision (May 8, 2018)

ACCESSDATA®

www.accessdata.com

Contents

AccessData® Enterprise Overview and System Specifications Guide

The Enterprise system specifications guide is intended to ensure proper sizing and capacity for a successful AccessData Enterprise deployment.

The AD Enterprise solution is a comprehensive set of forensically-sound live-box forensic collection and analytical capabilities. The solution dramatically expands on the core analytical capabilities of FTK® software by adding an agent, central manager and advanced live forensic and post-incident forensic analysis functionality. This enables investigations to be conducted quickly and securely over the network and on multiple machines simultaneously. This allows analysts to move beyond the typical single-box reactive investigations toward a much more efficient, timely and streamlined approach that allows organizations to promptly address employee malfeasances, policy violations, and security breaches with analysis. The AD Enterprise solution enables much faster, more efficient, more complete and discreet responses to any given incident.

Overview of Components

Enterprise is made up of three separate application components, each of which is installed separately and performs a different function. These components include a database, Enterprise Case Manager and Examiner Client User Interface (UI), and the Evidence Processing Engine (EP) with the optional Distributed Processing Engine (DPE). Enterprise also utilizes an Agent that can be installed on target computers to gather data for investigation. When configuring a system to run Enterprise, it is helpful to understand the hardware requirements for each of these components and the impact each of them places on the hardware.

- **Database**—The database is a key component of the Enterprise application. It stores the processed metadata, performs all the queries, sorts, filters, file listings, and other functions requested by the FTK Client UI. AD Enterprise works with both PostgreSQL® and MS SQL Server®. PostgreSQL is a free database and is included in the installation. This option is best for lower loads. MS SQL Server should be purchased for users with heavy usage, needing automated backups and for performance installs. For more information on using other database platforms, please see the FTK Install Guide at accessdata.com/product-download/digital-forensics.

- **Enterprise Case Manager and Examiner**—The Case Manager's primary function is to manage the application, such as managing database settings, cases, users, groups, roles, processing engine settings, agent configuration setting and other application settings and features.

The Examiner is the primary component of the AD Enterprise solution, as it facilitates the capture and analysis of data, both live and static, for the analyst. At its core is the flagship FTK® computer forensics product, which has been enhanced and streamlined to deliver secure, network-enabled forensics capabilities. From a logical standpoint, the Examiner consists of three key components: a Worker, Database, and GUI console. Essentially, the Worker processes data based on specified criteria, metadata is stored in the database, and the GUI provides a single interface to easily capture, acquire, view, analyze and report to support even the most complex investigations. It contains an agent deployment/update capability, backup facility, archive facility, and has an automated recovery mechanism in the event of a failure to ensure work is not lost and analysis continues. This component is also provides authentication, authorization, logging and administrative functions. These features enable organizations to control who can access which resources at which time, and defines down to the node exactly what type of investigative and user operations can be performed. It also has a number of role based permissions functions to control user access and rights.

- **Evidence Processing Engine (EP) and Distributed Processing Engine (DPE)**—The processing engine and distributed processing engines, as their names suggest, perform the majority of the work when processing data.

- **Agent**—Modular application that runs on workstations and servers providing secure forensic-level access, analysis, and preservation of static (data on disk), volatile, and RAM (Windows®).

Hardware/Software Requirements

AccessData Enterprise is based largely on Microsoft® technologies and should, when possible, meet the following hardware specifications. Several additional software packages (e.g., .NET Framework 3.5.1, 4.0, Microsoft Visual C++, etc.) may be required during installation and will be installed as part of the component automatic prerequisite check or manually from the Microsoft website. The performance of the system is directly related to the hardware used for each component and processing option selected.

OS supported are Windows Server 2012R2 and 2016 64-bit

Single Server Install		
Component	**Basic**	**Recommended**
Processor	8 Physical Cores – 16 Threads	24 Physical Cores – 48 Threads
Memory	16GB RAM	96GB RAM (2GB/thread)
Storage	• 10k RPM / SSD (OS/Apps) • SSD – 512 GB (ADTemp) • 10k RPM RAID 5 (Database) • 10k RPM RAID 5 (Evidence / Case Data)	• 10k RPM disk (OS/Apps) • SSD – 512 GB (ADTemp) • 15k RPM RAID 5 (Database) • 15k RPM RAID 5 (Evidence / Case Data)
OS	Windows	Server 2012 R2, 2016
Network	1Gbit NIC minimum	10Gbit NIC
Other	USB interface for license dongle unless using soft dongle	

Distributed Install—Enterprise Examiner Client User Interface (UI)		
Component	**Basic**	**Recommended**
Processor	4 Physical Core – 8 threads	
Memory	16GB RAM (2GB/thread)	
Storage	• 10k RPM / SSD (OS/Apps) • SSD – 512 GB (ADTemp)	
OS	Windows 64-bit, Server 2012 R2, 2016	
Network	1Gbit NIC minimum	10Gbit NIC
Other	USB interface for license dongle unless using soft dongle	

Distributed Install—Database Refer to our Accessdata SQL Server Guide for additional information.		
Component	**Basic**	**Recommended**
Processor	4 Physical Core – 8 threads	The amount of cores needed is calculated by 25%-50% of the total physical cores of all DPEs.
Memory	4GB RAM /thread	4GB RAM /thread
Storage	• RAID 1 – OS/Apps • 10k RPM drives minimum • SSD – TempDB	• RAID 1 – OS/Apps • RAID 10 – Database (15k or SSD) • SSD – TempDB
OS	Windows 64-bit, Server 2012 R2, 2016	
Network	1Gbit NIC minimum	10Gbit NIC

Distributed Install—Distributed Processing Engine (DPE)		
Component	**Basic**	**Recommended**
Processor	4 Physical Core – 8 threads	16 Physical Cores – 32 threads
Memory	16GB RAM (2GB/thread)	64GB RAM (2GB/thread)
Storage	Windows 64-bit, Server 2012 R2, 2016	
OS	Windows 64-bit, Server 2012 R2, 2016	
Network	1Gbit NIC minimum	10Gbit NIC
Storage (ADTemp)	SSD - ADTemp	SSD - ADTemp

Considerations for Data Storage

Storage requirements for Enterprise are driven by case loads and retention policies. Here are a few considerations when determining the amount of storage needed:

- What is the typical number of evidence items processed for each case?
- What is the typical source image size?
- How long will processed case(s) be stored in the system?

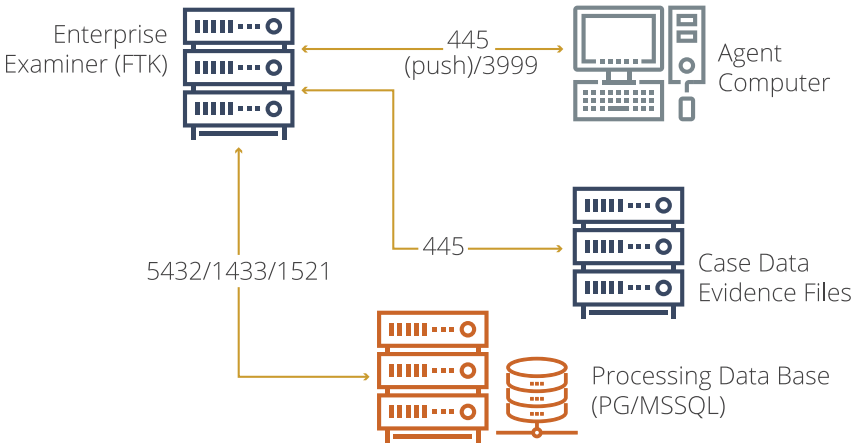
ESI Storage Matrix				
Evidence Files	Local, DAS device, or file server (SAN/NAS)	AD1, E01, Native	Driven by needs of organization	RAID 5 separate from case data
Case Data (Index of processed evidence)	Local, DAS device, or file server (SAN/NAS)	IDX, IX	Roughly 25 – 30% size of processed evidence image files	RAID 5 separate from evidence files
Metadata of Processed ESI	Local to database server	various	Every 1 million items requires roughly 4 – 5GB of disk space in the database	RAID 0 / SSD, or RAID 10 for redundancy and performance

Evidence files and case folders can be stored locally on the Enterprise system(s) or on a dedicated storage device, depending on the need. In larger environments with dozens of large cases, it is recommended that a dedicated storage device be used.

System Recommendations

- Installing the Database or Processing Engine in a virtualized environment is supported, but not recommended.
- The processing engine requires a temporary space with very fast I/O (read and write) and low fragmentation. This is referred to as "ADTemp" throughout this document. Among other things, the ADTemp is used by the engine to store data while it is being expanded, indexed, and prepared for insertion into the database (e.g., DtSearch indexes, thumbnails, compressed files and metadata).
- It is strongly recommended that on each system running AccessData Enterprise components antivirus, EFS, and Microsoft Indexing are disabled or configured to exclude directories (or entire drives) containing case data, ADTemp data, database files, evidence files, and any other directory containing data used by Enterprise.
- When using distributed processing engines (DPE), you will likely experience a greater benefit using a small number of powerful servers rather than a large number of less powerful servers.
- Any disk array that will utilize RAID technology should use a hardware RAID controller. Software RAID is not recommended. RAID controllers with at least 512MB of write-through cache provide the greatest performance increase.
- Unless it is being used, IPv6 should be disabled using the article http://support.microsoft.com/kb/929852.
- It is recommended that the database be on its own physical volume to minimize fragmentation. This volume should also be defragmented regularly to improve performance. However, defragmentation of this drive should not occur while processing or reviewing data.
- If using DPE technology, it is important to understand that each DPE will be accessing the same evidence source, which can quickly create an I/O bottleneck.
- Windows updates should not be set to install automatically. Enabling automatic updates will likely cause the system to reboot during long processing jobs and/or review. Manual installation of updates is recommended.
- Power settings should be adjusted so that the system(s) will not enter a sleep or hibernation mode.
- If PST export is going to be used, Microsoft Outlook® must be installed.

Network Topology



ACCESSDATA®

Whether it's for investigation, litigation or compliance, AccessData® offers industry-leading solutions that put the power of forensics in your hands. For over 30 years, AccessData has worked with more than 130,000 clients in law enforcement, government agencies, corporations and law firms around the world to understand and focus on their unique collection-to-analysis needs. The result? Products that empower faster results, better insights, and more connectivity. For more information, visit www.accessdata.com

Visit us online:
www.accessdata.com

Global Headquarters
+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7010 7800
internationalsales@accessdata.com