AD Enterprise 6.5 Installation & Upgrade Guide

Contents

Preparing to Install AD Enterprise

Supported Operating Systems

- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Windows 10
- Windows 7

Hardware Considerations

The more powerful the available hardware, the faster our product can analyze, process and prepare evidence. Larger evidence files require more processing time than smaller evidence files. An in depth AccessData System Spec Guide is available for review.

To maximize performance, AccessData recommends the following:

- Install the database to a large hard disk drive the database can use exclusively.
- Recommended RAM is at least 2 GB per processing core (e.g. an 8 core machine should have at least 16 GB of RAM). The minimum RAM must not be less than 1 GB per core.
    - **Note:** AccessData has changed the way jobs are allocated to each engine based upon available resources. The new approach works by calculating the Number of Cores or hyper-threading times two (2), which determines the total number of processing threads the engine will use. Each job requires minimum of two threads plus one GB of FREE physical memory to start. So when the engine gets a request to process something, it looks at the total number of jobs it is already working on. If it has at least two threads it can use on the new job, then it looks at free physical memory. If it also finds one GB free RAM available, then it will start up an adprocessor.exe to process the job.
- The Evidence Processing Engine recommends 100 GB or more of free space to use as temp space during processing.
- The database requires a minimum of 1 GB for every 200,000 items discovered/processed.
- Additional space is required for collections/evidence and case/project storage.
    - **Note:** If disk space depletes while processing a job, the job and case/project data may become corrupted.
- We do not recommend running resource-intensive third-party applications that may compete for hardware resources.

Obtaining the Software

The AD Enterprise ISO image is available for download through the AccessData FTP site. To obtain login information, please contact AccessData support at 1-800-658-5199 or email support@accessdata.com. Once the ISO image is downloaded, mount the image with drive emulation software (e.g. MagicDisc) or burn the image to a DVD using a program capable of burning ISO images (e.g. ImgBurn).

New AD Enterprise Installation

There are 4 main components to AD Enterprise:

- Database Server
- Examiner
- Distributed Processing Manager (Optional)
- Distributed Processing Engine(s) (Optional)

These 4 components can be combined as needed, but they are all necessary (except those specifically marked as such) for AD Enterprise to function correctly. You should plan and map out where all the components will be installed prior to beginning installation.

Most of the applications for AD Enterprise should be installed from the mounted or burned AD Enterprise ISO, and all applications should be installed from an account with full Administrator permissions. In any type of multi-box configuration, this should be a domain-level service account existing on all involved machines.

Prerequisites

Prior to installing AD Enterprise, please do the following on all involved machines:

1. Install all current Windows updates.
2. Disable all Windows Firewall profiles.
3. Disable Internet Explorer Enhanced Security.
4. Disable Windows User Account Control.
5. Disable any antivirus/malware scanning software.

Database Server

AD Enterprise supports MSSQL 2012, MSSQL 2014, and PostgreSQL. PostgreSQL 9.6 is included with AD Enterprise.

Install PostgreSQL

1. Insert the AD Enterprise installation media.
2. From the disc's autorun menu, click "Install Database 64 bit", and follow the prompts to complete the installation.
    a. If the server has a dedicated database drive or partition, install the data folder (named pgData by default) to that dedicated location.
    b. You must create a database password when prompted by the installer.

Examiner

Install the Enterprise Examiner & Processing Engine

1. Insert the AD Enterprise installation media.
2. From the disc's autorun menu, click "Other Products".
3. Click "Install License Manager" and follow the prompts to complete the installation.
4. Click "Install CodeMeter 64 bit" and follow the prompts to complete the installation.
5. If you have a physical Codemeter dongle:

    a. Connect the dongle to the PC.
    b. Use License Manager to ensure it has your current licenses, and update the dongle if necessary.
6. If you received an activation code for a virtual Codemeter dongle, follow the steps here to activate it.
7. Click “Back to Main Menu”.
8. Click “Examiner 64 Bit Install”.
9. If you are using a single-box system with a local database, click “Install Processing Engine” and follow the prompts to complete the installation.
    a. If the server has a dedicated temp drive or partition, place the Processing Temporary Folder on that dedicated location.
    b. At the “Destination Folder” dialog, do not check “Install as distributed processing engine”.
10. Back in the installation menu, click “Install Examiner” and follow the prompts to complete the installation.

Distributed Processing Manager (Optional)

In any environment sharing a database and cases between multiple Examiner machines, a shared Distributed Processing Manager with Distributed Processing Engines must be used.

Install the Distributed Evidence Processing Manager

1. Insert the AD Enterprise installation media.
2. From the disc’s autorun menu, “Distributed Engine”.
3. Click “Install 64 bit Distributed Processing Manager” and follow the prompts to complete the installation.
    a. If the server has a dedicated temp drive or partition, place the Processing State Folder on that dedicated location.
    b. When prompted, specify the Windows account that the AccessData Evidence Processing Engine should run under.
    Note: In any type of multi-box configuration, this should be your domain-level service account.
4. When the Distributed Processing Manager Configuration window opens, add all your Distributed Processing Engine machines and click “Done”.

Distributed Processing Engine(s) (Optional)

Install the Distributed Evidence Processing Engine

1. Insert the AD Enterprise installation media.
2. From the disc’s autorun menu, “Distributed Engine”.
3. Click “Install 64 bit Distributed Processing Engine” and follow the prompts to complete the installation.
    a. If the server has a dedicated temp drive or partition, place the Processing Temporary Folder on that dedicated location.
    b. At the “Destination Folder” dialog, check “Install as distributed processing engine”.
    c. When prompted, specify the Windows account that the AccessData Evidence Processing Engine should run under.
    Note: In any type of multi-box configuration, this should be your domain-level service account.

AD Enterprise First Run

Initialize the Database and Create an Administrator

1. Open Enterprise Examiner.
2. At the “Add Database” dialog, select the database you’d like to connect to.
    a. If desired, you may give the database connection a nickname in the “Display Name” field.
    b. The “dbname” should be set to “ADG” for PostgreSQL and MSSQL.
3. Click “OK”.
4. When prompted, authenticate to the database using the password specified during the database installation.
5. When prompted, create your first Administrator user.

Configure the Agent Certificates

1. Generate or obtain a public/private certificate pair that meets the following criteria, and put them in an easy to find folder (like “%PROGRAMFILES%\AccessData\Certificates”):
    - Follow the X.509 standard
    - Be RFC 5280 compliant
    - Use either SHA1 or SHA 256
    - Private Certificates must be signed by a trusted root CA
    - Public Certificates must include the full chain (root CA and any intermediate CAs)
    - **Supported formats for Public Certificates:**
      Binary DER encoded P7B (including all certificates in the certification path)
    - **Supported formats for Private Certificates:**
      ADP12
      Unencrypted PEM (converted to ADP12 by our software)
      PFX (converted to ADP12 by our software)
2. Log in to Enterprise Examiner.
3. Create or open a case.
4. Go to Tools > Configure Agent Push.
5. When the “Path info for agent push” window appears, do the following:
    a. Next to the “Path to public key” box, browse to the public key from step 1.
    b. Next to the “Path to private key” box, browse to the private key from step 1.
    c. Click “OK”.

Configure Distributed Processing

If you are in a shared environment with a Distributed Processing Manager, you will need to select your Processing Manager when creating a case or performing any processing.

Basic Functionality Test

Create a Case

1. Open Enterprise Examiner and log in.
2. Under the “Case” menu, click “New”.
3. Specify a Case Name and Case Folder Directory, then click “OK”.

Push the Enterprise Agent

1. Open your newly created case.
2. From the “Tools” menu, click “Push Agents”.
3. Enter the IP or computer name of the target Node.
4. Click “Add”.
5. Enter the domain name and Administrator credentials of the target Node.
    a. If the target Node is not on a domain, enter the machine’s name in the “Domain” field.
6. Click “Add”.
7. Click “OK”.
8. * Wait for the “Data Processing Status” dialog to indicate that the Agent was successfully installed.

* If the Agent push/installation fails, refer to this article to ensure all requirements are met.

Collect & Process Data

1. Open your newly created case.
2. From the “Evidence” menu, click “Add Remote Data”.
3. In the “Manual Entry” field, enter the IP or computer name of the target Node.
4. Click “Add”.
5. Under “Browse and Select Nodes”, check and highlight the newly added Node.
6. Under “Select Information”, check what data you’d like to collect.
    a. For simple testing purposes, Volatile Data jobs are typically fastest.
7. Click “OK”.
8. * Wait for the “Data Processing Status” dialog to indicate job completion.

* If AD Enterprise is unable to collect remote data from an Agent, the Agent Certificate settings in “Configure Agent Push” may have not been set correctly when the Agent was pushed/installed.

Upgrading AD Enterprise

Organize Your Certificates

This may have been done during the initial installation, but you should follow the steps to ensure it has been done correctly before proceeding to ensure your certificates are preserved during the upgrade.

1. Log in to the existing Enterprise Examiner.
2. Create or open a case.
3. Go to Tools > Configure Agent Push.
4. When the "Path info for agent push" window appears, do the following:
    a. Note the "Path to public key".
    b. Note the "Path to private key".
5. If they're not there already, copy the certificates from step 4 to an easy to find folder (like "%PROGRAMFILES%\AccessData\Certificates").

Examiner

Uninstall Any Existing Processing Engines

1. Open "Programs & Features" or "Uninstall a Program" via the Windows Control Panel.
2. Uninstall any existing "AccessData Evidence Processing Engine".

Install the Enterprise Examiner & Processing Engine

1. Insert the AD Enterprise installation media.
2. Click "Examiner 64 Bit Install".
3. If you are using a single-box system with a local database, click "Install Processing Engine" and follow the prompts to complete the installation.
    a. If the server has a dedicated temp drive or partition, place the Processing Temporary Folder on that dedicated location.
    b. At the "Destination Folder" dialog, do not check "Install as distributed processing engine".
4. Back in the installation menu, click "Install Examiner" and follow the prompts to complete the installation.

Distributed Processing Manager (Optional)

In any environment sharing a database and cases between multiple Examiner machines, a shared Distributed Processing Manager with Distributed Processing Engines must be used.

Uninstall Any Existing Processing Manager

1. Open "Programs & Features" or "Uninstall a Program" via the Windows Control Panel.
2. Uninstall any existing "AccessData Distribute Processing Manager".

Install the Distributed Evidence Processing Manager

1. Insert the AD Enterprise installation media.
2. From the disc's autorun menu, "Distributed Engine".
3. Click "Install 64 bit Distributed Processing Manager" and follow the prompts to complete the installation.
    a. If the server has a dedicated temp drive or partition, place the Processing State Folder on that dedicated location.
    b. When prompted, specify the Windows account that the AccessData Evidence Processing Engine should run under.
    Note: In any type of multi-box configuration, this should be your domain-level service account.
4. When the Distributed Processing Manager Configuration window opens, add all your Distributed Processing Engine machines and click "Done".

Distributed Processing Engine(s) (Optional)

Uninstall Any Existing Processing Engines

1. Open "Programs & Features" or "Uninstall a Program" via the Windows Control Panel.
2. Uninstall any existing "AccessData Evidence Processing Engine".

Install the Distributed Evidence Processing Engine

1. Insert the AD Enterprise installation media.
2. From the disc's autorun menu, "Distributed Engine".
3. Click "Install 64 bit Distributed Processing Engine" and follow the prompts to complete the installation.
    a. If the server has a dedicated temp drive or partition, place the Processing Temporary Folder on that dedicated location.
    b. At the "Destination Folder" dialog, check "Install as distributed processing engine".
    c. When prompted, specify the Windows account that the AccessData Evidence Processing Engine should run under.
    Note: In any type of multi-box configuration, this should be your domain-level service account.

AD Enterprise First Run

Initialize the Database and Create an Administrator

1. Open Enterprise Examiner.
2. At the “Add Database” dialog, select the database you’d like to connect to.
    a. If desired, you may give the database connection a nickname in the “Display Name” field.
    b. The “dbname” should be set to “ADG” for PostgreSQL and MSSQL.
3. Click “OK”.
4. When prompted, authenticate to the database using the password specified during the database installation.
5. When prompted, create your first Administrator user.

Configure the Agent Certificates

1. Log in to Enterprise Examiner.
2. Create or open a case.
3. Go to Tools > Configure Agent Push.
4. When the “Path info for agent push” window appears, do the following:
    a. Next to the “Path to public key” box, browse to the public key.
    b. Next to the “Path to private key” box, browse to the private key.
    c. Click “OK”.

Configure Distributed Processing

If you are in a shared environment with a Distributed Processing Manager, you will need to select your Processing Manager when creating a case or performing any processing.

Upgrade Old Cases

1. Log in to Enterprise Examiner.
2. Go to Case > Copy Previous Case.
3. Follow the wizard to upgrade any old cases as desired.