# AccessData

## Forensic Toolkit

## Installation Guide

5.x

AccessData®

A Pioneer in Digital Investigations Since 1987

# AccessData Legal and Contact Information

Document date: December 5, 2014

## Legal Information

AccessData Group, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Group, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Group, Inc.
1100 Alma Street
Menlo Park, California 94025
USA

www.accessdata.com

## AccessData Trademarks and Copyright Information

AccessData®

AccessData Certified Examiner® (ACE®)

AD Summation®

Discovery Cracker®

Distributed Network Attack®

DNA®

Forensic Toolkit® (FTK®)

Mobile Phone Examiner Plus®

MPE+ Velocitor™

Password Recovery Toolkit®

PRTK®

Registry Viewer®

ResolutionOne™

SilentRunner®

Summation®

ThreatBridge™

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Third party acknowledgements:

- FreeBSD ® Copyright 1992-2011. The FreeBSD Project .
- AFF® and AFFLIB®   Copyright® 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
- Copyright © 2005 - 2009 Ayende Rahien

BSD License: Copyright (c) 2009-2011, Andriy Syrov. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer; Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution; Neither the name of Andriy Syrov nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WordNet License

This license is available as the file LICENSE in any downloaded version of WordNet.

WordNet 3.0 license: (Download)

WordNet Release 3.0 This software and database is being provided to you, the LICENSEE, by Princeton University under the following license. By obtaining, using and/or copying this software and database, you agree that you have read, understood, and will comply with these terms and conditions.: Permission to use, copy, modify and distribute this software and database and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software, database and documentation, including modifications that you make for internal use or for distribution. WordNet 3.0 Copyright 2006 by Princeton University. All rights reserved. THIS SOFTWARE AND DATABASE IS PROVIDED "AS IS" AND PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANT- ABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE, DATABASE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. The name of Princeton University or

Princeton may not be used in advertising or publicity pertaining to distribution of the software and/or database. Title to copyright in this software, database and any associated documentation shall at all times remain with Princeton University and LICENSEE agrees to preserve same.

## Documentation Conventions

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using [*variable_data*] format. Steps that require the user to click on a button or icon are indicated by **Bolded text**. This *Italic* font indicates a label or non-interactive item in the user interface.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

## Registration

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchase.

## Subscriptions

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to access technical support, and to download and install the latest releases for your licensed products during the active license period.

Following the initial licensing period, a subscription renewal is required annually for continued support and for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use License Manager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our web site,

www.accessdata.com anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData website.

## AccessData Contact Information

Your AccessData Sales Representative is your main contact with AccessData. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments

## Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

**AccessData Mailing Address, Hours, and Department Phone Numbers**

| | |
|---|---|
| Corporate Headquarters: | AccessData Group, Inc.<br>1100 Alma Street<br>Menlo Park, California 94025 USAU.S.A.<br>*Voice*: 801.377.5410; *Fax*: 801.377.5426 |
| General Corporate Hours: | Monday through Friday, 8:00 AM – 5:00 PM (MST)<br>AccessData is closed on US Federal Holidays |
| State and Local<br>Law Enforcement Sales: | *Voice*: 800.574.5199, option 1; *Fax*: 801.765.4370<br>*Email*: Sales@AccessData.com |
| Federal Sales: | *Voice*: 800.574.5199, option 2; *Fax*: 801.765.4370<br>*Email*: Sales@AccessData.com |
| Corporate Sales: | *Voice*: 801.377.5410, option 3; *Fax*: 801.765.4370<br>*Email*: Sales@AccessData.com |
| Training: | *Voice*: 801.377.5410, option 6; *Fax*: 801.765.4370<br>*Email*: Training@AccessData.com |
| Accounting: | *Voice*: 801.377.5410, option 4 |

## Technical Support

Free technical support is available on all currently licensed AccessData solutions.
You can contact AccessData Customer and Technical Support in the following ways:

**AD Customer & Technical Support Contact Information**

| | |
|---|---|
| **AD SUMMATIONand AD EDISCOVERY** | Americas/Asia-Pacific:<br>800.786.8369 (North America)<br>801.377.5410, option 5<br>Email: legalsupport@accessdata.com |
| **AD IBLAZE and ENTERPRISE**: | Americas/Asia-Pacific:<br>800.786.2778 (North America)<br>801.377.5410, option 5<br>Email: support@summation.com |
| **All other AD SOLUTIONS** | Americas/Asia-Pacific:<br>800.658.5199 (North America)<br>801.377.5410, option 5<br>Email: support@accessdata.com |
| **AD INTERNATIONAL SUPPORT** | Europe/Middle East/Africa:<br>+44 (0) 207 010 7817 (United Kingdom)<br>Email: emeasupport@accessdata.com |

**AD Customer & Technical Support Contact Information (Continued)**

| | |
|---|---|
| *Hours of Support*: | Americas/Asia-Pacific:<br>Monday through Friday, 6:00 AM– 6:00 PM (PST), except corporate holidays.<br>Europe/Middle East/Africa:<br>Monday through Friday, 8:00 AM– 5:00 PM (UK-London) except corporate holidays. |
| *Web Site*: | http://www.accessdata.com/support/technical-customer-support |
| | The Support website allows access to Discussion Forums, Downloads, Previous Releases, our Knowledge base, a way to submit and track your “trouble tickets”, and in-depth contact information. |

## Documentation

Please email AccessData regarding any typos, inaccuracies, or other problems you find with the documentation: *documentation@accessdata.com*

## Professional Services

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of FTK, FTK Pro, Enterprise, eDiscovery, Lab and the entire Resolution One platform. They can help you resolve any questions or problems you may have regarding these solutions.

## Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

**AccessData Professional Services Contact Information**

| Contact Method | Number or Address |
|---|---|
| *Phone* | North America Toll Free: 800-489-5199, option 7 |
| | International: +1.801.377.5410, option 7 |
| *Email* | *services@accessdata.com* |

# Contents

Chapter 1

# Planning to Install FTK

This guide details the installation of the components required for the operation of AccessData Forensic Toolkit (FTK).

Also refer to the Release Notes for specific issues regarding installation. The Release Notes are available :

http://www.accessdata.com/support/product-downloads/ftk-download-page

## About 32-bit and 64-bit computers

Many of the AccessData software components that you install have both 32-bit and 64-bit versions.

Make sure that you know whether you are using a 32-bit or 64-bit computer.

## Prerequisites

The following prerequisites apply for installing and running FTK:

- A computer running a supported operating system

  For a list of supported operating systems that you can install FTK on, see the bottom-right panel on the FTK download page:

  http://www.accessdata.com/support/product-downloads/ftk-download-page
- A supported database

  Choosing a Database Application to Use (page 14)
- A WIBU-SYSTEMS CodeMeter USB or Virtual CmStick

  See Managing Security Devices and Licenses on page 71.
- CodeMeter Runtime software for the CodeMeter Virtual or USB CmStick.

  See Managing Security Devices and Licenses on page 71.
- Evidence Processing Engine

### *Hardware Considerations*

The more powerful the available hardware, the faster FTK can analyze, process and prepare case evidence. Larger evidence files require more processing time than smaller evidence files. AccessData recommends that the various components be installed on separate machines to make more hardware resources available to the program. Thus, while the FTK and Oracle components can be installed on a single workstation, the ideal and recommended configuration uses two workstations connected by a Gigabit Ethernet connection, thus making more hardware resources available to each.

If the KFF Library is installed, it must be installed on the same computer as the database. Ideally, the latest CodeMeter Runtime, Language Selector, and License Manager software that AccessData provides should be installed on the same computer as the FTK application.

To further maximize performance, AccessData recommends the following:

- For both the single- and separate-workstation configurations, install the database to a large hard disk drive the database can use exclusively.
- Recommended RAM is 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.
- If your machine has less than 1 GB per core when processing multiple pieces of evidence under certain circumstances processing will fail and not recover. We recommend that the amount of RAM be 2 GB per processing core (e.g. an 8-core machine should have at least 16 GB of RAM).

**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.

- Do not run third-party applications on either the FTK or the database machine that will compete with FTK or the database for hardware resources.
- If you need PRTK or DNA, install it on the network, then copy any files for decryption to that machine.

## *Estimating Hard Disk Space Requirements*

The FTK program requires a minimum of 500 megabytes of disk space for installation, although 5 gigabytes is recommended.

Oracle, where case data is stored, requires a minimum of 6 gigabytes (5 gigabytes for the basic installation) and plenty of additional room for case processing.

Additional space is required for the actual cases and for drive images and other evidence files that need to remain intact, separate from the database. These can be stored on other computers within the network.

**Important:** If disk space depletes while processing a case, the case data is corrupted.

To estimate the amount of hard drive space needed, apply these suggested guidelines:

- Data: every 500,000 items require one gigabyte of space in the Oracle storage location.
- Index: every 100 megabytes of text in the evidence requires 20 megabytes of space for processing in the case storage folder.

# Distributed Processing Guideline Summary

This release of FTK supports Distributed Processing Engines (DPEs). Distributed Processing allows the installation of up to three additional processing engines to share the work load of processing evidence in a case.

Note the following:

- The distributed processing engines (cluster) require significant I/O capacity to properly read the image/ evidence. To avoid bottlenecks and failures ensure the evidence is stored in a location with sufficient I/O. Failure notices will appear in the evidence log if capacity is not sufficient.
- To avoid bottlenecks in processing, ensure that there is sufficient I/O bandwidth/capacity into the database and case folder.
- UNC paths must be used for evidence and case folders.
- Make sure the distributed processing engine (DPE) services are running with a user account that has read/write access to the evidence and case folder.
- Ensure a minimum 1 Gigabit network connection is used for all communication in the distributed processing cluster.
- Distributed processing generates a lot of traffic.
- Refer to the *AccessData Distributed Processing* appendix in the *User Guide* for additional information on setup and usage of distributed processing.
- If you are installing KFF in a distributed processing environement, you must specify the KFF server by its IP address and not use ‘localhost’. Otherwise you may get inccorect KFF counts.

For More information, see AccessData Distributed Processing (page 90)

# Configuration Options

FTK can be set up in three different configurations, each with its own benefits and advantages.

- Single Machine

  FTK and the database are both installed on the same box. It may be helpful in this scenario if the database is installed on a secondary drive to provide better throughput.
- Separate Machines with a new database install

  FTK and the database can be installed on separate boxes or on the same box. If both are installed on the same box, it is recommended that the database be installed either on a separate drive, or on a separate partition from FTK.
- Separate Machines with an existing database install

  If a compatible database is already installed, you may be able to use it with FTK. The installer runs a check for compatibility.

**Note:** The database software should be installed to a physical system drive. Installing the database in a virtual machine is not supported. Installing the CodeMeter software in a virtual machine is not recommended.

**Note:** AccessData recommends that you turn off firewalls and anti-virus software during installation.

**Important:** If installation is being done using remote desktop to Server 2003, the remote connection needs to be established using either the `/admin` or the `/console` command.

# Choosing a Database Application to Use

FTK requires using one of the following database applications:

| | |
|---|---|
| PostgreSQL 9.0.x, 9.1.6, 9.1.11, 9.1.15, or 9.3.5 | PostgreSQL is provided free of charge by AccessData.<br>See Download & Preparation on page 17.<br>For information on upgrading to 9.1.11, see About Upgrading PostgreSQL (page 23). |
| Microsoft SQL Server 2008 R2 or 2012 | See Configuring and Managing Databases for FTK on page 65. |
| Oracle 10.2.0.4 | Oracle 11g is not supported.<br>See Best Practices for Using Oracle on page 65. |

When you install FTK, you select which database application to use. If you are upgrading from a previous version of FTK, you are not required to use the same database. You can install and migrate cases to a new database application from a different database.

The database must be installed before installing FTK.

PostgreSQL is provided free of charge by AccessData. You can use your own installations of Microsoft SQL or Oracle,

# Planning for a New Installation

## Planning a New FTK Installation using PostgreSQL

- PostgreSQL 9.3.5 is available free of charge on the FTK download page.

  See Download & Preparation on page 17.
- You must install PostgreSQL before installing FTK.

## Planning a New FTK Installation using Microsoft SQL Server

- You can use either Microsoft SQL Server 2008 R2 or 2012 with FTK.
- Before installing FTK, you must install SQL and configure it so that it will work with FTK.

  See Best Practices for using Microsoft SQL Server on page 67.

## Planning a New FTK Installation using Oracle

- You can use Oracle 10.2.0.4 with FTK.
- You must install Oracle before installing FTK.
- When adding the database, you must configure the Oracle SID as FTK2.

  See Initializing the FTK Database and Creating an Application Administrator Account on page 20.
- For information about obtaining and applying Oracle Critical Patch Updates, see Best Practices for Using Oracle (page 65).

# Planning for an FTK Upgrade from a Previous Version

See Upgrading FTK on page 23.

# About Installing CodeMeter and Managing Licenses

See Managing Security Devices and Licenses on page 71.

Chapter 2

# Installing FTK

## Process for Installing AccessData Forensic Toolkit

There are two discs that ship with FTK:

- The Database and FTK program install disc
- The KFF Server and KFF data install disc.

Each disc has an **Autorun.exe** to streamline the installation process.

The FTK program can be installed on either the same or different computer as the database.

If you install FTK and the database on the same computer, it is considered a one-box, or single-box, install. To perform a one-box install, perform the prescribed steps in the order presented, all on the same computer.

If you install FTK and the database on a different computer, it is known as a two-box install. To perform a two-box install, perform the prescribed steps in the order presented, on the specific computer.

### Installation Process

| Step | Computer | Task |
|---|---|---|
| 1 | Database | Choose and install a supported database.<br>See Installing the Database on page 17. |
| 2 | Database | If using Oracle or Microsoft SQL, optimize your database.<br>See Configuring and Managing Databases for FTK on page 65. |
| 3 | FTK | Install the FTK Suite:<br>● CodeMeter<br>● Evidence Processing Engine<br>● FTK<br>See Installing the FTK Suite on page 18. |
| 4 | FTK | Run FTK and initialize the database<br>See Initializing the FTK Database and Creating an Application Administrator Account on page 20. |
| 5 | FTK | Install other components, such as KFF.<br>See Installing Additional Programs on page 33. |

**Important:** For information regarding backup and restore for FTK when the database is installed on a separate box, see “Appendix F Back-up and Restore Case Data on a Two-Box Installation” in the *FTK User Guide*.

# *Download & Preparation*

You may have installation disks or you can download the required files. Use the following procedure to download the FTK installation files from the AccessData website.

1. Go to the AccessData website at http://www.accessdata.com/product-download.
2. On the *Product Downloads* page, click *Forensic Toolkit (FTK).*
3. Click **Download Page**.
4. On the *Forensic Toolkit Download* page, download the following ISO files. (AccessData recommends using a download manager program such as Filezilla.)
   - For a new installation:
     - *FTK Full Disk ISO Files* -- This disk contains the following:
       - PostgreSQL installation files if you need to install a database.
       - Code Meter, Processing Engine, and FTK installation files
     - *KFF Installation Disks* -- Theses disk contains the following:
       - 32-bit KFF Server and data installation files
       - 64-bit KFF Server and data installation files
   - For an upgrade
     - *FTK Upgrade* (32 or 64-bit)
       - PostgreSQL installation files if you need to install a database.
       - FTK upgrade installation files
5. Verify the MD5 hashes match what is posted on the main FTK download page to ensure there was no data corruption in the download process.
6. Do one of the following:
   - Mount the ISO directly using a program like MagicDisc.

     AccessData recommends mounting an ISO image for the installation as it eliminates some of the problems associated with burning discs.
   - Burn the ISO to a DVD with a program such as ImgBurn.

**Important:** If you install the database from a mounted ISO image, make sure there are no discs in the optical drives before you start the installation.

## Required Software

FTK requires

- Microsoft .NET Framework 4.0 Full
- BlackIce ColorPlus Driver
- InstallMSDTC

If these are not installed, the FTK installer will install them automatically.

# *Installing the Database*

Before installing FTK, you must have a database installed.

If you do not have one of the supported databases installed, you can install PostgreSQL, which is provided by AccessData.

If you are using Microsoft SQL, Oracle, or PostgreSQL on a different computer, install it before installing the FTK application.

To install PostgreSQL on the same computer as FTK, use the FTK Suite installer.

**Important:** During the installation, you will specify a password that is required for FTK database administrative tasks. Record this password. AccessData cannot recover this password if it is lost.

If using Oracle or Microsoft SQL, optimize your database.
See Configuring and Managing Databases for FTK on page 65.

## *Installing the FTK Suite*

When installing FTK, you use the *AccessData FTK Suite* installer. This suite installer can install the following FTK applications:

- CodeMeter Runtime Kit
- PostgreSQL database (on the same computer)
- Evidence Processing Engine
- FTK

In the installation wizard, you can choose one of two installation methods:

| | |
|---|---|
| Default | This option is a “single-click” installation that installs all of the applications with default settings.<br>This option is used for a single-box installation which is best suited for evaluation only.<br>If a database is already installed, the Advanced option is only available.<br>Note: This installation uses a pre-set PostgreSQL database administrator account detailed below.<br>See Performing a Default Installation of the FTK Suite on page 18.<br>See Initializing the FTK Database and Creating an Application Administrator Account on page 20. |
| Advanced | This option lets you select which applications to install. It also lets you choose folder locations for the features.<br>If you are not going to install PostgreSQL on the same computer, install your Oracle, Microsoft SQL or PostgreSQL database before installing the FTK suite.<br>See Performing an Advanced Installation of the FTK Suite on page 19. |

### Performing a Default Installation of the FTK Suite

**To perform a default installation**

1. Insert your license dongle into the computer you will be installing FTK on.
2. Using the FTK Install disc or ISO, launch the installation `FTK_autorun.exe` on the computer where FTK will reside.

   See Download & Preparation on page 17.
3. Click **FTK Install** to launch the FTK Suite installation wizard.
4. On the *Welcome* page of the wizard, click **Next**.
5. On the *License Agreement* page of the wizard, read the agreement, and accept the license, and click **Next**.
6. On the *Setup Type* page of the wizard, click **Default**.

7. On the *PostgreSQL License Agreement* page of the wizard, read the agreement, and accept the license, and click **Next**.
8. If not already installed, the following applications are installed.
    - CodeMeter
    - PostgreSQL
    - Evidence Processing Engine
    - FTK
    - Other prerequisite components, such as the BlackIce ColorPlus Driver
9. When this installation is completed, click **Finish**.
10. Click the FTK shortcut icon to launch FTK and initialize the database.

    See Initializing the FTK Database and Creating an Application Administrator Account on page 20.
11. (Optional) Install KFF or other products.

    You must initialize the database before you do this step.

    See Installing Additional Programs on page 33.

## Performing an Advanced Installation of the FTK Suite

If you are not going to install PostgreSQL on the same computer, install your Oracle, Microsoft SQL or PostgreSQL database before installing the FTK suite.

### To perform an advanced installation

1. Insert your license dongle into the computer you will be installing FTK on.
2. Using the FTK Install disc or ISO, launch the installation `FTK_autorun.exe` on the computer where FTK will reside.

    See Download & Preparation on page 17.
3. Click **FTK Install** to launch the FTK Suite installation wizard.
4. On the *Welcome* page of the wizard, click **Next**.
5. On the *License Agreement* page of the wizard, read the agreement, and accept the license, and click **Next**.
6. On the *Setup Type* page of the wizard, click **Advanced**.
7. On the *Custom Setup* page of the wizard, select the features that you want to install.
    - If you already have PostgreSQL installed on the computer, it will skip the database installation.
    - If you want to install PostgreSQL on this computer, select it.
    - If you are using a different database, such as Oracle or Microsoft SQL, or PostgreSQL on a different computer, clear the PostgreSQL option.
8. Click **Install**.
9. The CodeMeter application, if not already installed, is automatically installed.
10. If needed, install the PostgreSQL database by doing the following:

    10a. On the *PostgreSQL Setup Welcome* page, click **Next**.

    10b. On the *License Agreement* page of the wizard, read the agreement, and accept the license, and click **Next**.

    10c. Accept the default *Destination Folder* of the PostgreSQL application files or change it and click **Next**.

    10d. Accept the default *Destination Folder* of the PostgreSQL data files or change it and click **Next**.

10e. Accept the default PostgreSQL port he server should listen on or change it and click **Next**.

Use the default port, usually 5432, unless you need to change it.

Record the port used.

10f. On the *Optimize for environment* page, select the second option for **Using PostgreSQL with FTK/Lab** and click **Next**.

10g. In the *PostgreSQL User Create* dialog, enter and confirm a password for the PostgreSQL admin user and click **Next**.

**Important:** You are required to provide this password when launching FTK for the first time and when performing certain database administrative tasks.

Record this password in a secure place.

10h. To install the PostgreSQL database, click **Install**.

10i. When the PostgreSQL installation is completed, click **Finish**.

11. Install the Evidence Processing Engine by doing the following:

11a. If required software is required to be installed, such as the BlackIce ColorPlus Driver, click **Install**.

11b. On the *Evidence Processing Engine Installation Welcome* page, click **Next.**

11c. Complete the Evidence Processing Engine installation wizard.

Because you are installing the Evidence Processing Engine on the same computer as FTK, do not select the **Install as distributed processing engine** option in the *Destination Folder* window.

12. Install the FTK application by doing the following:

12a. Select the language for the installation and click **OK**.

12b. On the *FTK Installation Welcome* page, click **Next**.

12c. On the *License Agreement* page of the wizard, read the agreement, and accept the license, and click **Next**.

12d. On the *Destination Folder* page of the wizard, use the default path or change the path to a new location, and click **Next**.

12e. To install FTK, click **Install**.

12f. When the FTK installation has completed, click **Finish**.

13. Click **Finish**.

14. Click the FTK shortcut icon to launch FTK and initialize the database.

See Initializing the FTK Database and Creating an Application Administrator Account on page 20.

15. (Optional) Install KFF or other products.

This step can only be done on the computer where the database resides. You must initialize the database before you do this step.

See Installing Additional Programs on page 33.

## Initializing the FTK Database and Creating an Application Administrator Account

The database and application must already be installed prior to this step.

The first time you launch FTK, you specify the database for FTK to use. The application then creates the database schema which is required before any case data can be loaded into the database. You will be prompted to give the location of the database. This option allows a non-local database to be specified even if a local database is present.

After initializing the database, you are prompted to create an Application Administrator account. This account lets you create other user accounts and perform other administrative tasks.

**To initialize the FTK database and create an Application Administrator account**

1. Click the FTK shortcut icon to open FTK.
2. If FTK does not detect a configured database connection for that version of FTK, you will be prompted to *Add Database*.
3. In the *RDBMS* drop-down menu, select the brand of database that you are connecting to.
4. Specify the server hosting the database in the *Host* field.

   If the database is on the same computer as FTK, you can leave this field empty.
5. (Optional) Give the database connection a nickname in the *Display name* field.
6. Specify the database name by doing one of the following:
   - If you are using Oracle, you must configure the *Oracle SID* to be FTK2.
   - If you are using PostgreSQL or MS SQL Server, for the *PostgreSQL dbname* or *mssql sa,* you can use the default values or enter your own value. If you enter your own value, make sure that you record it so that you know the database name.
7. Do not change the *Port number* fields unless you have a custom database configuration.
8. If you are using MS SQL Server, you can check **Use Integrated Security** to use your Windows authentication credentials.
9. Click **OK.**

   If the connection attempt to the database was successful, the database will be initialized.
10. In the *Please Authenticate* dialog, log into the database using you database administrator account credentials.
    - If you used the default installation, enter the following credentials:

      Username: postgres<br>
      Password: AD@Password
    - If you used the advanced installation or installed a different database, enter your credentials.

    A successful login initializes the database and opens the *Case Manager* window.
11. In the *Add New User* dialog, create an Application Administrator account for this version of the database schema.
    - Enter a name and password.
    - Record this information in a secure place.
12. Click **OK**.
13. Refer to the *User Guide* for information on how to configure and use FTK.

## *Uninstalling FTK*

**Important:** Here are some things to remember when uninstalling FTK.

- Prompts to close running processes will not automatically close as indicated. When a user uninstalls FTK after they have been using the program and have since closed it, the dialog box on uninstall will notify the user that processes are still running and gives an option to close them automatically. If the user selects to have the process close them automatically, it cannot. The uninstall cannot work correctly until the user kills all running FTK processes manually.
- If you uninstall after a successful install, the pointer to the database will be left behind. If you want to re-install and point to a new Oracle location, you need to delete the `databases.xml` file found in the

following path (in Vista):
[*drive*]:\ProgramData\AccessData\Products\Forensic Toolkit\FTK Databases.xml.

Chapter 3

# Upgrading FTK

## About Upgrading FTK

### *About Upgrading PostgreSQL*

PostgreSQL 9.1.13 is now provided on the installation disc. Please be aware of the following:

- If you have a previous version of PostgreSQL, such as 9.1.6, you can upgrade to 9.1.13 but it is not required.
- For new installations, PostgreSQL 9.1.13 is the default database.
- For information about version 9.1.13, see
  http://www.postgresql.org/docs/9.1/static/index.htm

### PostgreSQL Upgrade Instructions

You must follow these instructions or you may no longer have access to your previous cases.

- To upgrade to PostgreSQL 9.1.13:
  - Do not uninstall the previous version of PostgreSQL.
  - Run the PostgreSQL installation from the installation disc.
  - At the *Data Folder* dialog, specify the same `pgData91` folder as used by your existing AccessData PostgreSQL 9.1.6 installation.
  - At the *PostgreSQL Port* dialog, specify the same port as used by your existing AccessData PostgreSQL 9.1.6 installation.
  - At the *Port Substitution* dialog, click “Yes” to confirm that you do want to use that port.

### *About Installing Upgrades and Patches*

When you install a newer major or minor version of FTK (3.0, 3.1, 4.0, 4.1, 4.2, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6), it does not replace the previous version of FTK and both versions are usable as stand-alone products. You must upgrade or migrate your cases to work with the new version.

If you install a patch (5.3.5), it replaces the previous version (5.3). You do not need to upgrade your cases to work with the new patch.

## *About Upgrading, Migrating, and Moving Cases*

If you have a previous version of FTK (3.x, 4.x, 5.x), and install a new version (like 5.6), both versions are usable as stand-alone products. However, the two installations do not share cases or instances of the database. When you install a newer major or minor version of FTK, it creates a new database and does not have any cases associated with it. You can upgrade or migrate cases from the previous FTK database to work with the new version.

You can also change the database that FTK is using without changing the version of FTK.

Depending on the situation, you can do one of the following with your existing cases:

- Upgrade - You upgrade a case when you are upgrading to a new version of FTK and you are using the same type and version of the database.
- Migrate - You migrate a case when you are upgrading to a new version of FTK and you are using a different type or version of the database.
- Move - You move a case when you are using the same version of FTK and you are changing to a different type or version of the database.

When you upgrade or migrate a case to a newer version of FTK, the case is copied and the original case is still available for use with the previous version of FTK.

**Important:** You cannot upgrade cases from version 4.0 or earlier directly to version 5.x. You must first upgrade to version 4.1 or 4.2 and then upgrade to version 5.x.

You can use the DBUPGRADE.EXE utility to perform the first part of a two-step migration of cases from FTK 3.4 through 4.0 to version 5.x. You can use the DBUPGRADE.EXE utility to perform the first part of a two-step migration of cases from FTK 3.4 through 4.0 to version 5.x.

For information on upgrading FTK 3.x to 4.1 or 4.2, contact your Technical Account Manager or Technical Support.

**Important Considerations**

- Some features supported by newer versions may not be available when reviewing a case that has been upgraded. Depending on the feature, you may need to reprocess some or all of the evidence in the case to be able to use a particular feature.
- The following information assumes that you have already created user accounts in the new database.

## Scenarios for Upgrading, Migrating, and Moving Cases

There are several scenarios where you may want to upgrade, migrate, or move your cases. How you upgrade, migrate, or move your cases depends on the source and the desired destination of the cases.

The following table lists the possible scenarios and the general process to perform the upgrade, migration, or move.

| | |
|---|---|
| Upgrading a case from FTK TK 4.2.x or 5.x to FTK 5.6 and using the same type and version of the database.<br>For example:<br>● FTK 4.2 with Oracle 10g to FTK 5.6.x with Oracle 10g<br>● FTK 4.2 with PostgreSQL 9.1.6 to FTK 5.6.x with PostgreSQL 9.1.x | One-step upgrade process:<br>1. In FTK 5.1, upgrade the case using the Copy Previous Case feature.<br>See Upgrading Cases on page 25. |

| | |
|---|---|
| Migrating a case from FTK 4.2.x or 5.x to FTK 5.6 and changing to a different type or version of the database.<br>For example:<br>● FTK 4.2 with Oracle to FTK 5.x with either PostgreSQL or SQL<br>● FTK 4.2 with PostgreSQL 9.0.x to FTK 5.x with PostgreSQL 9.1.11<br>● FTK 4.2 with PostgreSQL 9.0.x to FTK 5.x with SQL | Two-step migration process:<br>1. In FTK 4.2.x or 5.0.x, backup the case using the database independent format.<br>2. In FTK 5.0.x, restore the backed-up case.<br>See Migrating Cases to a Newer Version of FTK and Different Database on page 26. |
| Moving a case from one type or version of a database to another while using the same version of FTK.<br>For example:<br>● FTK 5.x with Oracle to FTK 5.x with either PostgreSQL or SQL<br>● FTK 5.x with PostgreSQL to FTK 5.x with SQL or Oracle<br>● FTK 5.x with SQL to FTK 5.x with either PostgreSQL or Oracle | Two-step move process:<br>1. In FTK 5.0.x, backup the case using the database independent format.<br>2. In FTK 5.0.x, restore the backed-up case.<br>Moving Cases from One Database to Another (page 27) |

## *Upgrading Cases*

If you are upgrading a case from 4.1 and above to 5.0x and above and you are using the same type and version of the database, you perform a one-step upgrade process.

For example:

- Upgrading from FTK 4.1 with Oracle 10g to FTK 5.x with Oracle 10g
- Upgrading from FTK 4.1 with PostgreSQL 9.1.6 to FTK 5.x with PostgreSQL 9.1.6

**Note:** If you are changing either the type or the version of the database, you must perform a two-step migration.

### Important Considerations

- You cannot upgrade cases from 3.x or 4.0 to 5.x. You must upgrade to 4.1 or 4.2 first. Then you can upgrade from 4.1 or 4.2 to 5.x. For information on upgrading from 4.0.x or older, contact your Technical Account Manager or Technical Support.
- This version does not support upgrading cases from 2.x. If you have 2.x cases that you want to upgrade, you must first upgrade the cases to 3.0 or newer.
- Some features supported by newer versions may not be available when reviewing a case that has been upgraded. Depending on the feature, you may need to reprocess some or all of the evidence in the case to be able to use a particular feature.

The following information assumes that you have already created user accounts in the new database.

### To upgrade a case

1. In FTK 5.x, open the *Case Manager*.
2. Click **Case** > **Copy Previous Case...**
3. On the *Copy Case(s)* dialog, in the *Select Database* drop-down menu, select the version of the database from which you would like to copy your case.

   **Note:** If prompted to authenticate, enter the system administrator (sys) credentials for the Oracle database and then click **OK**.

4. Highlight the case(s) which you would like to upgrade into the new database.

   Use **Shift+Click** or **Ctrl+Click** to select more than one case at a time.

**Important:** The selected case(s) must not be in use at the time of upgrade.

5. Click **OK**.
6. On the *Case Attach* dialog, use the *Case:* drop-down menu to view the list of users that are associated to each case.
7. For each case that is upgraded, use the *Associate Users* control box to map the user names that exists in the previous database (*Old User Name*) to the appropriate user name(s) that exist in the new database (*New User Name*).
8. To associate users, do the following:

   8a. Highlight the old user name(s) to which you would like to associate to a username in the new database. Use **SHIFT+Click** or **CTRL+Click** to select more than one username at a time.

   8b. Click **Associate to...**

   8c. Select the user name from the new database to which you would like to associate with the old user names.

9. Click **OK**.
10. The selected user associations are mapped and the case is copied into the new database.

**Note:** The copied case is written to the same main case folder as the source case. The upgraded case name will be appended with a number to make it unique. For example, My Example Case Name (1).

## Migrating Cases to a Newer Version of FTK and Different Database

You perform a two-step migration process for cases if you are upgrading a case from 4.2 to 5.x and are also changing to a different type or version of the database.

For example:

- Migrating from FTK 4.2 with Oracle to FTK 5.x with PostgreSQL 9.1.6
- Migrating from FTK 4.2 with Oracle to FTK 5.x with Microsoft SQL
- Migrating from FTK 4.2 with PostgreSQL 9.0.x to FTK 5.x with PostgreSQL 9.1.6

**Note:** If you are not changing the type or the version of the database, you can perform a one-step upgrade. See Upgrading Cases on page 25.

When you migrate a case, the original case is maintained for the previous version and a new copy is migrated for use with the new version of FTK.

### To migrate a case from 4.2 or 5.x to 5.x

1. In FTK 4.2 or 5.x Case Manager, back up the case using the database independent format.
   See Backing Up a Case on page 27.
2. Open the Case Management interface (connected to the new database).
3. Restore your cases to the new database.
   See Restoring a Case on page 29.

## Moving Cases from One Database to Another

Your FTK 5.x cases can be moved from one database type or version to another.

For example:

- Moving cases in FTK 5.x with PostgreSQL 9.1.6 to FTK 5.x with PostgreSQL 9.1.11
- Moving cases in FTK 5.x with Oracle to FTK 5.x with either PostgreSQL or SQL
- Moving cases in FTK 5.x with SQL to FTK 5.x with either PostgreSQL or Oracle

To move cases, do the following:

- Backup each case that you want moved.
- Restore each case to the new database.

**To move cases from database to another**

1. Open the Case Management interface.
2. Back up ALL cases that need to be moved.
   See Backing Up a Case on page 27.
3. Connect to the new database. If the instance you are running has been connected to a database previously, you will need to follow these steps to switch default databases:
   3a. After all cases have been backed up successfully, close the *Case Manager*.
   3b. Shut down the database service(s). (In Windows, you can use the services.msc management snap-in to stop the database services.)
   3c. Ensure the new database is up and accepting connection requests.
   3d. Launch the application (you should receive a message stating that it was unable to connect to the database).
   3e. Connect to the new database and complete the initialization process. For help, see “Initializing the Database.”
4. Open the Case Management interface (connected to the new database).
5. Restore your cases to the new database.
   See Restoring a Case on page 29.

# Backing Up a Case

## Performing a Backup and Restore on a Two-Box Installation

If you have installed the Examiner and the database on separate boxes, there are special considerations you must take into account. For instructions on how to back up and restore in this environment, see “*Configuring for a Two-box Back-up and Restore.*”

## Performing a Backup of a Case

At certain milestones of an investigation, you should back up your case to mitigate the risk of an irreversible processing mistake or perhaps case corruption.

Case backup can also be used when migrating or moving cases from one database type to another. For example, if you have created cases using 4.1 in an Oracle database and you want to upgrade to 5.0.x and migrate the case(s) to a PostgreSQL database. Another example is if you have created cases using 5.0.x in an Oracle database and you want to move the case(s) to the same version that is running a PostgreSQL database.

When you back up a case, the case information and database files (but not evidence) are copied to the selected destination folder. AccessData recommends that you store copies of your drive images and other evidence separate from the backed-up case.

**Important:** Case Administrators back up cases and must maintain and protect the library of backups against unauthorized restoration, because the user who restores an archive becomes that case's administrator.

**Note:** Backup files are not compressed. A backed-up case requires the same amount of space as that case's database table space and the case folder together.

Starting in 4.2, all backups are performed using the database independent format rather than a native format. The database independent format facilitates migrating and moving cases to a different database application or version. You can perform a backup using a native format using the dbcontrol utility. For more information, contact AccessData Technical Support.

**Important:** Do not perform a backup of a case while any data in that case is being processed.

### To back up a case

1. In the *Case Manager* window, select the case to back up. You can use Shift + Click, or Ctrl + Click to select multiple cases to backup.
2. Do one of the following:
   - Click **Case > Backup > Backup**.
   - Right-click on the case in the *Cases* list, and click **Backup**.
3. In the field labeled *Backup folder*, enter a destination path for the backup files.

   **Important:** Choose a folder that does not already exist. The backup will be saved as a folder, and when restoring a backup, point to this folder (not the files it contains) in order to restore the case.
4. If you are using 4.1 to backup a case in order to migrate it to 4.2, make sure that you select **Use database independent format**.

   In 4.2, all backups are performed using the database independent format.
5. (Optional) Back up the Summation or Resolution1 application database.

   If you have a licence for Summation or Resolution1, when you back up a case, you can also select to backup the Summation or Resolution1 application database by doing the following:

   5a. Click **App DB...**.

   5b. Specify the App DB properties and credentials.
6. Click **OK**.

   **Note:** The following information may be useful:

   - Each case you back up should have its own backup folder to ensure all data is kept together and cannot be overwritten by another case backup. In addition, AccessData recommends that backups be stored on a separate drive or system from the case, to reduce space consumption and to reduce the risk of total loss in the case of catastrophic failure (drive crash, etc.).
   - The absolute path of the case folder is recorded. When restoring a case, the default path is the original path. You can choose the default path, or enter a different path for the case restore.

# Restoring a Case

Do not use the *Restore...* function to attach an archive (instead use *Attach...*). When your case was backed up, it was saved as a folder. The folder selected for the backup is the folder you must select when restoring the backup.

**To restore a case**

1. Open the *Case Manager* window.
2. Do either of these:
    - Click **Case > Restore > Restore**.
    - Right-click on the *Case Manager* case list, and click **Restore > Restore**.
3. Browse to and select the backup folder to be restored.
4. (Optional) Select **Specify the location of the DB files** and browse to the path to store the database files for this case.

    4a. Select **In the case folder** to place the database files in subfolderof the case folder.
5. You are prompted if you would like to specify a different location for the case folder. The processing status dialog appears, showing the progress of the archive. When the archive completes, close the dialog.

# Configuration for a Two-box Backup and Restore

By default, a two-box installation (also known as a distributed installation, where the application and its associated database have been installed on separate systems) is not configured to allow the user to back up and restore case information. Some configuration changes must be performed manually by the system administrator to properly configure a two-box installation. Please note that the steps required to complete this configuration differ slightly for domain systems than for workgroup systems.

## *Configuration Overview*

The following steps are required before you can perform two-box case back ups and restoration.

- Create a service account common to all systems involved. See Create a Service Account on page 30.
- Share the case folder and assign appropriate permissions. See Share the Case Folder on page 30.
- Configure the database services to run under service account. See Configure Database Services on page 31.
- Share back up destination folder with appropriate permissions. See Share the Backup Destination Folder on page 31.

**Note:** When prompted to select the backup destination folder, *always* use the UNC path of that shared folder, even when the backup destination folder is local.

Each of these items is explained in detail later in this chapter.

# Create a Service Account

To function in a distributed configuration, all reading and writing of case data should be performed under the authority of a single Windows user account. Throughout the rest of this document, this account is referred to as the “service account.” If all the systems involved are members of the same domain, choosing a domain user account is the recommended choice. If not all of the systems are members of the same domain, then you can configure “Mirrored Local Accounts” as detailed in the following steps:

**To set up Mirrored Local Accounts**

1. On the Examiner host system, create (or identify) a local user account.
2. Ensure that the chosen account is a member of the Local Administrators group.
3. On the database host system, create a user that has the exact same username and password as that on the Examiner host system.
4. Ensure that this account is also a member of the Local Administrators group on the database host system.

## Instructions for Domain User Accounts

Choose (or create) a domain user account that will function as the service account. Verify that the chosen domain user has local administrator privilege on both the Examiner host system and the database host system.

**To verify the domain user account privileges**

1. Open the “Local Users and Groups” snap-in.
2. View the members of the Administrators group.
3. Ensure that the account selected earlier is a member of this group (either explicitly or by effective permissions).
4. Perform this verification for both the examination and the database host systems.

# Share the Case Folder

On the system hosting the Examiner, create a network share to make the main case folder available to other users on the network. The case folder is no longer assigned by default. The user creating the case creates the case folder. It is that folder that needs to be shared.

For this example, it is located at the root of the Windows system volume, and the pathname is:

C:\FTK-Cases.

**To share the case folder**

1. Before you can effectively share a folder in Windows you must make sure that network file sharing is enabled. Windows XP users should disable Simple File Sharing before proceeding. Windows Vista/7 users will find the option in the Sharing and Discovery section of the Network and Sharing Center. If you encounter any issues while enabling file sharing, please contact your IT administrator.
2. Open the *Properties* dialog for the case folder.
3. Click the **Sharing** tab to share the folder.
4. Edit the permissions on both the *Sharing* and *Security* tabs to allow the one authoritative user Full Control permissions.
5. Test connectivity to this share from the database system:

5a. Open a Windows Explorer window on the system hosting the database.

5b. Type \\*servername**sharename* in the address bar, where “servername” = the hostname of the Examiner host system, and “sharename” = the name of the share assigned in Step 1.

For example: If the name of the system hosting the Examiner is ForensicTower1 and you named the share “FTK-Cases” in Step #1 above, the UNC path would be **\\forensictower1\FTK-Cases**.

5c. Click **OK**. Check to see if the contents of the share can be viewed, and test the ability to create files and folders there as well.

## *Configure Database Services*

To ensure access to all the necessary resources, the services upon which the database relies must be configured to log on as a user with sufficient permissions to access those resources.

### To configure the database service(s) to Run As [ service account ]

1. On the database server system, open the Windows Services Management console:

   1a. Click **Start > Run**.

   1b. Type **services.msc**.

   1c. Press **Enter.**

2. Locate the following services:

   Oracle

   - Oracle TNS Listener service listed as **OracleFTK2TNSListener** or **OracleAccessDataDBTNSListener** (Found on Oracle System)
   - **OracleServiceFTK2** (Found on Oracle System)

   PostgreSQL

   - postgresql-x64-9.0

     or

   - postgresql-x86-9.0

3. Open the properties of the service and click the **Log On** tab.
4. Choose **This account**.
5. Click **Browse** to locate the service account username on the local system or domain. Ensure that “From this location” displays the appropriate setting for the user to be selected. Note that “Entire Directory” is used to search for a domain user account, while the name of your system will be listed for a workgroup system user.
6. In the object name box, type in the first few letters of the username and click **Check Names**. Highlight the desired username. Click **OK** when finished.
7. Enter the current password for this account and then enter it again in the *Confirm Password* box. Click **Apply** and then **OK**.
8. Repeat Steps #3-8 for each database service.
9. Restart database service(s) when finished.

## *Share the Backup Destination Folder*

Using the same steps as when sharing the main case folder, share the backup destination folder. Use the UNC path to this share when performing backups. For a two-box backup to work correctly, you must use a single UNC path that both the examiner, and the database application have read/write access to.

## *Test the New Configuration*

**To test the new configuration**

1. Launch the Case Manager and log in normally.
2. Select (highlight) the name of the case you want to backup.

   2a. Click **Case > Back up.**

   2b. Select a back up destination folder.

   **Note:** The path to the backup location must be formatted as a UNC path.

The *Data Processing* window opens, and when the progress bar turns green, the backup is complete. If the *Data Processing* window results in a red progress bar (sometimes accompanied by “Error 120”), the most likely cause is that the database service does not have permission to write to the backup location. Please double check all the steps listed in this document.

# Chapter 4

# Installing Additional Programs

You can install the following applications

- Language Selector (See Installing Language Selector on page 33.)
- Known File Filter - KFF (See Getting Started with KFF (Known File Filter) on page 35.)
- License Manager  (See Managing Security Devices and Licenses on page 71.)
- PRTK (See the *Password Recovery Toolkit and Distributed Network Attack User Guide*)
- Registry Viewer (See the *Registry Viewer User Guide*)
- Imager (See the *FTK Imager User Guide*)

## Installing Language Selector

To change to another supported language other than the default English (United States) that ships with FTK, Language Selector must be installed.

**To install Language Selector**

1. From the FTK install disc Autorun Main Menu, click **Install Other Products**, then click **Install Language Selector.**
2. The Language Selector Installer runs. Click **Next** to continue.
3. Read and accept the License Agreement. Click **Next** to continue.
4. Click **Finish**.

### Using Language Selector

Language Selector has a very simple interface.

**To run Language Selector**

1. Do one of the following:
   - Click **Start > All Programs > AccessData > Language Selector > Language Selector.**
   - Click the Language Selector Icon on your desktop.

2. Click the **Select Languages** drop-down to select the language to use. Languages to choose from are as follows: The “Products supporting this language” text box indicates the AccessData programs that will be affected by the language selection.

## Language Selector Supported Languages

| | |
|---|---|
| • Chinese (Simplified, PRC) | • Korean (Korea) |
| • Dutch (Netherlands) | • Portuguese (Brazil) |
| • English (United States) | • Russian (Russia) |
| • French (France) | • Spanish (Spain, Traditional Sort) |
| • German (Germany) | • Swedish (Sweden) |
| • Italian (Italy) | • Turkish (Turkey) |
| • Japanese (Japan) | |

The File menu contains two choices:

- Select Language
- Exit

The Help menu contains one choice:

- About — Provides version and copyright information.

3. Click **Save Settings** to save selections and close Language Selector.

Chapter 5

# Getting Started with KFF (Known File Filter)

This document contains the following information about understanding and getting started using KFF (Known File Filter).

**Important:** AccessData applications versions 5.6 and later use a new KFF architecture. If you are using one of the following applications version 5.6 or later, you must install and implement the new KFF architecture:

- Resolution1 (Resolution1 Platform, Resolution1 CyberSecurity, Resolution1 eDiscovery)
- Summation
- FTK-based products (FTK, FTK Pro, AD Lab, AD Enterprise)

See What has Changed in Version 5.6 on page 61.

## About KFF

KFF (Known File Filter) is a utility that compares the file hash values of known files against the files in your project. The known files that you compare against may be the following:

- Files that you want to ignore, such as operating system files
- Files that you want to be alerted about, such as malware or other contraband files

The hash values of files, such as MD5, SHA-1, etc., are based on the file’s content, not on the file name or extension. The helps you identify files even if they are renamed.

Using KFF during your analysis can provide the following benefits:

- Immediately identify and ignore 40-70% of files irrelevant to the project.
- Immediately identify known contraband files.

## Introduction to the KFF Architecture

There are two distinct components of the KFF architecture:

- KFF Data - The KFF data are the hashes of the known files that are compared against the files in your project. The KFF data is organized in KFF Hash Sets and KFF Groups. The KFF data can be comprised of hashes obtained from pre-configured libraries (such as NSRL) or custom hashes that you configure yourself.

  See Components of KFF Data on page 36.
- KFF Server - The KFF Server is the component that is used to store and process the KFF data against your evidence. The KFF Server uses the AccessData Elasticsearch Windows Service. After you install the KFF Server, you import your KFF data into it.

**Note:** The KFF database is no longer stored in the shared evidence database or on the file system in EDB format.

## Components of KFF Data

| Item | Description |
|---|---|
| **Hash** | The unique MD5 or SHA-1 hash value of a file. This is the value that is compared between known files and the files in your project. |
| **Hash Set** | A collection of hashes that are related somehow. The hash set has an ID, status, name, vendor, package, and version. In most cases, a set corresponds to a collection of hashes from a single source that have the same status. |
| **Group** | KFF Groups are containers that are used for managing the Hash Sets that are used in a project.<br>KFF Groups can contains Hash Sets as well as other groups.<br>Projects can only use a single KFF Group.  However, when configuring your project you can select a single KFF Group which can contains nested groups. |
| **Status** | The specified status of a hash set of the known files which can be either Ignore or Alert. When a file in a project matches a known file, this is the reported status of the file in the project. |
| **Library** | A pre-defined collection of hashes that you can import into the KFF Serve.<br>There are three pre-defined libraries:<br>● NSRL<br>● NDIC HashKeeper<br>● DHS<br>See About Pre-defined KFF Hash Libraries on page 38. |

| Item | Description |
|---|---|
| **Index/Indices** | When data is stored internally in the KFF Library, it is stored in multiple indexes or indices.<br>The following indices can exist:<br>● NSRL index<br>A dedicated index for the hashes imported from the NSRL library.<br>● NDIC index<br>A dedicated index for the hashes imported from the NDIC library.<br>● DHC index<br>A dedicated index for the hashes imported from the DHC library.<br>● KFF index<br>A dedicated index for the hashes that you manually create or import from other sources, such as CSV.<br>These indices are internal and you do not see them in the main application. The only place that you see some of them are in the KFF Import Tool.<br>See Using the KFF Import Utility on page 46.<br>The only time you need to be mindful of the indices is when you use the KFF binary format when you either export or import data.<br>See About CSV and Binary Formats on page 52. |

## About the Organization of Hashes, Hash Sets, and KFF Groups

Hashes, such as MD5, SHA-1, etc., are based on the file's content, not on the file name or extension.

You can also import hashes into the KFF Server in **.CSV** format.

For FTK-based products, you can also import hashes into the KFF Server that are contained in **.TSV**, **.HKE**, **.HKE.TXT**, **.HDI**, **.HDB**, **.hash**, **.NSRL**, or **.KFF** file formats.

You can also manually add hashes.

Hashes are organized into Hash Sets. Hash Sets usually include hashes that have a common status, such as Alert or Ignore.

Hash Sets must be organized into to KFF Groups before they can be utilized in a project.

## About Pre-defined KFF Hash Libraries

All of the pre-configured hash sets currently available for KFF come from three federal government agencies and are available in KFF libraries.

See About KFF Pre-Defined Hash Libraries on page 56.

You can use the following KFF libraries:

- NIST NSRL
  See About Importing the NIST NSRL Library on page 48.
- NDIC HashKeeper  (Sept 2008)
  See Importing the NDIC Hashkeeper Library on page 50.
- DHS (Jan 2008)
  See Importing the DHS Library on page 50.

It is not required to use a pre-configured KFF library in order to use KFF. You can configure or import custom hash sets. See your application’s *Admin Guide* for more information.

# *How KFF Works*

The Known File Filter (KFF) is a body of MD5 and SHA1 hash values computed from electronic files. Some pre-defined data is gathered and cataloged by several US federal government agencies or you can configure you own. KFF is used to locate files residing within project evidence that have been previously encountered by other investigators or archivists. Identifying previously cataloged (known) files within a project can expedite its investigation.

When evidence is processed with the MD5 Hash (and/or SHA-1 Hash) and KFF options, a hash value for each file item within the evidence is computed, and that newly computed hash value is searched for within the KFF data. Every file item whose hash value is found in the KFF is considered to be a known file.

**Note:** If two hash sets in the same group have the same MD5 hash value, they must have the same metadata. If you change the metadata of one hash set, all hash sets in the group with the same MD5 hash file will be updated to the same metadata.

The KFF data is organized into Groups and stored in the KFF Server. The KFF Server service performs lookup functions.

## Status Values

In order to accelerate an investigation, each known file can labeled as either Alert or Ignore, meaning that the file is likely to be forensically interesting (Alert) or uninteresting (Ignore). Other files have a status of Unknown.

The Alert/Ignore designation can assist the investigator to hone in on files that are relevant, and avoid spending inordinate time on files that are not relevant. Known files are presented in the Overview Tab’s File Status Container, under “KFF Alert files” and “KFF Ignorable.”

## Hash Sets

The hash values comprising the KFF are organized into hash sets. Each hash set has a name, a status, and a listing of hash values. Consider two examples. The hash set “ZZ00001 Suspected child porn” has a status of Alert and contains 12 hash values. The hash set “BitDefender Total Security 2008 9843” has a status of Ignore and contains 69 hash values. If, during the course of evidence processing, a file item’s hash value were found to belong to the “ZZ00001 Suspected child porn” set, then that file item would be presented in the KFF Alert files list. Likewise, if another file item’s hash value were found to belong to the “BitDefender Total Security 2008 9843” set, then that file would be presented in the KFF Ignorable list.

In order to determine whether any Alert file is truly relevant to a given project, and whether any Ignore file is truly irrelevant to a project, the investigator must understand the origins of the KFF’s hash sets, and the methods used to determine their Alert and Ignore status assignments.

You can install libraries of pre-defined hash sets or you can import custom hash sets. The pre-defined hash sets contain a body of MD5 and SHA1 hash values computed from electronic files that are gathered and cataloged by several US federal government agencies.

See About KFF Pre-Defined Hash Libraries on page 56.

## Higher Level Structure and Usage

Because hash set groups have the properties just described, and because custom hash sets and groups can be defined by the investigator, the KFF mechanism can be leveraged in creative ways. For example, the investigator may define a group of hash sets created from encryption software and another group of hash sets created from child pornography files and then apply only those groups while processing.

# About the KFF Server and Geolocation

In order to use the Geolocation Visualization feature in various AccessData products, you must use the KFF architecture and do the following:

- Install the KFF Server.
  See Installing the KFF Server on page 41.
- Install the  Geolocation (GeoIP) Data (this data  provide location data for evidence)
  See Installing the Geolocation (GeoIP) Data on page 51.
  From time to time, there will be updates available for the GeoIP data.
  See Installing KFF Updates on page 55.

If you are upgrading to 5.6 or later from an application 5.5 or earlier, you must install the new KFF Server and the updated Geolocation data.

# Installing the KFF Server

## *About Installing the KFF Server*

In order to use KFF, you must first configure an KFF Server.

For product versions 5.6 and later, you install a KFF Server by installing the AccessData Elasticsearch Windows Service.

Where you install the KFF Server depends on the product you are using with KFF:

- For FTK and FTK Pro applications, the KFF Server must be installed on the same computer that runs the Examiner.
- For all other applications, such as AD Lab, Resolution1, or Summation, the KFF Server can be installed on either the same computer as the application or on a remote computer. For large environments, it is recommended that the KFF Server be installed on a dedicated computer.

After installing the KFF Server, you configure the application with the location of the KFF Server.

See Configuring the Location of the KFF Server on page 42.

## *About KFF Server Versions*

The KFF Server (AccessData Elasticsearch Windows Service) may be updated from time to time. It is best to use the latest version.

| AccessData Elasticsearch Windows Service | Released | Installation Instructions |
|---|---|---|
| Version 1.3.2 | November 2014 with 5.6 versions of<br>● Resolution1<br>● Summation<br>● FTK-based products | See Installing the KFF Server Service on page 41. |

For applications 5.5 and earlier, the KFF Server component was version 1.2.7 and earlier.

### About Upgrading from Earlier Versions

If you have used KFF with applications versions 5.5 and earlier, you can migrate your legacy KFF data to the new architecture.

See Migrating Legacy KFF Data on page 43.

## *Installing the KFF Server Service*

For instructions on installing the AccessData Elasticsearch Windows Service, see Installing the AccessData Elasticsearch Windows Service (page 62).

# Configuring the Location of the KFF Server

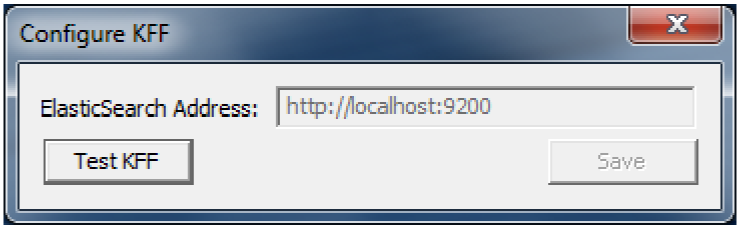
After installing the KFF Server, on the computer running the application, such as FTK, Lab, Summation, or Resolution1, you configure the location of the KFF Server.

Do one of the following:

- Configuring the KFF Server Location on FTK-based Computers (page 42)
- Configuring the KFF Server Location on Resolution1 and Summation Applications (page 42)

## *Configuring the KFF Server Location on FTK-based Computers*

Before using KFF with FTK, FTK Pro, Lab, or Enterprise, with KFF, you must configure the location of the KFF Server.



ElasticSearch Address: http://localhost:9200

**Important:** To configure KFF, you must be logged in with Admin privileges.

### To view or edit KFF configuration settings

1. In the *Case Manager*, click **Tools > Preferences > Configure KFF**.
2. You can set or view the address of the KFF Server.
   - If you installed the KFF Server on the same computer as the application, this value will be localhost.
   - If you installed the KFF Server on a different computer, identify the KFF server.
3. Click **Test** to validate communication with the KFF Server.
4. Click **Save**.
5. Click **OK**.

## *Configuring the KFF Server Location on Resolution1 and Summation Applications*

When using the KFF Server with Summation or Resolution1 applications, two configuration files must point to the KFF Server location.

These setting are configured automatically during the KFF Server installation. If needed, you can verify the settings.

However, if you change the location of the KFF Server, do the following to specify the location of the KFF Server.

1. Configure AdgWindowsServiceHost.exe.config:

   1a. On the computer running the application (for example, the server running Summation), go to C:\Program Files\AccessData\Common\FTK Business Services.

   1b. Open AdgWindowsServiceHost.exe.config.

1c. Modify the line <add key="KffElasticSearchUrl" value="http://localhost:9200" />.

1d. Change *localhost* to be the location of your KFF server (you can use hostname or IP).

1e. Save and close file.

1f. Restart the business services common service.

2. Configure AsyncProcessingServices web.config:

2a. On the computer running the application (for example, the server running Summation), go to C:\Program Files\AccessData\AsyncProcessingServices.

2b. Open web.config.

2c. Modify the line <add key="KffElasticSearchUrl" value="http://localhost:9200" />.

2d. Change *localhost* to be the location of your KFF server (you can use hostname or IP).

2e. Save and close file.

2f. Restart the AsyncProcessing service.

# Migrating Legacy KFF Data

If you have used KFF with applications versions 5.5 and earlier, you can migrate that data from the legacy KFF Server to the new KFF Server architecture.

**Important:** Applications version 5.6 and later can only use the new KFF architecture that was introduced in 5.6. If you want to use KFF data from previous versions, you must migrate the data.

**Important:** If you have NSRL, NDIC, or DHS data in your legacy data, those sets will not be migrated. You must re-import them using the 5.6 versions or later of those libraries. Only legacy custom KFF data will be migrated.

Legacy KFF data is migrated to KFF Groups and Hash Sets on the new KFF Server.

Because KFF Templates are no longer used, they will be migrated as KFF Groups, and the groups that were under the template will be added as sub-groups.

You migrate data using the KFF Migration Tool. To use the KFF Migration Tool, you identify the following:

- The Storage Directory folder where the legacy KFF data is located.

  This was folder was configured using the KFF Server Configuration utility when you installed the legacy KFF Server. If needed, you can use this utility to view the KFF Storage Directory. The default location of the KFF_Config.exe file is Program Files\AccessData\KFF.

- The URL of the new KFF Server ( the computer running the AccessData Elastic Search Windows Service)

  This is populated automatically if the new KFF Server has been installed.

### To install the KFF Migration Tool

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the autorun.exe.
2. Click the *64 bit* or *32 bit* **Install KFF Migration Utility**.
3. Complete the installation wizard.

### To migrate legacy KFF data

1. On the legacy KFF Server, you must stop the KFF Service.

   You can stop the service manually or use the legacy KFF Config.exe utility.

2. On the new KFF Server, launch the KFF Migration Tool.
3. Enter the directory of the legacy KFF data.
4. The URL of Elasticsearch should be listed.
5. Click **Start**.
6. When completed, review the summary data.

# Importing KFF Data

## *About Importing KFF Data*

You can import hashes and KFF Groups that have been previous configured.

You can import KFF data in one of the following formats:

**KFF Data sources that you can import**

| Source | Description |
|---|---|
| Pre-configured KFF libraries | You can import KFF data from the following pre-configured libraries<br>● NIST NSRL<br>● NDIC HashKeeper<br>● DHS<br>To import KFF libraries, it is recommended that you use the KFF Import Utility.<br>See Using the KFF Import Utility on page 46.<br>See Importing Pre-defined KFF Data Libraries on page 48.<br>See KFF Library Reference Information on page 56. |
| Custom Hash Sets and KFF Groups | You can import custom hashes from CSV files.<br>See About the CSV Format on page 52.<br>For FTK-based products, you can also import custom hashes from the following file types:<br>● Delimited files (CSV or TSV)<br>● Hash Database files (HDB)<br>● Hashkeeper files (HKE)<br>● FTK Exported KFF files (KFF)<br>● FTK Supported XML files (XML)<br>● FTK Exported Hash files (HASH)<br>To import these kinds of files, use the KFF Import feature in your application.<br>See *Using the Known File Feature* chapter. |
| KFF binary files | You can import KFF data that was exported in a KFF binary format, such an an archive of a KFF Server.<br>See About CSV and Binary Formats on page 52.<br>When you import a KFF binary snapshot, you must be running the same version of the KFF Server as was used to create the binary export.<br>To import KFF binary files, it is recommend that you use the KFF Import Utility.<br>See Using the KFF Import Utility on page 46. |

## About KFF Data Import Tools

When you import KFF data, you can use one of two tools:

**KFF Data Import Tools**

| | |
|---|---|
| The application’s Import feature | The KFF management feature in the application lets you import both .CSV and KFF Binary formats. Use the application to import .CSV files.<br>See *Using the Known File Feature* chapter.<br>Even though you can import KFF binary files using the application, it is recommend that you use the KFF Import Utility. |
| KFF Import Utility | It is recommended that you use the KFF Import Utility to import KFF binary files.<br>See Using the KFF Import Utility on page 46. |

## About Default Status Values

When you import KFF data, you configure a default status value of Alert or Ignore. When adding Hash Sets to KFF Groups, you can configure the KFF Groups to use the default status values of the Hash Set or you can configure the KFF Group with a status that will override the default Hash Set values.

See Components of KFF Data on page 36.

## About Duplicate Hashes

If multiple Hash Set files containing the same Hash identifier are imported into a single KFF Group, the group keeps the last Hash Set’s metadata information, overwriting the previous Hash Sets’ metadata. This only happens within an individual group and not across multiple groups.

# *Using the KFF Import Utility*

## About the KFF Import Utility

Due to the large size of of some KFF data, a stand-alone KFF Import utility is available to use to import the data. This KFF Import utility can import large amounts of data faster then using the import feature in the application.

It is recommend that you install and use the KFF Import utility to import the following:

- NSRL, DHC, and NIST libraries
- An archive of a KFF Server that was exported in the binary format

After importing NSRL, NDIC, or DHS libraries, these indexes are displayed in the *Currently Installed Sets* list.

See Components of KFF Data on page 36.

You can also use the KFF Import Utility to remove the NSRL, NDIC, or DHS indexes that you have imported.

An archive of a KFF Server, which is the exported *KFF Index*, is not shown in the list.

## Installing the KFF Import Utility

You should use the KFF Import Utility to import some kinds of KFF data.

### To install the KFF Import Utility

1. On the computer where you have installed the KFF Server, access the KFF Installation disc, and run the `autorun.exe`.
2. Click the *64 bit* or *32 bit* **Install KFF Import Utility**.
3. Complete the installation wizard.

## Importing a KFF Server Archive Using the KFF Import Utility

You can import an archive of a KFF Server that you have exported using the binary format.

If you are importing a pre-defined KFF Library, see Importing Pre-defined KFF Data Libraries (page 48).

### To import using the KFF Import Utility

1. On the KFF Server, open the KFF Import Utility.
2. To test the connection to the KFF Server's Elasticsearch service at the displayed URL, click **Connect**.
   If it connects correctly, no error is shown.
   If it is not able to connect, you will get the following error: Failed after retrying 10 times: 'HEAD accessdata_threat_indicies'.
3. To import, click **Import**.
4. Click **Browse**.
5. Browse to the folder that contains the KFF binary files.
   Specifically, select the folder that contains the Export.xml file.
6. Click **Start**.
7. Close the dialog.

## Removing Pre-defined KFF Libraries Using the KFF Import Utility

You can remove a pre-defined KFF Library that you have previously imported.

You cannot see or remove existing custom KFF data (the *KFF Index*).

### To remove pre-defined KFF Libraries

1. On the KFF Server, open the KFF Import Utility.
2. Select the library that you want to remove.
3. Click **Remove**.

# *Importing Pre-defined KFF Data Libraries*

## About Importing Pre-defined KFF Data Libraries

After you install the KFF Server, you can import pre-defined NIST NSRL, NDIC HashKeeper, and DHS data libraries.

See About Pre-defined KFF Hash Libraries on page 38.

In versions 5.5 and earlier, you installed these using an executable file. In versions 5.6 and later, you must import them. It is recommend that you use the KFF Import Utility.

After importing pre-defined KFF Libraries, you can remove them from the KFF Server.

See Removing Pre-defined KFF Libraries Using the KFF Import Utility on page 47.

See the following sections:

- About Importing the NIST NSRL Library (page 48)
- Importing the NDIC Hashkeeper Library (page 50)
- Importing the DHS Library (page 50)

## About Importing the NIST NSRL Library

You can import the NSRL library into your KFF Server. During the import, two KFF Groups are created: NSRL_Alert and NSRL_Ignore. In FTK-based products, these two groups are automatically added to the Default KFF Group.

The NSRL libraries are updated from time to time. To import and maintain the NSRL data, you do the following:

**Process for Importing and Maintaining the NIST NSRL Library**

| | |
|---|---|
| 1. Import the complete NSRL library. | You must first install the most current complete NSRL library. You can later add updates to it.<br>To access and import the complete NSRL library, see Importing the Complete NSRL Library (page 49) |
| 2. Import updates to the library | When updates are made available, import the updates to bring the data up-to date.<br>See Installing KFF Updates on page 55.<br>**Important:** In order to use the NSRL updates, you must first import the complete library. When you install an NSRL update, you must keep the previous NSRL versions installed in order to maintain the complete set of NSRL data. |

**Available NRSL library files (new format)**

| NSRL Library Release | Released | Information |
|---|---|---|
| Complete library version 2.45 (source .ZIP file) | Nov 2014 | For use only with applications version 5.6 and later.<br>Contains the full NSRL library up through update 2.45.<br>See Importing the Complete NSRL Library on page 49. |

**Available Legacy NRSL library files**

| Legacy NSRL Library Release | Released | Information |
|---|---|---|
| version 2.44<br>(.EXE file) | Nov 2013 | For use with the legacy KFF Server that was used with applications versions 5.5 and earlier.<br>Contains the full NSRL library up through update 2.44.<br>Install this library first.<br>Note: NSRL updates for the legacy KFF format will end in the 2nd quarter of 2015. From that time, NSRL updates will only be provided in the new format. |

## Importing the Complete NSRL Library

To add the NSRL library to your KFF Library, you import the data. You start by importing the full NSRL library. You can then import any updates as they are available.

See About Importing the NIST NSRL Library on page 48.

See Installing KFF Updates on page 55.

**Important:** The complete NSRL library data is contained in a large (3.4 GB) .ZIP file. When expanded, the data is about 18 GB. Make sure that your file system can support files of this size.

**Important:** Due to the large amount of NSRL data, it will take 3-4 hours to import the NSRL data using the KFF Import Utility. If you import from within an application, it will take even longer.

### To install the NSRL complete library

1. Extract the NSRLSOURCE_2.45.ZIP file from the KFF Installation disc.
2. On the KFF Server, launch the *KFF Import Utility*.

   See Installing the KFF Import Utility on page 47.
3. Click **Import**.
4. Click **Browse**.
5. Browse to and select the NSRLSource_2.45 folder that contains the **NSRLFile.txt** file.

   (Make sure you are selecting the folder and not drilling into the folder to select an individual file. The import process will drill into the folder to get the proper files for you.)
6. Click **Select Folder**.
7. Click **Start**.
8. When the import is complete, click **OK**.
9. Close the *Import Utility* dialog and the NSRL library will be listed in the *Currently Installed Sets*.

## Importing the NDIC Hashkeeper Library

You can import the Hashkeeper 9.08 library.

For application versions 5.6 and later, these files are stored in the KFF binary format.

### To import the Hashkeeper library

1. Have access the NDIC source files by download the ZIP file from the web:
   1a. Go to  http://www.accessdata.com/product-download.
   1b. **Click Known File Filter (KFF)**.
   1c. For *KFF Hash Sets*, click **Download Page**.
   1d. Click the KFF NDIC library that you want to download.
2. Extract the ZIP file.
3. On the KFF Server, launch the *KFF Import Utility*.
   See Installing the KFF Import Utility on page 47.
4. Click **Import**.
5. Click **Browse**.
6. Browse to and select the NDIC source folder that contains the **Export.xml** file.
   (Make sure you are selecting the folder and not drilling into the folder to select an individual file. The import process will drill into the folder to get the proper files for you.)
7. Click **Select Folder**.
8. Click **Start**.
9. When the import is complete, click **OK**.
10. Close the *Import Utility* dialog and the NDIC library will be listed in the *Currently Installed Sets*.

## Importing the DHS Library

You can import the DHS 1.08 library.

For application versions 5.6 and later, these files are stored in the KFF binary format.

### To import the DHS library

1. Have access the NDIC source files by download the ZIP file from the web:
   1a. Go to  http://www.accessdata.com/product-download.
   1b. **Click Known File Filter (KFF)**.
   1c. For *KFF Hash Sets*, click **Download Page**.
   1d. Click the KFF DHS library that you want to download.
2. Extract the ZIP file.
3. On the KFF Server, launch the *KFF Import Utility*.
   See Installing the KFF Import Utility on page 47.
4. Click **Import**.
5. Click **Browse**.
6. Browse to and select the DHS source folder that contains the **Export.xml** file.
   (Make sure you are selecting the folder and not drilling into the folder to select an individual file. The import process will drill into the folder to get the proper files for you.)

7. Click **Select Folder**.
8. Click **Start**.
9. When the import is complete, click **OK**.
10. Close the *Import Utility* dialog and the DHS library will be listed in the *Currently Installed Sets*.

## *Installing the Geolocation (GeoIP) Data*

Geolocation (GeoIP) data is used for the Geolocation Visualization feature of several AccessData products.

See About the KFF Server and Geolocation on page 40.

You can also check for and install GeoIP data updates.

If you are upgrading to 5.6 or later from an application 5.5 or earlier, you must install the new KFF Server and the updated Geolocation data.

The Geolocation data that was used with versions 5.5 and earlier is version 1.0.1 or earlier.

The Geolocation data that is used with versions 5.6 and later is version 2014.10 or later.

### To install the Geolocation IP Data

1. On the copmuter where you have installed the KFF Server, access the KFF Installation disc, and run the `autorun.exe`.
2. Click the *64 bit* or *32 bit* **Install Geolocation Data**.
3. Complete the installation wizard.

# About CSV and Binary Formats

When you export and import KFF data, you can use one of two formats:

- CSV
- KFF Binary

## About the CSV Format

When you use the .CSV format, you use a single .CSV file. The .CSV file contains the hashes that you import or export.

When you export to a CSV file, it contains the hashes as well as all of the information about any associated Hash Sets and KFF Groups. You can only use the CSV format when exporting individual Hash Sets and KFF Groups.

When you import using a CSV file, it can be a simple file containing only the hashes of files, or it can contain additional information about Hash Sets and KFF Groups.

However, CSV files will usually take a little longer to export and import.

To view the sample of a .CSV file that contains binaries and Hash Sets and KFF Groups, perform a CSV export and view the file in Excel.

You can also use the format of CSV files that were exported in previous versions.

To import .CSV files, use the application’s KFF Import feature.

## About the KFF Binary Format

When you use the KFF binary format, you use a set of files that are in an internal KFF Server (Elasticsearch) format that is referred to as a Snapshot. The binary format is essentially a snapshot of one of the indices contained in the KFF Server. You can only have one binary format snapshot for each index.

See Components of KFF Data on page 36.

The benefit of the binary format is that it is able to support larger amounts of data than the CSV format. For large data sets, the binary format will export and import faster than the CSV format.

For example, when you import the DHC or NDIC Hashkeeper libraries, they are imported from a KFF binary format.

If you export your custom Hash Sets or KFF Groups using the KFF binary format, everything in the *KFF Index* is included.

See About Choosing to Export in CSV or KFF Binary Format on page 53.

When exporting in a Binary format, you specify an existing parent folder and then the name of a new sub-folder for the binary data. The new sub-folder must not previously exist and will be created by the export process.

After export, the binary export folder contains the following:

- **Indices** sub-folder - The folder contains the exported KFF data
- **Export.xml** - This file is the only file that is not an Elasticsearch file and is created by the export feature and contains the KFF Group and Hash Set definitions for the index.

- `Index` - an index file generated by Elasticsearch
- `metadata-snaphot` file with the data and time it was created
- `snapshot-snaphot` file with the data and time it was created

**Note:** The binary format is dependent on the version of the KFF Server. When exporting and importing the binary format, the systems must be using the same version of the KFF Server.

When new versions of the KFF Server are released in the future, an upgrade process will also be provided.

## About Choosing to Export in CSV or KFF Binary Format

When you export your own KFF data, you have the option of using either the CSV or the binary format. The results are different based on the format that you use:

| | |
|---|---|
| **CSV format** | |
| Exporting in CSV format | When you export KFF data using the CSV format, you can export specific specific pieces of KFF data, such as one or more Hash Sets or one or more KFF Groups.<br>The exported data is contained in one .CSV file.<br>The benefits of the CSV format are that CSV files can be easily viewed and can be manually edited. They are also less dependent on the version of the KFF Server. |
| Importing from CSV format | When you import a CSV file, the data in the file is data is added to your existing KFF data that is in the *KFF Index*.<br>See Components of KFF Data on page 36.<br>For example, suppose you started by manually created four Hash Sets and one KFF Group. That would be the only contents in your *KFF Index*. Suppose you import a .CSV file that contains five hash sets and two KFF Groups. They will be added together for a total of nine Hash Sets and three KFF Groups.<br>To import .CSV files, use the KFF Import feature in your application.<br>See *Using the Known File Feature* chapter. |
| **KFF binary format** | |
| Exporting in KFF binary format | If you export your KFF data using the KFF binary format, all of the data that you have in the *KFF Index* will be exported together. You cannot use this format to export individual Hash Sets or KFF Groups.<br>See Components of KFF Data on page 36.<br>You will only want to use this format if you intend to export all of the data in the *KFF Index* and import it as a whole. This can be useful in making an archive of your KFF data or copying KFF data from one KFF Server to another.<br>Because NSRL, NIST, and DHC data is contained in their own indexes, when you do an export using this format, those sets are not included. Only the data in the *KFF Index* is exported. |

| | |
|---|---|
| Importing KFF binary format | **IMPORTANT:** When you import a KFF binary format, it will import the complete index and will *replace* any data that is currently in that index on the KFF Server.<br>For example, if you import the DHC library, and then later you import the DHC library again, the DHC index will be replaced with the new import.<br>If you have a KFF binary format snapshot of custom KFF data (which would have come from a binary format export) it will replace all KFF data that already exists in your *KFF Index*.<br>For example, suppose you manually created four Hash Sets and one KFF Group. Suppose you then import a binary format that has five hash sets and two KFF Groups. The binary format will be imported as a complete index and will replace the existing data. The result will be only be the imported five Hash Sets and two KFF libraries.<br>When importing KFF binary files, it is recommend that you use the KFF Import Utility.<br>See Installing the KFF Import Utility on page 47. |

# Installing KFF Updates

From time to time, AccessData will release updates to the KFF Server and the KFF data libraries.

Some of the KFF data updates may require you to update the version of the KFF Server.

To check for updates, do the following:

1. Go to the AccessData Product Download website at http://www.accessdata.com/product-download.
2. On the *Product Downloads* page, click **Known File Filter (KFF)**.
3. Check for updates.
   - See About KFF Server Versions on page 41.
   - See About Importing the NIST NSRL Library on page 48.
4. If there are updates, download them.
5. Install or import the updates.

# Uninstalling KFF

You can uninstall KFF application components independently of the KFF Data.

| Main version | Description |
|---|---|
| Applications 5.6 and later | For applications version 5.6 and later, you uninstall the following components:<br>● *AccessData Elasticsearch Windows Service* (KFF Server) v1.2.7 and later<br>Note: Elasticsearch is used by multiple features in various applications, use caution when uninstalling this service or the related data.<br>● *AccessData KFF Import Utility* (v5.6 and later)<br>● *AccessData KFF Migration Tool* (v1.0 and later)<br>● *AccessData Geo Location Data* (v2014.10 and later)<br>Note: This component is not used by the KFF feature, but with the KFF Server for the the geolocation visualization feature.<br>The location of the KFF data is configured when the *AccessData Elasticsearch Windows Service* was installed. By default, it is lactated at C:\Program Files\AccessData\Elacticsearch\Data. |
| Applications 5.5 and earlier | For applications version 5.5 and earlier, you can uninstall the following components:<br>● KFF Server (v1.2.7 and earlier)<br>Note: The KFF Server is also used by the geolocation visualization feature.<br>● AccessData Geo Location Data (1.0.1 and earlier)<br>This component is not used by the KFF feature, but with the KFF Server for the the geolocation visualization feature.<br>The location of the KFF data was configured when the *KFF Server* was installed. You can view the location of the data by running the *KFF.Config.exe* on the KFF Server.<br>If you are upgrading from 5.5 to 5.6, you can migrate your KFF data before uninstalling the KFF Server. |

# KFF Library Reference Information

## *About KFF Pre-Defined Hash Libraries*

This section includes a description of pre-defined hash collections that can be added as AccessData KFF data.

The following pre-defined libraries are currently available for KFF and come from one of three federal government agencies:

- NIST NSRL (The default library installed with KFF)
- NDIC HashKeeper (An optional library that can be downloaded from the AccessData Downloads page)
- DHS (An optional library that can be downloaded from the AccessData Downloads page)

**Note:** Because KFF is now multi-sourced, it is no longer maintained in HashKeeper format. Therefore, you cannot modify KFF data in the HashKeeper program. However, the HashKeeper format continues to be compatible with the AccessData KFF data.

### Use the following information to help identify the origin of any hash set within the KFF

- The NSRL hash sets do not begin with “ZZN” or “ZN”. In addition, in the AD Lab KFF, all the NSRL hash set names are appended (post-fixed) with multi-digit numeric identifier. For example: “Password Manager & Form Filler 9722.”
- All HashKeeper Alert sets begin with “ZZ”, and all HashKeeper Ignore sets begin with “Z”. (There are a few exceptions. See below.) These prefixes are often followed by numeric characters (“ZZN” or “ZN” where N is any single digit, or group of digits, 0-9), and then the rest of the hash set name. Two examples of HashKeeper Alert sets are:
  - “ZZ00001 Suspected child porn”
  - “ZZ14W”

  An example of a HashKeeper Ignore set is:
  - “Z00048 Corel Draw 6”
- The DHS collection is broken down as follows:
  - In 1.81.4 and later there are two sets named “DHS-ICE Child Exploitation JAN-1-08 CSV” and “DHS-ICE Child Exploitation JAN-1-08 HASH”.
  - In AD Lab there is just one such set, and it is named “DHS-ICE Child Exploitation JAN-1-08”.

Once an investigator has identified the vendor from which a hash set has come, he/she may need to consider the vendor’s philosophy on collecting and categorizing hash sets, and the methods used by the vendor to gather hash values into sets, in order to determine the relevance of Alert (and Ignore) hits to his/her project. The following descriptions may be useful in assessing hits.

## NIST NSRL

The NIST NSRL collection is described at: http://www.nsrl.nist.gov/index.html. This collection is much larger than HashKeeper in terms of the number of sets and the total number of hashes. It is composed entirely of hash sets being generated from application software. So, all of its hash sets are given Ignore status by AccessData staff except for those whose names make them sound as though they could be used for illicit purposes.

The NSRL collection divides itself into many sub-collections of hash sets with similar names. In addition, many of these hash sets are “empty”, that is, they are not accompanied by any hash values. The size of the NSRL collection, combined with the similarity in set naming and the problem of empty sets, allows AccessData to modify (or selectively alter) NSRL’s own set names to remove ambiguity and redundancy.

Find contact info at http://www.nsrl.nist.gov/Contacts.htm.

## NDIC HashKeeper

NDIC’s HashKeeper collection uses the Alert/Ignore designation. The Alert sets are hash values contributed by law enforcement agents working in various jurisdictions within the US - and a few that apparently come from Luxemburg. All of the Alert sets were contributed because they were believed by the contributor to be connected to child pornography. The Ignore sets within HashKeeper are computed from files belonging to application software.

During the creation of KFF, AccessData staff retains the Alert and Ignore designations given by the NDIC, with the following exceptions. AccessData labels the following sets Alert even though HashKeeper had assigned them as Ignore: “Z00045 PGP files”, “Z00046 Steganos”, “Z00065 Cyber Lock”, “Z00136 PGP Shareware”, “Z00186 Misc Steganography Programs”, “Z00188 Wiping Programs”. The names of these sets may suggest the intent to conceal data on the part of the suspect, and AccessData marks them Alert with the assumption that investigators would want to be “alerted” to the presence of data obfuscation or elimination software that had been installed by the suspect.

The following table lists actual HashKeeper Alert Set origins:

**A Sample of HashKeeper KFF Contributions**

| Hash | Contributor | Location | Contact Information | Case/Source |
|---|---|---|---|---|
| ZZ00001 Suspected child porn | Det. Mike McNown & Randy Stone | Wichita PD | | |
| ZZ00002 Identified Child Porn | Det. Banks | Union County (NJ) Prosecutor's Office | (908) 527-4508 | case 2000S-0102 |
| ZZ00003 Suspected child porn | Illinois State Police | | | |
| ZZ00004 Identified Child Porn | SA Brad Kropp, AFOSI, Det 307 | | (609) 754-3354 | Case # 00307D7-S934831 |
| ZZ00000, suspected child porn | NDIC | | | |

**A Sample of HashKeeper KFF Contributions (Continued)**

| Hash | Contributor | Location | Contact Information | Case/Source |
|---|---|---|---|---|
| ZZ00005 Suspected Child Porn | Rene Moes, Luxembourg Police | | rene.moes@police.etat.lu | |
| ZZ00006 Suspected Child Porn | Illinois State Police | | | |
| ZZ00007b Suspected KP (US Federal) | | | | |
| ZZ00007a Suspected KP Movies | | | | |
| ZZ00007c Suspected KP (Alabama 13A-12-192) | | | | |
| ZZ00008 Suspected Child Pornography or Erotica | Sergeant Purcell | Seminole County Sheriff's Office (Orlando, FL, USA) | (407) 665-6948, dpurcell@seminolesheriff.org | suspected child pornogrpahy from 20010000850 |
| ZZ00009 Known Child Pornography | Sergeant Purcell | Seminole County Sheriff's Office (Orlando, FL, USA) | (407) 665-6948, dpurcell@seminolesheriff.org | 200100004750 |
| ZZ10 Known Child Porn | Detective Richard Voce CFCE | Tacoma Police Department | (253)594-7906, rvoce@ci.tacoma.wa.us | |
| ZZ00011 Identified CP images | Detective Michael Forsyth | Baltimore County Police Department | (410)887-1866, mick410@hotmail.com | |
| ZZ00012 Suspected CP images | Sergeant Purcell | Seminole County Sheriff's Office (Orlando, FL, USA) | (407) 665-6948, dpurcell@seminolesheriff.org | |
| ZZ0013 Identified CP images | Det. J. Hohl | Yuma Police Department | 928-373-4694 | YPD02-70707 |
| ZZ14W | Sgt Stephen May | | Tamara.Chandler@oag.state.tx.us, (512)936-2898 | TXOAG 41929134 |
| ZZ14U | Sgt Chris Walling | | Tamara.Chandler@oag.state.tx.us, (512)936-2898 | TXOAG 41919887 |
| ZZ14X | Sgt Jeff Eckert | | Tamara.Chandler@oag.state.tx.us, (512)936-2898 | TXOAG Internal |

**A Sample of HashKeeper KFF Contributions (Continued)**

| Hash | Contributor | Location | Contact Information | Case/Source |
|---|---|---|---|---|
| ZZ14I | Sgt Stephen May | | Tamara.Chandler@oag.state.tx.us, (512)936-2898 | TXOAG 041908476 |
| ZZ14B | Robert Britt, SA, FBI | | Tamara.Chandler@oag.state.tx.us, (512)936-2898 | TXOAG 031870678 |
| ZZ14S | Sgt Stephen May | | Tamara.Chandler@oag.state.tx.us, (512)936-2898 | TXOAG 041962689 |
| ZZ14Q | Sgt Cody Smirl | | Tamara.Chandler@oag.state.tx.us, (512)936-2898 | TXOAG 041952839 |
| ZZ14V | Sgt Karen McKay | | Tamara.Chandler@oag.state.tx.us, (512)936-2898 | TXOAG 41924143 |
| ZZ00015 Known CP Images | Det. J. Hohl | Yuma Police Department | 928-373-4694 | YPD04-38144 |
| ZZ00016 | Marion County Sheriff's Department | | (317) 231-8506 | MP04-0216808 |

The basic rule is to always consider the source when using KFF in your investigations. You should consider the origin of the hash set to which the hit belongs. In addition, you should consider the underlying nature of hash values in order to evaluate a hit’s authenticity.

## Higher Level KFF Structure and Usage

Since hash set groups have the properties just described (and because custom hash sets and groups can be defined by the investigator) the KFF mechanism can be leveraged in creative ways. For example:

- You could define a group of hash sets created from encryption software and another group of hash sets created from child pornography files. Then, you would apply only those groups while processing.
- You could also use the Ignore status. You are about to process a hard drive image, but your search warrant does not allow inspection of certain files within the image that have been previously identified. You could do the following and still observe the warrant:

  5a. Open the image in Imager, navigate to each of the prohibited files, and cause an MD5 hash value to be computed for each.

  5b. Import these hash values into custom hash sets (one or more), add those sets to a custom group, and give the group Ignore status.

  5c. Process the image with the MD5 and KFF options, and with AD_Alert, AD_Ignore, and the new, custom group selected.

5d. During post-processing analysis, filter file lists to eliminate rows representing files with Ignore status.

## Hash Set Categories

The highest level of the KFF's logical structure is the categorizing of hash sets by owner and scope. The categories are AccessData, Project Specific, and Shared.

**Hash Set Categories**

| Category | Description |
|---|---|
| AccessData | The sets shipped with as the Library. Custom groups can be created from these sets, but the sets and their status values are read only. |
| Project Specific | Sets and groups created by the investigator to be applied only within an individual project. |
| Shared | Sets and groups created by the investigator for use within multiple projects all stored in the same database, and within the same application schema. |

**Important:** Coordination among other investigators is essential when altering Shared groups in a lab deployment. Each investigator must consider how other investigators will be affected when Shared groups are modified.

# What has Changed in Version 5.6

WIth the 5.6 release of Resolution1, Summation, and FTK-based products, the KFF feature has been updated.

If you used KFF with applications version 5.5 or earlier, you will want to be aware of the following changes in the KFF functionality.

## Changes from version 5.5 to 5.6

| Item | Description |
|---|---|
| KFF Server | KFF Server now runs a different service.<br>● In 5.5 and earlier, the KFF Server ran as the *KFF Server* service.<br>● In 5.6 and later, the KFF Server uses the *AccessData Elasticsearch Windows Service*.<br>For applications version 5.6 and later, all KFF data must be created in or imported into the new KFF Server . |
| KFF Migration Tool | This is a new tool that lets you migrate custom KFF data from 5.5 and earlier to the new KFF Server.<br>NIST NSRL, NDIC HashKeeper, or DHS library data from 5.5 will not be migrated. You must re-import it.<br>See Migrating Legacy KFF Data on page 43. |
| KFF Import Utility | This is a new utility that lets you import large amounts of KFF data quicker than using the import feature in the application.<br>See Using the KFF Import Utility on page 46. |
| KFF Libraries, Templates, and Groups | In 5.5, all Hash Sets were configured within KFF Libraries. KFF Libraries could then contain KFF Groups and KFF Templates.<br>KFF Libraries and Templates have been eliminated. You now simply create or import KFF Groups and add Hash Sets to the groups.<br>You can now nest KFF Groups. |
| NIST NSRL, NDIC HashKeeper, or DHS libraries | In 5.5 and earlier, to use these libraries, you ran an installation wizard for each library. You now import these libraries using the KFF Import Utility.<br>See About Importing Pre-defined KFF Data Libraries on page 48. |
| Import Log | FTK-based products no longer include the Import Log.<br>Resolution1 and Summation products did not have it previously. |
| Export | When you export KFF data you can now choose two formats:<br>● CSV format which replaced XML format<br>● A new binary format<br>See About CSV and Binary Formats on page 52. |

Chapter 6

# Installing the AccessData Elasticsearch Windows Service

## About the Elasticsearch Service

The AccessData Elasticsearch Windows Service is used by multiple features in multiple applications, including the following:

- ThreatBridge in Resolution1
- Mobile Threat Monitoring in Resolution1
- KFF (Known File Filter) in all applications
- Visualization Geolocation in all applications

The AccessData Elasticsearch Windows Service uses the Elasticsearch open source search engine.

### *Prerequisites*

- For adequate performance, you should install the AccessData Elasticsearch Windows Service on a dedicated computer that is different from the computer running the application that uses it.

  A single instance of an AccessData Elasticsearch Windows Service is usually sufficient to support multiple features. However, if your network is extensive, you may want to install the service on multiple computers on the network. Consult with support for the best configuration for your organization's network.
- You can install the AccessData Elasticsearch Windows Service on 32-bit or 64-bit computers.
- 16 GB of RAM or higher
- Microsoft .NET Framework 4

  To install  the AccessData Elasticsearch Windows Service, Microsoft .NET Framework 4 is required. If you do not have .NET installed, it will be installed automatically.

# Installing the Elasticsearch Service

## *Installing the Service*

**To install the AccessData Elasticsearch Windows Service**

1. Click the the AccessData Elasticsearch Windows Service installer.

   It is avaialable on the KFF Installation disc by clicking *autorun.exe*.
2. Accept the License Agreement and click **Next**.
3. On the *Destination Folder* dialog, click **Next** to install to the folder, or click **Change** to install to a different folder.

   This is where the Elasticsearch folder with the Elasticsearch service is installed.
4. On the *Data Folder* dialog, click **Next** to install to the folder, or click **Change** to install to a different folder.

   This is where the Elasticsearch data is stored.

   **Note:** This folder may contain up to 10GB of data.
5. (For use with KFF) In the *User Credentials* dialog, you can configure credentials to access KFF Data files that you want to import if they exist on a different computer.

   This provides the credentials for the Elasticsearch service to use in order to access a network share with a user account that has permissions to the share.

   Enter the user name, the domain name, and the password. If the user account is local, do not enter any domain value, such as localhost. Leave it blank instead.
6. In the *Allow Remote Communication* dialog, enter the IP address(es) of any machine(s) that will have ThreatBridge installed. If you plan on installing ThreatBridge on the same server as the AccessData Elasticsearch Windows Service, click **Next**.
7. *Select Enable Remote Communication*.

   **Note:** If Enable Remote Communication is selected, a firewall rule will be created to allow communication to the AccessData Elasticsearch Windows Service service for every IP address added to the IP Address field. If no IP addresses are listed, then ANY IP address will be able to access the AccessData Elasticsearch Windows Service.
8. In the following *Allow Remote Communication* dialog, accept the default HTTP and Transport TCP Port values and click **Next**. However, if there are conflicts with these ports on the network, change the values to use other ports.
9. The *Configuration 1* dialog contains the following fields:
   - **Cluster name** - This field automatically populates with the system's name.
   - **Node name** - This field automatically populates with the system's name.

   **Note:** If installing the AccessData Elasticsearch Windows Service on more than one system, allow the first system to install with the system's name in the cluster and the node fields. In the second and subsequent systems, enter the first system's name in the cluster field, and in the node field, enter the name of the system to which you are installing.

   - **Heap size** - This is the memory allocated for  the AccessData Elasticsearch Windows Service. Normally you can accept the default value. For improved performance of the AccessData Elasticsearch Windows Service, increase the heap size.

10. The *Configuration 2* dialog contains the following options:
    - **Discovery** - Selecting the default of *Multicast* allows the AccessData Elasticsearch Windows Service search to communicate across the network to other Elasticsearch services. If the network does not give permissions for the service to communicate this way, select *Unicast* and enter the IP address(es) of the server(s) that the AccessData Elasticsearch Windows Service is installed on in the *Unicast* host names field. Separate multiple addresses with commas.
    - **Node** - The Master node receives requests, and can pass requests to subsequent data nodes. Select both Master node and Data node if this is the primary system on which the AccessData Elasticsearch Windows Service is installed. Select only Data node if this is a secondary system on which the AccessData Elasticsearch Windows Service is installed. Click **Next**.
11. In the next dialog, click **Install**.
12. If the service installs properly, a command line window appears briefly, stating that the service has installed properly.
13. At the next dialog, click **Finish**.

## Troubleshooting the AccessData Elasticsearch Windows Service

Once installed, the AccessData Elasticsearch Windows Service service should run without further assistance. If there are issues, go to **C:\Program Files\Elasticsearch\logs** to examine the logs for errors.

Chapter 7

# Configuring and Managing Databases for FTK

This section provides information that you need to know to configure and manage the database for use with FTK.

For more information, see your SQL Server documentation or contact Technical Support.

This chapter contains the following sections:

## Best Practices for Using Oracle

If you are using Oracle 10g, you should consider installing Oracle Critical Patch Updates. You can download the Oracle Critical Patch Update 38 and 45 (April 2011) from the AccessData Support Downloads web page:

http://www.accessdata.com/support/product-downloads > Utilities

**Important:** Oracle 10g is not compatible with Windows 8.

For newer updates of Oracle 10, you must have an Oracle support contract. You can upload updates from the Oracle web site (http://www.oracle.com/technetwork/topics/security/alerts-086861.html).

To install an Oracle Critical Patch Update, first back up the database, and then close all programs before you install the patch. (58583, 58248)

If you do not have an Oracle support contract, consider changing from an Oracle database to PostgreSQL, which is available at no cost on the FTK Download page. You can easily migrate your cases from Oracle to PostgreSQL. For more information, contact your Technical Account Manager (TAM) at AccessData.

Oracle must be installed on a computer with a name that begins with a letter (a-z and A-Z). Due to a restriction on domain names in RFC 1035, applications cannot connect to Oracle if the computer’s name begins with a number. If the Oracle computer name begins with a number, you must change the machine name before installing Oracle.

**Note:** When you first launch FTK and add the database, change the Oracle SID from ADG to FTK2 after selecting Oracle as your database.

## *Optimize the Oracle Database*

AccessData Oradjuster.exe optimizes Oracle's memory usage on your computer. This utility is particularly useful for 64-bit systems with large amounts of RAM installed. The Oradjuster utility is included on the FTK Application install disc. It can also be downloaded from the AccessData web site, www.accessdata.com/downloads. Look under Utilities.

For more information about Oradjuster, including its installation, configuration, and use, see "Appendix G AccessData Oradjuster" of the FTK User Guide.

Choose **Optimize the Database** to run Oradjuster for the first time. During installation is the ideal time to run it because you will not have any processes running that will delay the optimization. Respond to the prompts as they appear.

### Patch the Database

Choose to apply patches to the Oracle 10g database in preparation for the FTK schema to be laid down when you run FTK for the first time after all components are installed.

**Note:** Installing the patch can take as long as the original Oracle installation.

# Best Practices for using Microsoft SQL Server

## *Configuring Microsoft SQL Server*

If you are installing Microsoft SQL Server, perform the following configuration steps:

### Configure SQL options during the SQL Installation

1. From the *Setup Role* page, choose **SQL Server Feature Installation**.
2. From the *Feature Selection* page, select the following features:
   - *Database Engine Services*
     - *Full-Text Search*
   - *Management Tools- Basic*
     - *Management Tools - Complete*
3. On the *Instance Configuration* page you can choose either **Default instance** or **Named instance**.

   If this SQL database is used exclusively by FTK, it is much simpler to choose default instance. If you choose named instance, remember the name that you give to the instance.)
4. On the *Server Configuration* page, do the following:

   4a. Click **Use the same account for all SQL Server services**.

   4b. Specify a username and password for all service accounts.
5. On the *Database Engine Configuration* page, choose the **Mixed Mode** authentication mode.

### Configure SQL with the following collation

- "SQL_Latin1_General_CP1_CI_AS"

### Enable TCP/IP for SQL Server

1. Open the SQL Server Configuration Manager.

   (Start > All Programs > Microsoft SQL Server > Configuration Tools > SQL Server Configuration Manager)
2. Expand *SQL Server Network Configuration*.
3. Select the SQL Instance to check or change.
4. Right-click Protocol Name **TCP/IP** and click **Enable**.
5. Stop and Start the SQL Service.

### Configure Microsoft SQL Server authentication mode, remote connections, and default storage location settings

1. Open the SQL Server Management Studio (SSMS).

   (Start > All Programs > Microsoft SQL Server > Configuration Tools > SQL Server Configuration Manager.)
2. Enter the correct server name or servername/instance, authentication (Windows Authentication, SQL Authentication), and credentials.
3. Once connected to the SQL Server, in the *Object Explorer Pane*, right-click **Properties** of the server/ instance that you want to configure.
4. To check or change the SQL authentication mode, do the following:

   4a. Click the **Security** tab.

   4b. Under *Server Authentication*, select **SQL Server and Windows**.

5. (Optional) To enable remote connections to the server, do the following:
   5a. Click the **Connections** tab.
   5b. Under *Remote Server Connections*, check **Allow remote connections to this server** is enabled.
6. To make changes to the database default storage locations, do the following:
   6a. Click the **Database Settings** tab.
   6b. Under *Database default locations*, change the *Data* and *Log* locations as desired.
7. Click **OK**.
8. Stop and restart the SQL service.

## *Maintaining and Optimizing Microsoft SQL Server*

After you install FTK and initialize the database, you can do the following to manage and optimize SQL.

Upon installation, dbowner rights need to be added to ediscovery, infrastructure, workflow, and workflow40 databases for a non-sysadmin services user. However, there is no need to add dbowner rights to the adg database. (18505)

If you are using a single computer installation, where the SQL database and other applications are installed together, it will improve your performance to limit the amount of memory that SQL can use. The default SQL setting is to use all the memory that it can, which can cause performance issues. If the SQL database is on a dedicated computer, this is not an issue

### Configuring Case User Databases: Initial Size and Autogrowth

Case databases should be set to an estimated size based on the initial size of the data that will be ingested into it after the case is created. This can be found under the *Database Properties* > *Files* tab.

AccessData applications use files and filegroups. The files and data stored is within the following:

File (ex ADG53_####_TSf) in Filegroup (ex ADG53_####_TS)

This is what should be considered for changes to initial size and autogrowth settings.

A very rough rule is that the database will grow to 1/3 of the ingested data. This is not an exact estimate as multiple factors have to be taken into account regarding the data. Depending on the size and work being done in the case, Autogrowth should be considered as a percent or static size. Autogrowth for the case file can be initially set to 100 MB and 50 MB for the log file for the case database. These values should be monitored and changed as appropriate.

The database requiring growth during operation can hamper performance due to the server and disk activity required to grow the database as it becomes full.

**To configure datafile and transaction log file settings**

1. Open the SQL Server Management Studio (SSMS).
   (Start > All Programs > Microsoft SQL Server > Configuration Tools > SQL Management Studio.)
2. Enter the correct server name or servername/instance, authentication (Windows Authentication, SQL Authentication), and credentials.

3. Once connected to the SQL Server, in the *Object Explorer Pane*, right-click **Properties** on the FTK database.

   The default database name that FTK created is ADG. If you used a different name, select that database.
4. Click **Files**.
5. Under *Database* files, do the following:

   5a. For the datafile (first row), set the autogrowth setting from 1 MB to 100 MB.

   5b. For the transaction log file (second row), set the autogrowth setting from 10% to 50 MB.
6. Repeat for all FTK databases.
7. Click **OK**.
8. Stop and restart the SQL service.

## MS SQL Memory Allocation

A general rule for memory allocation to the Windows OS is that for first 16 GB of Memory the operating system is allocated 4 GB. Afterwards for every additional 4 GB of memory the system gets 1 GB. SQL by default will take as much memory as possible. For Windows servers running only Microsoft SQL Server the following rule should be adhered to for Maximum memory allocated to the application subtracted by what will be required by the OS. Systems sharing memory with application other than MSSQL a maximum memory should be set as to not take away all available memory for the other applications.

## MS SQL Temp DB

SQL and the application use the tempdb database for storage of various temporary tables. Improved performance can be found with setting an increased size for the MDF file as well as having additional tempdb files allocated to the database.

We recommend increasing the initial tempdb mdf file to 2 GB and Log file to 1 GB. We also recommend adding additional tempdb mdf files, at least 2 db in size, for every physical core (up to a maximum of 8 total files).

## Maintenance Jobs

You can create maintenance jobs to perform defragmentation and rebuilding of indexes, integrity and consistency checks, DBCC checkdb, backups, blocking sessions and database file monitor.

Maintenance jobs for backup, defragmentation and rebuild of indexes are default maintenance tasks that can be created via SSMS.

A rough estimate of a defragmentation job would be every day with a rebuild once a week. Actual expected rules are indexes with pages > 100 and fragmentation over 60 become rebuild and anything below to be re-org.

Maintenance jobs for Backups Full, Differential, Transaction should be based on your environment.These maintenance tasks can hamper performance as they can run into production hours depending on size of the database.

## Other SQL Best Practices

Additional improvements can be made by setting the SQL Recovery Model to “Simple”. This can result in less writes, providing less I/O to disk, and storage to the Log file (LDF). However, this can put you at risk as this disallows transaction backups and Tail Log restores.

DBCC, database file monitoring, and blocking sessions are advanced SQL items used to troubleshoot ad resolve issues that may be occurring. These are least likely to be needed for your system's day-to-day operation.

Chapter 8

# Managing Security Devices and Licenses

This appendix includes information AccessData product licenses, Virtual CodeMeter activation, and Network License Server configurations.

## Installing and Managing Security Devices

AccessData products require a licensing security device that communicates with the program to verify the existence of a current license.

You must install the security device software and drivers before you can manage licenses with LicenseManager. This section explains installing and using the CodeMeter Runtime software and the License Manager.

### Installing the Security Device

AccessData products require a licensing security device that communicates with the program to verify the existence of a current license. The device is a WIBU-SYSTEMS (Wibu) CodeMeter (CmStick). This USB device requires specific software to be installed prior to connecting the devices and running your AccessData products. You will need the WIBU-SYSTEMS CodeMeter Runtime software with a WIBU-SYSTEMS CodeMeter (CmStick), either the physical USB device, or the Virtual device.

**Note:** Without a license security device and its related software, you can run applications in Demo mode only.

Store the CmStick or dongle in a secure location when it is not in use.

#### Installing the CodeMeter Runtime Software

When you purchase a product, AccessData provides a USB CmStick with the product package. To use the CmStick, you must first install the CodeMeter Runtime software, either from the shipping disc or from the setup file downloaded from the AccessData Web site.

**Note:** The CodeMeter software is automatically installed as part of the FTK suite.

**To download the CodeMeter installer from the AccessData web site**

1. Go to the AccessData download page at:
   http://www.accessdata.com/product-download.

2. On the download page, click **CodeMeter**.
3. Click **Download Page**.
4. Click **Download Now**.
5. Save the installation file to your download directory or other temporary directory on your drive.

### To install CodeMeter

1. Do one of the following:
   - Launch the installer from the FTK installer by doing the following:

     1a. Launch the FTK installer `Autorun.exe` file.

     1b. Click **Other Products**.

     1c. Click Install License Manager.
   - Launch the installer from the download by doing the following:

     1a. Navigate to, and double-click the installation file.
2. Wait for the *Preparing to Install* processes to complete.
3. In the Welcome dialog, click **Next**.
4. Read and accept the License Agreement
5. Enter User Information.
6. Click **Next**.
7. Select the features you want to install.
8. Click **Next**.
9. Click **Install**.
10. Click **Finish**.
11. Click **OK**.

### CodeMeter Error

If you are not using NLS for your security device configuration, after clicking **No,** you will see the following additional message.

*Security Device Not Found*

To remedy, click **OK**, then install the correct CodeMeter Runtime software, and connect the CmStick or run License Manager to generate your Virtual CmStick. Then, restart FTK.

# Installing LicenseManager

LicenseManager lets you manage product and license subscriptions using a security device or device packet file.

You can can access the LicenseManager installer from the Web or from the FTK installer.

### To download the LicenseManager installer from the AccessData web site

1. Go to the AccessData download page at:
   http://www.accessdata.com/product-download.
2. On the download page, click **LicenseManager**.
3. Click **Download Page**.
4. Click **Download Now**.
5. Save the installation file to your download directory or other temporary directory on your drive.

### To install LicenseManager

1. Do one of the following:
   - Launch the installer from the FTK installer by doing the following:

     1a. Launch the FTK installer Autorun.exe file.

     1b. Click **Other Products**.

     1c. Click Install License Manager.
   - Launch the installer from the download by doing the following:

     1a. Navigate to, and double-click the installation file.
2. Wait for the *Preparing to Install* processes to complete.
3. Click **Next** on the Welcome screen
4. Read and accept the License Agreement.
5. Click **Next.**
6. Accept the default destination folder, or select a different one.
7. Click **Next.**
8. In the Ready to Install the Program dialog, click **Back** to review or change any of the installation settings. When you are ready to continue, click **Install**.
9. Wait while the installation completes.
10. If you want to launch LicenseManager after completing the installation, mark the **Launch AccessData LicenseManager** check box.
11. Select the **Launch AccessData LicenseManager** check box to run the program upon finishing the setup. The next section describes how to run LicenseManager later.
12. Click **Finish** to finalize the installation and close the wizard.

## *Starting LicenseManager*

### To launch LicenseManager

1. Launch LicenseManager by clicking the **LicenseManager** icon on your desktop.

   When starting, LicenseManager reads licensing and subscription information from the installed and connected WIBU-SYSTEMS CodeMeter Stick, or Keylok dongle.

   **Note:** If using a Keylok dongle, and LicenseManager either does not open or displays the message, “Device Not Found”

2. Verify the correct dongle driver is installed on your computer.
3. With the dongle connected, check in Windows Device Manager to make sure the device is recognized. If it has an error indicator, right click on the device and choose Uninstall.
4. Remove the dongle after the device has been uninstalled.
5. Reboot your computer.
6. After the reboot is complete, and all startup processes have finished running, connect the dongle.
7. Wait for Windows to run the Add New Hardware wizard. If you already have the right dongle drivers installed, do not browse the internet, choose, “No, not this time.”
8. Click **Next** to continue.
9. On the next options screen, choose, “Install the software automatically (Recommended)
10. Click **Next** to continue.
11. When the installation of the dongle device is complete, click Finish to close the wizard.
12. You still need the CodeMeter software installed, but will not need a CodeMeter Stick to run LicenseManager.

    **Note:** If using a CodeMeter Stick, and LicenseManager either does not open or displays the message, “Device Not Found”

13. Make sure the CodeMeter Runtime 4.20b software is installed. It is available at www.accessdata.com/support. Click Downloads and browse to the product. Click on the download link. You can **Run** the product from the Website, or **Save** the file locally and run it from your PC. Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray.
14. Make sure the CodeMeter Stick is connected to the USB port.

If the CodeMeter Stick is not connected, LicenseManager still lets you to manage licenses using a security device packet file if you have exported and saved the file previously.

### To open LicenseManager without a CodeMeter Stick installed

1. Click **Tools** > **LicenseManager**.

   LicenseManager displays the message, “Device not Found”.

2. Click **OK**, then browse for a security device packet file to open.

**Note:** Although you can run LicenseManager using a packet file, AccessData products will not run with a packet file alone. You must have the CmStick or dongle connected to the computer to run AccessData products that require a license.

## *Using LicenseManager*

LicenseManager provides the tools necessary for managing AccessData product licenses on a WIBU-SYSTEMS CodeMeter Stick security device, a Keylok dongle, a Virtual Dongle, or in a security device packet file.

LicenseManager displays license information, allows you to add licenses to or remove existing licenses from a dongle or CmStick. LicenseManager, and can also be used to export a security device packet file. Packet files can be saved and reloaded into LicenseManager, or sent via email to AccessData support.

In addition, you can use LicenseManager to check for product updates and in some cases download the latest product versions.

LicenseManager displays CodeMeter Stick information (including packet version and serial number) and licensing information for all AccessData products. The Purchase Licenses button connects directly to the AccessData website and allows you to browse the site for information about products you may wish to purchase. Contact AccessData by phone to speak with a Sales Representative for answers to product questions, and to purchase products and renew licenses and subscriptions.

## The LicenseManager Interface

The LicenseManager interface consists of two tabs that organize the options in the LicenseManager window: the Installed Components tab and the Licenses tab.

### The Installed Components Tab

The Installed Components tab lists the AccessData programs installed on the machine. The Installed Components tab is displayed in the following figure.

The following information is displayed on the Installed Components tab:

**LicenseManager Installed Components Tab Features**

| | |
|---|---|
| Program | Lists all AccessData products installed on the host. |
| Installed Version | Displays the version of each AccessData product installed on the host. |
| Newest Version | Displays the latest version available of each AccessData product installed on the host. Click **Newest** to refresh this list. |
| Product Notes | Displays notes and information about the product selected in the program list. |
| AccessData Link | Links to the AccessData product page where you can learn more about AccessData products. |

The following buttons provide additional functionality from the Installed Components tab:

**LicenseManager Installed Components Buttons**

| | |
|---|---|
| Help | Opens the LicenseManager Help web page. |
| Install Newest | Installs the newest version of the programs checked in the product window, if that program is available for download. You can also get the latest versions from our website using your Internet browser. |
| Newest | Updates the latest version information for your installed products. |
| About | Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager. |
| Done | Closes LicenseManager. |

Use the Installed Components tab to manage your AccessData products and stay up to date on new releases.

## The Licenses Tab

The Licenses tab displays CodeMeter Stick information for the current security device packet file and licensing information for AccessData products available to the owner of the CodeMeter Stick, as displayed in the following figure.

The Licenses tab provides the following information:

**LicenseManager Licenses Tab Features**

| | |
|---|---|
| Program | Shows the owned licenses for AccessData products. |
| Expiration Date | Shows the date on which your current license expires. |
| Status | Shows these status of that product’s license:<br>● **None**: the product license is not currently owned<br>● **Days Left**: displays when less than 31 days remain on the license.<br>● **Never**: the license is permanently owned. This generally applies to Hash Tables and Portable Office Rainbow Tables. |
| Name | Shows the name of additional parameters or information a product requires for its license. |
| Value | Shows the values of additional parameters or information a product contained in or required for its license. |
| Show Unlicensed | When checked, the License window displays all products, whether licensed or not. |

The following license management actions can be performed using buttons found on the License tab:

**License Management Options**

| | |
|---|---|
| Remove License | Removes a selected license from the Licenses window and from the CodeMeter Stick or dongle. Opens the AccessData License Server web page to confirm success. |
| Refresh Device | Connects to the AccessData License Server. Downloads and overwrites the info on the CodeMeter Stick or dongle with the latest information on the server. |
| Reload from Device | Begins or restarts the service to read the licenses stored on the CodeMeter Stick or dongle. |

**License Management Options (Continued)**

| | |
|---|---|
| Release Device | Click to stop the program reading the dongle attached to your machine, much like Windows’ Safely Remove Hardware feature. Click this button before removing a dongle.<br>This option is disabled for the CodeMeter Stick. |
| Open Packet File | Opens Windows Explorer, allowing you to navigate to a .PKT file containing your license information. |
| Save to File | Opens Windows Explorer, allowing you to save a .PKT file containing your license information. The default location is My Documents. |
| Finalize Removal | Finishes the removal of licenses in the unbound state. Licenses must be unbound from the CmStick or dongle before this button takes effect. |
| View Registration Info | Displays an HTML page with your CodeMeter Stick number and other license information. |
| Add Existing License | Allows you to bind an existing unbound license to your CodeMeter Stick, through an internet connection to the AccessData License Server. |
| Purchase License | Brings up the AccessData product page from which you can learn more about AccessData products. |
| About | Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager. |
| Done | Closes LicenseManager. |

## Opening and Saving Dongle Packet Files

You can open or save dongle packet files using LicenseManager. When started, LicenseManager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file. You must have already created and saved a dongle packet file to be able to browse to and open it.

### To save a security device packet file

1. Click the **Licenses** tab, then under License Packets, click **Save to File**.
2. Browse to the desired folder and accept the default name of the **.**PKT file; then click **Save**.

> **Note:** In general, the best place to save the .PKT files is in the AccessData LicenseManager folder. The default path is C:\Program Files\AccessData\Common Files\AccessData LicenseManager\.

### To open a security device packet file

1. Select the **Licenses** tab.
2. Under License Packets, click **Open Packet File**.
3. Browse for a dongle packet file to open. Select the file and click **Open**.

## Adding and Removing Product Licenses

On a computer with an Internet connection, LicenseManager lets you add available product licenses to, or remove them from, a dongle.

To move a product license from one dongle to another dongle, first remove the product license from the first dongle. You must release that dongle, and connect the second dongle before continuing. When the second dongle is connected and recognized by Windows and LicenseManager, click on the Licenses tab to add the product license to the second dongle.

### Removing a License

**To remove (unassociate, or unbind) a product license**

1. From the Licenses tab, mark the program license to remove.

   This action activates the Remove License button below the Program list box.
2. Click **Remove License** to connect your machine to the AccessData License Server through the internet.
3. When you are prompted to confirm the removal of the selected licenses from the device, click **Yes** to continue, or **No** to cancel.
4. Several screens appear indicating the connection and activity on the License Server, and when the license removal is complete, the following screen appears.
5. Click **OK** to close the message box.

   Another internet browser screen appears from LicenseManager with a message that says, “The removal of your licenses from Security Device was successful!” You may close this box at any time.

### Adding a License

**To add a new or released license**

1. From the Licenses tab, under Browser Options, click **Add Existing License.**

   The AccessData LicenseManager Web page opens, listing the licenses currently bound to the connected security device, and below that list, you will see the licenses that currently are not bound to any security device. Mark the box in the Bind column for the product you wish to add to the connected device, then click **Submit**.
2. An AccessData LicenseManager Web page will open, displaying the following message, “The AccessData products that you selected has been bound to the record for Security Device *nnnnnnn* within the Security Device Database.

   “Please run LicenseManager’s “Refresh Device” feature in order to complete the process of binding these product licenses to this Security Device.” You may close this window at any time.
3. Click **Yes** if LicenseManager prompts, “Were you able to associate a new product with this device?”
4. Click **Refresh Device** in the Licenses tab of LicenseManager. Click **Yes** when prompted.

You will see the newly added license in the License Options list.

## Adding and Removing Product Licenses Remotely

While LicenseManager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer, such as a forensic lab computer, that does not have an Internet connection.

If you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, and then physically move the dongle back to the original computer. However, if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

## Adding a License Remotely

### To remotely add (associate or bind) a product license

1. On the computer where the security device resides:

   1a. Run LicenseManager.

   1b. From the **Licenses** tab, click **Reload from Device** to read the dongle license information.

   1c. Click **Save to File** to save the dongle packet file to the local machine.

2. Copy the dongle packet file to a computer with an Internet connection.

3. On the computer with an Internet connection:

   3a. Remove any attached security device.

   3b. Launch LicenseManager. You will see a notification, “No security device found”.

   3c. Click OK.

   3d. An “Open” dialog box will display. Highlight the **.**PKT file, and click **Open**.

   3e. Click on the **Licenses** tab.

   3f. Click **Add Existing License.**

   3g. Complete the process to add a product license on the Website page.

   3h. Click **Yes** when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”

   3i. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file, **[serial#].wibuCmRaU.**

   3j. Save the update file to the local machine.

4. After the update file is downloaded, copy the update file to the computer where the dongle resides:

5. On the computer where the dongle resides:

   5a. Run the update file by double-clicking it. (**[serial#].wibuCmRaU** is an executable file.)

   5b. After an update file downloads and installs, click **OK.**

   5c. Run LicenseManager.

   5d. From the Licenses tab, click **Reload from Device** to verify the product license has been added to the dongle.

## Removing a License Remotely

### To remotely remove (unassociate, or unbind) a product license

1. On the computer where the dongle resides:

   1a. Run LicenseManager.

   1b. From the Licenses tab, click **Reload from Device** to read the dongle license information.

   1c. Click **Save to File** to save the dongle packet file to the local machine.

2. Copy the file to a computer with an Internet connection.

3. On the computer with an Internet connection:

   3a. Launch LicenseManager. You will see a notification, “No security device found”.

   3b. Click **OK**.

   3c. An “Open” dialog box will display. Highlight the **.**PKT file, and click **Open**.

3d. Click on the Licenses tab.

3e. Mark the box for the product license you want to unassociate; then click **Remove License.**

3f. When prompted to confirm the removal of the selected license from the dongle, click **Yes**.

3g. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.

3h. Click **Yes** to save the update file to the local computer.

3i. The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.

3j. Save the update file to the local machine.

4. After the update file is downloaded, copy the update file to the computer where the dongle resides.
5. On the computer where the dongle resides:

5a. Run the update file by double-clicking it. This runs the executable update file and copies the new information to the security device.

5b. Run LicenseManager

5c. On the Licenses tab, click **Reload from Device** in LicenseManager to read the security device and allow you to verify the product license is removed from the dongle.

5d. Click **Save to File** to save the updated dongle packet file to the local machine.

6. Copy the file to a computer with an Internet connection.

# *Updating Products*

You can use LicenseManager to check for product updates and download the latest product versions.

## Checking for Product Updates

To check for product updates, on the Installed Components tab, click **Newest**. This refreshes the list to display what version you have installed, and the newest version available.

## Downloading Product Updates

To install the newest version, mark the box next to the product to install, then click **Install Newest**.

**Note:** Some products are too large to download, and are not available. A notification displays if this is the case.

### To download a product update

1. Ensure that LicenseManager displays the latest product information by clicking the Installed Components tab. Click **Newest** to refresh the list showing the latest releases, then compare your installed version to the latest release.

   If the latest release is newer than your installed version, you may be able to install the latest release from our Website.
2. Ensure that the program you want to install is not running.
3. Mark the box next to the program you want to download; then click **Install Newest**.
4. When prompted, click **Yes** to download the latest install version of the product.

4a. If installing the update on a remote computer, copy the product update file to another computer.

5. Install the product update. You may need to restart your computer after the update is installed.

## Purchasing Product Licenses

Use LicenseManager to link to the AccessData Web site to find information about all our products.

Purchase product licenses through your AccessData Sales Representative. Call 801-377-5410 and follow the prompt for Sales, or send an email to sales@accessdata.com.

**Note:** Once a product has been purchased and appears in the AccessData License Server, add the product license to a CodeMeter Stick, dongle, or security device packet file by clicking **Refresh Device**.

# *Sending a Dongle Packet File to Support*

Send a security device packet file **only** when specifically directed to do so by AccessData support.

### To create a dongle packet file

1. Run LicenseManager
2. Click on the Licenses tab.
3. Click **Load from Device**.
4. Click **Refresh Device** if you need to get the latest info from AD’s license server.
5. Click **Save to File**, and note or specify the location for the saved file.
6. Attach the dongle packet file to an e-mail and send it to: support@accessdata.com.

# Virtual CodeMeter Activation Guide

## Introduction

A Virtual CodeMeter (VCM) allows the user to run licensed AccessData products without a physical CodeMeter device. A VCM can be created using AccessData License Manager, but requires the user to enter a Confirmation Code during the creation process.

The latest revision of this guide can be found at:

http://accessdata.com/downloads/media/VCM_Activation_Guide.pdf

## Preparation

- Contact your AccessData sales rep to order a VCM confirmation code.
- Install CodeMeter Runtime 4.10b or newer (available on the AccessData download page).
- Install the latest release of License Manager (available on the AccessData download page).
- The following steps are to be run on the system where you want to permanently attach the VCM.

> **Note:** Once created, the VCM cannot be moved to any other system.

- AD Lab WebUI and eDiscovery administrators, please also follow steps outlined under in Additional Instructions for AD Lab WebUI and eDiscovery (page 84) in order to enable VCM licensing on the AccessData License Service.

## Setup for Online Systems

**To setup a Virtual CodeMeter**

1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.

> **Note:** When creating a VCM on Windows Server 2003 or 2008, please refer to the special set of steps written for those platforms. See Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions (page 83).

3. Select **Create A Local Virtual CMStick**
4. Click **OK.**
   The Confirmation Code Required dialog appears.
5. Enter your confirmation code.
6. Click **OK**, AccessData License Manager will automatically synchronize with the License Server over the Internet.
7. Click **OK** when the update completes. License Manager will then create the VCM on your system.
8. At this point, AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

## Setting up VCM for Offline Systems

You can setup a Virtual CodeMeter on a system that is not connected to the internet (offline). You must also have one machine that connects to the internet to perform certain steps. This section details what to do on which machine.

### Perform these steps on the Online system

1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.

> **Note:** When creating a VCM on Windows Server 2003 or 2008 Enterprise Edition, please refer to the special set of steps written for those platforms. See Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions (page 83).

3. Select **Create Empty Virtual CMStick (offline)**.
4. Click **OK.**
5. The resulting dialog prompts you to save the ***.wibucmrau** file. Enter a name and path for the file, then click **Save**.
6. Transfer the ***.wibucmrau** to the Online system.

### Perform these steps on the Online system

7. Unplug any AccessData dongles you currently have connected.
8. Launch License Manager.
9. Select **Create Activation File (online)**.
10. Click **OK**.
11. In the Confirmation Code Required dialog, enter your confirmation code and click **OK**.
12. AccessData License Manager will automatically synchronize with the License Server over the internet. Data synchronized from the server will be written to the ***.wibucmrau** file. Click **OK** when the update completes.
13. Transfer ***.wibucmrau** back to the offline system.

### Perform these steps on the Offline system

14. Unplug any AccessData dongles you currently have connected.
15. Launch License Manager.
16. Select **Create Activate Virtual CMStick (offline)**.
17. Click **OK**.
18. The resulting dialog prompts you to browse to the location of the newly updated ***.wibucmrau** file. Locate the file, then click **Open**. License Manager creates the VCM on your system.
19. 19.At this point, AccessData License Manager should now display a serial number for the VCM on the “Licenses” tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

## Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions

This section contains special instructions for using a VCM with Windows Server 2003 or 2008 Enterprise Editions. Complete each section in order.

### To Create an Empty CodeMeter License Container

1. On the Server 2003/2008 machine, unplug any CodeMeter devices.
2. Open the CodeMeter Control Center. Make sure the window on the License tab is, empty indicating that no licenses are currently loaded.
3. Select **File > Import License.**
4. Browse to the License Manager program files directory.
   - 32 bit systems: **C:\Program Files\AccessData\LicenseManager\**
   - 64 bit systems: **C:\Program Files (x86)\ AccessData\LicenseManager\**
5. Highlight the TemplateDisc5010.wbb file, then click **Import**.
6. Click the **Activate License** button.
7. When the *CmFAS Assistant* opens, click **Next**.
8. Select **Create license request**, and click **Next**.
9. Confirm the desired directory and filename to save **.WibuCmRaC**. (Example: Test1.WibuCmRaC)
10. Click **Commit**.
11. Click **Finish**.

### To Copy to another machine

1. Copy the new **.WibuCmRaC** to another machine that is not running Windows Server 2003/2008 Enterprise.

   **Note:** The destination system must have an active internet connection.

2. Unplug any AccessData dongles you currently have connected.
3. Launch *License Manager*.
4. Select **Create Activation File (online)**.
5. Click **OK**.
6. In the Confirmation Code Required dialog enter your confirmation code and click **OK**.
7. AccessData License Manager will automatically synchronize with the License Server over the internet. Data synchronized from the server will be written to the ***.wibucmrau** file. Click **OK** when the update completes.

### To Finish the activation on the Windows Server 2003/2008 Enterprise system

1. Copy the activated .WibuCmRaC file to the Server 2003/2008 machine.
2. On the Server 2003/2008 machine, unplug any CodeMeter devices.
3. Open the CodeMeter Control Center. Make sure the window on the License tab empty indicating that no licenses are currently loaded.
4. Select **File > Import License.**
5. Browse to the location where the activated **.WibuCmRaC** is stored. Click **Import**.
6. AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

## *Additional Instructions for AD Lab WebUI and eDiscovery*

This section provides additional information for enabling the Web User Interface to recognize a VCM.

**To enable AD Lab WebUI and eDiscovery to use VCM**

1. Open Registry Editor.
2. Navigate to the following key:

   **HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products**

   Add the following DWORD registry string to the key and set the value to 1:

   **HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products | EnableACTTest**

The *AccessData License Service* will know to expect a VCM when *EnableACTTest* is set to “1.”

## Virtual CodeMeter FAQs

*Q:* How do I get a Virtual CodeMeter (VCM)?

*A:* Contact your AccessData product sales representative. They will provide you with a VCM confirmation code.

*Q:* How do VCMs work?

*A:* A VCM operates in almost exactly the same way as a hardware CodeMeter device, except that they exist as a file stored on the hard disk. During activation, the VCM file (named with a WBB extension) is tied to the hardware of the system using unique hardware identifiers. Those unique identifiers make VCMs non-portable. When AccessData License Manager is launched, it will automatically load the VCM and display its license information. From there, you can refresh, remove, add existing licenses, etc just the same you would with a hardware security device.

*Q:* Are VCMs supported on virtual machines (VM)?

*A:* No. Due to the fact that virtual machines are portable and VCMs are not, VCMs are not supported on virtual machines. Currently it is recommended to use AccessData Network License Service (NLS) to license systems running as virtual machines. CLICK HERE for more information.

*Q:* Does the AccessData Network License Service (NLS) support VCMs?

*A:* The current release of NLS does not support using VCM as a network dongle. AccessData is considering this support for a future release.

*Q:* How can I “unplug” a VCM?

*A:* If you want to prevent License Manager from automatically loading the VCM you can "unplug" it by stopping the CodeMeter Runtime Service server and then moving (cut and paste) the WBB file to a new location (renaming the file does not suffice). By default the WBB file is located at:

*32 bit systems:*

**C:\Program Files\CodeMeter\CmAct\**

*64 bit systems:*

**C:\Program Files (x86)\CodeMeter\CmAct\**

*Q:* I have activated a VCM on my system, but now I need to activate it on a different system. What should I do?

*A:* Since a VCM is uniquely tied to the system on which it is activated, it cannot be moved to any other system. If you need to activate a VCM on a different system, you need to contact your AccessData Sales Representative.

*Q:* What if I need to reinstall Windows, format my drive, change my system's hardware, or back up my VCM in case of a disaster? Will the VCM still work?

*A:* The VCM can be backed up by simply copying the WBB file to a safe location. It can be restored by copying the WBB file to the CmAct folder. The VCM cannot be restored without a WBB file. If you do not have a backup of your WBB file, you will need to get a new confirmation code from your AccessData Sales Representative.

*Q:* My AccessData product does not seem to recognize the license stored on a VCM. What am I doing wrong?

*A:* VCMs are supported by the following versions of AccessData products:

- FTK 1.81.6 and newer
- FTK 3.1.0 and newer
- PRTK 6.5.0 and newer
- DNA 3.5.0 and newer
- RV 1.6.0 and newer
- eDiscovery 3.1.2 and newer
- AD Lab 3.1.2 and newer
- AD Enterprise 3.1.0 and newer
- MPE+ 4.0.0.1 and newer

Ensure that the version of the product you are running support VCMs. If the version you are running is listed as supported, verify that according to License Manager, the release date of the version you are running falls before the expiration date of the license.

# Network License Server (NLS) Setup Guide

## Introduction

This section discusses the installation steps and configuration notes needed to successfully setup an AccessData Network License Server (NLS).

**Note:** Click on this link to access the latest version of this guide:

Network License Server (NLS) Setup Guide.

## Preparation Notes

- CodeMeter Runtime 3.30a or newer must be installed on all Client and Server systems
- AccessData License Manager must be used to prepare the network dongle. The system running License Manager must have internet access and have CodeMeter Runtime installed.
- The current release of NLS supports the following versions of Windows:
  - Windows XP 32/64 bit
  - Windows Server 2003 32/64 bit
  - Windows Vista 32/64 bit
  - Windows Server 2008 R1 32/64 bit
  - Windows 7 32/64 bit
  - Windows Server 2008 R2 64 bit

## Setup Overview

**To setup NLS**

1. Download the latest release of NLS located in the utilities section of the AccessData download page.
2. Extract contents of ZIP to a folder of your choice.
3. On the NLS server system, run through the NLS Installation MSI and accept all defaults.
4. Prepare network dongle:

   4a. Provide the serial number to AD Support and request to have the “Network Dongle Flag” applied.

   4b. Migrate any additional licenses to the network dongle

   4c. Refresh the network dongle device using AccessData License Manager.
5. Launch the AccessData product on the NLS client system.
6. Enter the NLS server configuration information:
   - IP address or hostname of NLS server system
   - Port 6921
7. Click, **OK**.

If you encounter any problems, please read the notes below for troubleshooting information.

## Network Dongle Notes

- AccessData License Manager 2.2.6 or newer should be installed in order to manage licenses on the network dongle.
- Network dongles can hold up to 120 physical licenses. Each License has a capacity to hold thousands of sub licenses (i.e. Client count or worker count).
- Contact AccessData Technical Support to have your CodeMeter device flagged as a Network Dongle (required for NLS).

## NLS Server System Notes

- Make sure the CodeMeter device is flagged as Network Dongle (i.e. License Manager will show the serial as “1181234N”. To have this flag set on your CodeMeter device, please contact AccessData Technical Support).
- Server system must be configured to allow incoming and outgoing traffic on TCP port 6921.
- A web interface to view and revoke licenses all licenses is accessible at

  `http://localhost:5555`

  This page can be reached only from a web browser running locally on the NLS server system.
- A Network Dongle cannot be used to run AccessData products locally unless the NLS server is running locally.
- Some versions of Windows may not find a local NLS server when the DNS hostname of the server is provided. In those cases, it is recommended to use a static IP address.
- When using the NLS across domains, users must have permissions to access resources on both domains (either by dual-domain membership or cross-domain trust).
- When running NLS on Windows Server 2008, Terminal Services must be installed and accepting connections. If Terminal Services is not configured it will not open the port and share out the licenses correctly.
- The name of the service according to Windows is “AccessData Network License Service.”

## NLS Client System Notes

- When launched, any NLS client application that needs to lease a license from the NLS server will automatically check for the following values within the Windows Registry.
  - **NetDonglePath**: The IP address or DNS hostname of the system hosting the Network License Server service which is found in the following registry key on the client system:

    `HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common`
  - **NetDonglePort**: The TCP port number through which the client and server systems have been configured to use. This value is located in the same key as NetDonglePath.
  - **uniqueId**: In order to lease a license from the server, the client system must first posses a unique identification value. This value is automatically generated by applications such as FTK, PRTK, or DNA. (Registry Viewer and FTK 1.x cannot be used setup initial client NLS configuration at this time.)

    You can find the each client system’s uniqueId by inspecting the following registry key:

    `HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared`
- The Client system must be configured to allow all incoming and outgoing traffic on TCP port 6921.
- The following products support the ability to lease a license from a NLS server:
  - FTK 2.2.1 and newer
  - FTK 1.81.2 and newer

  - FTK Pro 3.2 and newer
  - PRTK 6.4.2 and newer
  - DNA 3.4.2 and newer
  - Registry Viewer 1.5.4 and newer
  - AD Enterprise 3.0.3 and newer
  - AD Lab 3.0.4 and newer
  - AD Lab Lite 3.1.2 and previous
  - Mobile Phone Examiner 3.0 and newer
  - Explicit Image Detection (EID) Add-on
  - Glyph Add-on
- Use AccessData License Manager (ver. 2.2.4 or newer) to migrate licenses off other devices and onto a network device.
- When running AccessData products on Windows Vista, 7, or Server 2008 you must choose **Run as administrator** at least once in order to lease a license from a NLS server.
- If the NLS client application is having trouble leasing a license either from the NLS server, AccessData recommends that you reset the licensing configuration to default.
- To reset the licensing configuration, delete and recreate the NLS registry key located at:
  HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common

Chapter 9

# AccessData Distributed Processing

Distributed Processing allows the installation of the Distributed Processing Engine (DPE) on additional computers in your network, allowing you to apply additional resources of up to three additional computers at a time to the processing of your cases.

Distributed Processing may not help reduce processing times unless the number of objects to be processed exceeds 1,000 times the number of cores. For example, on a system with eight cores, the additional distributed processing engine machines may not assist in the processing unless the evidence contains greater than 8,000 items.

This appendix includes the following topics

- See Distributed Processing Prerequisites on page 90.
- See Installing Distributed Processing on page 92.
- See Configuring Distributed Processing on page 94.
- See Using Distributed Processing on page 96.

## Distributed Processing Prerequisites

Before installing the AccessData (AD) Distributed Processing Engine, the following prerequisites must be met (if you are not familiar with any one of these tasks, contact your IT administrator):

- The following software must be installed:
  - Evidence Processing Engine installed on the local examination machine.
  - CodeMeter Runtime software and either a USB or a Virtual CmStick.
    (For more information regarding the CmStick, see  (page 71).)
  - Database either on the same computer, or on a second computer.
  - KFF Library.
  - McAfee Virus Scan must have an exception added for processes added to and run from the Temp Directory.
  - The Windows Temp directory must be set as default.
- A New user account that is a member of the Administrators group on the examiner machine. If you are installing on a Microsoft network with a Domain Controller, this is easily accomplished. If you are on a non-domain network or workgroup, create this same user account and password on each DPE machine, as well as on the machine holding the Case Folder and the machine holding the Evidence Folder.
  - Make a note of the user account, domain or workgroup, and the IP address of each machine.

- A familiarity with UNC paths. UNC paths are required whenever a path statement is needed during installation and configuration of the DPE, and when the path to the Case Folder, or the path to the Evidence Folder is required.
  - The UNC format is \\[*machine name or IP address*]\[*pathname*]\[*casefolder*].
- Computers that are all on the same network, and in the same domain or workgroup.
- A familiarity with the Windows **Services.msc** to ensure appropriate Login rights for the DPE, and for restarting the service, if necessary.
- A familiarity with IP addresses and how to find them on a computer.
- A knowledge of the case folder path. The case folder must be shared for DPE to access it and write to it as it processes case data.

## Using PostgreSQL with Distributed Processing

- When using PostgreSQL, please note the following:
  - If the computer has fewer than 16 cores ( < 16), then in the PostgreSQL configuration file, set the max_connections to 60 per computer.

    For example, if there are 4 computers in the Distributed Processing Model in which every computer has fewer than 16 cores, then set max_connections to 240 (60*4).
  - If the computer has 16 or more cores ( >= 16), then in the PostgreSQL configuration file, set the max_connections to 125 per computer. For example, if there are 4 computers in the Distributed Processing Model in which 3 computers are 8 core (<16) and 1 computer is 16 core (>=16), then set max_connections to 245 (60*3 + 125*1).
  - If there is just one computer in the Distributed Processing Model, the max_connections should be no less than 100.

# Installing Distributed Processing

**Important:** Do not install the Distributed Processing Engine on the examiner machine. The install required the installation of the local Evidence Processing Engine on that machine.

Installing the Distributed Processing Engine on the examination machine disables both processing engines.

*Remedy*: If you have already installed both the Evidence Processing Engine and the Distributed Processing Engine on a single machine, you must:

a) stop the processes

b) uninstall from both the examination machine and the Evidence Processing Engine machines

c) restart your machine

d) install on the examination machine.

e) start the Evidence Processing Engine again

### To install AccessData Distributed Processing

1. Install the Distributed Processing Engine (AccessData Distributed Processing Engine.EXE) on the computers that are to participate in case processing, (record the IP address of each one for use when configuring the DPE on the examination machine).

   The DPE install file can be found on the installation disc in the following path:

   [*Drive*]:\FTK\AccessData Distributed Processing Engine.EXE

   If you do not know the IP address of the machine you are installing on, do the following:

   1a. Click **Start** on the Windows Startbar.

   1b. Click **Run**.

   1c. Enter cmd.EXE in the *Run* text box.

   1d. If the prompt is not **c:\>**, type **c:** and press **Enter**.

   At the new prompt, type cd\ and press **Enter**.

   The resulting prompt should be **c:\>**.

   1e. At the c:\> prompt, type ipconfig /all.

   1f. From the resulting information, locate the Ethernet adapter Local Area Connection, and find the associated IP address. That is what you will need when you configure the Distributed Processing Engine.

   **Note:** AccessData recommends that you write down the IP addresses for all machines on which the DPE will be installed.

   1g. At the prompt, type exit and press **Enter** to close the cmd.EXE box.

   **Note:** The domain listed here is not necessarily the correct one to use in installation. To find the correct domain or workgroup name, right-click **My Computer** (On Vista or Server 2008, click **Computer**), click **Properties** > **Computer Name**. The Domain or Workgroup name is listed midway down the page. Please make a note of it for future use.

2. If a *Security Warning* appears, click **Run** to continue.
3. If you want to stop the install, click **Cancel** on the Preparing to Install screen.
4. Click **Next** on the Welcome screen to continue the install.
5. Read and accept the License Agreement.

6. Click **Next** to continue.
7. Accept the default destination folder (recommended), or click **Change** to specify a different destination folder.
8. Click **Next** to continue.
9. Enter the credentials to be used for running the service.
   - *User name*: This user account must be a member of the Administrators group on the DPE machine, and must also have access to both the case folder, and the evidence folder. If this user account is not a member of the Administrators group, or if you are not sure, check with your IT services department.
   - While it is not generally necessary on a domain, it is recommended that whether you are on a domain network, a non-domain network, or a workgroup network, you create this same user account with the same password as a member of the Administrators group on all machines involved. This acts as a fail-safe in case the domain server goes down.
   - *Domain*: The name of the domain all related computers are on. If a non-domain or workgroup network is in place, use the local DPE's machine name or IP address in place of the domain name for this step in the installation.
   - *Password*: This user account's password for authenticating to the domain, or to the machine on the non-domain network or workgroup. The password must be the same for this user account on each machine.

   The figure below illustrates the user name and password setup.

   The components on the top row of the figure can be all on one machine, all on separate machines, or on any combination of machines. The key is that the administrator account and password (or user account in the Administrators group—it can be any name as long as the correct permissions are assigned, and the same name/password combination is used on each machine) must exist on all the machines related to the DPE installation, including the examination and database machines, and on both the Case Folder machine and on the Evidence Folder machine. This means physically going to those machines and adding the correct user accounts manually.
10. When you have finished adding the User Credentials, click **Next** to continue.
11. Click **Install** when the Ready to Install the Program screen appears.
12. Wait while the AccessData Distributed Processing Engine files are copied into the selected path on the local machine.
13. The default path is:

    **[*Drive*]:\Program Files\AccessData\Distributed Processing Engine\<Version>.**
14. Click **Finish** to complete the install and close the wizard.

### If the service fails to start

1. Leave the *Retry/Quit* dialog open and launch the Services (**services.msc**) dialog from the run command.
2. Open the *Properties* dialog for the AccessData Processing Engine Service.
3. Click the **Log On** tab.
4. Verify that the logon credentials used have full Administrative rights.
5. Save the settings and exit the *Properties* dialog.
6. Stop and start the service manually.
7. Click **Retry** on the installer screen.

# Configuring Distributed Processing

Once the AccessData Distributed Processing Engine is installed on the non-examination machines, configure Distributed Processing to work with the local Processing Engine.

### To configure Distributed Processing to work with the local Lab Processing Engine

1. In *Case Manager*, click **Tools > Processing Engine Config**.
2. Enter the appropriate information in each field, according to the following guidelines:
   - *Computer Name/IP*: Enter the IP address of the computers where the Distributed Processing Engine is installed. The computer name can also be used if the name can be resolved.
   - *Port:* The default port is 34097. This is the port the processing host will use to communicate with the remote processing engines.
   - *Add*: Adds the computer and port to the list. You can add up to three remote processing engines (for a total of 4 engines). When the maximum number of DPE machines is reached, the Add button will become inactive.
   - *Remove*: Removes a processing engine from the list of available engines. The localhost engine cannot be removed.
   - *Enable*: Enables the engine for use by the processing host. Until implemented, each engine you add will be set to enabled (Disabled = False) by default. When implemented, you will be able to change the selected computer's status from Disabled to Enabled.
   - *Disable*: Makes the engine unavailable for use in processing. When implemented, you will be able to change the selected computer's status from Enabled to Disabled. The disabled remote engine will remain on the list, but will not be used.
   - *Disabled* = *True:* Displays for that engine in the DPE list.
   - *Maintain* UI *performance while processing*: Allows you to decide whether processing speed or UI performance is more important.

   **Note:** This will slow processing, and when selected, applies to *all* Remote DPEs.

3. When all DPE machines have been added to the Processing Engine Configuration dialog, click **Close**.

If you have not yet configured the Distributed Processing Engine on the remote computers, or if you have, but it is not working properly, you will see the warning shown in the following figure.

### To correct this

1. On the remote computer having the Distributed Processing Engine installed, click **Start**.

   1a. Right-click **My Computer.**

   1b. Click **Manage.**

   1c. Under *System Tools*, click **Local Users and Groups.**

   1d. Click **Groups**.

   1e. Double-click **Administrators.**

   1f. Verify that the user account name that was used in installation is in this group.

   1g. Click **OK** to close this dialog.

2. Under Local Users and Groups, click **Users.**

   2a. Find the user account name in the list, and double-click it.

   2b. Mark the box **User cannot change password**.

   2c. Mark the box **Password never expires**.

2d. Click **Apply**.

2e. Click **OK.**

3. Do one of the following:

- Under Services and Applications, click **Services**.
- If you already closed the Computer Management dialog, launch the Services (`services.msc`) dialog from the Run command on the Start menu.

3a. Open the Properties dialog for the AccessData Processing Engine Service.

3b. In the General tab, find Startup Type. If it says Automatic, proceed to the next step. If it says anything else, click the drop-down on the right side of the text box and select Automatic from the list. Click **Apply** and proceed to the next step.

3c. Open the *Log On* tab.

3d. Verify that the *Log On information* is set to the user name, domain or DPE machine name, and password that matches the user account you just verified (should be the one that was entered during installation).

3e. Click **OK**.

4. Right-click on the *AccessData Processing Engine Service.*
5. Click **Stop** to stop the service.
6. Click **Start** to re-start the service manually.
7. Click **Retry** on the installer screen.
8. Ensure that the user name provided during installation is a member of the Administrators account.

# Using Distributed Processing

**To utilize the Distributed Processing Engine when adding evidence to a case**

1. Make sure the case folder is shared before trying to add and process evidence.
2. Enter the path to the case folder in the *Create New Case* dialog in UNC format.
3. Click **Detailed Options**, and select options as you normally would.
4. Click **OK** to return to the *New Case Options* dialog.
5. Mark **Open the case** and then click **OK** to create the new case and open it.
6. The new case is opened and the *Manage Evidence* dialog is automatically opened. Click **Add**. Select the evidence type to add. Select the evidence file to add and then click **Open**.
7. The path to the evidence is designated by drive letter by default. Change the path to UNC format by changing the drive letter to the machine name or IP address where the evidence file is located, according to the following syntax:

   \\[*computername_or_IP_address*]\[*pathname*]\[*filename*]
8. Leave the remaining path as is.
9. Click **OK**.

## *Checking the Installation*

When you have completed the installation, open the Task Manager on the remote computer, and keep it open while you add the evidence and begin processing. This will allow you to watch the activity of the ProcessingEngine.EXE in the Processes tab.

The Distributed Processing Engine does not activate until a case exceeds approximately 30,000 items. When it does activate, you will see the CPU percentage and Memory usage increase for the ProcessingEngine.EXE in Task Manager.