

AccessData FTK Quick Installation Guide

Document date: December 5, 2014

©2014 AccessData Group, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Introduction

This guide focuses on the more basic aspects of the installation and is not intended to address all installation possibilities. The procedures in this guide assume a single-box installation.

For more detailed installation instructions, see the *FTK Installation Guide*. You can access this guide on the FTK download page at:

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

Also refer to the *Release Notes* for specific issues regarding installation. The Release Notes are available on the same web page.

Planning to Install FTK

Prerequisites

The following prerequisites apply for installing and running FTK:

- A computer running a supported operating system
For a list of supported platforms for FTK, see the following:
<http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk/technical>
- A supported database
[Choosing a Database Application to Use](#) (page 2)
- A WIBU-SYSTEMS CodeMeter USB or Virtual CmStick
See the *FTK Installation Guide*.

Choosing a Database Application to Use

FTK requires using one of the following database applications:

PostgreSQL	PostgreSQL is provided free of charge by AccessData and can be installed automatically as part of the FTK suite. For information about upgrading PostgreSQL, see the <i>FTK Installation Guide</i> . The following versions are supported: 9.0.x, 9.1.6, 9.1.11, 9.1.13, or 9.3.5
Microsoft SQL Server 2008 R2 or 2012	You can use your own installations of Microsoft SQL. See the <i>FTK Installation Guide</i> .
Oracle 10.2.0.4	You can use your own installations of Microsoft Oracle. Oracle 11g is not supported. See the <i>FTK Installation Guide</i> .

Before installing FTK, you must choose which database application to use. If you are not going to use PostgreSQL and will use Oracle or Microsoft SQL, you must first install the database before installing the FTK suite.

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.

Planning for a New Installation

Planning a New FTK Installation using PostgreSQL

- PostgreSQL 9.3.5 is available free of charge with the FTK installation files.
See [Download & Preparation](#) on page 3.
- You can do one of the following:
 - Use the simplified installation to install PostgreSQL, and all FTK components
 - Perform a custom installation and install PostgreSQL manually 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 the *FTK Installation Guide*.

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 7.

- For information about obtaining and applying Oracle Critical Patch Updates, see the *FTK Installation Guide*.

Planning for a Upgrade

See [Upgrading FTK](#) on page 9.

Installing AccessData Forensic Toolkit

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* -- These 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.

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	<p>This option is a “single-click” installation that installs all of the applications with default settings.</p> <p>This option is used for a single-box installation which is best suited for evaluation only. If a database is already installed, the Advanced option is only available.</p> <p>Note: This installation uses a pre-set PostgreSQL database administrator account detailed below.</p> <p>See Performing a Default Installation of the FTK Suite on page 5.</p> <p>See Initializing the FTK Database and Creating an Application Administrator Account on page 7.</p>
Advanced	<p>This option lets you select which applications to install. It also lets you choose folder locations for the features.</p> <p>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.</p> <p>See Performing an Advanced Installation of the FTK Suite on page 5.</p>

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 7.
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 the 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 7.

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 your database administrator account credentials.
 - If you used the default installation, enter the following credentials:
Username: postgres
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.

Installing Additional Programs

For information about installing Known File Filter (KFF), License Manager, and Language Selector, see the *FTK Installation Guide*.

Configuring and Managing Databases for FTK

See the *FTK Installation Guide*.

Upgrading FTK

For information about upgrading PostgreSQL, see the *FTK Installation Guide*.

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.

<p>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. For example:</p> <ul style="list-style-type: none"> • FTK 4.2 with Oracle 10g to FTK 5.6.x with Oracle 10g • FTK 4.2 with PostgreSQL 9.1.6 to FTK 5.6.x with PostgreSQL 9.1.x 	<p>One-step upgrade process:</p> <ol style="list-style-type: none"> 1. In FTK 5.1, upgrade the case using the Copy Previous Case feature. <p>See Upgrading Cases on page 10.</p>
<p>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. For example:</p> <ul style="list-style-type: none"> • FTK 4.2 with Oracle to FTK 5.x with either PostgreSQL or SQL • FTK 4.2 with PostgreSQL 9.0.x to FTK 5.x with PostgreSQL 9.1.11 • FTK 4.2 with PostgreSQL 9.0.x to FTK 5.x with SQL 	<p>Two-step migration process:</p> <ol style="list-style-type: none"> 1. In FTK 4.2.x or 5.0.x, backup the case using the database independent format. 2. In FTK 5.0.x, restore the backed-up case. <p>See Migrating Cases to a Newer Version of FTK and Different Database on page 11.</p>
<p>Moving a case from one type or version of a database to another while using the same version of FTK. For example:</p> <ul style="list-style-type: none"> • FTK 5.x with Oracle to FTK 5.x with either PostgreSQL or SQL • FTK 5.x with PostgreSQL to FTK 5.x with SQL or Oracle • FTK 5.x with SQL to FTK 5.x with either PostgreSQL or Oracle 	<p>Two-step move process:</p> <ol style="list-style-type: none"> 1. In FTK 5.0.x, backup the case using the database independent format. 2. In FTK 5.0.x, restore the backed-up case. <p>Moving Cases from One Database to Another (page 12)</p>

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 10.

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 13.
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 14.

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 13.
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 14.

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 subfolder of 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 15.
- Share the case folder and assign appropriate permissions. See [Share the Case Folder](#) on page 16.
- Configure the database services to run under service account. See [Configure Database Services](#) on page 16.
- Share back up destination folder with appropriate permissions. See [Share the Backup Destination Folder](#) on page 17.

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.

Uninstalling KFF

To uninstall KFF, you uninstall the following components:

- AccessData FTK Suite
 - AccessData Forensic Toolkit
 - AccessData Evidence Processing Engine
- Database

Important: If you plan on re-installing FTK and want access to your cases, do not delete the database without backing it up.

- Other AccessData components:
 - Code Meter Runtime Kit
 - AccessData License Manager
 - ColorPlus Driver VB