DBControl for FTK 4.2.x

Introduction: DBContol is a command line database administration tool, used to manipulate the database(s) used by AccessData's products. The following explains how to use the versions of DBControl shipped with FTK 4.2. Full documentation for DBControl can be found at http://wiki.accessdata.dev/index.php?title=Dbcontrol, but the commands listed are the ones most commonly used with FTK.

Notes:

- You should always use the version of DBControl shipped with the version of FTK whose data you wish to manipulate
- The DBControl executable is usually located at "C:\Program Files\AccessData\Forensic Toolkit\[version]\bin\ "

Usage:

dbcontrol [param=value ...] [-noprompt] -command [args ...]

Parameters

Parameter	Value	Description
dbtype=	oracle|postgres|mssql	Specifies the database type.
host=	<IP or Host Name>	Specifies the location of database. "Localhost" is assumed if not specified.
sid=	<SID>	Specifies the SID. "ADG" is assumed if not specified. Must specify "FTK2" for Oracle.
port=	<Port>	Specifies the database port. Default ports are assumed if not specified.
sysuser=	<System Username>	Specifies the database system username. Default usernames are assumed if not specified.
syspass=	<System Password>	Specifies the database system password. If one is needed but not specified, you will be prompted to enter it.
schema=	<Schema>	Specifies the database schema. "ADG53" is assumed if not specified.
schematype=	unified|adms	Specifies the schema type. "Unified" is assumed if not specified.
schemapass=	<Schema Password>	Specifies the schema password. If one is needed but not specified, you will be prompted to enter it.
pgdb=	<SID>	Specifies the SID for PostgreSQL. This parameter implies "dbtype=postgres sid=<SID>".

Commands

Most commands affect the version of FTK that DBControl was bundled with (eg. the version of DBControl packaged with FTK 4.2 affects FTK 4.2 and the ADG53 schema).

Command	Argument	Description
-help		Lists DBcontrol usage help.
-noprompt		Hides any prompts.
-install		Creates the ADGxx schema associated with your current version of FTK.
-uninstall		Deletes the ADGxx schema and cases associated with your current version of FTK. If used in conjunction with "schematype=adms", it will delete the ADMS schema.
-reinstall		Deletes the ADGxx schema and cases associated with your current version of FTK, then re-creates the appropriate schema.
-deletecase	<Case ID>	Deletes the specified case from your current version of FTK.
-validate	<Case ID> |BLANK	Validates the specified case in your current version of FTK. If you do not specify a Case ID it will validate all cases in the current version.
-validate fix	<Case ID> | BLANK	Attempts to repair the specified case in your current version of FTK. If you do not specify a Case ID it will attempt to repair all cases in the current version.
-ftkmigration	See below for arguments and usage.	Migrates an FTK 4.1 case from a database independent backup to your current version of FTK.
-ftkcopyschema	See below for arguments and usage.	Migrates a live FTK 4.1 case to your current version of FTK. Only works when both FTK 4.1 and your current version use the same database.
-ftkgetavailableschemas		Lists all valid FTK 4.1 cases existing on the current server.
-backup	See below for arguments and usage.	Backs up an existing case from your current version of FTK.
-archive	See below for arguments and usage.	Archives an existing case from your current version of FTK. If an archive (in "DB f-0") already exists, you must manually rename the current archive folder so DBControl can create a new "DB f-0" folder.
-restore	See below for arguments and usage.	Restores a case backup to your current version of FTK.
-attach	See below for arguments and usage.	Attaches a case archive to your current version of FTK.
-updatekffconfig		Update old KFF Server syntax to Elastic Search syntax in Case Preferences.

Usage for –ftkmigration

-ftkmigration backuppath=<Folder Path> preserve

Argument	Value	Description
backuppath=	<Folder Path>	Specifies the path of the FTK 4.1 case's database independent backup. Quotes must be used if the path has spaces. This argument is required.
casepath=	<Folder Path>	Specified the folder for the new case. Quotes must be used if the path has spaces. If not specified, it will use the same case folder as the old case.
preserve		Preserves that case, user, and custodian IDs from the backup. If not used, you will be prompted what new IDs to link to.

Usage for –ftkcopyschema

-ftkcopyschema db=<SID> caseid=<Case ID>

Argument	Value	Description
db=	<SID>	Specifies the SID with the FTK 4.1 cases (usually "FTK2"). This argument is required.
caseid=	<Case ID>	Specifies the case ID of the FTK 4.1 case that will be migrated. This argument is required.

Usage for –backup

-backup caseid=<Case ID> backuppath=<Folder Path> usenative=[true|false] dbpath=<Folder Path> keepcasefolder=[true|false]

Argument	Value	Description
caseid=	<Case ID>	Specifies the ID of the case to backup. This argument is required.
backuppath=	<Folder Path>	Specifies the destination path for the backup. This folder should not already exist. Quotes must be used if the path has spaces. This argument is required.
usenative=	true|false	"True" will create the backup in database-native format. "False" will create the backup in database-independent format. "False" is assumed if not specified.
dbpath=	<Folder Path>	Specifies the intermediate path for DB files. Quotes must be used if the path has spaces. This argument is required if the DB doesn't have write access to the backup path.
keepcasefolder=	true|false	"True" keeps a copy of the case folder. "False" does not. "True" is assumed if not specified.

Usage for –archive

-archive caseid=<Case ID> usenative=[true|false] dbpath=<Folder Path> keepcasefolder=[true|false]

Argument	Value	Description
caseid=	<Case ID>	Specifies the ID of the case to archive. This argument is required.
usenative=	true|false	"True" will create the archive in database-native format. "False" will create the archive in database-independent format. "False" is assumed if not specified.
dbpath=	<Folder Path>	Specifies the intermediate path for DB files. Quotes must be used if the path has spaces. This argument is required if the DB doesn't have write access to the case folder.

keepcasefolder=	true|false	"True" keeps a copy of the case folder. "False" does not. "True" is assumed if not specified.

Usage for –restore

-restore backuppath=<Folder Path> dbpath=<Folder Path> casepath=<Folder Path> keepcasefolder=[true|false]

Argument	Value	Description
backuppath=	<Folder Path>	Specifies the backup path. Quotes must be used if the path has spaces. This argument is required.
dbpath=	<Folder Path>	Specifies the intermediate path for DB files. Quotes must be used if the path has spaces. This argument is required if the DB doesn't have read access to the backup path.
casepath=	<Folder Path>	Specifies the destination path for the restored case. Quotes must be used if the path has spaces. Backup path is assumed as the destination if not specified.
keepcasefolder=	true|false	"True" keeps a copy of the case folder. "False" does not. "True" is assumed if not specified.

Usage for –attach

-attach casearchivefolder=<Folder Path> dbpath=<Folder Path> keepcasefolder=[true|false]

Argument	Value	Description
casearchivefolder=	<Folder Path>	Specifies the archive path. Quotes must be used if the path has spaces. This argument is required.
dbpath=	<Folder Path>	Specifies the intermediate path for DB files. Quotes must be used if the path has spaces. This argument is required if the DB doesn't have read access to the backup path.
keepcasefolder=	true|false	"True" keeps a copy of the case folder. "False" does not. "True" is assumed if not specified.

Examples:

Create the FTK 4.2 shared schema, using Oracle:

dbcontrol dbtype=oracle sid=FTK2 -install

Delete the ADMS schema, using PostgreSQL on port 5433:

dbcontrol pgdb=ADG port=5433 schematype=adms -uninstall

Delete and rebuild the FTK 4.2 shared schema, using MSSQL on 192.168.1.150:

dbcontrol dbtype=mssql host=192.168.1.150 -reinstall

Delete case 10 from FTK 4.2, using PostgreSQL:

dbcontrol dbtype=postgres -deletecase 10

Validate case 15 in FTK 3.3, using Oracle:

dbcontrol dbtype=oracle sid=FTK2 -validate 15

Validate and attempt to repair case 20 in FTK 4.2, using MSSQL:

dbcontrol dbtype=mssql -validate fix 20

Migrate a case from a FTK 4.1 database independent backup at C:\Backup, to FTK 4.2, using PostgreSQL, storing the new case folder at C:\Case:

```
dbcontrol pgdb=ADG-ftkmigration backuppath=C:\Backup casepath=C:\Case
```

Migrate case 1005 from FTK 4.1, using Oracle, to FTK 4.2, using Oracle:

```
dbcontrol dbtype=oracle sid=FTK2 -ftkcopyschema db=FTK2 caseid=1005
```

Backup case 5 from FTK 4.2, using PostgreSQL, to C:\Case Backups\5:

```
dbcontrol pgdb=ADG -backup caseid=5 backuppath="C:\Case Backups\5"
```

Archive case 15 from FTK 4.2, using MSSQL:

```
dbcontrol dbtype=mssql -archive caseid=15 usenative=true
```

Restore a backed up case to FTK 4.2, using Oracle, from C:\Case Backups\5 to the same path:

```
dbcontrol dbtype=oracle sid=FTK2 -restore backuppath="C:\Case Backups\5"
```

Attach an archived case to FTK 4.2, using MSSQL, from C:\Cases\30:

```
dbcontrol dbtpe=mssql -attach casearchivefolder=C:\Cases\30
```