

AccessData[®] Enterprise

System Security Overview



AccessData

A Pioneer in Digital Investigations Since 1987

The primary purpose of AccessData (AD) Enterprise is to provide a means for an investigator working in a corporate setting to gather forensic and runtime data directly from operating end-user workstations. AD Enterprise is an augmented version of FTK with the ability to acquire data remotely. Software running on an end user's workstation (Agent) acquires data directly from that workstation, making it available for forensic analysis by AD Enterprise (Examiner). In addition to drive and mounted volume information, an Examiner can acquire volatile data (e.g. currently running processes, loaded DLLs, memory).

This paper focuses on the security aspects of AD Enterprise. It describes two classes of users who interact with AD Enterprise, the security procedures that they must follow, and the protection mechanisms that have been put in place to limit access to the collected data.

AD Enterprise is composed of three primary components supporting two distinct roles. Each of these components (Authentication Server, Examiner Workstation and Agent Software) is illustrated in Figure 1.

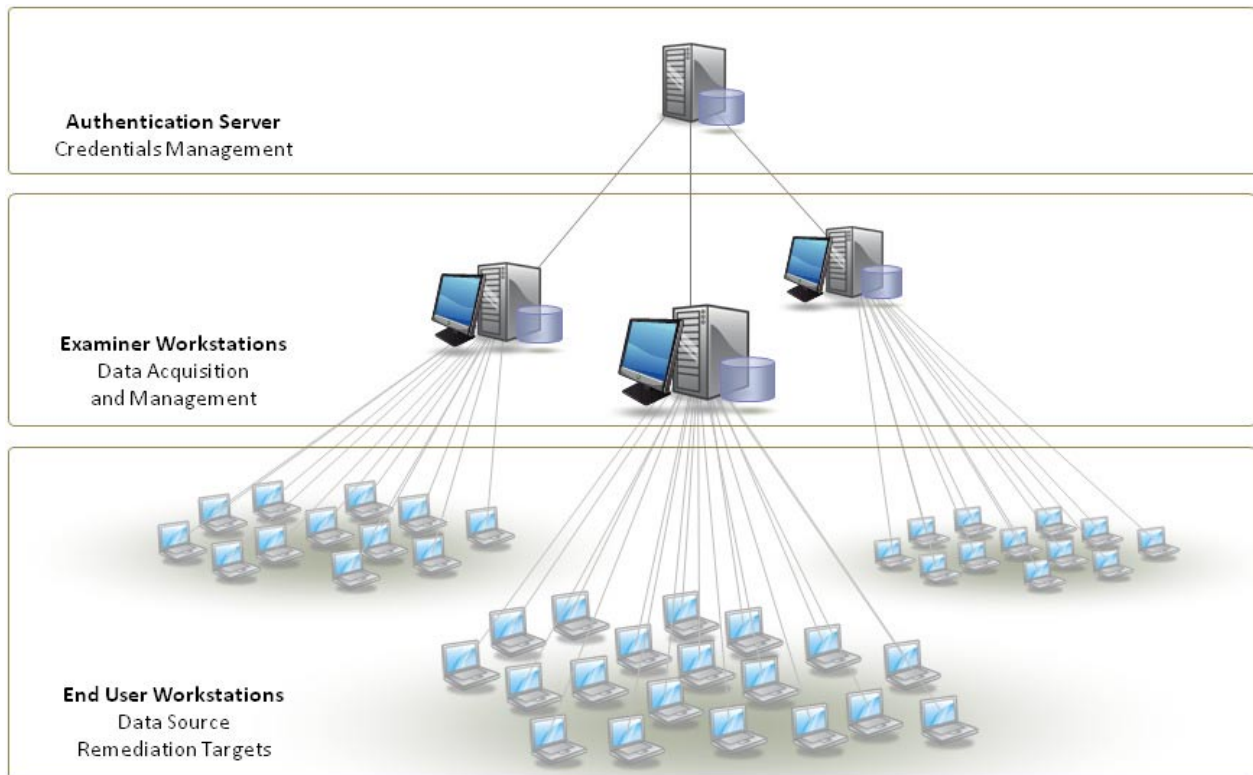


Figure 1: AccessData® Enterprise System

The two roles are Administrator and Investigator.

Administrators are responsible for managing the AD Enterprise Investigator authentication credentials and assignment of authorization rights to Investigators.

Within the upper tier of Figure 1 appears a single instance of an Authentication Server. It is operated exclusively by one or more Administrators. The primary purpose of this server is to provide authentication and authorization services for Investigators and to serve as the certificate authority between the components of the system.

Investigators are responsible for the collection and analysis of data originating on remote workstations running the Agent software. Multiple instances of Examiners appear in the middle tier; these are operated exclusively by Investigators. The primary purpose of the Examiner is to collect forensic and operational data from remote workstations and perform analysis on the collected data. Provided that an Investigator has been granted the appropriate rights, he or she may also execute remediation tasks on the remote workstation running the Agent software.

The end user does not have any direct involvement with the AD Enterprise system. The Agent operates entirely by an Examiner's remote control, and unless involved in the collection, transmission or execution of a remediation task, the Agent is dormant.

Agent Distribution

One problem associated with a system that requires software to be installed on a large number of computers is the issue of software distribution and upgrades. Installation of the Agent involves two operations: the installation of the AD Enterprise Agent software itself, and placement of the public key generated on the Authentication Server.

On Unix systems, the Administrator must distribute and install the Agent manually; unless the organization is using a desktop management system, such as LANDesk. On Windows systems the process of distribution, installation and placement of the public key can be automated. The ability to complete this operation requires the establishment of an administrator account on each node of interest. If an administration account has not been established, an Administrator must follow the same steps necessary for Unix-based systems.

Provided that an administration account has been established, an administrative named pipe is created between the Examiner and each node of interest. Once the administrative named pipe is established, a small rudimentary client is installed on the node of interest. The Examiner then attempts to establish a TCP/IP connection with the client using a symmetrical block cipher to encrypt and decrypt both ends of the connection. Once the Agent is installed, the client is removed from the local system, and the AD Enterprise Agent is launched.

Investigators may be able to push out a new version of the Agent software to any system upon which the Agent is running, provided they have the authorization rights to complete that operation.

Certificate Distribution

AD Enterprise uses digital signatures (certificates) to verify the authenticity of a computer attempting to establish a network connection. There are two aspects to the use of certificates: the initial distribution of the certificates and verification of authenticity during the establishment of a network connection.

Distribution of certificates is completed during installation of the Examiner and Agent. Verification of authenticity occurs when an Examiner attempts to establish a secure communication session with one or more Agents.

In order to ensure that network connections are secure within the entire system of computers, several certificates must be generated, signed and distributed. The following is a certificate inventory list:

Certificate:	Usage
Server Private:	(SX) Generated during Installation of the Authentication Server. This certificate is used to sign all other certificates. It is considered the Private Key for the entire system
Server Certificate:	(SC) Generated during Installation of the Authentication Server. Used during the initiation of an HTTPS connection and contains a copy of the Authentication Server's Public Key
Examiner Private:	(EX) Generated during Installation of the Examiner. This certificate is used to establish the FIPS 140-2 communications between the Examiner and the Agent. It is signed by the Authentication Server's Private Key (SX).
Examiner Certificate:	(EC) Generated during Installation of the Examiner. This certificate is distributed to each Agent and used to establish the FIPS 140-2 communication between the Examiner and the Agent. It is signed by the Authentication Server's Private Key (SX).

The sequence of steps taken to generate and distribute certificates appears below. It is assumed that the customer has put in place the procedures necessary to ensure that private certificates are not compromised.

- 1.) The Authentication Server software is installed.
- 2.) The Authentication Server Private (SX) and Public certificates (SP) are generated; the Authentication Server Public (SP) certificate is signed by the Authentication Server Private (SX) Key.
- 3.) The Microsoft IIS Server Private and Public certificates are generated and signed by the Authentication Server Private Key (SX).
- 4.) The Authentication Server Private (SX) and Public certificates (SP) are copied to a known location and protected via file system access rights.
- 5.) The Examiner Private (EX) and Public certificates (EP) are generated and signed by the Authentication Server Private Key (SX).
- 6.) The Authentication Server Public (SP) certificate, Examiner Private (EX) and Public (EP) certificates are copied to a known location and protected via file system access rights.
- 7.) The Examiner software (AD Enterprise) is installed.
- 8.) The Authentication Server Public certificates (SP) are copied to a known location on a remote workstation and encrypted using a symmetrical block cipher algorithm.
- 9.) The Agent software is installed.

Event Recording and Auditing

Every action executed on the Authentication Server and Examiner is recorded in an event log, hosted on the Authentication Server and stored in the Oracle database. Only Administrators are allowed to gain access (view, purge...) to the event logs. Placing the event log in a database makes log information available to SQL queries.

The event logging facility is made available to any workstation in the system, via a web services interface, using an HTTPS communication session. The Server Private Key (SX) and Public Key (SP) are used to establish the communication session.

Every event entry includes the following:

- ◆ date and time an event occurred (Authentication Server time specific)
- ◆ severity of the error (Fatal, Error, Warning, Information)
- ◆ name of the user that generated the event (authenticated name)
- ◆ device (Authentication Server / Examiner) on which the event was executed
- ◆ an English description of the event

Critical events include:

- ◆ Administrator authentication
- ◆ Modification of event entries (purging)
- ◆ Creation of an Administrator or Investigator account
- ◆ Assignment or modification of access rights
- ◆ Investigator authentication
- ◆ Data collection from a given remote workstation
- ◆ Modification of data on an remote workstation
- ◆ Remediation of an event (e.g. kill a process) on an remote workstation
- ◆ Success or failure of establishing a secure communication session

Authentication Server

The primary purpose for the Authentication Server is to provide an Administrator with a means of managing Investigator authentication credentials and authorization rights. The server is managed exclusively by one or more individuals that have been granted rights to administer the server. The Authentication Server also serves as the certificate authority for X509 certificates used to establish secure communications between computers operating in all three tiers.

Administrative functions are provided via a web browser interface running entirely within an HTTPS session. Administrators are required to provide authentication credentials (username and password) prior to being granted access

to management pages. The username and password associated with each user are independent of any organization-wide authentication service, such as Microsoft's Active Directory.

Once an Administrator's credentials are submitted and verified, they are permitted to do the following:

- ◆ Manage the authentication credentials of Administrators and Investigators
- ◆ Associate authorization rights to Administrators and Investigators
- ◆ Establish limits on the remote workstations an Investigator can access

Each Authentication Server includes a local instance of an Oracle database. The database serves as a storage mechanism for the authentication credentials, authorization rights and environment information as defined by an Administrator.

Access to the database requires the caller to authenticate prior to being granted access to the data within the database. The Oracle database software relies upon Windows authentication to authenticate the Authentication Server software when attempting to gain access to the database.

With the exception of passwords, the data stored in the database is not encrypted. Passwords are stored as MD5 hash derivatives of the passwords entered by an Administrator. When an Administrator or Investigator submits credentials to be authenticated, an MD5 hash value is generated from the password and the two hash values are compared. The user is considered authenticated when the MD5 hash values match for a given username.

An Administrator may assign authorization rights to any system user. Rights include the following:

- ◆ Administration of the Authentication Server
- ◆ Preview drive/device of a node of interest
- ◆ Search the drive/device of a node of interest
- ◆ Node of interest IP address ranges
- ◆ Acquire drive/device data from nodes of interest
- ◆ Acquire runtime data from a node of interest (memory, process list ...)
- ◆ Browse the file structure of a node of interest's drives/devices
- ◆ Browse pictures on a node of interest's drives/devices
- ◆ Modify a node of interest (wipe files, place files, kill a process, remove execution ...)
- ◆ Set IP access ranges of nodes of interest
- ◆ Analyze runtime data
- ◆ Acquire the memory from nodes of interest
- ◆ Push a new Agent to a node of interest

During the installation of the Authentication Server an Administrator generates a pair (private/public) of keys that are used to establish secure network communication between the computers participating in the system. The Private Key is stored in a location known only to the Administrator and protected with the same care that must be taken with any Private Key.

The Public Key is distributed to each Examiner, to each Administrator, and to each node of interest that is running the Agent software. The Public Key is used to establish HTTPS sessions when an Administrator is managing the Authentication Server, to establish an HTTPS session between the Authentication Server and each Examiner to authenticate Investigators, and when an Examiner establishes a secure communication session (FIPS 140-2 L1) with a given Agent.

Examiner

When AD Enterprise is launched, an Investigator is required to provide authentication credentials prior to gaining access to AD Enterprise functionality. Credentials are verified via the Authentication Server. Proper authentication permits the Investigator to select nodes of interest with which to interact, via the Agent software (workstations appearing at the bottom of Figure 1).

Communication between AD Enterprise and the Authentication Server is done via an HTTPS web services protocol. The Authentication Server Private Key (SX) and the Server Public Key (SP) are used to establish the HTTPS communication session. Once established, an MD5 hash value is generated using the password provided by the Investigator. Both the username and hashed password are then sent to the Authentication Server.

The following sequence describes the steps of execution each time an Investigator attempts to use AD Enterprise (Examiner). Note that the steps in bold represent those steps that occur the first time the system is used.

Actor:	Action
Investigator:	Launches the AD Enterprise application
Examiner:	Uses the Server Public Key (SP) to establish the HTTPS connection between the Examiner and the Authentication Server
	A dialog is presented requesting the Investigator's authentication credentials (previously entered by an Administrator into the Authorization Server's database)
Investigator:	Enters the credentials
Examiner:	Generates an MD5 hash of the Investigator's password
	Sends the credentials to the Authentication Server via the HTTPS connection
Authentication Server:	Verifies the Examiner credentials
	Sends the authorization rights and IP address range of the Agents accessible to the Investigator
Examiner:	Attempts to open the database with the Investigator username
Database:	Database responds that no such user exists
Examiner:	Creates a new user account with the Investigator's credentials
	Opens the database using the Investigator's credentials
	Displays the AD Enterprise user interface

Provided that the credentials verify, the Authentication Server passes back the list of access rights specific to the authenticated Investigator. The access rights are cached in the memory of AD Enterprise; the rights are never stored on disk. The rights determine which nodes of interest an Investigator is permitted to contact (establish a secure TCP/IP communication session).

The Investigator may then attempt to establish a secure TCP/IP connection with an Agent operating on one or more nodes of interest to execute any authorized operations. The communication between an Examiner and an Agent is facilitated via the AccessData Secure Communication Module—a FIPS 140-2 L1 communication module.

AD Enterprise uses a FIPS 140-2 Level 1 certified version of OpenSSL (version 1.1.2) operating exclusively in FIPS mode to manage the Examiner/Agent authentication and encryption/decryption of data sent over a network. The Examiner Private Key (EX) and Public Key (EP), installed on the Agent, are used to establish FIPS mode communication. The FIPS communication software restricts OpenSSL to use RSA asymmetrical keys for authentication. Authentication assumes that asymmetrical key pairs have been properly generated and distributed to both the Examiners and the nodes of interest.

Once an Agent is authorized, a symmetrical key (AES) is generated and used to encrypt/decrypt data over the network. The current AES standard is an algorithm named Rijndael. It is a block cipher adopted as an encryption standard by the U.S. government. AES is an iterative, symmetric-key block cipher that can use keys of 128, 192 and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes).

Dynamic Self Test

To ensure that the AD Enterprise authentication, encryption and decryption code has not been modified after construction, a HMAC_SHA1 digest is produced during the build process of both the OpenSSL library and the AccessData code that manages the OpenSSL configuration. Both libraries are compiled and linked into a small utility that loads the code into memory and generates an HMAC_SHA1 digest of the loaded code. The digest is then compiled into AccessData Enterprise and the AD Enterprise Agent. The generation process is repeated during the initialization phase of a loading application. If a dynamically generated digest does not match the one previously compiled into the application, secure communication services are disabled for the life cycle of the host application.

Agent

The AD Enterprise Agent operates as a Windows Service or a daemon on Unix-based operating systems. In both cases, the Agent is launched automatically when the system is booted. There is no interaction with the end user, and unless the user explicitly displays a list of running processes, they would not know that the Agent is operational.

The Agent operates on several operating systems, including the following:

- ◆ Windows 2K/2K3/XP/Vista/2008 (32/64)bit
- ◆ Linux
- ◆ Solaris 8, 9, 10
- ◆ Apple OSX 10.4, 10.5

The Agent will remain dormant until contacted by an Examiner, at which time a TCP/IP connection is established. Communication is always unsolicited. AD Enterprise, operating on an Examiner workstation, and the Agent, operating on a node of interest, use the AccessData Secure Communication Module (FIPS 140-2 L1) as a means to establish secure communications. It is also the only means of authentication used by an Examiner to verify an Agent. The previously distributed X509 certificate (Examiner Public Key) is used to establish trust between the two computers. Once a secure connection is established, the Investigator commands are executed.

The same build of the FIPS secure communication module is used in both the Examiner and Agent software. The same self test operation executed by the Examiner is performed by each Agent every time a communication session is established. In addition, a tamper resistance mechanism has been incorporated into the Agent.

The Public Key distributed to a node of interest (EP) is encrypted with a symmetrical block cipher algorithm named TwoFish; a 128-bit block cipher. The key length can vary, but for AD Enterprise it is defined to be 128 bits long and the key is compiled into the Agent. TwoFish is used strictly to encrypt and decrypt the public key required for Examiner/Agent authentication and does not fall within the cryptographic boundary of the FIPS module.