AccessData

Forensic Toolkit

Upgrading, Migrating, and Moving Cases

Version: 5.x

AccessData®

A Pioneer in Digital Investigations Since 1987

AccessData Legal and Contact Information

Document date: March 27, 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.
588 W. 400 S.
Suite 350
Lindon, Utah 84042
U.S.A.

www.accessdata.com

AccessData Trademarks and Copyright Information

- AccessData® is a registered trademark of AccessData Group, Inc.
- AD InSight® is a registered trademark of AccessData Group, Inc.
- AD Summation is a registered trademark of AccessData Group, Inc.
- Distributed Network Attack® is a registered trademark of AccessData Group, Inc.
- DNA® is a registered trademark of AccessData Group, Inc.
- Forensic Toolkit® is a registered trademark of AccessData Group, Inc.
- FTK® is a registered trademark of AccessData Group, Inc.
- Password Recovery Toolkit® is a registered trademark of AccessData Group, Inc.
- PRTK® is a registered trademark of AccessData Group, Inc.

- Registry Viewer® is a registered trademark of AccessData Group, Inc.

Upgrading, Migrating, and Moving Cases

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), 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 (4.0.1, 4.2.1), it replaces the previous version. 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 5.3), 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 5.3and using the same type and version of the database. For example: • FTK 4.2 with Oracle 10g to FTK 5.3.x with Oracle 10g • FTK 4.2 with PostgreSQL 9.1.6 to FTK 5.3.x with PostgreSQL 9.1.x	One-step upgrade process: 1. In FTK 5.1, upgrade the case using the Copy Previous Case feature. See Upgrading Cases on page 5.
Migrating a case from FTK 4.2.x or 5.x to FTK 5.3 and changing to a different type or version of the database. For example: • 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	Two-step migration process: 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. See Migrating Cases to a Newer Version of FTK and Different Database on page 6.
Moving a case from one type or version of a database to another while using the same version of FTK. For example: • 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	Two-step move process: 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. Moving Cases from One Database to Another (page 7)

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 5.

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 8.
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 9.

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 8.
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 9.

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. 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. 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 10.
- Share the case folder and assign appropriate permissions. See Share the Case Folder on page 10.
- Configure the database services to run under service account. See Configure Database Services on page 11.
- Share back up destination folder with appropriate permissions. See Share the Backup Destination Folder on page 12.

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.