AD Enterprise 7.1 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 from https://accessdata.com/product-download. The eDiscovery ISO image (for collecting with the API) is available from the AccessData FTP. To obtain login information, please contact AccessData at support@accessdata.com. The ISO images can be mounted image with drive emulation software (e.g. MagicDisc) or burned to DVD using a program capable of burning ISO images (e.g. ImgBurn).

Licensing

AD Enterprise requires a license (either physical or virtual) provided via CodeMeter software. If a license is not provided, Enterprise will not open. If you wish to use the Enterprise API, you will also need an additional "ADAPI" license.

All licensing requests should go through an Account Executive in Sales.

Firewall Requirements

The following ports should be opened on the server(s) running their respective components:

Component	**Port**
Microsoft SQL Server	1433 (or custom port)
PostgreSQL	5432 (or custom port)
Distributed Processing Manager	34096
Distributed Processing Engine	34097
Quin-C Server	4443
Site Server	54321, 54545, 54555
All machines (if using MSSQL)	135 (DTC), 1024-65535 (DCOM)

New AD Enterprise Installation

There are 5 main components to AD Enterprise:

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

These 5 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 (including .NET 4.7.2).
2. Disable IE Enhanced Security.
3. Disable any antivirus/malware scanning software.
4. Generate or obtain a public/private certificate pair for Agent collections 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:**
      CER/CRT (only for self-signed 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)

Database Server

AD Enterprise supports MSSQL and PostgreSQL. PostgreSQL 11.2 is included with AD Enterprise.

Install MSSQL or PostgreSQL

Install MSSQL

1. Install MSSQL 2012, MSSQL 2014, or MSSQL 2016 according to their associated linked guides.
2. Configure MSDTC as documented here.
3. Set firewall allowances for incoming traffic on ports 1433 (or your custom MSSQL port), 135 (DTC), and 1024-65535 (DCOM).
4. Open the Services snap-in (services.msc) and restart the SQL Server service.

Install PostgreSQL

1. Insert the AD Enterprise installation media.
2. From the disc's autorun menu, click "Examiner 64 Bit Install".
3. At the "AccessData Enterprise Suite" dialog, click "Next".
4. Accept the terms of the EULA and click "Next".
5. Click "Advanced".
6. At the "Custom Setup" dialog, check *only* "PostsgreSQL" and click "Install".
7. 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.
8. Set firewall allowances for incoming traffic on port 5432 (or your custom PostgreSQL port).

Examiner

Install the Enterprise Examiner, Quin-C, & 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. At the "AccessData Enterprise Suite" dialog, click "Next".
10. Accept the terms of the EULA and click "Next".
11. Check "Install Quin-C as a Windows Service" and click "Advanced".
12. At the "Custom Setup" dialog, uncheck *only* "PostsgreSQL" and click "Install".
    Note: If you plan on using Distributed Processing, also uncheck "Evidence Processor".
13. Follow the prompts to complete the installation.
    a. For the Processing Engine:
        i. If the server has a dedicated temp drive or partition, place the Processing Temporary Folder on that dedicated location.
        ii. At the "Destination Folder" dialog, do not check "Install as distributed processing engine".
    b. For Quin-C:
        i. In any multi-box setup, the Quin-C Server service must run under the service account.
14. Set firewall allowances for incoming traffic on port 4443.

15. If using MSSQL:
    a. Configure MSDTC as documented here.
    b. Set firewall allowances for incoming traffic on ports 135 (DTC) and 1024-65535 (DCOM).
16. Open the Services snap-in (services.msc) and restart the Quin-C Self Host service.

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. The AccessData Distributed Processing Manager service must run under the service account.
4. When the Distributed Processing Manager Configuration window opens, add all your Distributed Processing Engine machines, then click "Save" and "Close".
5. Set firewall allowances for incoming traffic on port 34096.
6. If using MSSQL:
    a. Configure MSDTC as documented here.
    b. Set firewall allowances for incoming traffic on ports 135 (DTC) and 1024-65535 (DCOM).

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. The AccessData Evidence Processing Engine service must run under the service account.
4. Set firewall allowances for incoming traffic on port 34097.
5. If using MSSQL:
    a. Configure MSDTC as documented here.
    b. Set firewall allowances for incoming traffic on ports 135 (DTC) and 1024-65535 (DCOM).

Site Server (Optional)

Site Server is needed if you wish to perform collections via the Enterprise API.

Install PostgreSQL

Site Server requires a local installation of PostgreSQL 9.6. If you've already installed PostgreSQL 11 on this machine to use as the main database, PostgreSQL 9.6 will have to use a different port and "pgdata" folder than PostgreSQL 11.

1. Insert the AD eDiscovery installation media.
2. Launch ""[Disc]:\PG_Database\PostgreSQLSetup_x64.exe"", and follow the prompts to complete the installation.
    a. If PostgreSQL 11 already exists on this machine, make sure that you use a different port at "pgdata" folder for PostgreSQL 9.6.
    b. You must create a database password when prompted by the installer.

Install and Configure Site Server

1. Launch ""[Disc]:\Site Server\AccessData_Site_Server.exe"", and follow the prompts to complete the installation.
    a. The Site Server service must run under the service account.
2. Launch "Site Server Configuration", and configure Site Server:
    a. Set Type to "Root".
    b. Give the Site Server a Friendly Name.
    c. Select the Private and Public certificates to be used with Agents.
    d. Specify the password and port used when installing PostgreSQL 9.6.
    e. Set the Internet Protocol Version to "IPv4".
    f. Specify a Results Directory.
    g. Clear out the Children Instances box.
    h. Specify the Managed Subnet Addresses (CIDRs) that Site Server will be allowed to collect from.
    i. Click "Apply" and confirm Site Server correctly connects to the database and restarts.
    j. Click "Close".
3. Set firewall allowances for incoming traffic on ports 54321, 54545, and 54555.
4. On the Examiner, navigate to the Enterprise install "bin" folder (typically "C:\Program Files\AccessData\Forensic Tools\7.1\bin\") and modify "ADG.WebLabSelfHost.exe.config" in a text editor:
    a. Change the value of the "CertificatePath" key to point to your Agent private certificate.
    b. Change the value of the "TrustedCertificatePath" key to point to the agent.p7b in the Site Server installation folder.
    c. Change the value of the "ModulesPath" key to point to the "Windows\x64" modules folder in the Site Server installation folder.
    d. Change the value of "SiteServerHost" and "SiteServerPort" keys to point to your Site Server.
    e. Save your changes and close the file.

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. Go to Tools > Preferences.
3. Note the “private key” and “public key” certificate paths.
4. If they’re not there already, copy the certificates from step 3 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”.

Distributed Processing Manager (Optional)

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”.

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”.

Follow the New AD Enterprise Installation steps to install the new version

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.
6. Open the Services snap-in (services.msc) and restart the Quin-C Self Host service.

Configure the Agent Certificates

1. Log in to Enterprise Examiner.
2. Go to Tools > Preferences.
3. Next to the “Enter the private key file name” box, browse to your Agent private certificate.
   Note: This must match the settings for your Site Server.
4. In the “Agent TCP/IP connection port” box, enter “3999”.
5. Next to the “Enter the public key file name” box, browse to your Agent public certificate.
   Note: This must match the settings for your Site Server.
6. 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.

Configure the API (Optional)

1. On the Examiner, navigate to the Enterprise installation’s bin folder (typically "C:\Program Files\AccessData\Forensic Tools\7.1\bin).
2. Modify “ADG.WeblabSelfHost.exe.config” in a text editor as follow:
    - Change the value of “CertificatePath” to point to your Agent private certificate.

      ```
      <add key="CertificatePath" value="C:\Program Files\AccessData\Certificates\CERBERUS_private.pem.adp12" />
      ```

    - Change the value of “TrustedCertificatePath” to point to your agent.p7b in the Site Server installation folder.

      ```
      <add key="TrustedCertificatePath" value="C:\Program Files\AccessData\SiteServer\Agent\Modules\adata.p7b" />
      ```

    - Change the value of “SiteServerHost” and “SiteServerPort” to point to your Site Server.

      ```
      <add key="SiteServerHost" value="localhost" />
      <add key="SiteServerPort" value="54321" />
      ```

3. Log in to Enterprise Examiner.
4. Go to Tools > Access API Key.

5. Highlight your user and click “Generate Key”.
   Note: This will not be available without an “ADAPI” license.
6. Copy the key out and save it as it won’t be shown again.
7. Close Enterprise.
8. Open the Services snap-in (services.msc) and restart the Quin-C Self Host service.

Upgrade Old Cases (Optional)

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

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.