globalscape
by HelpSystems

EFT v8.0.7
Auditing and Reporting Guide

Copyright Terms and Conditions

202112150409

Table of Contents

Auditing and Reporting

The topics below provide the procedures for configuring and using Auditing and Reporting with EFT.

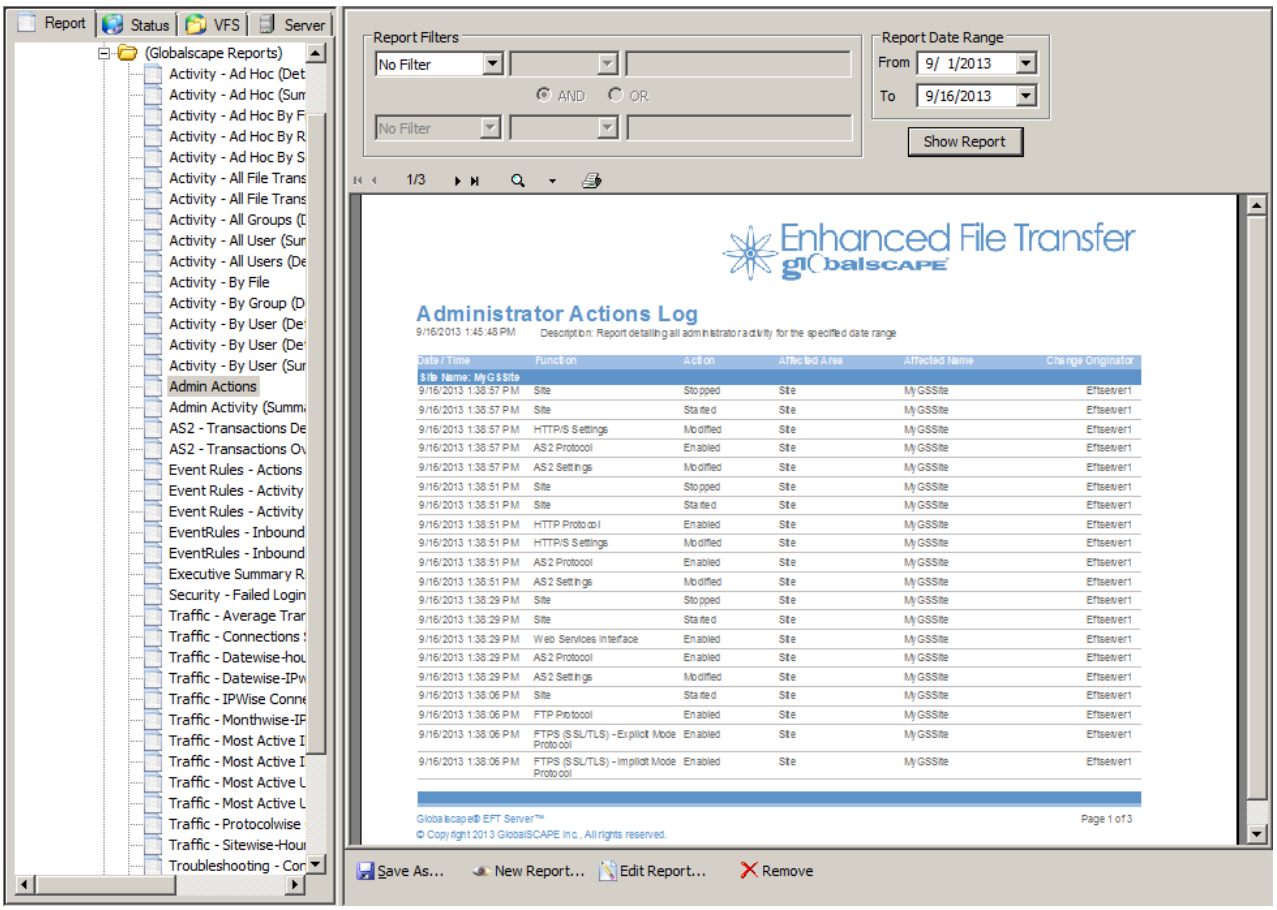
Introduction to the Auditing and Reporting Module

The Auditing and Reporting Module (ARM) captures the transactions passing through EFT and provides an interface in the administration interface where you can use preconfigured reports or create your own custom reports to query, filter, and view transaction data. Data is stored in a relational database and can be analyzed in real time.

The ARM comes with a number of preconfigured reports to help you start analyzing data right away. The built-in reports were designed to respond to the most common data analysis requests.

Auditing and Reporting Interface

The **Report** tab of the administration interface is the interface for Auditing and Reporting.



- When you click the **Report** tab in the left pane, the right pane displays the report. Using the controls in the right pane, you can view, edit, print, and save the report or create a new report.
- When you define a new report template, it appears in the **Custom Reports** node of the tree.
- Refer to Generating a Report, Managing Reports, and Custom Reports for details of running, managing, and defining reports.
- Refer to Descriptions of Preconfigured Reports for descriptions of the report templates in the Globalscape Reports node of the tree.

Installing and Configuring Auditing and Reporting

The topics below provide the procedures for installing and configuring the Auditing and Reporting module.

See also: Script for Creating Necessary ODBC Tables

Installing and Configuring Auditing and Reporting

Auditing and Reporting is normally installed and configured when you install EFT. If you did not install it when you installed EFT, you can run the installer again, choose **Modify**, and then select the **Auditing and Reporting** check box. (Leave the **EFT** and **EFT administrator Interface** check boxes selected; clearing the check boxes will uninstall them.)

Refer to Installing EFT, administrator, and Modules for the procedure for installing ARM using the EFT installer and for the system requirements.

- For EFT to connect to any database, the proper drivers need to be installed on the EFT computer. If the right client-side software (driver) is installed on the EFT computer, the Advanced Workflow Engine can make the database connection string to get to that database.
- EFT uses Microsoft ActiveX Data Objects (ADO) 2.7 or later to handle database communication, which in turn should load the Oracle drivers to handle Oracle implementation details. How and what is connected largely depends upon the connection string. By default, if you do not supply the entire connection string in EFT, the Oracle connection string should look like:

```
Provider=OraOLEDB.Oracle.1; Data Source=(DESCRIPTION =
(ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = {host
value})(PORT = {port})))"

(CONNECT_DATA =(SERVICE_NAME = {database name})));

Persist Security Info=true;PLSQLRSet=1;PwdChgDlg=0;User Id=
{username};Password={password};
```

Installation and configuration of the module consists of:

1. Running the EFT installer. The Auditing and Reporting module is normally installed and configured when you install EFT. If you did not install it when you installed EFT, you can run the installer again and choose **Modify**. On the **ARM** page of the installer, click **Configure Auditing and Reporting**. (Follow the procedure in Installing EFT, administrator, and Modules.)

   During installation, EFT needs full DB Owner access to the auditing database to set up the schema. During updates or upgrades, EFT needs full DB Owner access to update the schema. Once it is set up, EFT only needs to be able to read, write, and execute stored procedures.

2. Activating the software with a serial number that includes ARM
3. Enabling EFT to record data

How does EFT know which TCP/IP port it should use to connect to SQL Server?

When the SQL Server browser service (installed with SQL Server) starts up, it searches the advanced properties for any "named instances" of SQL Server and which TCP ports they're listening on. When a client wants to connect to a named instance, it asks the browser service (on UDP port 1434) on which TCP/IP port is that instance listening. This is how Microsoft implemented support for multiple instances of SQL Server on the same computer. The default instance listens on TCP port 1433. If you have a named instance, the TCP port is dynamically configured.

This is standard SQL Server functionality and doesn't require special port syntax in the EFT connection string or host name. It's all abstracted by the API used, which looks at the host string and figures out whether you're trying to connect to a named instance or a default instance (by determining whether host\instance or just host was specified).

The SQL Server TCP settings are stored in:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\
MSSQL10.<InstanceName>\MSSQLServer\SuperSocketNetLib\TCP\
```

Refer to the following Microsoft topics for more information:

- For details of how to view/change the TCP information in the SQL Server Configuration Manager, refer to the following MSDN article: http://msdn.microsoft.com/en-us/library/ms177440%28SQL.90%29.aspx, "How to: Configure a Server to Listen on a Specific TCP Port (SQL Server Configuration Manager)."

- http://support.microsoft.com/kb/287932, "Configure the Windows Firewall to Allow SQL Server Access"
- http://msdn.microsoft.com/en-us/library/ms175483.aspx, "Connecting to SQL Server over the Internet"
- http://msdn.microsoft.com/en-us/library/ms181087.aspx, "SQL Server Browser Service"

EFT Database Utility

A command line utility is included in the installer that is capable of performing various database-related tasks. This same utility is used by the EFT installer to handle upgrades of existing databases. Typically, all common database tasks are handled by the EFT installer. However, on occasion it may be useful to use the command-line utility to verify the status of a database or perform an upgrade independent of the EFT installation process.

The database utility (DBUtility.exe) is included as part of the core EFT installation. Once installed it is located in the "DBUtility" sub-directory of the EFT program files installation directory. Typically this will be **C:\Program Files (x86)\Globalscape\EFT Server\DBUtility**.

Requirements

- The utility requires the .NET Framework 4 (Full version)
- When operating against an Oracle database, the utility requires the 32-bit version of the Oracle Data Access Components (ODAC)

Capabilities

The database utility is capable of performing the following tasks:

- Check the version of the database to see if it is up to date. This may be used to see if an upgrade must be performed on a database before it is ready to be used by EFT.
- Generate an SQL script that may be used to create a new database schema (tables, views, etc.) manually within an existing database.
- Generate an SQL script that may be used to upgrade an existing database schema manually.
- Analyze an existing database prior to performing an upgrade. The analysis will verify prerequisites, display information about the database, and display the SQL that will be used to upgrade the database.
- Upgrade an existing database schema to the latest version.

Logging

The utility is capable of outputting various levels of information ranging from errors to debug/trace level information.

By default, the utility will output errors, warnings, and informational messages to the command window. If the "-verbose" command line parameter is specified, the utility will also output more fined-grained debug/trace level messages to the command window.

The utility may also optionally output to a log file as specified using the "-logfile" command line option. The output to the log file will include all levels of messages from errors to debug/trace level information.

SQL Scripts

The utility requires the presence of various SQL Scripts located in database-specific subdirectories to perform its actions. These subdirectories contain scripts such as:

- create_* - scripts used for creating new, clean database schemas for use by the EFT application
- Purge* - scripts that may be used for purging data from the database
- *ODBC - scripts that may be used to create the necessary tables to use an ODBC data source for user authentication
- upgrade_* - upgrade scripts for upgrading various versions of the database

By default, the utility will look for the "SQL Server" and "Oracle" directories under its current working directory. During installation of the Database utility, these script directories will be created under the <InstallDir>\DBUtility directory, so the scripts will be available to the utility.

If the utility is unable to locate these subdirectories, it will also look for the EFT "AppData" path in advanced properties and then look for the subdirectories under that location.

Additionally, the user may specify an alternate parent directory using the "-scripts" command line parameter.

Usage

The database utility is a command line utility and may be executed by opening a Windows Command Prompt and navigating to the "DBUtility" subdirectory of the EFT installation folder (for example, **C:\Program Files (x86)\Globalscape\EFT Server\DBUtility**) and running the command "DBUtility.exe."

Each of the scripts has comments at the top describing their usage.

Help

The utility includes built-in help documentation. Additionally, the utility will provide feedback on incorrect or missing command line parameters.

The built-in help documentation for the utility may be accessed using the command:

```
DBUtility.exe -help
```

More detailed help for the various top-level actions may be accessed using the command:

```
DBUtility.exe -help -action <Action ID>
```

Where <Action ID> is one of:

- **CheckVersion** - checks the version of the database to see if it is up to date
- **CreateScript** - generates a SQL script that may be used to manually create a new database schema
- **UpgradePreview** - used prior to upgrading a database. This action will generate and display useful pre-upgrade information as well as the actual SQL that will be used to upgrade the database
- **UpgradeSchema** - upgrades the database, if needed
- **UpgradeScript** - generates a script that may be used to manually upgrade a database

Examples

Example executions for each of the actions supported by the utility may be viewed in the command line help for each action.

DBUtility Command Line Parameters

The following section describes each of the command line parameters for the utility. Depending on the action performed, only a subset of the parameters will be applicable or required.

For the command line parameters that accept a value, the value should be enclosed in double-quotes if the value contains spaces. For example,

```
-logfile="C:\My Logs\MyLogFile.txt"
```

Parameter Definitions

- -help
  - Description: Display help on the command line. Refer to the "Help" section above for additional information.
- -logfile=<file>
  - Description: When specified the utility will log output of the execution to the specified log file.
  - Default: None
  - Example:

    ```
    -logfile="C:\My Logs\MyLogFile.txt"
    ```

- -optionsfile=<file>
  - Description: When specified the utility will load command line parameters from the file. The file should specify parameters in a "parameter=value" pair with one pair specified per line. Parameters specified on the command line override parameters specified in the file.
  - Default: None
  - Example:

    ```
    -optionsfile="C:\My Scripts\MyOptionsFile.txt"
    ```
- -scriptfile=<file>
  - Description: For actions that generate output SQL scripts this parameter defines the file to which the script should be written.
  - Default: None
  - Example:

    ```
    -scriptfile="C:\My Scripts\MySQLScript.sql"
    ```
- -errorfile=<file>
  - Description: When specified the utility will log terminal errors to the specified file. Mainly used for error handling when the utility is called by the EFT installer.
  - Default: None
  - Example:

    ```
    -errorfile="C:\My Scripts\MyErrorFile.txt"
    ```
- - resultfile=<file>
  - Description: When specified the utility will output result status codes for the execution to the file. Mainly used for state handling when the utility is called by the EFT installer.
  - Default: None
  - Example:

    ```
    =resultfile="C:\My Scripts\MyResultFile.txt"
    ```
- -pause
  - Description: When specified the utility will pause at the end of the execution. Useful when executing the utility through a shortcut to keep the console window from closing before the user has a chance to review the results.
  - Default: None
- -verbose

  - Description: When specified the utility will output additional debug level logging.
  - Default: None
- -action=<id>
  - Description: Specifies the overall action to be performed by the utility.
  - Valid values:
    - **CheckVersion** - checks the version of the database to see if it is up to date
    - **CreateScript** - generates a SQL script that may be used to manually create a new database schema
    - **UpgradePreview** - used prior to upgrading a database. This action will generate and display useful pre-upgrade information as well as the actual SQL that will be used to upgrade the database
    - **UpgradeSchema** - upgrades the database, if needed
    - **UpgradeScript** - generates a script that may be used to manually upgrade a database
  - Default: None
  - Example:

```
-action=UpgradeSchema
```

- -type=<type>
  - Description: The dialect of the database.
  - Valid values:
    - SQLServer - a SQL Server/SQL Server Express database
    - Oracle - an Oracle database
  - Default: None
  - Example:

```
-type=SQLServer
```

- -server=<server>
  - Description: The database server host or IP address
  - Default: None
  - Example:

```
-server="Jupiter"
```

- -port=<port>

  - Description: The listener port for the database on the database server/host.
  - Default: None
  - Example:

```
-port=1433
```

- -instance=<instance>
  - Description: The database server instance name.
  - Default: None
  - Example:

```
-instance="MSSQLSERVER"
```

- -database=<database>
  - Description: The name of the database.
  - Default: None
  - Example:

```
-database="GLOBALSCAPE"
```

- -timeout=<timeout>
  - Description: The timeout, in seconds, to continue trying to connect to the database. A value of 0 causes the utility to wait indefinitely and should be used with caution.
  - Default: 30 seconds
  - Example:

```
-timeout=5
```

- -auth=<auth>
  - Description: The type of authentication to use when connecting to a SQL Server database.
  - Valid values:
    - SQLServer - Use SQL Server authentication which requires specification of the username and password.
    - Windows - Use Windows authentication which will use the currently logged in user account.
  - Default: None
  - Example:

```
-auth=SQLServer
```

- -user=<user>
  - Description: The login name to use when connecting to the database.
  - Default: None
  - Example:

```
-user="eftdbuser"
```

- -pass=<pass>
  - Description: The password to use when connecting to the database.
  - Default: None
  - Example:

```
-pass="3qym9NCebHDJ"
```

- -scripts=<dir>
  - Description: Parent directory containing the SQL Server and Oracle SQL Scripts subdirectories. Refer to the "SQL Scripts" section above for additional information.
  - Default: Refer to the "SQL Scripts" section above for additional information.
  - Example:

```
-scripts="C:\ProgramData\Globalscape\EFT Server"
```

Advanced Parameter Definitions

The following parameters are typically reserved for use by the EFT installer and will normally not be useful to end users. However, they are documented here for completeness.

- -conn=<connection string>
  - Description: When specified this string will be used as the full connection string to the database rather than constructing the string based on the distinct parts.
  - Default: None
  - Example:

```
-conn="Data Source=(DESCRIPTION=(ADDRESS_LIST=
(ADDRESS=(PROTOCOL=TCP)(HOST=mth-oracle)(PORT=1521)))
(CONNECT_DATA=(SERVICE_NAME=orastart));PersistSecurity
Info=true;User Id=eftdbuser;Password=3qym9NCebHDJ"
```

- -app=<application name>
  - Description: The application name to present to the database for use when identifying connections.

    - Default: None
    - Example:

```
-app="EFT Database Utility"
```

- -installerdir=<directory>
    - Description: The directory containing the EFT Installer. May be used during some upgrades for accessing or storing additional files.
    - Default: None
    - Example:

```
-
installerdir="C:\Users\administrator\AppData\Local\Temp
\nsdB57C.tmp"
```

- -installationdir=<directory>
    - Description: The directory where EFT is installed or will be installed. May be used during some upgrades for accessing or storing additional files.
    - Default: None
    - Example:

```
-installationdir="C:\Program Files
(x86)\Globalscape\EFT Server"
```

- -appdatadir=<dir>
    - Description: The directory that will be used for the EFT application data. May be used during some upgrades for accessing or storing additional files.
    - Default: None
    - Example:

```
-appdatadir="C:\ProgramData\Globalscape\EFT Server"
```

- -backupdir=<dir>
    - Description: The directory in which to store backup data. May be used during some upgrades.
    - Default: None
    - Example:

```
-backupdir="C:\ProgramData\Globalscape\EFT
Server\Backup"
```

Database User Account Privileges

The database user account used by EFT must have certain privileges within the database for the application to function correctly. Additionally, a different set of privileges are needed for Installation, Upgrade, and Runtime, as described below.

Installation—When creating a new database, the EFT installer is capable of creating the database user account for you. Alternatively, you may create the database user account ahead of time. Either way, the EFT database user account must have certain privileges during the creation process. Once the creation process is complete, the privileges may be reduced to those necessary for runtime operation. (Refer to Runtime below.)

The following privileges, or their equivalents, are required during the creation process:

- SQL Server—The database user account must have the "db_owner" database role membership.
- Oracle—The database user account must have the following privileges:
  - CREATE SESSION
  - CREATE TABLE
  - CREATE TRIGGER
  - CREATE SEQUENCE
  - CREATE PROCEDURE
  - CREATE VIEW

Upgrade—When upgrading the ARM database, either through the EFT Installer or the Database Utility (**DBUtility.exe**), you should use the EFT database user account to connect to the database to perform the upgrade. The upgrade process may temporarily require that additional privileges be temporarily given to the EFT database user account. The actual set of privileges depends on the version of the database schema being upgraded. Before upgrading the database, the EFT Installer will perform an analysis of the database. Additionally, the "UpgradePreview" action may be used with the Database Utility to perform the analysis. Part of this analysis will verify that the database user account possesses the necessary privileges to perform the upgrade. The analysis results will display any privileges that the account is lacking. **You will need to grant the appropriate privileges to the account temporarily before proceeding with the upgrade.** These privileges may be revoked once the upgrade process is complete. Refer to the Runtime section below for the privileges required during subsequent operation of EFT. To minimize the chance of encountering missing privileges, you should grant the privileges described in Installation, above, before performing the upgrade preview analysis.

Runtime—During normal operations, the EFT only manipulates the data within the database while auditing, and so requires less powerful privileges. EFT does not modify the database schema during normal operation. If you want to lock down the EFT database user accounts during normal operation, ensure that the following minimal privileges, or their equivalents, are granted to the account:

- SQL Server—When operating against SQL Server, the EFT database user account only needs to be able to read data, write data, and execute stored procedures. The following permissions are required during normal operation:
  - CONNECT
  - DELETE
  - EXECUTE
  - INSERT
  - SELECT
  - UPDATE
- Oracle—During normal operation, the EFT database operates only within its own schema. Additionally, it has no need to create objects during runtime. Only the following privilege is required during normal operations:
  - CREATE SESSION

Activating the Auditing and Reporting Module

The Auditing and Reporting Module (ARM) is an add-on to EFT that comes with a unique activation serial number.

- If you have purchased EFT with ARM and have your serial number, follow the normal activation process.
- If you are upgrading, follow the upgrade process.

Upgrading the EFT Database

This introduction describes in general how an EFT database upgrade works.

A Database Utility (**DBUtility.exe**) is used to upgrade the database, when applicable. You have the option of either upgrading the database during the upgrade process within the EFT Installer or choose to upgrade the database "out of band" later using the Database Utility. Because the EFT installer uses the same Database Utility internally to perform the upgrade, the methods are synonymous.

As part of this new approach to upgrading the ARM database, the database schema maintains an independent version number. This version is used to determine if the database schema and data require an upgrade across various releases of the EFT application. This

version number is maintained in a new table called "TBL_SCHEMA_VERSION." This new table is created as part of the initial ARM upgrade process when upgrading EFT.

During the upgrade, you will be prompted to provide the user credentials that should be used when connecting to the database. **You must provide the credentials for the EFT database user account, as opposed to the super-user accounts such as "sa" or "sys"**, because the upgrade process assumes it is operating as the database account that owns the schema to be upgraded. (Refer to Database User Account Privileges > Upgrade for information on the required database user account privileges necessary to successfully upgrade.)

When upgrading from within the EFT installation process, the installer will analyze the database prior to performing the actual upgrade. The results of this analysis are displayed in an upgrade preview page of the installer. Administrators are urged to read the results carefully prior to continuing with the upgrade. (EFT's upgrader does not check the database for fragmentation.)

The analysis step will determine whether the database requires an upgrade by examining the version number in the new version table. Across many builds and releases of the EFT application, the ARM database may not require any changes. As such, the version number for the database may not change as often as the EFT version. If the database does not require an upgrade, then the installer will state this and essentially skip the ARM upgrade process.

As with the database upgrade, the database analysis process used in the EFT installer is actually performed by the Database Utility and is equivalent to running the utility with the "-action=PreviewUpgrade" command line option. In addition to checking the database version number, the installer/utility will also check for various prerequisites needed to perform the upgrade. Prerequisites that have been met will be displayed with a "PASS" status. Any prerequisites that have not been met will be displayed with a "FAIL" or "WARN" status. These issues should be researched and rectified prior to proceeding with the upgrade.

Recommendations are provided along with any failed prerequisites suggesting how to resolve the issue. After remedying any errors, you can run the analysis again by clicking **Reanalyze**.

The analysis will also display information about the database such as the approximate size of the user data as well as the age of the user data within the database. Additionally, the SQL script that will subsequently be used to perform the actual upgrade will be displayed.

You may decide to upgrade the database later. If so, you can retain the upgrade script by clicking **View** to open the database analysis results in a text editor and then save to a file of your choosing.

Alternatively, you can run the EFT installer in maintenance mode or run the Database Utility using the "-action=UpgradeSchema" option to upgrade the database another time.

User Account Permission/Privilege Requirements

When upgrading the ARM Database, either through the EFT Installer or the Database Utility, you should use the EFT Database user account to connect to the database to perform the upgrade. This is as opposed to using one of the more privileged system accounts such as the "sa" account on SQL Server or the "sys" or "system" accounts on Oracle.

For additional information related to database user account privileges refer to Database User Account Privileges.

SQL Server

The user account used to upgrade the database should have the "db_owner" privilege. This is the default for the user account created for, and used by, the EFT. As such, no action is required on your part prior to upgrading.

Oracle

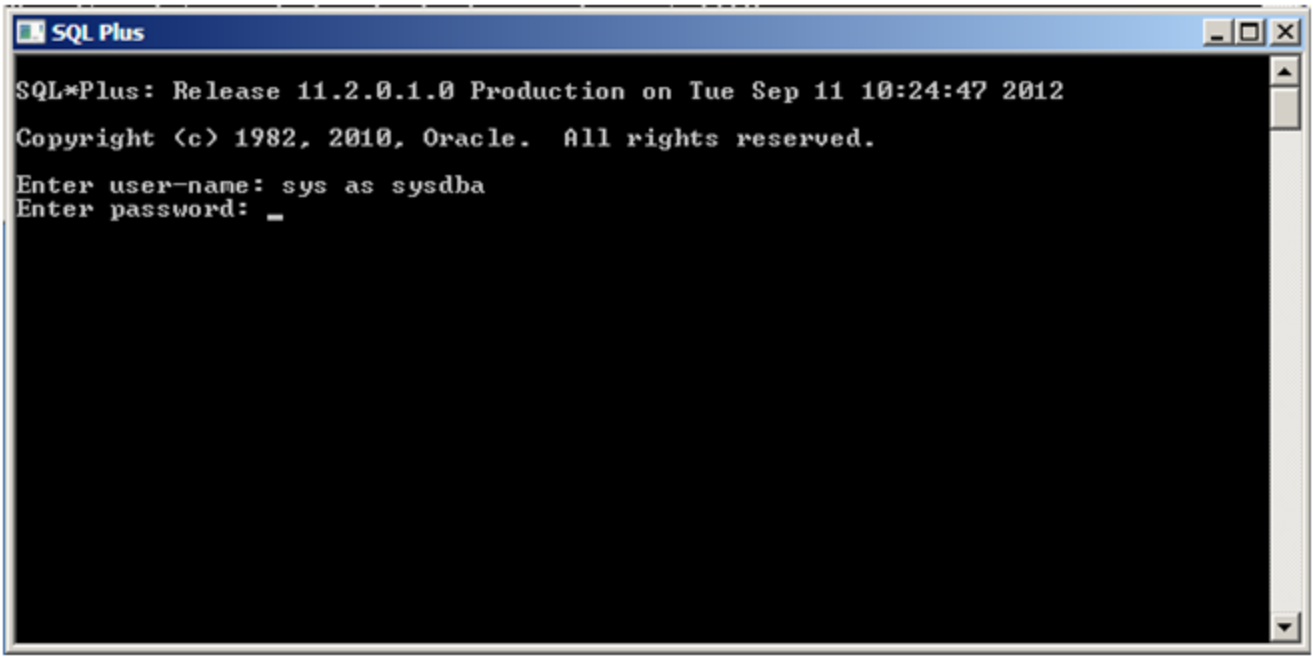
The ARM module makes use of database views. In previous releases, the database user account created for use by the EFT was not granted the ability to create views. As such, prior to upgrading an Oracle ARM database, you must grant this privilege to the EFT database user account manually. This is done by granting the "CREATE VIEW" privilege to the account using a more privileged account such as the "sys" or "system" account.

One method of granting the privilege is to connect to the database using the Oracle command line "SQL Plus" utility. On the computer where Oracle is installed, launch the SQL Plus utility:

- Click the SQL Plus **Start** menu shortcut (for example, **Start Menu > All Programs > Oracle - OraDb11g_home1 > Application Development > SQL Plus**)
- If the utility is available on the system path, then open a Windows command prompt (for example, **Start > Run > cmd.exe**), type `sqlplus` at the command prompt, and then press ENTER.

Once SQL Plus has started, you will be prompted for login credentials. Connect using a privileged account such as "sys" or "system". Be aware that when connecting as the "sys" account you must provide the "as sysdba" option; for example:

```
sys as sysdba
```



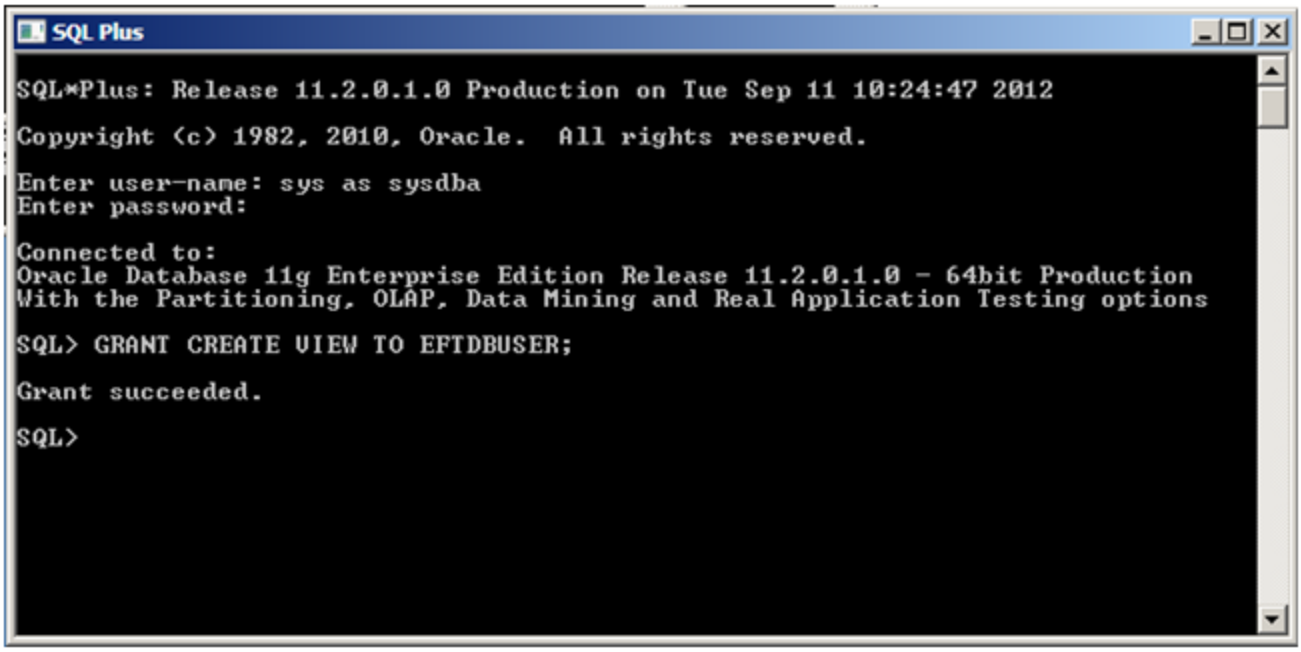
Complete the login process by providing the password.

Use the following command to grant the "CREATE VIEW" privilege to the EFT database user account:

```
GRANT CREATE VIEW TO <User>;
```

Where <User> is the name of the EFT database user account. For example:

```
GRANT CREATE VIEW TO EFTDBUSER;
```



Exit the SQL Plus tool by typing `Exit` and pressing ENTER.

Time Requirements

The time it takes to perform the upgrade depends both on the size of the database and the performance characteristics of the computer on which the database resides.

Our internal testing has shown that the database upgrade can take as little as 15 minutes for a moderately sized database of 5GB, up to 3 hours or longer for larger databases of 30GB or more. Because the time it takes to perform the upgrade is greatly dependent on CPU and Disk I/O speed, it is difficult to provide an exact time for any given situation.

For additional information related to upgrading large databases please refer to Upgrading Large Databases.

Refer to Upgrade Paths below for a discussion of the available upgrade paths that may be used to minimize down time.

Disk Space Requirements

The size of the database will grow as part of the upgrade because of changes in the data types used for storing character-based data.

Our internal testing indicates that, on average, the size of user data in the database will increase by approximately 31% as part of the upgrade process. For example, if your database consumes 10GB before upgrading, then it will use approximately 13GB after upgrading.

If disk space is limited, you should consider purging older data from the database prior to upgrading. For information on purging data from the ARM database, refer to Purging Data from the Database.

For additional information related to upgrading large databases, refer to Upgrading Large Databases.

SQL Server Considerations

If you have limited disk space and are using SQL Server, it may be possible to reduce the size of the database prior to proceeding with the upgrade. This may be accomplished by "shrinking" the database, which will reclaim unused space.

For information and considerations on shrinking a SQL Server database, please refer to the Shrink a Database topic on the Microsoft Developer Network site.

During the upgrade process, the increase in size of the user data will be reflected by an increase in the size of the database's MDF file by approximately 31%.

Additionally, the database transaction log file, the LDF file, may temporarily grow in size. In testing, the LDF file typically increased to between 1% and 3% of the starting size of the corresponding MDF file. For example, if your MDF file is 10GB in size, then the LDF file could be expected to grow temporarily to approximately 300 MB in size.

Oracle Considerations

When upgrading Oracle databases you must ensure that not only is the appropriate amount of disk space available, but that the USERS tablespace is capable of growing to accommodate the additional storage requirements. You may consider allowing the USERS tablespace data files to auto extend during the upgrade process. Additionally it may be necessary or desirable to create additional data files for use with the USERS tablespace.

Upgrade Paths

Depending on the size of the ARM database and the time constraints on performing the upgrade of EFT, you may choose to consider alternate methods of upgrading the ARM database. Described below are pros and cons of two alternate methods of upgrading the database, when each method is appropriate, and how to perform the upgrade using each method.

Method 1: During the EFT upgrade

This is the typical method of upgrading the ARM database. When running the EFT installer, you can upgrade the ARM database as part of the full upgrade process.

Pros

- Simplest method, requiring minimal manual steps

Cons

- The EFT will be unavailable for the time it takes to perform the entire upgrade

Appropriate When

- The ARM database is relatively small or the computer running the database is sufficiently powerful
- The ARM database is large, but a few hours of downtime is acceptable

How to Perform

- When upgrading using the EFT installer, on the **EFT Auditing and Reporting database configuration** page of the wizard, click **Configure Auditing and Reporting** and proceed accordingly.

Method 2: Out of band

With this method, EFT may be upgraded independent of the ARM Database. Specifically, you would upgrade EFT using the EFT installer application, but choose to skip upgrading the ARM database at that time. Once the EFT application has been upgraded, it may be restarted and will thus be available to service end users. During the time that the ARM Database has not yet been upgraded, the EFT application can temporarily store audit information to disk.

You can then upgrade the ARM database using the Database Utility. Once the upgrade has completed, the EFT will then be able to reconnect to the database as normal.

Pros

- Allows for minimal downtime of the main EFT facilities

Cons

- EFT Reporting capabilities will be temporarily unavailable
- Requires additional steps to perform the upgrade

Appropriate When

- Upgrading very large database and the necessary downtime of the main EFT facilities is unacceptable

How to Perform

- Prior to starting the upgrade process, configure the EFT application to audit to a folder while disconnected from the database. Refer to Audit Database Settings for information about this functionality.
- Upgrade the EFT application using the EFT installer. On the **EFT Auditing and Reporting database configuration** page of the installer, click **Skip Auditing and Reporting configuration** and proceed accordingly.
- After EFT has been upgraded, restart the EFT service.

- Upgrade the ARM database using the Database Utility.
  - First, perform a preview upgrade using the "-action=UpgradePreview" option of the utility. This will verify that the appropriate requirements for upgrading the database have been met.
  - After the requirements have been verified, use the "-action=UpgradeSchema" option to perform the actual upgrade. Optionally you may instead generate an upgrade script using the "-action=UpgradeScript" option and manually upgrade the database using vendor tools such as SQL Server Development Studio or SQL Plus.
  - Refer to EFT Database Utility for additional information.

ARM Upgrade Checklist

SQL Server

- Ensure a current backup of the database is available
- If necessary/desired, purge older data from the database
- Ensure the necessary disk space is available to perform the upgrade
- Remove any custom schema modifications made to the database
- Follow the desired upgrade method
- Recreate any custom schema modifications

Oracle

- Ensure a current backup of the database is available
- If necessary/desired, purge older data from the database
- Ensure the necessary disk space is available to perform the upgrade
- Ensure the USERS tablespace and associated data files are configured to allow for the necessary data growth
- Remove any custom schema modifications made to the database
- Grant the "CREATE VIEW" privilege to the EFT database user account
- Follow the desired upgrade method
- Recreate any custom schema modifications

Upgrading a Large Database

The majority of the modifications performed on the ARM database when upgraded take only minutes to complete. Occasionally, more modifications are needed when upgrading the database schema. These upgrades may take a long time, especially when they require modifications to the data stored within the database. As such, the time it takes to perform the upgrade may increase with the size of the database. Depending on the size of the database, such upgrades take hours instead of minutes.

The database upgrade preview process includes the age of the oldest data in the database as well as a rough estimate of the database size. Administrators should use this data to assess the current state of the database when deciding how and when to proceed with the database upgrade.

Administrators of large databases should consider the following options to ensure a smooth upgrade process:

- Administrators should consider purging older data from the database prior to upgrading. (Refer to Purging Data from the Database for details.)
- The database should be backed up prior to any upgrade to allow for quick recovery in case of errors.
- Administrators should consider making a copy of the ARM database and performing a test upgrade of the database. The script necessary to perform the test upgrade may be obtained by proceeding through the EFT Installer's upgrade process and choosing to upgrade the ARM Database. When prompted for the database credentials, specify the test database credentials. On the **Upgrade Preview** page of the installer, click **View**, save a copy of the upgrade script, and then cancel the EFT installer. You may now use the SQL script to upgrade the database manually. Alternatively, you can install a clean copy of EFT on another computer and use the Database Utility (**DBUtility.exe**) to perform the test upgrade.
- Administrators should consider upgrading the database out-of-band from upgrading the EFT installation. This may be done by skipping the ARM database upgrade in the EFT Installer when performing the initial EFT upgrade. The updated version of the EFT will temporarily audit database transactions to disk until the ARM database has been upgraded.

  To perform an out-of-band upgrade of ARM

  1. If desired, prior to upgrading the EFT, enable the ARM audit-to-folder feature.
  2. Use the installer to upgrade the EFT, but skip the ARM upgrade process, then do one of the following:

- Rerun the installer in maintenance mode later to upgrade the ARM database.
- Use the Database Utility (**DBUtility.exe**) to perform the upgrade.
- Manually upgrade using the SQL scripts generated by **DBUtility.exe**.

3. After the ARM database has been upgraded, click **Reconnect** in the EFT administration interface, on the Server's **Logs** tab to instruct EFT to connect to the upgraded database. EFT will then import any database transactions that were audited to disk in the interim.

Manually Creating the ARM Database in SQL Server

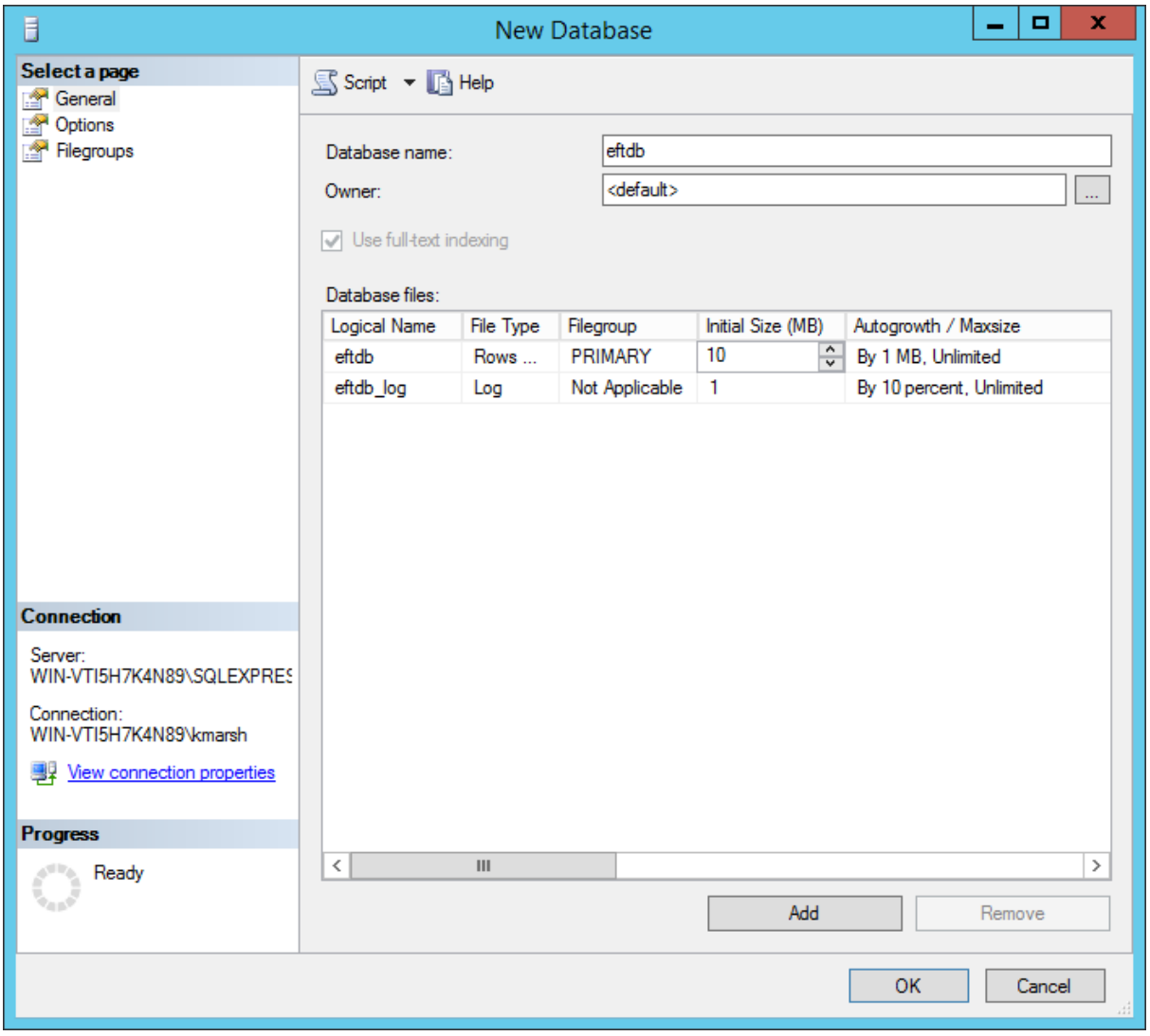
This procedure should only be used if you have not already created the ARM database using the EFT installer. All tables will be created in the schema regardless of which features and/or modules are actually in use.

The following instructions use the SQL Server Management Studio application from Microsoft. Optionally, users may prefer to use command line tools such as oSQL to create the database. The oSQL utility allows you to execute Transact-SQL statements, system procedures, and scripts for creating and maintaining the database. For additional information on the oSQL utility, including common script samples, refer to osql Utility on microsoft.com.

First you will create the database, then create the database user account, create the schema, configure EFT to connect to the database, and then test the connection.

To create the database

1. Using the SQL Server Management Studio application, connect to the SQL Server instance using an account that has the privileges necessary to create user accounts and databases. Typically the "sa" account will suffice.
2. In the left pane, right-click **Databases**, then click **New Database**.
3. The **New Database** dialog box appears. Name the database *eftdb.* (You can use a different database name, but be sure to use the name you chose throughout this procedure.)



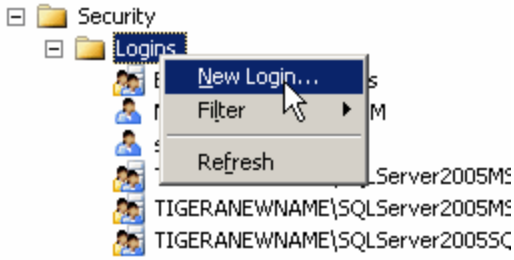
4. In the **Database files** table, change the **Initial size** value to 10 MB for the eftdb logical name (first row). Leave the **eftdb_log** row as is.
5. Click **OK** to finalize creation of the database.

Create the Database User Account

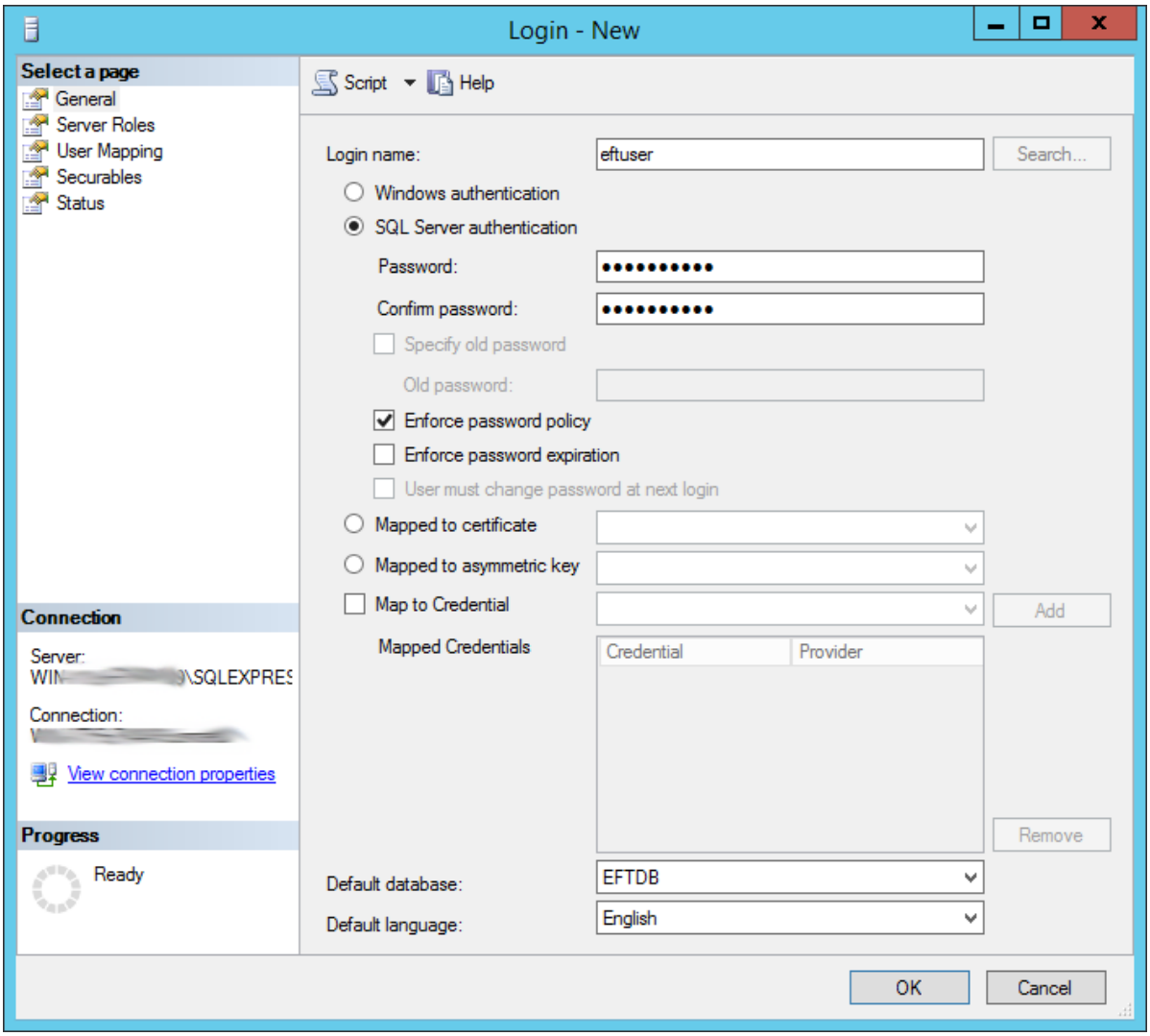
During installation, EFT needs full DB Owner access to the auditing database to set up the schema. During updates or upgrades, EFT needs full DB Owner access to update the schema. Once it is set up, EFT only needs to be able to read, write, and execute stored procedures. For more information on the required database privileges please refer to Database User Account Privileges.

To create the database user account

1. Using the SQL Server Management Studio application, connect to the SQL Server instance using an account that has the privilege to create user accounts and databases. Typically the "sa" account will suffice.
2. In the left pane, expand the **Security** node, right-click **Logins**, and then click **New Login**.



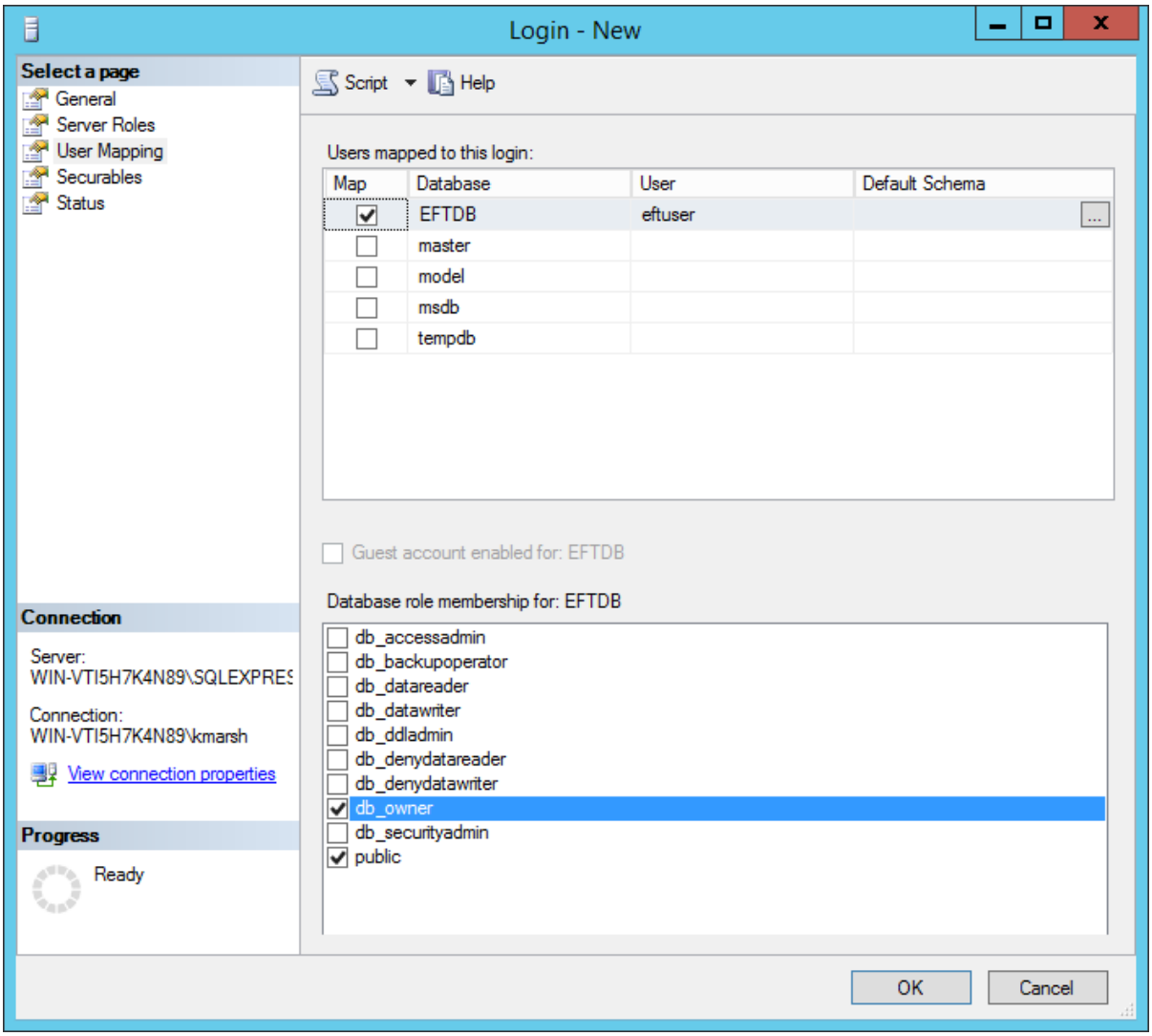
The **New Login** dialog box appears.



3. Create a new user called *eftuser* and then click **SQL Server Authentication**. (You can use a different user name, but be sure to use the same name throughout the procedure.)

   If SQL Server Authentication is not available as a choice, verify that the SQL Server has been configured to support mixed mode.

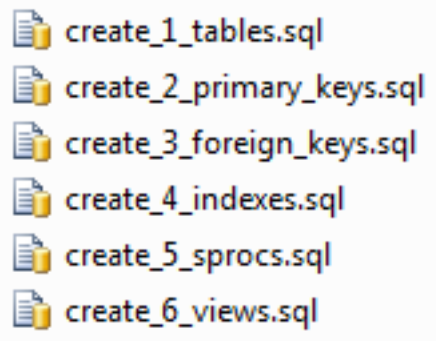
4. In the **Password** and **Confirm password** boxes, provide a complex password consisting of an alphanumeric and symbol mix of at least 8 characters.
5. Ensure the **Enforce Password Policy** check box is selected.
6. Ensure the **Enforce password expiration** check box is ***not*** selected. (Optionally, you can enable this setting, but be aware that the *eftuser* account password will need to be changed periodically to prevent expiration.)
7. Ensure the **User must change password at next login** check box is ***not*** selected.
8. Set the **Default** database to the **eftdb** database created earlier.
9. In **Default language**, click the list to select your language or leave it set to the <default> setting.
10. Select the **User Mapping** node in the left pane.
11. In the **Users mapped to this login** table, locate the entry for the eftdb database created earlier.
12. Select the check box in the **Map** column for the **eftdb** row and set the **Default Schema** to **dbo**.
13. While the **eftdb** row is selected, in the **Database role membership for** table, select the **dbo_owner** check box.



14. Click **OK** to finalize the user creation.

Create the Schema

During installation of the EFT, the installer will place a set of database creation SQL scripts in the **GlobalSCAPE\EFT Server\SQL Server** subfolder of the system **Program Data** folder. (Typically, **C:\ProgramData\GlobalSCAPE\EFT Server\SQL Server**.) The database creation scripts use the "create_#_" filename prefix. The # in the filename represents the order in which each script must be executed.



You will use these scripts to create the schema using the procedure below.

To create the schema

1. Using the SQL Server Management Studio application, connect to the SQL Server instance using an account that has the privilege to create user accounts and databases. Typically the "sa" account will suffice.
2. In the left pane, expand the **Databases** node, right-click on the **eftdb** node, and click **NewQuery**. A blank screen appears in the right pane in which you can type in a SQL query.
3. Execute each creation script in the specified order by copying/pasting the script file contents into the left pane and clicking **Execute**. A message appears each time you click **Execute** indicating whether the query was able to complete successfully.
4. In the left pane, expand **Databases**, then **eftdb**, then **Tables**. Verify that the database has populated correctly. (The tables defined in the script should have been created.)

Configure EFT

To configure EFT to connect to the newly created database, refer to Audit Database Settings.

To test the connection

1. Create a test connection with your FTP client to EFT and upload and download a few files.
2. In SQL Server Management Studio select the **dbo.tbl_ProtocolCommands** table under the **eftdb** database icon. It should return several rows with the commands issued by your client from the test connection.
3. You can now pull reports directly from EFT against data audited to SQL Server.

If you are running the administration interface, you must have an entry in that system's DNS for the name of the SQL Server, otherwise the administration interface will not be able to connect to the SQL Server when attempting to pull reports.

Manually Creating the ARM Database in Oracle

This procedure should only be used if you have not already created the ARM database using the EFT installer.

All tables will be created in the schema regardless of which features and/or modules are actually in use.

The following instructions assume you have already installed the Oracle database software and that an Oracle database is available. These instructions will make us of the Oracle SQLPlus command line utility to execute SQL against the Oracle database. Optionally, users may use an alternate utility of their preference.

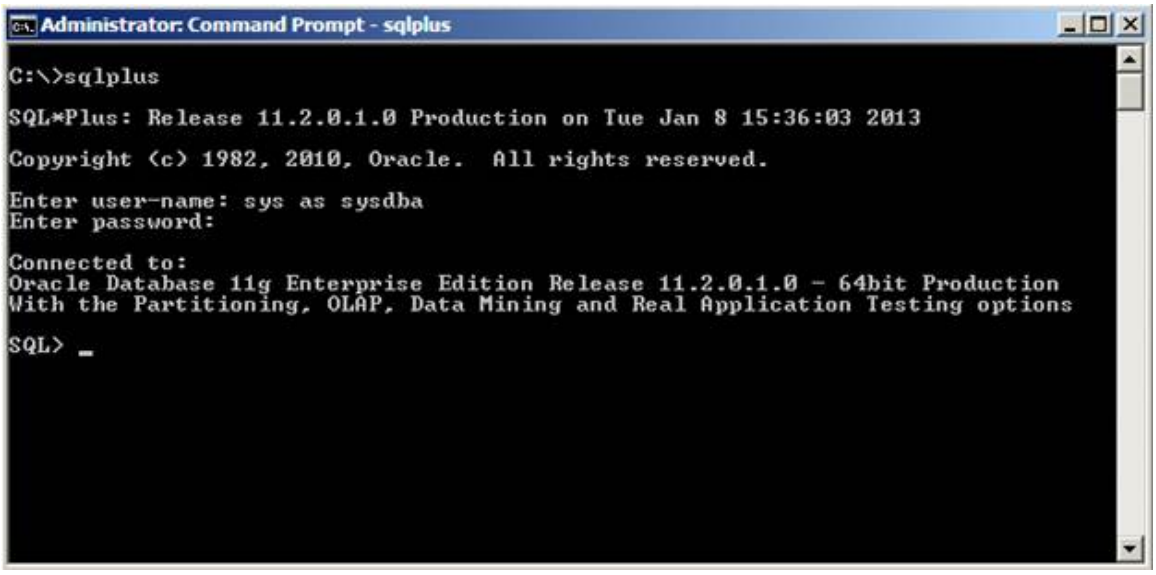
If you are running the administration interface, you must have an entry in that system's DNS for the name of the Oracle database computer, otherwise the administration interface will not be able to connect to the database when attempting to pull reports.

Create the Database User Account

During installation and upgrade, EFT needs creation privileges within the database. Once it is set up, EFT only needs to be able to read, write, and execute stored procedures. For the specific set of privileges required, please refer to Database User Account Privileges.

To create the database user account

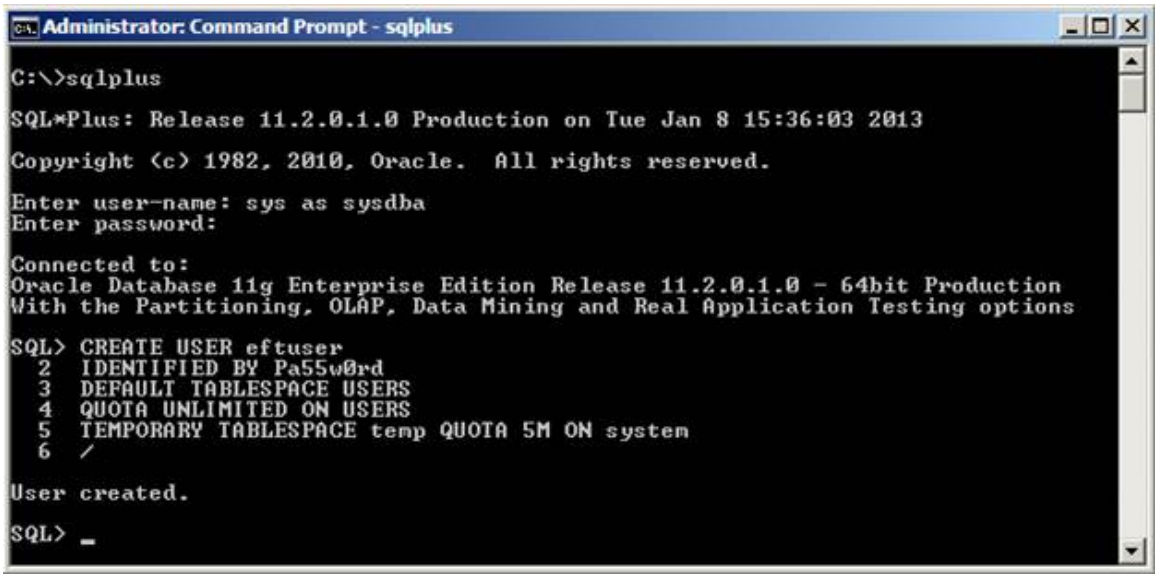
1. Using SQLPlus connect to the Oracle database using an account that has the privileges necessary to create user accounts and grant privileges. Typically the "sys" or "system" account will suffice. Note that when connecting as the "sys" account you will typically need to specify the "as sysdba" option.



2. Create the database user account by executing the following statement in SQLPlus, replacing `<username>` with the desired database user account name, such as `eftuser`, and `<password>` with the desired password.

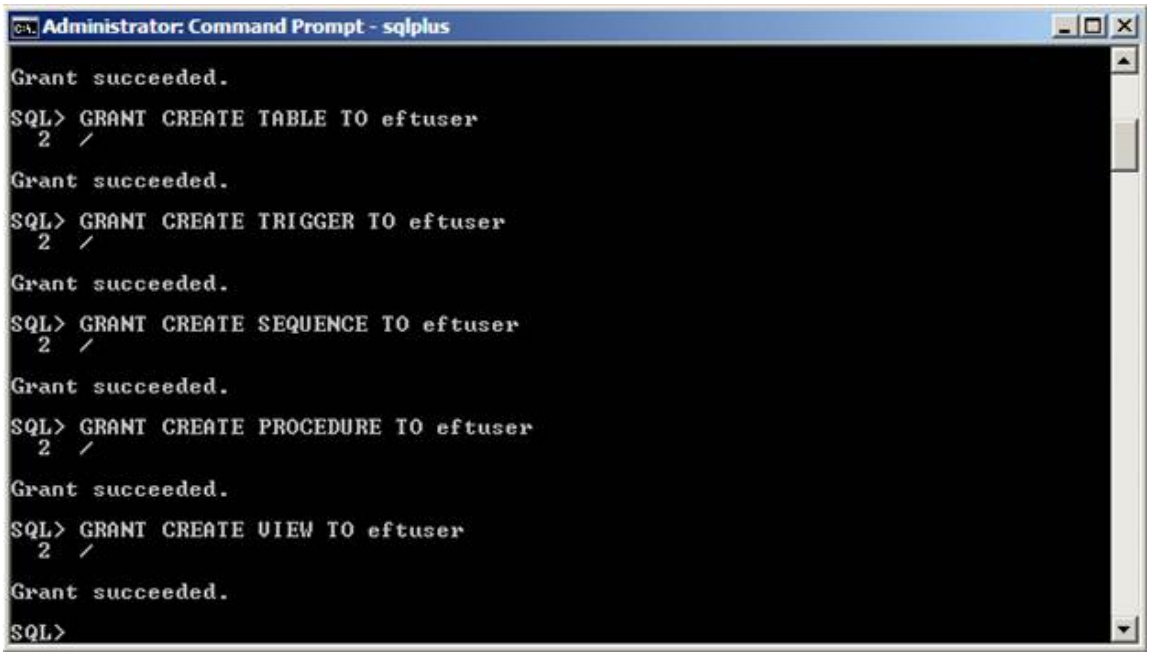
```
CREATE USER <username>
IDENTIFIED BY <password>
DEFAULT TABLESPACE USERS
QUOTA UNLIMITED ON USERS
TEMPORARY TABLESPACE temp QUOTA 5M ON system
/
```

   For example:



3. Grant the necessary privileges to the database user account by executing the following statements in SQLPlus, replacing <username> with the username of the account you just created, such as eftuser.

For example:

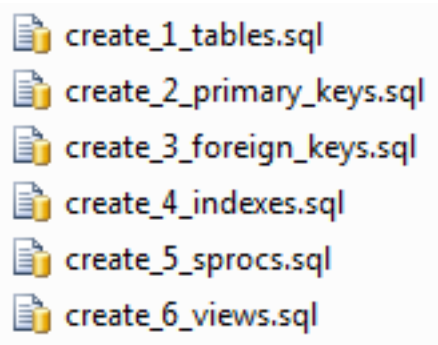


4. To exit SQLPlus, type `exit` and press ENTER.

Create the Database Objects

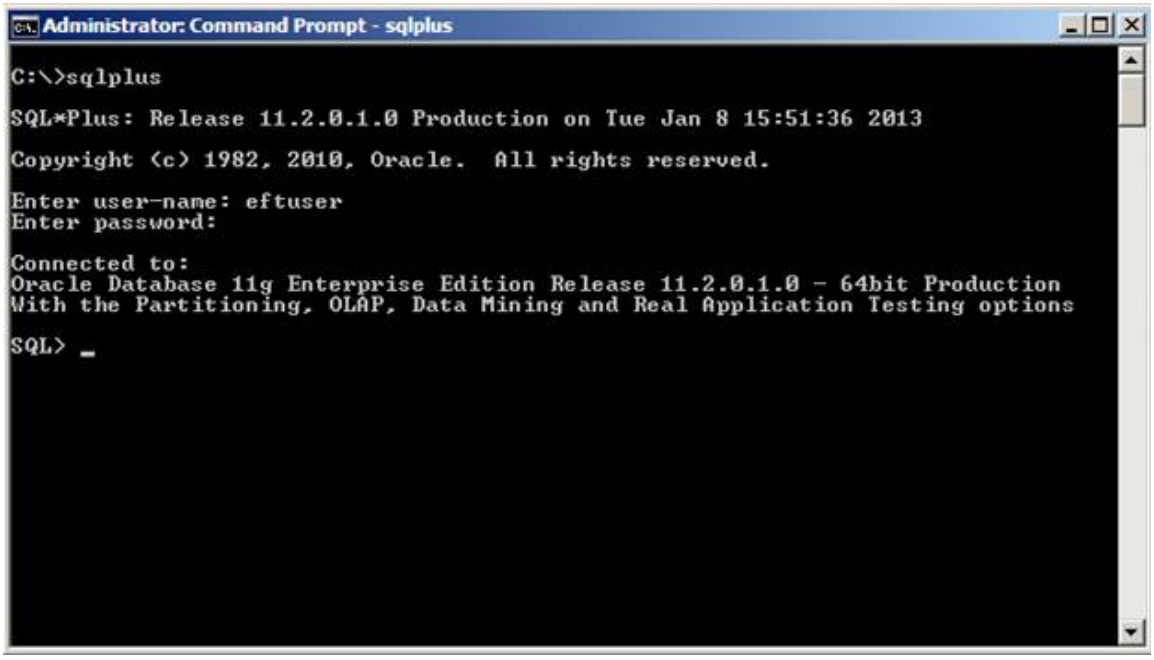
During installation of the EFT the installer will place a set of database creation SQL scripts in the **GlobalSCAPE\EFT Server\Oracle** subfolder of the system's **Program Data** folder. (Typically, **C:\ProgramData\GlobalSCAPE\EFT Server\Oracle**.)

The database creation scripts use the "create_#_" filename prefix. The # in the filename represents the order in which each script must be executed.



To create the database objects

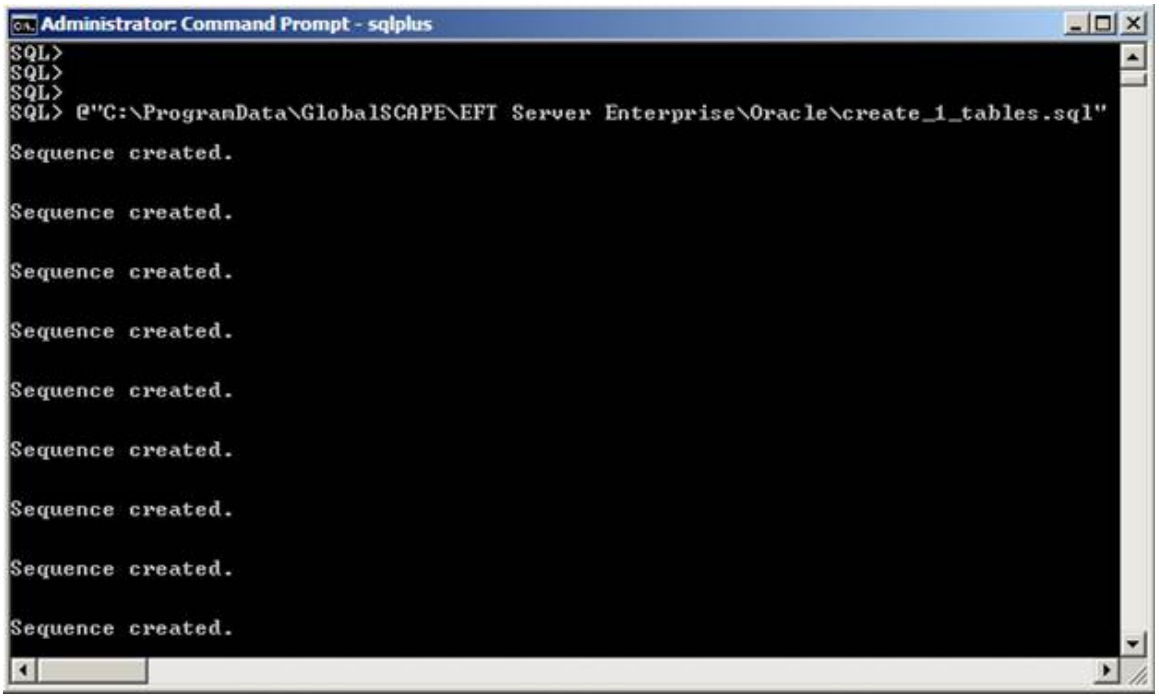
1. Using SQLPlus connect to the Oracle database using the EFT database user account created above.



2. In SQLPlus, execute each database creation SQL Script in the correct order using the command, replacing <Script File Path> with the full path and filename of the script.

   @"<Script File Path>"

   For example:



2. Once you have executed all of the creation scripts you may exit SQLPlus by typing `exit` and pressing ENTER.

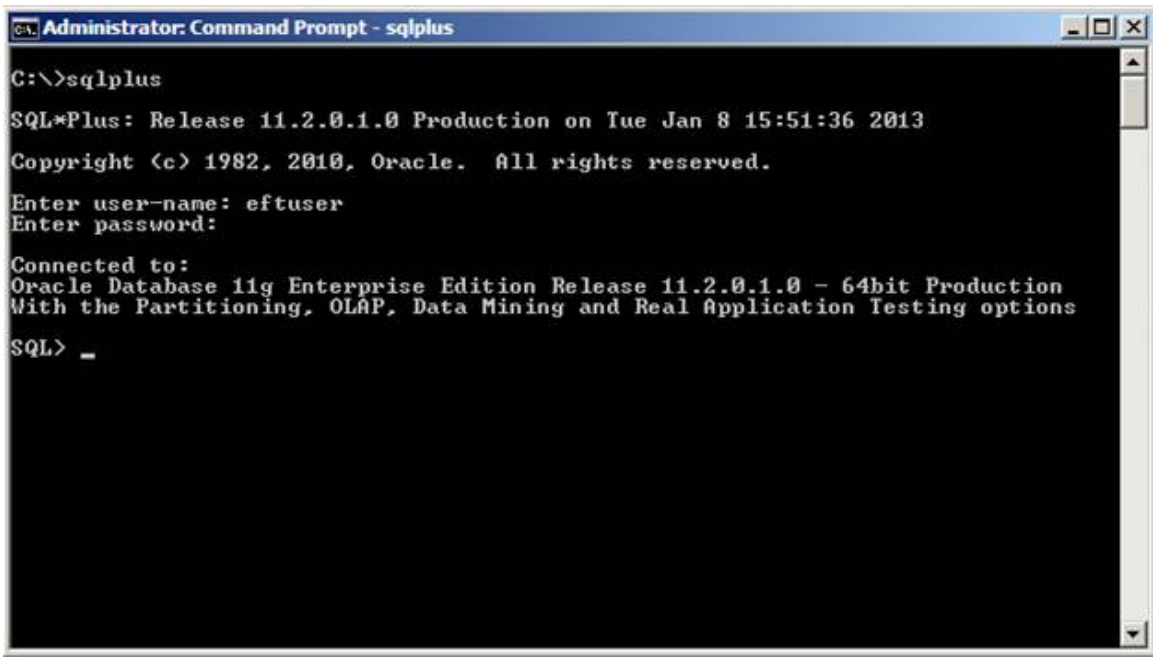
Configure EFT

To configure EFT to connect to the newly created database, refer to Audit Database Settings.

To test your connection

1. Create a test connection with your FTP client to EFT and upload and download a few files.
2. Using SQLPlus, connect to the Oracle database using the EFT database user account.

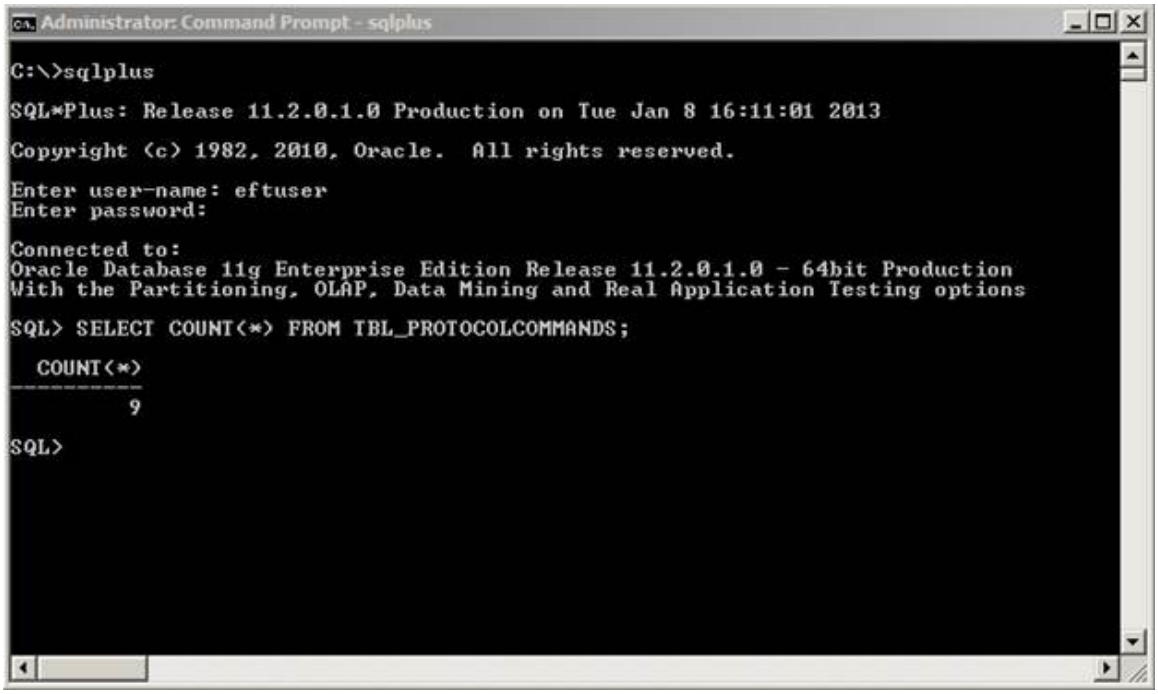
   For example:



3. Retrieve the number of rows in the *TBL_PROTOCOLCOMMANDS* table by executing the following statement in SQLPlus:

```
SELECT COUNT(*) FROM TBL_PROTOCOLCOMMANDS;
```

For example:



The above query should return a count of more than 0.

4. To exit SQLPlus, type `exit` and press ENTER.
5. You can now pull reports directly from EFT against data audited to Oracle.

ARM Database Schema Change Tracking

The ARM database schema may undergo many changes between versions. Each ARM schema version is described in Knowledgebase article #11031, from newest to oldest. The database version number appears in the installer during upgrade, and you can see what the changes were.

Changes to the database for EFT v8.x include tables for GDPR (Personal Data, Privacy Right Exercised, and Privacy Terms EU Status), and Scan Data Actions.

Fact Tables

Fact tables are really summary tables. From a SQL perspective, it is a group by of the regular ARM tables. This makes the tables smaller and faster to generate reports from. ARM groups the rows in the regular ARM table (detail table), so one row in the fact table represent many rows in an ARM table. Updating the fact tables could be seen as a pre-processing step to make the ARM reports faster. One example of this grouping is that ARM groups on date. While the detail tables have the time down to the second, the fact tables only show the date.

EFT database tables can grow very large. Fact tables are used to update EFT's tables every day and keep the database current. A check box on the **Server > Logs** tab, **Refresh facts table daily**, is selected by default.

- This feature is only available if the ARM database is managed in SQL Server. It is not available with Oracle databases.
- When the fact tables are enabled, a warning message explains that database performance can be affected temporarily while the tables are refreshed.
- The fact tables are updated as part of its hard-coded nightly cleanup routine (***not*** the Cleanup Event Rule). There is no logging or reporting on the nightly fact tables cleanup.
- Upon new install, the initial fact table creation stored procedures are run, unless those tables already exist, and then will back-fill the fact tables with historical data
- The nightly import process logs in the ARM logger when it starts the job, with TRACE. If calling the DBUtility.exe fails, it will log an ERROR.

Each night, EFT imports data into its fact tables. Those tables are used to populate the following reports, all of which represent inbound behavior:

- Executive Summary Report
- Traffic - Average Transfer Rates by User
- Traffic - Connections Summary
- Traffic - Datewise-hourly Bytes Transferred
- Traffic - Datewise-IPwise Bytes Transferred
- Traffic - IPWise Connections (Summary)
- Traffic - Monthwise-IPwise Bytes Transferred
- Traffic - Most Active IPs - Connections
- Traffic - Most Active IPs - Data Transferred
- Traffic - Most Active Users - Connections

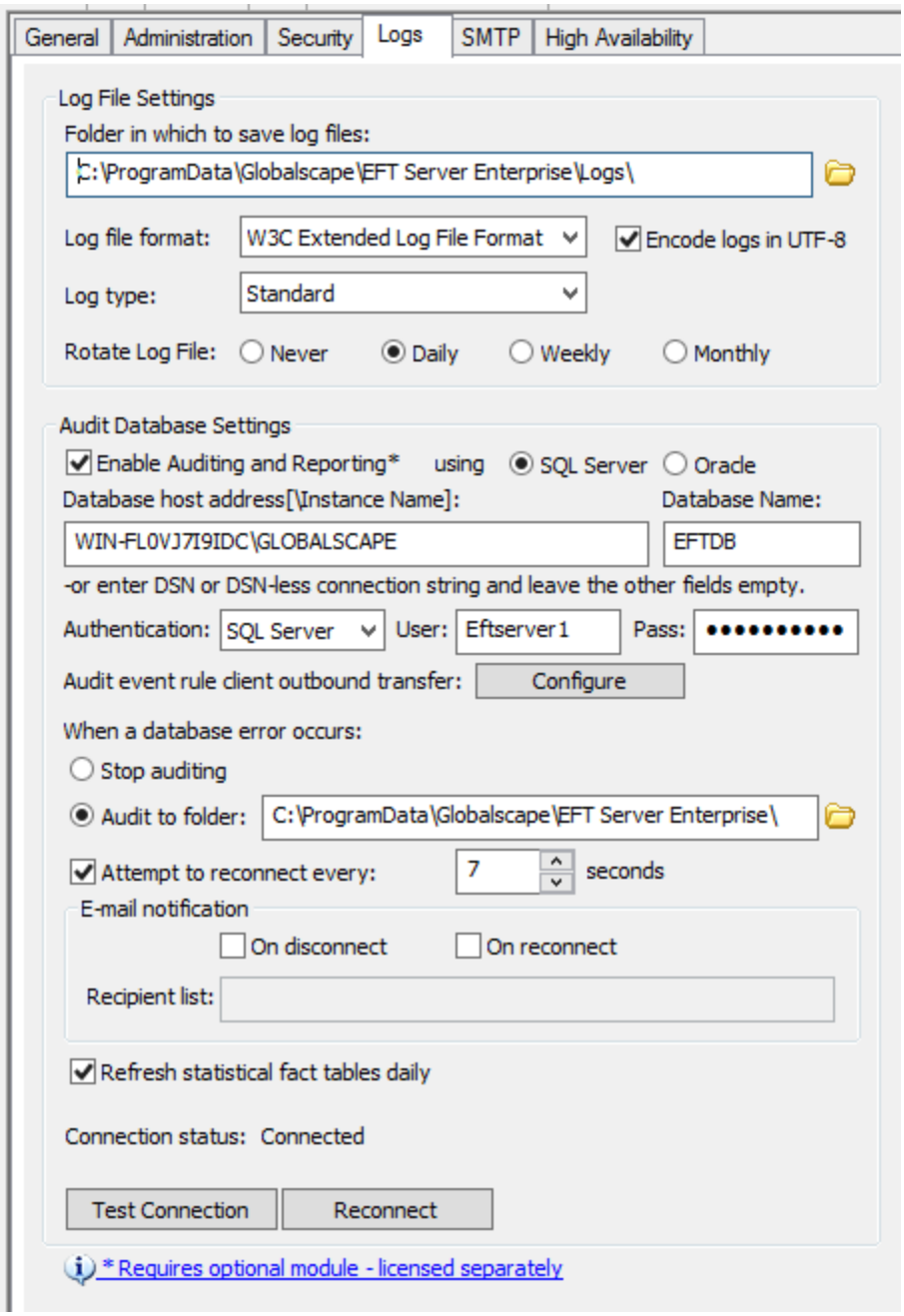
- Traffic - Most Active Users - Data Transferred (original report done)
- Traffic - Protocolwise Connections (Summary)
- Traffic - Sitewise-Hourly by User

Refreshing the Fact Tables

Rather than having to aggregate the data in real-time from the full set of data that may span multiple tables, "fact tables" are used to store daily pre-aggregated measurements, such as a daily record of “bytes transferred” for each user. These tables can alleviate load on the database server when running queries that are based off of these facts, as the reporting engine only needs to query sets of pre-aggregated data from an existing set of facts, resulting in lightning-fast reports.

By default, EFT will regularly update the fact tables so that EFT's analytics front end is always current.

The **Refresh fact tables** feature is only available if the ARM database is managed via SQL server; it is not available with an Oracle ARM database.



When the **Refresh statistical fact tables daily** check box is selected, EFT will refresh the fact table. Clear the check box if you do not want to refresh the fact tables.

- EFT will run the initial fact table creation stored procedures during installation, unless those tables already exist, in which case EFT will back-fill the fact tables with historical data.
- Fact table refreshes can severely affect database performance for a few minutes to several hours, depending on the volume of data audited since the last refresh.

- EFT will update the fact tables as part of its hard-coded nightly cleanup routine (at midnight).
- Using a SQLite databases viewer, in the ServerConfig.db, you can verify the ARM configuration data. In this you will find the **RefreshFactTables** value (true or false).
- When creating and configuring an EFT server administrative connection, the **Refresh statistical fact tables daily** check box is selected by default.

Auditing

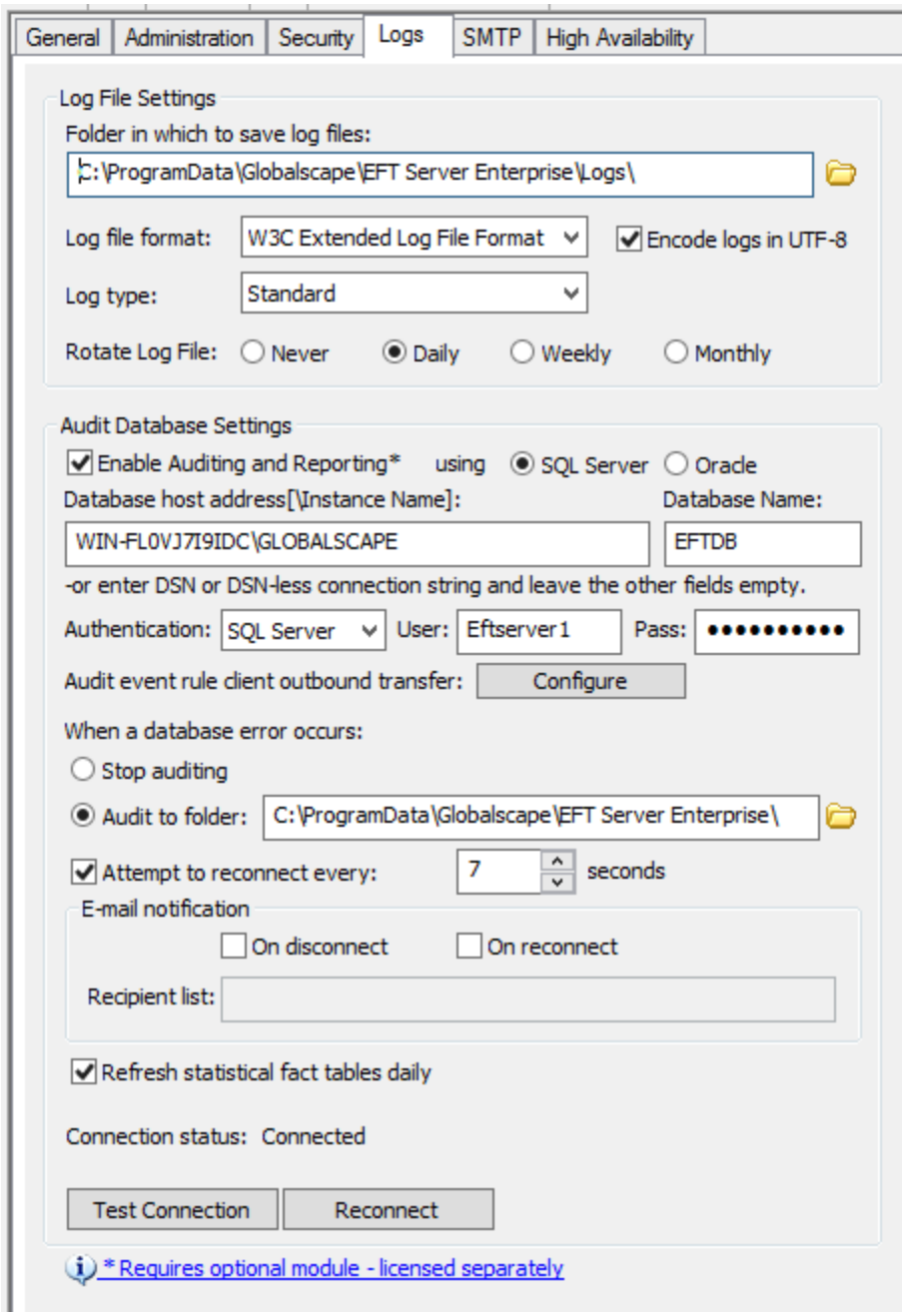
The topics below provide information about auditing EFT activity with the Auditing and Reporting module.

Audit Database Settings

When you run the Server Setup wizard, you are offered the opportunity to enable auditing and reporting and configure the connection information. If you chose to do that later or if you want to edit the database information, you can do so on the **Logs** tab in the **Audit Database Settings** area.

To enable and configure auditing and reporting

1. In the administration interface, connect to EFT and click the **Server** tab.
2. On the **Server** tab, click the Server node you want to configure.
3. In the right pane, click the Logs tab.



4. In the **Audit Database Settings** area, select the **Enable Auditing and Reporting** check box to enable communication with the database; clear the check box to disable auditing and reporting.
5. In the **Database type** area, select **SQL Server** or **Oracle**.

6. In the **Database host address[\Instance Name]** box, specify the host or database instance name of the database to which you want EFT to connect, or provide a DSN or DSN-less connection string. Refer to Establishing a System Data Source Name (DSN) or Using a DSN-Less Connection with ODBC Authentication, if you are using ODBC Authentication for your Site.
7. In the **Database Name** box, provide the name of the database or leave the box empty if you provided a connection string in the **Database host address[\Instance Name]** box.
8. For SQL Server databases, in the **Authentication** box, specify whether the database is to use **Windows Authentication** or **SQL Server Authentication**. If the database is using Windows Authentication, the EFT Insight server service needs to run as a Windows user with permission to access the database.
9. In the **Database username** and **Password** boxes, provide the username and password needed to connect to the database or leave the box empty if you provided a connection string in the **Database host address[\Instance Name]** box or if you are using Windows Authentication.
10. Next to **Audit event rule client outbound transfer**, click **Configure**, then specify whether to save Event Rule transfer failures to the database. Refer to Logging Event Rule Transfer Failures for details.
11. In the **When a database error occurs** area, specify whether you want to audit database errors to a folder:
    - If you do want to audit errors, or to stop it temporarily, click **Stop auditing**.
    - To **Audit to folder**, click the option, then specify the path to the folder in the box.
12. To automatically try to reconnect after an error occurs, select the **Attempt to reconnect every** check box and specify the frequency in seconds, from once every 7 seconds to once every 86,400 seconds (once per day).
13. In the **email notification** area, select the **On disconnect** check box and/or the **On reconnect** check box, and then in **Recipient list** specify one or more email addresses that you want EFT to send error notifications to in case of database failure. Multiple email addresses must be separated by semicolons **;** . When auditing is enabled, this email is sent any time that EFT cannot reach the database.
14. Select or clear the **Refresh statistical FACT tables daily** check box to indicate whether you want to refresh the FACT tables every night. Refer to FACT tables for more information.
15. If you make any changes to the database audit settings, click **Apply** to save the changes on EFT.

16. To verify the connection information, click **Test Connection**. The status of the database connection appears above the **Reconnect** button. If the database is not connected, click **Reconnect** to reconnect to the database.
    - **Test Connection** - EFT attempts a connection using the supplied parameters without applying the changes.
    - **Reconnect** - EFT applies the settings (a prompt appears if you made changes and did not click **Apply**) and attempts to connect to ARM with the new settings.

Auditing Database Recovery

If the auditing database has failed and EFT has been disconnected from the database for a while, you can prevent a loss of data by automatically saving auditing data to a text file when EFT is disconnected from the database. If EFT is configured to save auditing information to a text file, before reconnecting EFT to the database, repair the database, and then insert the data from the text file into the database. Then you can reconnect EFT to the database as described below.

The SQL statements logged in the text file must be loaded into the database before any reports are run.

If EFT is disconnected from the database and is configured to save auditing information to the log file, do the following:

1. Solve the connection problem.
2. Repair the database, and insert the data from the text file into the database. Be sure to insert the data only once, otherwise the auditing data will be corrupted.
3. In the administration interface, connect to EFT and click the **Server** tab.
4. On the **Server** tab, click the Server that you want to configure.
5. In the right pane, click the **Logs** tab and review the database connection information.
6. If you make any changes to the database host address, instance name, database name, etc., click **Apply** to apply these changes to EFT.)
7. Click **Test Connection** to test the status of the database connection.
8. The **Connection** status area indicates whether EFT is communicating with the database. To reconnect to the database, click **Reconnect**.

How EFT Handles SQL Data

EFT truncates data values within each audited SQL transaction to ensure the data value fits within the corresponding database field.

The special characters (as defined by the SQL interpreter) within each data value of an audit SQL event are escaped to ensure the data value is stored and retrieved properly from the database. The following special characters are escaped by EFT during generation of SQL statements prior to submission to the database engine:

- Single quote - %
- Open brace - [
- Percent - %
- Underscore - _

Auditing Event Rule Actions

Actions are audited to the Auditing and Reporting Module (ARM) database. For all Event Actions, the following items are audited:

- Time stamp
- Site Name
- Event Name
- Action Types such as move, copy, OpenPGP, and send email.
- Action Parameters - These are runtime values passed to the Action, not the replacement variables. For Advanced Workflow Actions, this is the path to the temporary file associated with the Workflow that was executed. This file contains more detailed debug logging if enabled for that particular workflow.
- Failed Action Flag - This is captured if this Action is the result of a FAILURE sequence on a prior Action.
- Action Result Code
- Result

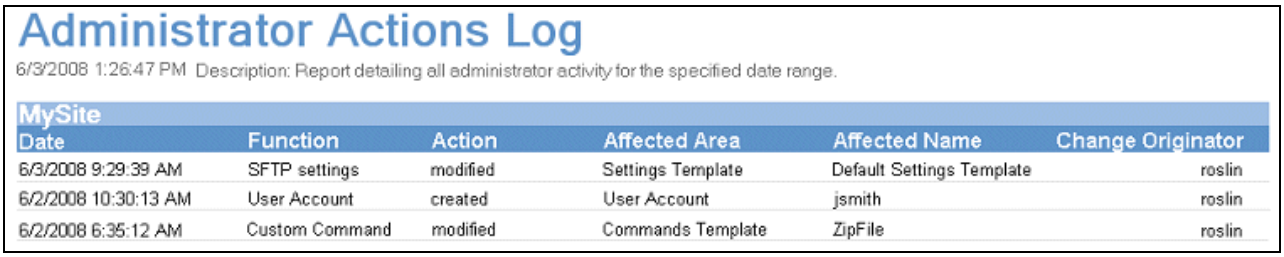
Auditing Administrator Changes to the ARM Database

(Requires ARM) Administrators often need to know when and what changes were made to EFT and who made them. The *administrator Actions Log* report provides information about administrator changes. When ARM expires, administrator changes are no longer audited.

EFT logs to the ARM database the following changes made to EFT:

- The **Date** the action occurred, in MM/DD/YYYY HH:MM:SS format.
- The affected feature or **Function**. (Refer to Functions Audited below.)
- The type of **Action** (created, added, removed, modified, enabled, disabled, started, and stopped).
- The **Affected Area** (Server, Site, Settings Template, User Account, Event Rule, Command, Group, VFS, Report).
- The name of the affected object, **Affected Name** (Server Name, Site Name, Settings Template Name, User or administrator Account Name, Event Rule Name, Command Name, Group Name, Folder Name, Report Name).
- The name of the administrator that made the change, **Change Originator**.

The data in the preconfigured report is arranged in columns, **Date**, **Function**, **Action**, **Affected Area**, **Affected Name**, and **Change Originator**, grouped by Site name, and sorted in reverse chronological order (newest change at the top).



Administrator Actions Log

6/3/2008 1:26:47 PM Description: Report detailing all administrator activity for the specified date range.

MySite

Date	Function	Action	Affected Area	Affected Name	Change Originator
6/3/2008 9:29:39 AM	SFTP settings	modified	Settings Template	Default Settings Template	roslin
6/2/2008 10:30:13 AM	User Account	created	User Account	jsmith	roslin
6/2/2008 6:35:12 AM	Custom Command	modified	Commands Template	ZipFile	roslin

Functions Audited

When the following functions are created, added, removed, modified, enabled, disabled, started, or stopped, the action is logged to the database. Many possible actions are grouped together. For example, modifying SSL cipher selection, changing SSL clear command channel values, or modifying SSL connection string all fall under "SSL settings." Also, intermediate states are not audited (for example, a toggle was checked, but later unchecked, rendering the transaction moot). Instead, only committed states are captured (once the administrator applies changes).

- SFTP protocol
- SFTP settings
- SFTP key
- SFTP authentication settings
- SSL protocol
- SSL settings
- SSL require client certificate
- SSL certificate
- SSL authentication settings
- FIPS mode for SSL
- FIPS mode for SSH
- HTTPS protocol
- HTTPS settings
- HTTP protocol
- FTP Implicit Protocol
- FTP Explicit Protocol
- FTP protocol
- FTP settings
- AS2 protocol
- AS2 settings
- PASV port mode settings
- Streaming repository encryption (EFS)
- OpenPGP settings
- OpenPGP key
- Web Transfer Client
- Password
- Password complexity
- Password reset
- Password expiration
- Password History
- Password initial reset
- Invalid login settings
- Inactive account settings
- Account expiration settings
- Connection limits
- Transfer limits
- Disk limits
- File type limits
- IP address ban list
- Group assignment
- Group (Permission)
- Data sanitization (wiping)
- DMZ Gateway
- DMZ Gateway settings
- Authentication settings
- Remote administration
- Auditing settings
- Log settings
- Default Configuration File Path
- Default User Database Refresh Interval
- SMTP settings
- DoS prevention settings
- Delegated administrators
- Server
- Site
- Settings Template
- User Account
- Real-time monitoring
- User kicked
- Web Services Interface
- Site root folder
- Site listening IP
- Custom command
- Event Rule
- Physical folder
- Virtual folder
- Folder permissions
- administrator
- Database refresh
- Server service settings
- Show Time In UTC/GMT
- Ban On Invalid Login Settings
- AWE Task
- Account details

Purging Data from the Database

Space requirements for transactions in the ARM Database depend on the estimated EFT activity, number of users, and installed modules. A general estimate is 3MB to 5MB of per 1000 files uploaded. A minimum of 3GB hard drive space is recommended for the initial database size, with additional space required for growth over time. As your database continues to grow, it is necessary to purge old records periodically.

The Helper script in (by default) C:\ProgramData\Globalscape\EFT Server\SQL Server\Helper scripts\PurgeEFT.sql describes in which order to run the scripts to improve database performance.

For detailed information on purging the database, refer to Knowledgebase article #10426: How can I purge EFT data from my ARM database?

Result IDs

The ARM captures the following transaction information from EFT, which can appear in reports:

Actions

ResultID	Description	Result Const
-1	If the Event Action is in progress	empty
0	If the Event Action is successfully executed	EAR_SUCCESS
1	If the Event Action fails	EAR_FAIL
2	If **STOP Processing this rule** is selected as Action.	EAR_STOP_RULE
4	If **STOP processing more rules** is selected as Action	EAR_STOP_ALL

Stop processing this rule and **Stop processing more rules** can be combined, in which case the value is the sum of the two individual values, that is, 6.

SocketConnection

ResultID	Description	Result Const
0	When socket successfully created	ER_NONE
8	Per Site socket connection limit exceeded	ER_CONNECT_FAILED_TOO_MANY_CONNECTIONS_PER_SITE
9	Max connections per IP address limit exceeded	ER_CONNECT_FAILED_TOO_MANY_CONNECTIONS_PER_IP
10	EFT denied the connection because the IP address was in the ban list or it is a remote IP address and EFT is in developer mode	ER_CONNECT_FAILED_RESTRICTED_IP

ResultID	Description	Result Const
11	EFT denied the connection (failed) and added the IP address to the auto-ban list	ER_CONNECT_FAILED_BANNED_IP
12	EFT in developer mode	
13	Internal server error	

Authentications

ResultID	Description	Result Const
0	Authentication successful	LR_OK
1	Incorrect password	LR_PASSWORD_NOT_ACCEPTED
2	If user account is disabled	LR_ACCOUNT_DISABLED
3	Max connections per Site limit exceeded	LR_TOO_MANY_CONNECTIONS_PER_SITE
4	Max connections per user limit exceeded	LR_TOO_MANY_CONNECTIONS_PER_USER
5	User per- IP address connection limit exceeded	LR_TOO_MANY_CONNECTIONS_PER_IP
6	If given protocol is not supported	LR_PROTOCOL_NOT_SUPPORTED
7	Connection on restricted IP address	LR_RESTRICTED_IP
8	If service is unavailable	LR_SERVICE_UNAVAILABLE
9	User is locked out	LR_ACCOUNT_LOCKED
10	Multi-factor authentication challenge	LR_ACCESS_CHALLENGE
11	MFA authentication required	LR_MFA_REQUIRED

ClientOperations

ResultID	Description	Result Const
1	If copy/move/download operation is successful	TRUE
0	If copy/move/download operation fails	FALSE

CustomCommands

ResultID	Description	Result Const
0	Command executed successfully	CER_OK
1	Command executed with socket output	CER_SYNC
2	Access is denied	CER_ACCESS_DENIED
3	Command is not found	CER_COMMAND_NOT_FOUND
4	Could not launch the selected process	CER_PROCESS_FAILED
5	Command is disabled	CER_COMMAND_DISABLED
6	Errors in parameters passed to the custom command	CER_ERROR_IN_PARAMS

ProtocolCommands

ProtocolCommands are the same as FTP result codes. Below is a brief general description.

ResultID	Description
1*xx*	Expected another reply before proceeding with a new command
2*xx*	Requested action completed successfully
3*xx*	On hold pending receipt of further information
4*xx*	Temporary failure
5*xx*	Permanent failure

Auditing Database Errors and Logging

EFT detects errors that occur while trying to connect to the ARM database and can detect errors returned from the database while attempting to perform transactions. If an error is detected while connecting to the database or when performing a transaction on the database (SQL INSERT, UPDATE, etc.) you can configure EFT to log the error to a file and to send a notification to a specified email address.

By default, database errors are logged to **\Logs** in the format *EFT_ARM_<YYYY_MM_DD_HH_MM_SS>.sql*. (By default, **C:\ProgramData\Globalscape\EFT Server\Logs**.) You can specify a different path or choose not to log the errors to a file.

For details of the **Log Settings** area, refer to Log Settings.

EFT also generates a Windows Event Log entry when there is an ARM database error. The log entry indicates whether auditing has stopped or if the auditing data is being stored to a log file.

If database access is lost because of a connection error or transaction error (INSERT or UPDATE), resumption of auditing to the database requires a restart of EFT or a RECONNECT request by the administrator. If EFT is configured to stop auditing, the administrator must repair the database, and then restart EFT or use RECONNECT to resume auditing to the database.

Logging to a Text File

In the **When a database error occurs** area of the Server's **Logs** tab, you can configure EFT to log the SQL statements to a text file. EFT continues to use the text file until either EFT is restarted or until a RECONNECT request is made by the administrator. EFT then notifies you by email that the logging has been saved to the text file. You can then repair the database, resume auditing to the database, and load the recorded text file SQL statements into the database. To ensure the completeness of the audit data, the SQL statements in the text file must be loaded into the database before executing reports over the time that SQL transactions were logged to the text file.

If you click **Reconnect** to resume auditing to the database, and EFT is recording auditing information to the text file, EFT continues to log EFT file transfers and/or user sessions that are in progress to that text file. New file transfers and new user sessions will continue to be logged in the database, but any in-process transfers/user sessions are logged to the text file to ensure that they can be inserted and linked appropriately in the database.

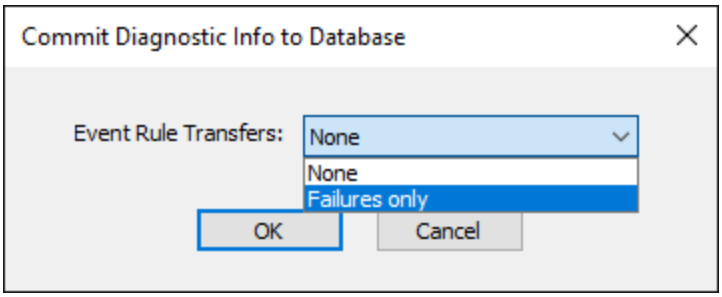
Refer to Audit Database Settings for information about configuring the connection information on EFT's **Logs** tab.

Audit Event Rule Client Outbound Transfer

You can configure whether to log no event rule transfers or event rule transfer failures.

To configure whether to log event rule transfer failures

1. On the **Server > Logs** tab, next to **Audit event rule client outbound transfer,** click **Configure**. The **Commit Diagnostic Info to Database** dialog box appears.



2. Next to **Event Rule Transfers**, click the drop-down list and click **Failures only**.
3. Click **OK**.
4. Click **Apply** on the tab to save the setting.

Security Auditing

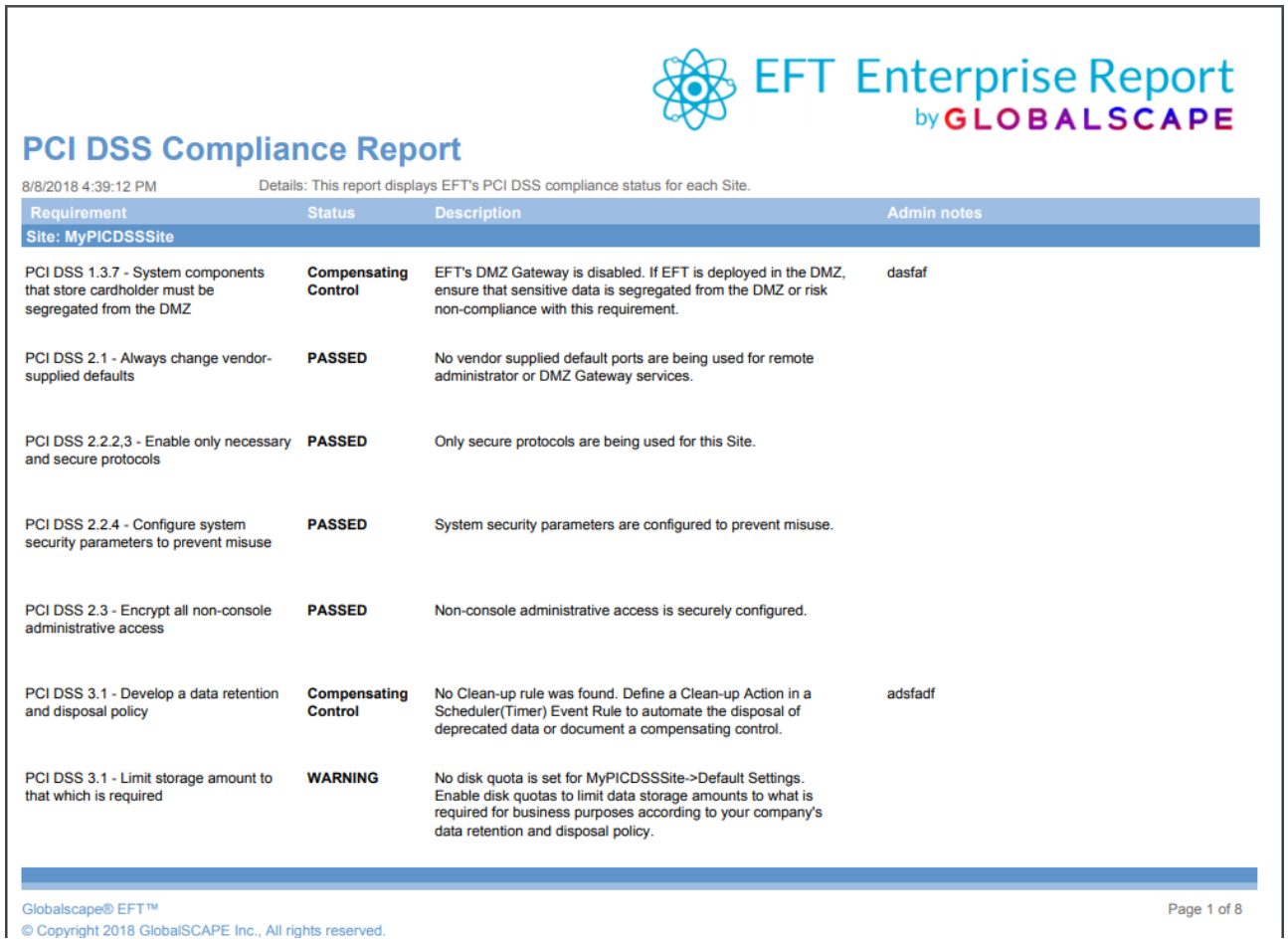
Review the topics below for details of generating a daily PCI DSS Compliance report.

PCI DSS Compliance Report

The RCM module includes the ability to audit EFT for compliance with the PCI DSS requirements. EFT scans all PCI DSS requirements addressed in EFT, and then reports on the compliance status of each requirement (Pass, Fail, or Warning). The report also provides a description of the requirement tested for each item. For failed requirements, the report presents a reason the non-compliant setting was used, if you provided one at the time that particular setting was disabled/changed.

To generate the PCI DSS Compliance report

- To generate the report in real time, do one of the following:
  - On the main menu, click **Report >PCI DSS Compliance Report**. A report is generated for each high security-enabled Site.
  - In the Site's **Event Rule** node, click **Report Event**. In the right pane, click **Run Now**. The report is emailed to the email address defined in the Rule.
- To generate the report on a recurring schedule, define a Scheduler Timer Event Rule with the Generate Report Action. In the Event Rule, you can define whether to email the report and/or save the report to a file. A report is generated specific to the Site on which the Event Rule is configured.



EFT Enterprise Report by GLOBALSCAPE

PCI DSS Compliance Report

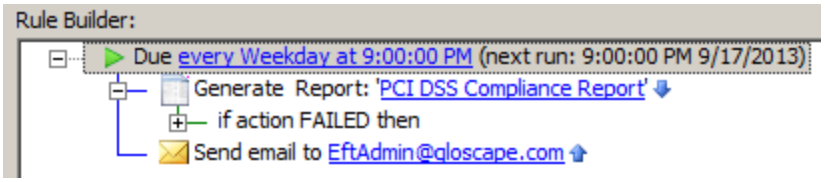
8/8/2018 4:39:12 PM Details: This report displays EFT's PCI DSS compliance status for each Site.

Requirement	Status	Description	Admin notes
Site: MyPICDSSSite			
PCI DSS 1.3.7 - System components that store cardholder must be segregated from the DMZ	**Compensating Control**	EFT's DMZ Gateway is disabled. If EFT is deployed in the DMZ, ensure that sensitive data is segregated from the DMZ or risk non-compliance with this requirement.	dasfaf
PCI DSS 2.1 - Always change vendor-supplied defaults	**PASSED**	No vendor supplied default ports are being used for remote administrator or DMZ Gateway services.	
PCI DSS 2.2.2,3 - Enable only necessary and secure protocols	**PASSED**	Only secure protocols are being used for this Site.	
PCI DSS 2.2.4 - Configure system security parameters to prevent misuse	**PASSED**	System security parameters are configured to prevent misuse.	
PCI DSS 2.3 - Encrypt all non-console administrative access	**PASSED**	Non-console administrative access is securely configured.	
PCI DSS 3.1 - Develop a data retention and disposal policy	**Compensating Control**	No Clean-up rule was found. Define a Clean-up Action in a Scheduler(Timer) Event Rule to automate the disposal of deprecated data or document a compensating control.	adsfadf
PCI DSS 3.1 - Limit storage amount to that which is required	**WARNING**	No disk quota is set for MyPICDSSSite->Default Settings. Enable disk quotas to limit data storage amounts to what is required for business purposes according to your company's data retention and disposal policy.	

Globalscape® EFT™ Page 1 of 8

Automating the PCI DSS Compliance Report

When you create a high security-enabled Site, EFT creates a Report Event Rule automatically. The **Report Event** Rule generates a PCI DSS Compliance Report once per week using the Generate Report Action. The report is converted to HTML and then emailed using the Send notification email Action and the %FS.REPORT_CONTENT% variable. You can edit the Rule to specify when to generate the report and to whom to send the report.



Optionally, you can run the PCI DSS Compliance Report "on the fly" by clicking **Reports > Run PCI DSS Compliance Report** on the administration interface main menu. If the RCM is not activated, the PC DSS Compliance Report is not available.

PCI DSS Possible Compliance Report Outcomes

The PCI DSS Compliance Report displays the requirement name, status (PASSED, FAILED, WARNING), description of the requirement, notes that you typed in the Warning box (explanation, justification, or compensating control), report name, and date the report was generated, and description of the report. The report is grouped by and sorted by PCI DSS Requirement.

If the report is generated after the trial has expired, the report contains a statement stating that the module has expired instead of the standard report.

When in trial or after the module is activate, the report contains the following information:

The status of audited PCI DSS requirements appears in the report.

- 1.x – DMZ Gateway disabled or no connectivity
- 2.x – Remote administrator enabled by not secure, vendor defaults in use, insecure protocols in use (FTP, HTTP) or insecure settings (NOOP and FXP), auto-ban/flood detection set too low or disabled, and login credential persistence enabled.
- 3.x – Disk quotas not present for limiting storage amounts, missing clean-up rule for data retention and disposal compliance.
- 4.x – Weak cryptography in use (SSL version, cipher strength, manually specified ciphers, weak HMACs), insecure settings such as SSL clear command clear data channel in use.
- 5.x – No checks
- 6.x – No checks
- 7.x – Presence of more than one full-control administrator account
- 8.x – Password length or complexity not enforced, password reuse allowed, idle session timeout disabled or set to high, inactive accounts not disabled or removed after 90 days, failed logins not resulting in account lockout after six (or less) attempts, password reset not allowed, password reset not forced on initial login, anonymous accounts present, and passwords not expiring after 90 days or sooner.
- 9.x – Secure wiping of deleted data not enabled
- 10.x – ARM not enabled or no connectivity
- 11.x – No checks
- 12.x – No checks

Refer to How EFT Addresses PCI DSS Requirements for details of each requirement.

Reporting

The Auditing and Reporting module provides numerous predefined reports which you can use as is, edit to your needs, or use as templates to create new reports. You can also define custom reports using the built-in Report Designer.

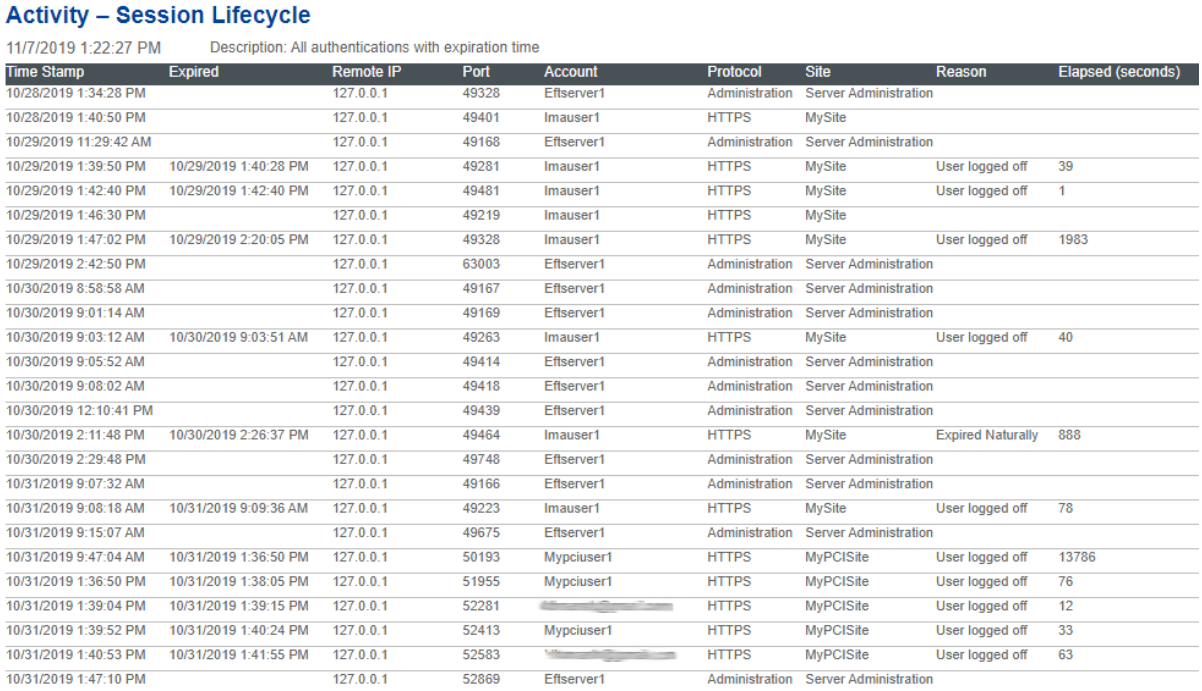
Descriptions of Preconfigured Reports

The Auditing and Reporting module comes with a number of preconfigured reports that allow you to start analyzing data right away. The report templates are **.xml** files and are installed in **%systemdrive%\ProgramData\Globalscape\EFT Server\Reports** or **\EFT Server\Reports**. If you plan to edit the default templates, it is a good idea to save a backup of them first. You can use these reports as is, or as templates to create your own custom reports.

The preconfigured reports described below are provided with the Auditing and Reporting module. You can run the reports as is or edit them to suit your specific needs.

- **Activity - AS2 Transfers (Detailed)** - A verbose AS2 file transfer report that provides the information necessary for troubleshooting problem transactions.
- **Activity - AS2 Transfers (Summary) -** A transaction report that displays the same information as shown on the Transfers - AS2 node. The report queries all AS2 transactions for the dates specified, grouped by site, sorted by date, and listed in reverse chronological order.
- **Activity - by Permissions Group** - This report displays the various Actions performed by all the groups, such as administrator, All users, and Guests, and it displays Date/Time, Remote IP address, protocol, Action, filename, folder, KB transferred, and the result.
- **Activity - by Users (Detailed) -** This report displays all folders and files created and the delete activity for all users who logged on to EFT during a particular period, grouped by username, and sorted in reverse chronological order. The report includes the time stamp, remote IP address of the user, protocol, Action, file name, folder, KB transferred, and the result.
- **Activity - by Users (Summary)** - This report displays the transfer activity (total number of uploads and downloads) for all users who logged on to EFT during the date range specified, grouped by username, subgrouped by date, sorted by username, then transfer direction, and date, in ascending order.
- **Activity - File Scanned Data Results** - This report displays all scanned data results.
- **Activity - File Transfers as Client -** This report displays all file transfers initiated by EFT.

- **Activity - File Transfers as Server** - This report displays all transfers initiated by remote clients.
- **Activity - Session Lifecycle** - This report displays authentications and session expired time. (NOTE: If an EFT user connects to EFT using CuteFTP over HTTPS and uploads several files, the report does not include data in the Expired (logout time), Reason, or Elapsed columns.)



Activity – Session Lifecycle

11/7/2019 1:22:27 PM Description: All authentications with expiration time

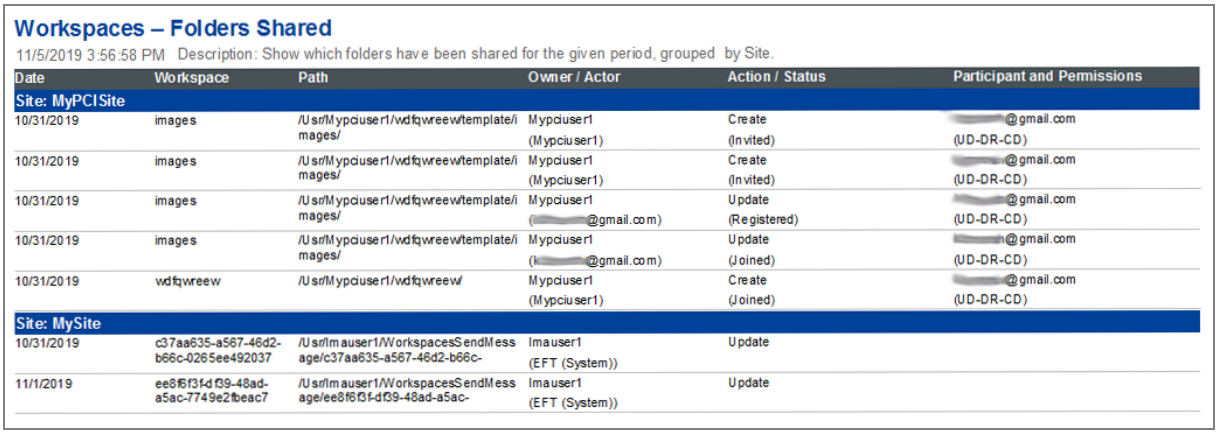
Time Stamp	Expired	Remote IP	Port	Account	Protocol	Site	Reason	Elapsed (seconds)
10/28/2019 1:34:28 PM		127.0.0.1	49328	Eftserver1	Administration	Server Administration		
10/28/2019 1:40:50 PM		127.0.0.1	49401	Imauser1	HTTPS	MySite		
10/29/2019 11:29:42 AM		127.0.0.1	49168	Eftserver1	Administration	Server Administration		
10/29/2019 1:39:50 PM	10/29/2019 1:40:28 PM	127.0.0.1	49281	Imauser1	HTTPS	MySite	User logged off	39
10/29/2019 1:42:40 PM	10/29/2019 1:42:40 PM	127.0.0.1	49481	Imauser1	HTTPS	MySite	User logged off	1
10/29/2019 1:46:30 PM		127.0.0.1	49219	Imauser1	HTTPS	MySite		
10/29/2019 1:47:02 PM	10/29/2019 2:20:05 PM	127.0.0.1	49328	Imauser1	HTTPS	MySite	User logged off	1983
10/29/2019 2:42:50 PM		127.0.0.1	63003	Eftserver1	Administration	Server Administration		
10/30/2019 8:58:58 AM		127.0.0.1	49167	Eftserver1	Administration	Server Administration		
10/30/2019 9:01:14 AM		127.0.0.1	49169	Eftserver1	Administration	Server Administration		
10/30/2019 9:03:12 AM	10/30/2019 9:03:51 AM	127.0.0.1	49263	Imauser1	HTTPS	MySite	User logged off	40
10/30/2019 9:05:52 AM		127.0.0.1	49414	Eftserver1	Administration	Server Administration		
10/30/2019 9:08:02 AM		127.0.0.1	49418	Eftserver1	Administration	Server Administration		
10/30/2019 12:10:41 PM		127.0.0.1	49439	Eftserver1	Administration	Server Administration		
10/30/2019 2:11:48 PM	10/30/2019 2:26:37 PM	127.0.0.1	49464	Imauser1	HTTPS	MySite	Expired Naturally	888
10/30/2019 2:29:48 PM		127.0.0.1	49748	Eftserver1	Administration	Server Administration		
10/31/2019 9:07:32 AM		127.0.0.1	49166	Eftserver1	Administration	Server Administration		
10/31/2019 9:08:18 AM	10/31/2019 9:09:36 AM	127.0.0.1	49223	Imauser1	HTTPS	MySite	User logged off	78
10/31/2019 9:15:07 AM		127.0.0.1	49675	Eftserver1	Administration	Server Administration		
10/31/2019 9:47:04 AM	10/31/2019 1:36:50 PM	127.0.0.1	50193	Mypciuser1	HTTPS	MyPCISite	User logged off	13786
10/31/2019 1:36:50 PM	10/31/2019 1:38:05 PM	127.0.0.1	51955	Mypciuser1	HTTPS	MyPCISite	User logged off	76
10/31/2019 1:39:04 PM	10/31/2019 1:39:15 PM	127.0.0.1	52281	[redacted]	HTTPS	MyPCISite	User logged off	12
10/31/2019 1:39:52 PM	10/31/2019 1:40:24 PM	127.0.0.1	52413	Mypciuser1	HTTPS	MyPCISite	User logged off	33
10/31/2019 1:40:53 PM	10/31/2019 1:41:55 PM	127.0.0.1	52583	[redacted]	HTTPS	MyPCISite	User logged off	63
10/31/2019 1:47:10 PM		127.0.0.1	52869	Eftserver1	Administration	Server Administration		

- **Admin - Audit Log** - This report displays a summary of all EFT administrator activity for the specified date range.
- **Admin - Audit Log (Detailed) -** This report displays all EFT administrator activity for the specified data range, with Before and After details.
- **Admin - Authentications -** This report shows administrator connections (success and failures) to the this EFT for the give date range.
- **Content Integrity Control** - A report showing all Event Rules with CIC actions, grouped by site name, sub-grouped by the user-defined event name, sorted by the unique event ID (not shown) in descending order. Includes Parameters, Begin and End Date\Time, and Result.
- **Event Rules - by Trigger Name (Summary)** - This report summarizes all Event Rules with their corresponding Actions, grouped by Site name, subgrouped by the user-defined Event name, sorted by the unique Event ID (not shown in report) in descending order.

- **Event Rules - by Trigger Type (Detailed)** - This report displays the Event Rule activity by user-defined Event name, grouped by Site name, subgrouped by the Event type, sorted by date in reverse chronological order.
- **Event Rules - by Trigger Type (Summary)** - This report summarizes the Event Rule activity by user-defined Event name, grouped by Site name, sub-grouped by the Event type, sorted by date in reverse chronological order.
- **Event Rules - Just Transfers** - This report details all offload and download Actions, grouped by Site subgrouped by Action, sorted by date in reverse chronological order.
- **Executive Summary Report** - This report summarizes the following information for the period specified:
  - Average transfer speed
  - Total number of downloads, uploads
  - Total bytes transferred (inbound/outbound)
  - Top 5 users (by # of connections)
  - Top 5 users (by bytes transferred)
- **Privacy - Admin Changes to Personal Data** - This report details changes to personal data fields, organized by date/time, Site, Template, Account, Field changed, and Before and After changes.
- **Privacy - Terms and EU Status Changes** - This report details privacy terms and EU status changes organized by date/time, Site, Template, Account, IP address, Right Exercised, and Reason a user exercised their privacy rights.
- **Privacy - User Rights Exercised** - This report details date/time, Site, Template, Account, IP address, Right Exercised, and Reason a user exercised their privacy rights. (See examples in Privacy Reports.)
- **Traffic - Average Transfer Rates by User** - This report displays the average transfer rate for specific users, grouped by username, subgrouped by date, sorted by username, transfer direction, and date, in descending order.
- **Traffic - Connections Summary** - This report details connections to EFT (IP address or user connections) and bytes transferred by date, grouped by Site name, sorted by date in reverse chronological order.
- **Traffic - Datewise - hourly Bytes Transferred** - This report details the connections and bytes transferred sorted by date and hour, in chronological order.
- **Traffic - Datewise - IPwise bytes transferred** - This report displays the connections established by remote IP addresses and total bytes transferred.
- **Traffic - IPwise Connections (Summary)** - This report displays the connections established by remote IP addresses and total bytes transferred.

- **Traffic - Monthwise-IPwise Bytes transferred** - This report displays the connections established by various remote IP addresses each month. It displays the Site name, month name, remote IP address, connections, and total bytes transferred.
- **Traffic - Most Active IPs - Connections** - This report displays the most active IP addresses; that is, the IP addresses of the users who frequently log on to EFT. It displays the data transferred, Site name, remote IP address, and bytes transferred. This report can be used to determine Denial of Service (DoS) attacks against EFT.
- **Traffic - Most Active IPs - Data Transferred** - This report displays the IP addresses of users who log on to EFT frequently; the number of connections established by various users. It displays the information on the total bytes transferred, number of connections, remote IP address, and Site name.
- **Traffic - Most Active Users - Connections** - This report displays the connections established by the most active users.
- **Traffic - Most Active Users - Data Transferred** - This report displays the usernames of users who log on to EFT frequently, the number of connections established by various users, and number of bytes transferred.
- **Traffic - Protocolwise Connections (Summary)** - This report displays the connections established by various users and the protocol used by the users to transfer the data, that is, whether the users have used FTP, HTTP, or any other protocol to upload or download the files.
- **Traffic - Sitewise - Hourly by User** - This report displays the total number of connection established by various users on a particular Site each hour.
- **Troubleshooting - Event Rules Failures** - This report displays failures related to the Event Rules.
- **Troubleshooting - Most Prolific Users -** This report details users with the most log on attempts.
- **Troubleshooting - Negotiated SSH Ciphers** - This report lists all negotiated SSH Ciphers organized by Time Stamp, Key Algorithm, Cipher, KEX, MAC, Compress Directory, Account, and Fingerprint
- **Troubleshooting - Negotiated SSH Ciphers (Summary)** - This report provides a summary of negotiated SSH Ciphers
- **Troubleshooting - Negotiated SSL Ciphers** - This report list all negotiated SSL Ciphers, organized by Time Stamp, Protocol version, EncryptionCipher, KEX, Authentication, MAC, Directory Account
- **Troubleshooting - Negotiated SSL Ciphers (Summary)** - This report a summary of SSL Ciphers used, organized by Protocol version, EncryptionCipher, KEX, Authentication, MAC, Directory, Account, Count

- **Troubleshooting - Operation Errors** - This report displays protocol error codes and corresponding commands, sorted in reverse chronological order. The report includes the date and time the error occurred, remote IP address, protocol used, username, command, filename, virtual folder, and result (for example, transfer completed).
- **Troubleshooting - Socket Connection Errors(Inbound)** - This report displays the number of connection errors occurred while connecting to a site. (Refer to Winsock Error Codes for a list of Socket ID error codes.)
- **Troubleshooting - Socket Connection Errors Summary (Inbound)** - This report displays a summary of the number of connection errors occurred while connecting to a site.
- **Web Service- Invoke Event Rules (Detailed)** - This report is used to view activity for invoking Event Rules through Web Service, grouped by username, and sorted by date in reverse chronological order.
- **Workspaces Files Picked Up** - Shows shared Workspace files picked up, organized by Send Date, Sender Email, Recipient Email, File Name, File Size (KB), Subject, and Expires date.
- **Workspaces - Files Sent** - This report lists Workspace files sent, organized by Send Date, Sender Email, Recipient Email, File Name, File Size (KB), Subject, and Expires date.
- **Workspaces - Folders Shared** - This report shows which folders have been shared for the given period, grouped by Site, organized by Date, Workspace, Path, Owner/Actor, Action/Status, and Participant/Permissions.



Workspaces – Folders Shared

11/5/2019 3:56:58 PM Description: Show which folders have been shared for the given period, grouped by Site.

Date	Workspace	Path	Owner / Actor	Action / Status	Participant and Permissions
Site: MyPCISite					
10/31/2019	images	/Usr/Mypciuser1/wdfqwreewtemplate/images/	Mypciuser1 (Mypciuser1)	Create (Invited)	[redacted]@gmail.com (UD-DR-CD)
10/31/2019	images	/Usr/Mypciuser1/wdfqwreewtemplate/images/	Mypciuser1 (Mypciuser1)	Create (Invited)	[redacted]@gmail.com (UD-DR-CD)
10/31/2019	images	/Usr/Mypciuser1/wdfqwreewtemplate/images/	Mypciuser1 ([redacted]@gmail.com)	Update (Registered)	[redacted]@gmail.com (UD-DR-CD)
10/31/2019	images	/Usr/Mypciuser1/wdfqwreewtemplate/images/	Mypciuser1 ([redacted]@gmail.com)	Update (Joined)	[redacted]@gmail.com (UD-DR-CD)
10/31/2019	wdfqwreew	/Usr/Mypciuser1/wdfqwreew/	Mypciuser1 (Mypciuser1)	Create (Joined)	[redacted]@gmail.com (UD-DR-CD)
Site: MySite					
10/31/2019	c37aa635-a567-46d2-b66c-0265ee492037	/Usr/Imauser1/WorkspacesSendMessage/c37aa635-a567-46d2-b66c-	Imauser1 (EFT (System))	Update	
11/1/2019	ee8f6f3f-df39-48ad-a5ac-7749e2fbeac7	/Usr/Imauser1/WorkspacesSendMessage/ee8f6f3f-df39-48ad-a5ac-	Imauser1 (EFT (System))	Update	

- **Workspaces - Folders Unshared** - This reports shows which folder shares of expired naturally or by their owner, organized by Date, Workspace, Path, Owner or Actor, Status, and Participant(s).

Generating a Report

The ARM comes with a number of preconfigured reports to help you start analyzing data right away. The built-in reports were designed to respond to the most common data analysis requests. Refer to Preconfigured Reports for a list of available reports. If you are using SQL Express as your database, you may not be able to generate a report remotely, unless the connecting account is a trusted SQL Server connection (that is, if SQL Server and the remote computer are in the same domain, or if SQL Server is configured to allow "mixed authentication.")

To generate a report

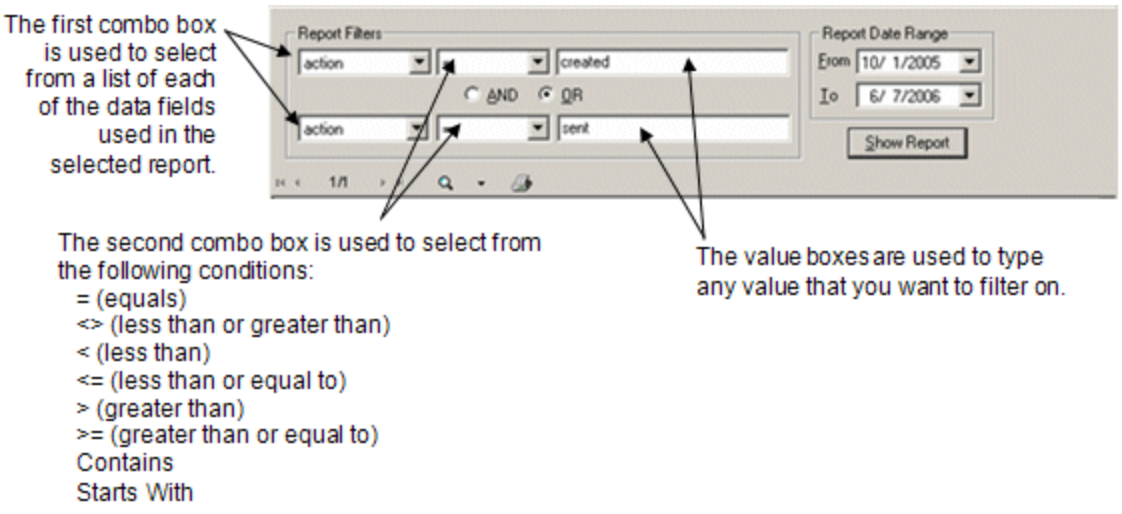
1. In the administration interface, connect to EFT and the reports database, and then click the **Reports** tab.
2. In the left pane, click the desired report.
3. In the right pane, specify any filters.
4. Specify a date range from which you want pull data.
5. Type the appropriate parameters/wildcards for the search if the following reports are used:
   - **Activity By File** - Type the file name.
   - **Activity By Group** - Type the group name.
   - **Troubleshooting IP address Activity** - Type the IP address.
6. Click **Show Report**. The ARM connects to the auditing database and displays the data in the right pane. ARM displays the first page of the report as soon as the data is ready, then continues to load additional pages. You can monitor the progress of loading by watching the current page/total pages indicator on the report filter bar.

If you want to stop a report from loading, click another report in the left pane.

Using Report Filters

You can filter the fields in a report based on various conditions to display only the data that meet the filtering criteria.

The **Report Filters** area contains two sets of combo boxes, operands (AND, OR), and a text box.



Use the second set of filters to further define the report using **AND** or **OR**.

For example, suppose you have generated a report like the one below:

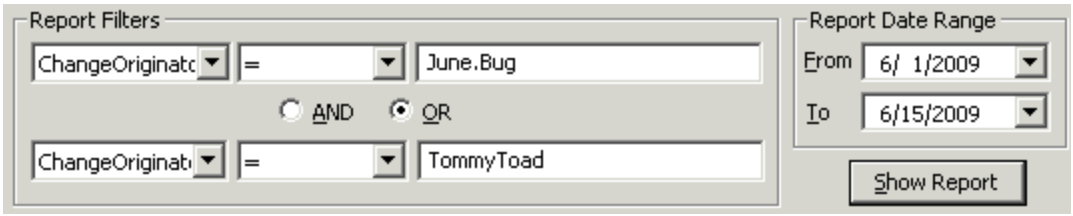
Administrator Actions Log

6/15/2009 4:22:07 PM Description: Report detailing all administrator activity for the specified date range

Date / Time	Function	Action	Affected Area	Affected Name	Change Originator
Site Name: MySite					
6/15/2009 4:21:35 PM	User Account	Created	User Account	OliveOil	TommyToad
6/15/2009 4:19:05 PM	User Account	Created	User Account	ysam	June.Bug
6/15/2009 4:17:34 PM	Group Assignment	Modified	Permission Group	Administrative	eft
6/15/2009 4:17:09 PM	User Account	Created	User Account	bbunny	eft
6/15/2009 4:16:44 PM	User Account	Created	User Account	jbug	eft
6/15/2009 4:16:36 PM	Site	Created	Site	MySite	eft
Site Name: Server					
6/15/2009 4:21:46 PM	Administrator	Connected	Administration	eft	eft
6/15/2009 4:21:40 PM	Administrator	Disconnected	Administration	TommyToad	TommyToad
6/15/2009 4:21:19 PM	Administrator	Connected	Administration	TommyToad	TommyToad
6/15/2009 4:21:12 PM	Administrator	Disconnected	Administration	eft	eft
6/15/2009 4:21:06 PM	Administrator	Connected	Administration	eft	eft
6/15/2009 4:20:59 PM	Administrator	Disconnected	Administration		
6/15/2009 4:20:49 PM	Administrator	Disconnected	Administration	eft	eft
6/15/2009 4:20:44 PM	Delegated Administrator	Modified	Administration	TommyToad	eft
6/15/2009 4:20:44 PM	Delegated Administrator	Created	Administration	TommyToad	eft
6/15/2009 4:19:23 PM	Administrator	Connected	Administration	eft	eft
6/15/2009 4:19:16 PM	Administrator	Disconnected	Administration	June.Bug	June.Bug
6/15/2009 4:18:42 PM	Administrator	Connected	Administration	June.Bug	June.Bug
6/15/2009 4:18:33 PM	Administrator	Disconnected	Administration	eft	eft

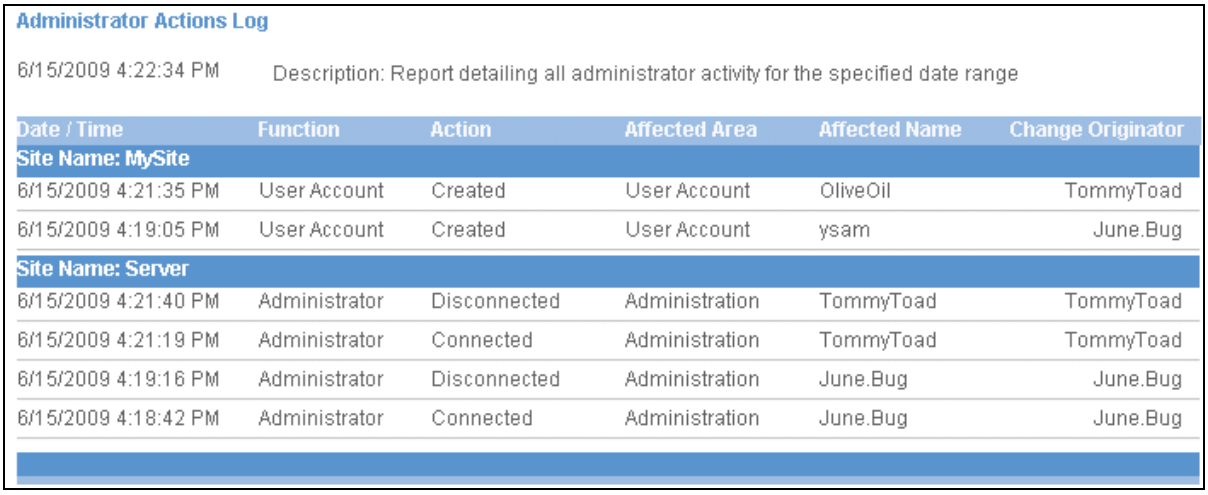
To show only changes made by TommyToad and June.Bug, set the following filters:

1. In the first combo box, click **Change Originator**.
2. In the second combo box, click the equals sign (**=**).
3. Type `June.Bug` in the text box.
4. Click **OR**.
5. In the bottom filter, click **Change Originator**, equals, and type `TommyToad`.



6. Specify a date range, and then click **Show Report**.

7. The report now displays only changes made by administrators TommyToad or June.Bug.



Administrator Actions Log

6/15/2009 4:22:34 PM Description: Report detailing all administrator activity for the specified date range

Date / Time	Function	Action	Affected Area	Affected Name	Change Originator
Site Name: MySite					
6/15/2009 4:21:35 PM	User Account	Created	User Account	OliveOil	TommyToad
6/15/2009 4:19:05 PM	User Account	Created	User Account	ysam	June.Bug
Site Name: Server					
6/15/2009 4:21:40 PM	Administrator	Disconnected	Administration	TommyToad	TommyToad
6/15/2009 4:21:19 PM	Administrator	Connected	Administration	TommyToad	TommyToad
6/15/2009 4:19:16 PM	Administrator	Disconnected	Administration	June.Bug	June.Bug
6/15/2009 4:18:42 PM	Administrator	Connected	Administration	June.Bug	June.Bug

(If you had clicked AND instead of OR, nothing would appear, because no changes can be made by 2 administrators at the same time.)

Defining Custom Reports

The topics below provide information regarding creating custom reports of EFT activity in the administration interface.

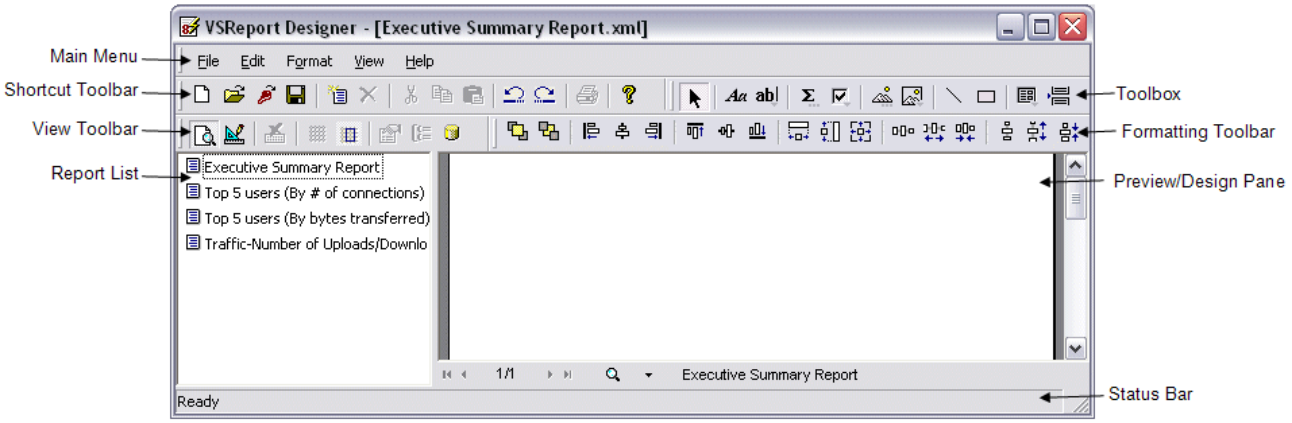
VSReport Designer

Querying, sorting, filtering, and reporting on EFT data can be accomplished by editing one of the existing reports or creating a new report in the provided report editor. This tool can be launched from within the administration interface.

The report editor tool bundled with ARM is a robust report designer licensed from Component One. During EFT evaluation period, VSReport Designer is available for use as a fully functional trial. A license for VSReport Designer is included with each purchase of ARM. After the trial, ARM must be activated along with EFT to continue using VSReport Designer. Most of the main functions of the report designer are described in this help file; however, the VSReport Designer has its own Help file, accessed by clicking **Help** on the report designer's main menu.

In VSReport Designer, you can work on existing report templates, change field locations and properties, add various levels of grouping, sorting, and so on. You can also create new reports and select ARM's database tables from which to retrieve data fields or paste in SQL code for advanced queries of the data source, giving customers complete freedom in designing their report. Styles for the report (colors, fonts, background logo images, etc.) can all be manipulated from within the designer. You can also import report definitions from Microsoft Access files (MDB, ADP) and VSReport Designer files (VSR) from within the Report Designer.

Translation of Access reports requires that Microsoft Access is installed. Once the report is imported into the Designer, Access is no longer required.

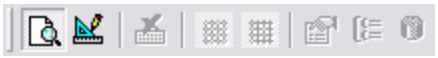


The main Designer dialog box includes the following:

- **Report list** - The left pane of the Report Designer lists all report templates contained in the current report definition file. (A report can contain multiple report templates.) You can double-click a report name to preview or edit the report. You can also right-click in the list to rename, copy, and delete report templates.
- **Preview/Design pane** - The right pane is the main working area of VSReport Designer. In preview mode, it displays the current report. In design mode, it shows the report's sections and fields and allows you to change the report definition.
- **Main Menu** - The main menu is used to access submenus, load and save report definition files, import report definitions, and print reports.

- **Shortcut toolbar** - Shortcuts are used to access the most common menu functions: new file, open, import, save, print, undo/redo, cut/copy/paste, create/delete report, and help.

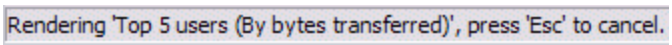
- **View toolbar** - The **View** toolbar allows you to easily switch between preview and design modes, activate the design grid, and display the property and grouping panes.



- **Toolbox** - The **Toolbox** provides tools for creating report fields. This toolbar is enabled only in design mode.

- **Formatting toolbar** - The **Formatting** toolbar provides shortcuts to tools for aligning, sizing, and spacing report fields. This toolbar is enabled only in design mode.

- **Status bar** - The **Status bar** at the bottom of the Report Designer displays information about what VSReport Designer is working on (for example, loading, saving, printing, rendering, importing, etc.).



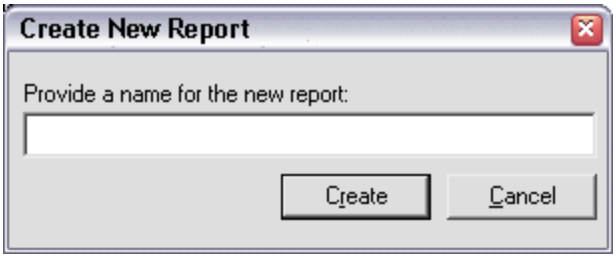
Opening VSReport Designer

When you create a new report, you create it manually or use the Report Wizard. Both methods are provided in the VSReport Designer, as described below.

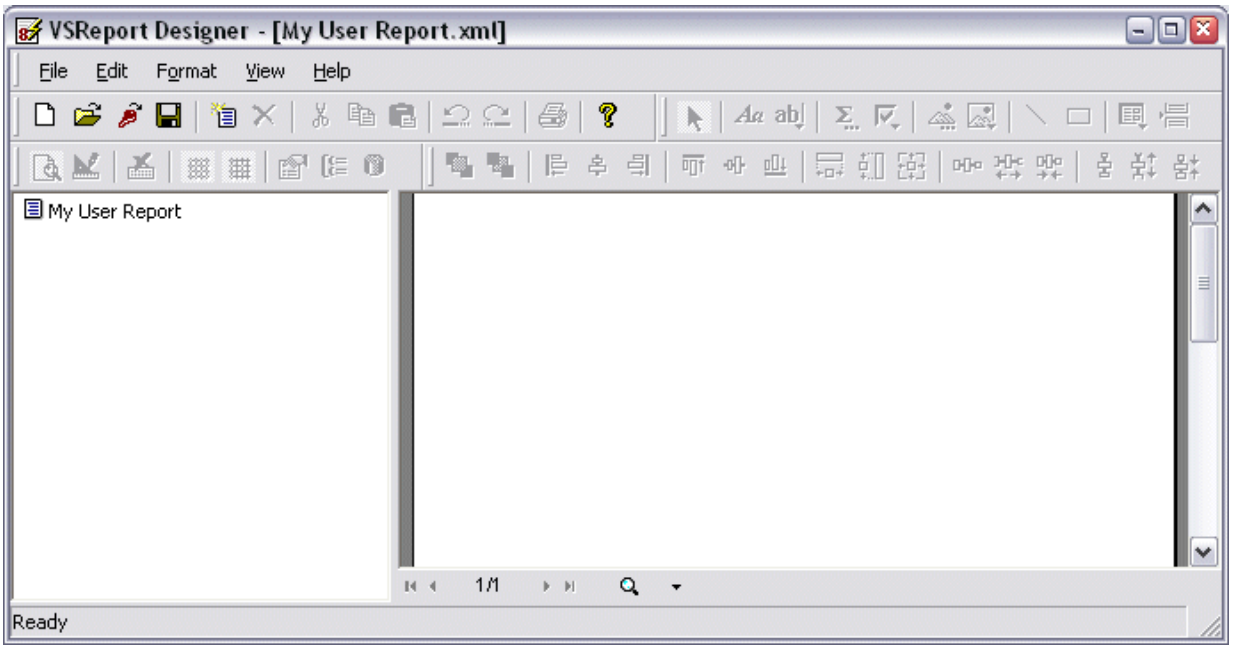
To open VSReport Designer

1. In the administration interface, connect to EFT, then do one of the following:
   - On the toolbar, click the click **New Report** icon .
   - On the main menu, click **Reports >New Report**.
   - Click the **Reports** tab, and then click the **New Report** icon at the bottom of the right pane.

   The **New Report** dialog box appears.



2. Type a title for the new report, and then click **Create**. The **Report Designer** appears.



3. Do one of the following to create a report:
    - **Manually define the report:** click the report name in the left pane, click the **Design** icon, then continue with the instructions in Using Design Mode, Changing Field, Section, and Report Properties, Changing the Data Source, Adding, Editing, and Deleting Fields in the Report, and Grouping and Sorting Data.
    - Use the Report Wizard: In the Report Designer, click **File >New Report** or click the **New Report** icon on the toolbar.

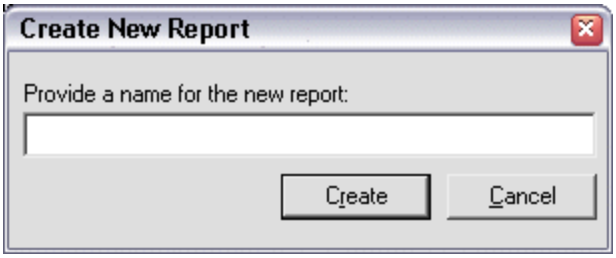
Creating a Report with the Report Wizard

The easiest way to start a new report is to use the Report Wizard. The Report Wizard will help you create a basic report, specify the data source, fields to include in the report, layout of the report, and styles or labels to use in the report.

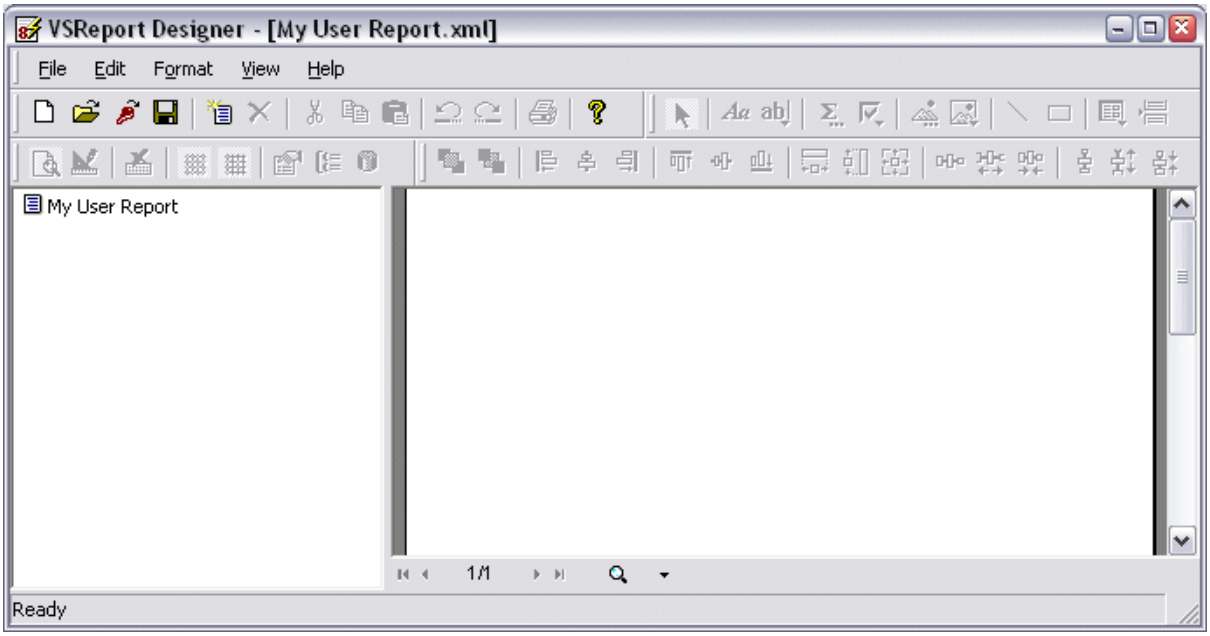
To use the Report Wizard

1. In the administration interface, connect to EFT, then do one of the following:
    - On the toolbar, click the click **New Report** icon.
    - On the main menu, click **Reports >New Report**.
    - Click the **Reports** tab, and then click the **New Reports** icon on the bottom toolbar.

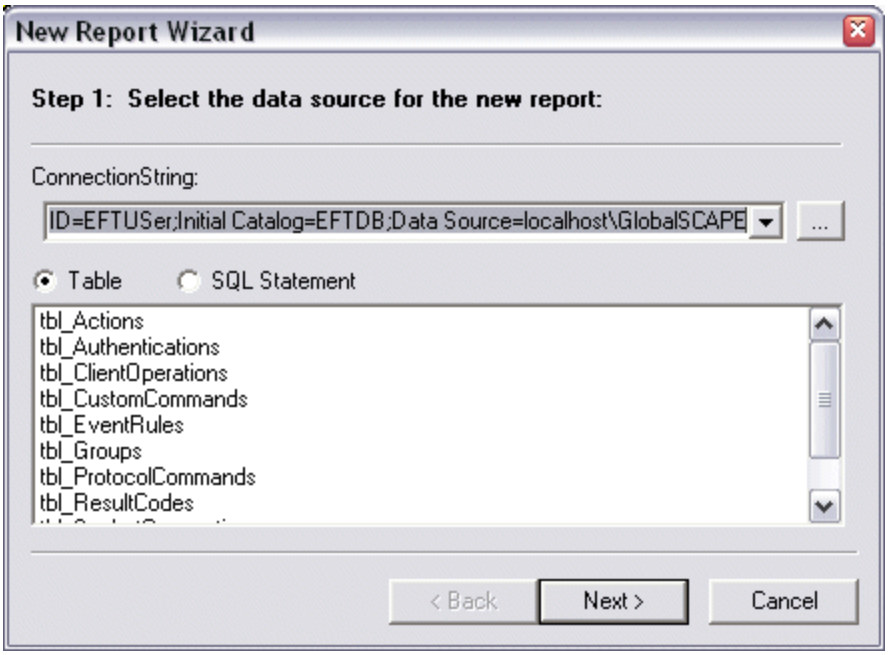
    The **New Report** dialog box appears.



2. Type a title for the new report, and then click **Create**. The **Report Designer** appears.



3. Click **File >New Report** or click the **New Report** icon on the toolbar. The **New Report Wizard** appears.



4. By default, the **ConnectionString** box displays information for the database that you specified when you installed the Auditing and Reporting module. Click **Next** and go to step 5 or, if necessary, you can type a different string that is used to connect to the data source.

a. Click the ellipsis to define the connection string. The **Data Link Properties** dialog box appears.

b. On the **Provider** tab, click **Microsoft OLE DB Provider for SQL Server** as the provider to connect to the SQL Server database, and then click **Next**. The **Connection** tab appears.

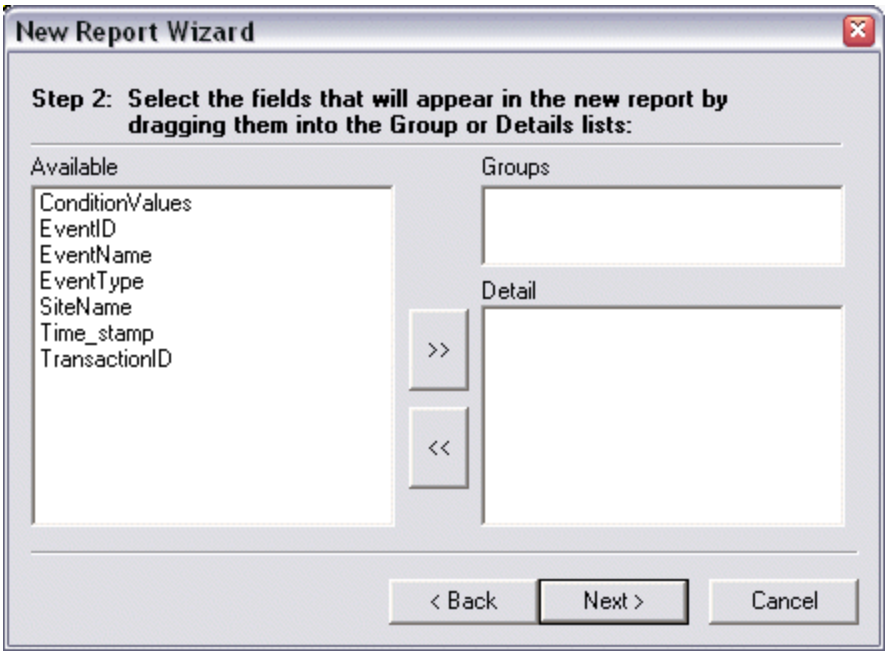
c. In **Select or enter a server name**, click the arrow to select a name or type the name of EFT.

d. In **Enter information to log on to EFT**, click an authentication option to log on to EFT:

- **Use Windows NT Integrated security** - Your computer automatically picks up the credentials from your computer and connects you to the database.
- **Use a specific user name and password** - Specify the user name and the password to be used to log on to EFT. Select the **Allow saving password** check box to save the password in the connection string.

> **NOTE:** Select the **Blank password** check box if EFT requires a blank password to log on the
> database server. Even if you do not type any password when you create a user account
> on a database server, you can select the **Allow saving password** check box. In this case,
> EFT takes a dummy password value and saves that value in the connection string.
> Selecting the **Blank password** check box disables the password field.

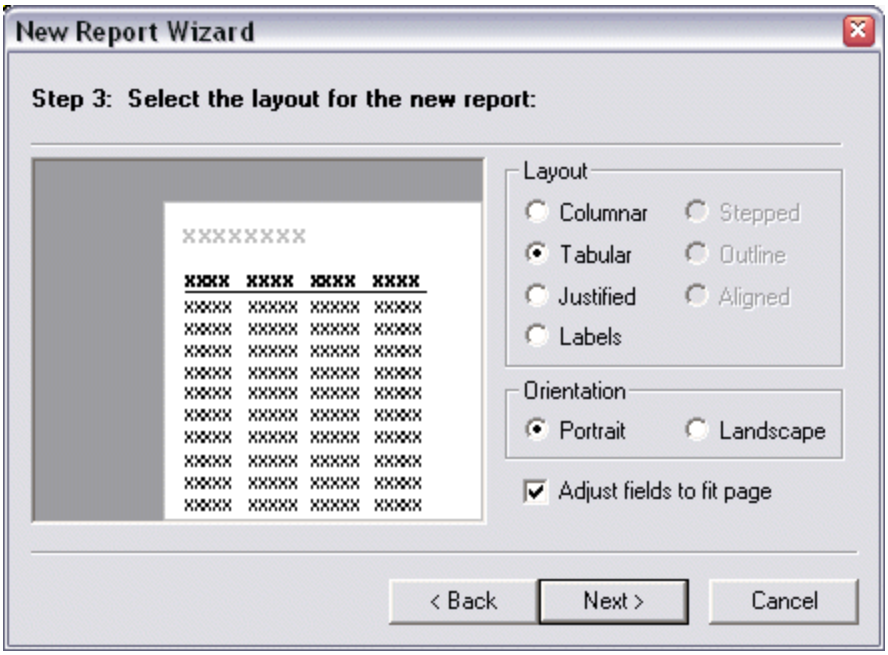
5. Click one of the following:
   - Select the database on EFT, and then click a database in the list.
   - Attach a database file as a database name - Click the ellipsis icon to browse for the SQL Server database file (*.mdf). The **Select SQL Server Database File** dialog box appears. Select a file, then click **Open**. The path to the file appears in the **Using the filename** box.
6. Click **OK** in the **Data Link Properties** dialog box to return to the **New Report Wizard**.
7. Click one of the following:
   - **Table** to select a database table, such as `tbl_EventRules`.
   - **SQL Statement** to type a SQL query in the bottom box, such as `SELECT * FROM tbl_EventRules`.
8. Click **Next**. The fields that appear in the **Available** list depend on your selection in the previous step. For example, if you selected `tbl_EventRules`, the fields for Event Rules appear.



9. Double-click a field, click it and use the arrows, or drag and drop one or more field to the **Groups** list. Group fields define how the data is sorted and summarized. The information in the **Detail** list is grouped according to the group name. The **Detail** list displays the details for each group. Detail fields define the information you want to appear in the report. For example, if you move SiteName to the **Groups** list and Time_stamp, EventName, and so on to the **Detail** list, then the report displays the time stamp and events under the respective Sites, considering different Sites as different groups.

   You can also drag and drop the available fields into the Groups or Detail section.

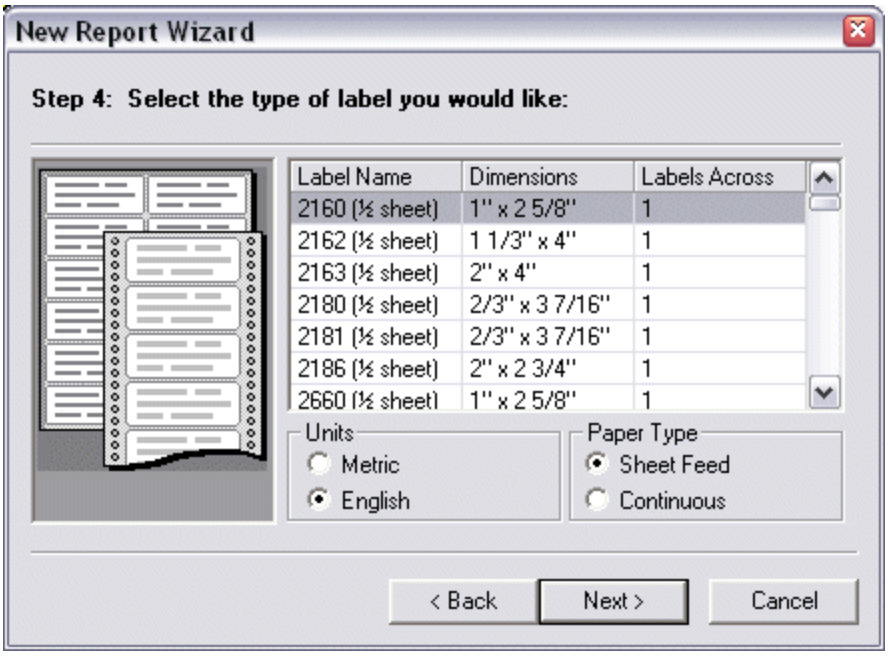
10. Click **Next**. The layout options appear.



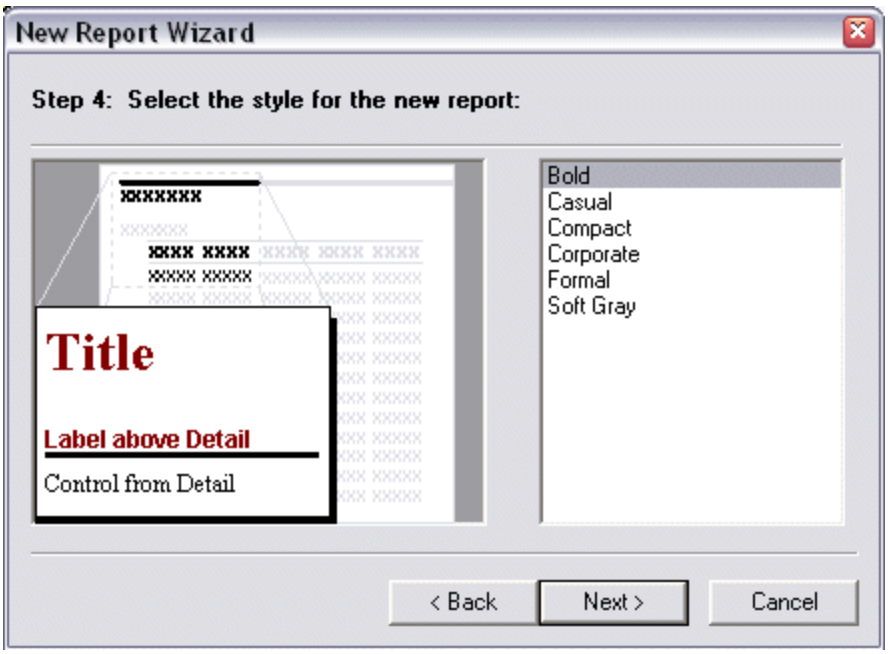
11. Click a layout for the report. When you select a layout, a thumbnail preview appears on the left to give you an idea of how the layout will appear on the page. There are two groups of layouts. The first is for the reports with no groups defined and other is for the reports with group fields defined.
    - If you did ***not*** define the Group field, the following options are available:
        - Columnar
        - Tabular
        - Justified
        - Labels. The **Labels** layout option is used to print Avery-style labels, available in a variety of sizes, blank or preprinted. If you select this option, the next page offers options for the type of label for your report.
    - If you defined the Group field, the following options are available:
        - Stepped
        - Outline
        - Aligned
    - If you selected any option other than **Labels**, click the report orientation from the following options. If you select the **Labels** option, the **Orientation** options are disabled.
        - Portrait
        - Landscape

- Select the **Adjust fields to fit page** check box to adjust fields in a way that they fit the page.

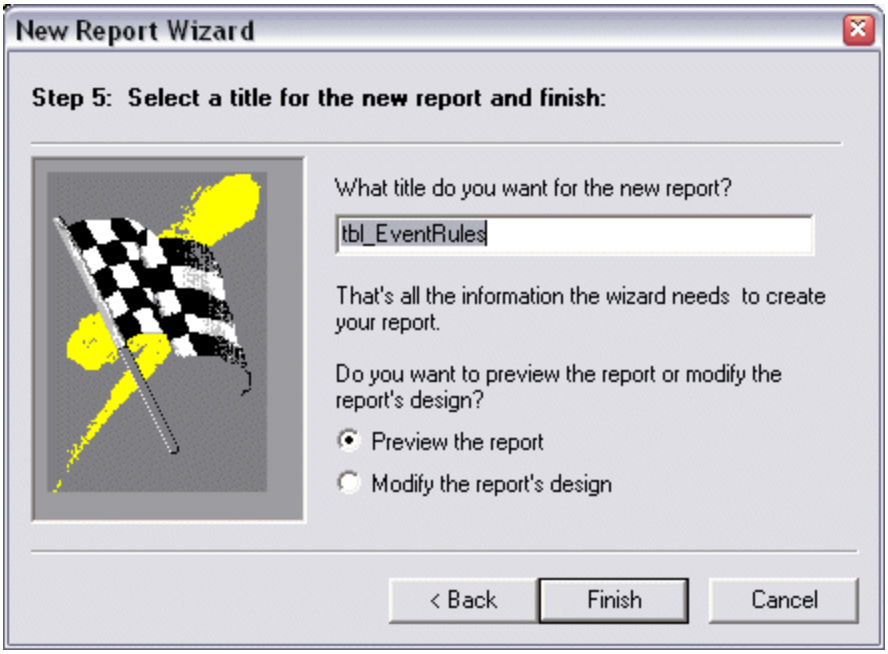
12. Click **Next**.
13. Do one of the following:
    - If you specified **Labels**, click a type of label in the **Labels** list, then specify the Units, **Metric** or **English**, and the paper type, **Sheet Feed** (single sheet) or **Continuous** (continuous paper).



- If you specified anything other than **Labels**, specify a style for the report title.



14. Click **Next**. The title page of the wizard appears.



15. Type a title for the report.
16. Do one of the following:
    - To view the report, click the **Preview the report**.
    - To modify the report in Design view, click the **Modify the report's design**.

17. Click **Finish**. Your new report name appears in the left pane of the Report Designer. The right pane displays a preview of the report or the design view, depending on your selection in the previous step.
18. Click **Save** to save the report.
19. Click **File >Close** to close VSReport Designer. The report appears on the **Reports** tab.
20. Use Design mode to add/remove fields, resize fields, add graphics, and so on.

Creating a Report in Design Mode

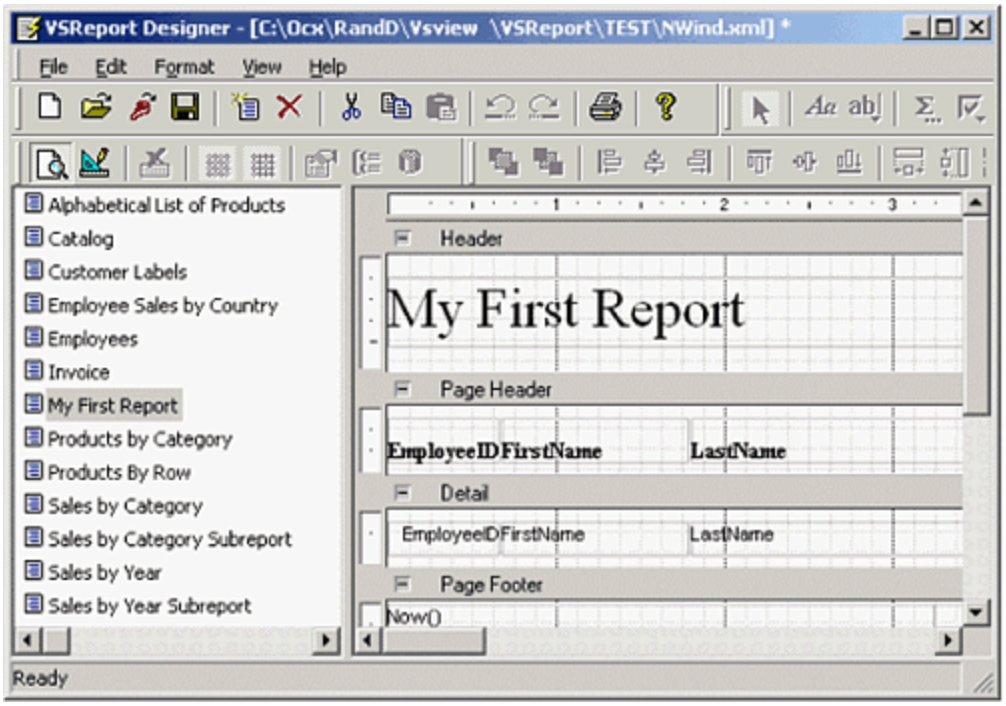
The New Report Wizard is used to specify a data source and a basic framework for the report. To get exactly the report you want, you can adjust and enhance the data fields and layout. The Report Designer provides the options to modify the report to fit your needs.

To use the Report Designer design mode

1. In the administration interface, click the **Reports** tab, then do one of the following:
   - Click the report that you want to modify, and then click **Edit Report**.
   - Create a new report. (Refer to Creating a Report with the Report Wizard for instructions.)

   The report appears in the Report Designer.
2. The left pane of the Report Designer lists all report templates contained in the current report definition file. Click the report that you want to modify, and then click the **Design**  icon on the **View** toolbar, or on the main menu, click **View >Design**.

The right pane switches from **Review** mode to **Design** mode, and displays the controls and fields that make up the report.



The Report Sections

The report is divided into sections, labeled **Header**, **Page Header**, **Detail**, and **Page Footer**, containing fields that hold the labels, variables, and expressions that you want in the generated report. The sections determine the appearance of the beginning and end of the report, and each page and group. The table below describes where each section appears in the report and the sort of data that typically appears in each section.

Section	Appears	Typically Contains
Report Header	Once per report	The report title and summary information for the whole report
Page Header	Once per page	Labels that describe detail fields and/or page numbers
Group Header	Once per group	Fields that identify the current group and possibly aggregate values for the group (e.g. total, percentage of the grand total)
Detail	Once per record	Fields containing data from the source record set
Group Footer	Once per group	Aggregate values for the group
Page Footer	Once per page	Page number, page count, date printed, report name
Report Footer	Once per report	Summary information for the entire report

You cannot directly add and delete sections. The number of groups determines the number of sections in a report. Each report has exactly five fixed sections (Report Header/Footer, Page Header/Footer, and Detail) plus two sections per group (a Header and a Footer).

To hide sections that you do not want to display

1. Right-click the field, click **Properties**. The **Field Properties** dialog box appears.
2. Change the property of **Visible** to **False**.

To resize a section

1. Click and hold the border of the section and drag it to the position where you want it. The rulers on the left and on top of the design dialog box show the size of each section (excluding the page margins). You cannot make the section smaller than the height and width required to contain the fields in it. To reduce the size of a section beyond that, move or resize the fields in the section first, then resize the section.
2. Press and hold SHIFT, and then click fields to toggle their selection status.
3. Press and hold CTRL, then drag the cursor to copy a selection.
4. Click on the corners of a field to resize it.
5. Press TAB to move the selection to the next field.
6. Press the arrow keys to move selected fields.
7. Press DELETE to remove selected fields.

If you make any mistakes while moving or editing the fields, click **Undo** and/or **Redo**.

When multiple fields are selected, you can use the buttons on the **Format** toolbar to align, resize, and space them.

You can control the design grid using the **Show Grid** and **Snap To Grid** icons.

Changing Field, Section, and Report Properties

You can view and edit the properties of the objects inserted in a report.

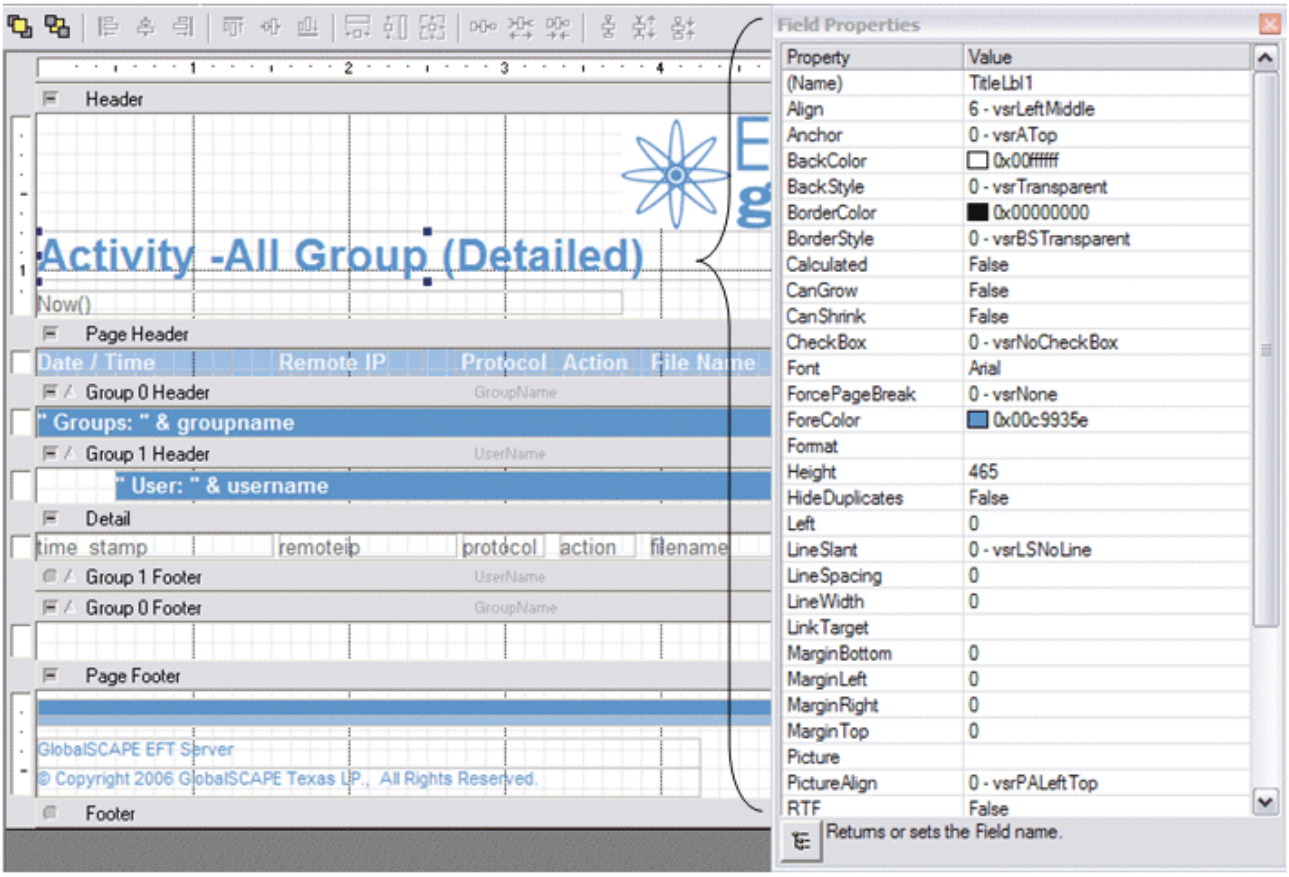
- When more than one field is selected, the **Field Properties** dialog box displays only the properties and values that all selected fields have in common and leaves the other properties blank.
- If no fields are selected and you click a section (or on the bar above a section), the selected section's properties are displayed.
- If you click the gray area in the background, the **Report** properties are displayed.

To view and edit an object's properties

- Double-click the object or select the object, then do one of the following:
  - Click **Property Window**.
  - Press F4
  - Right-click, and then click **Properties**.

  The **Field Properties** dialog box appears.

In the example below, the **Activity - All Group (Detailed)** label in the **Header** section is selected. The **Field Properties** dialog box displays the properties of the selected field.



In the **Field Properties** dialog box, you can change a property by changing its value. For example, you can change the text color by changing the **ForeColor** property. You can change the field's position and dimensions by typing new values for the **Left**, **Top**, **Width**, and **Height** properties.

The property dialog box expresses all measurements in *twips* (the native unit used by the ComponentOne report designer), but you can type in values in other units and they will be automatically converted into twips. For example, if you set the field's **Height** property to "0.5in," the property dialog box will convert it into 720 twips.

Adding, Editing, and Deleting Fields in the Report

VSReport Designer only has one type of field object; the icons in the Toolbox simply set the properties of the field to make it look and act in a certain way.

To add, edit, or delete fields in a report

1. In the Report Designer, click **View>Design** or click the **Design** icon  on the toolbar. The report opens in the design mode.
2. Use the ToolBox to add fields to your report. Follow the procedures below depending on the fields that you want to add, edit, or delete.

Each icon creates a field and initializes the field's properties as follows:

Icon	Name	Description
	Label field	Creates a field that displays static text.
	Bound field	Creates a field that is bound to the source recordset. When you click this button, a menu appears and you can select the recordset field. **Bound Fields** are not limited to displaying raw data from the database. You can edit their Text property and use any VBScript expression.
	Expression Field	Creates a calculated field. When you click this button, the code editor dialog will appear so you can enter the VBScript expression whose value you want to display.
	Check box Field	Creates a bound field that displays a Boolean value as a check box. By default, the check box displays a regular check mark. You can change it into a radio button or cross mark by changing the value of the field's **Checkbox** property after it has been created.
	Unbound Picture field	Creates a field that displays a static picture, such as a logo. When you click this button, a dialog box will appear to prompt you for a picture file to insert in the report. A copy is made of the picture you select and is placed in the same directory as the report file. You must distribute this file with the application unless you embed the report file in the application. When you embed a report file in your application, any unbound picture files are embedded too.
	Bound Picture field	Creates a field that displays a picture (or object) stored in the recordset. When you click this button, a menu appears so you can select a picture field in the source recordset (if there is one; not all recordsets contain this type of field).
	Line field	Creates a line. Lines are often used as separators.
	Rectangle field	Creates a rectangle. Rectangles are often used to highlight groups of fields or to create tables and grids.
	Subreport field	Creates a field that displays another report. When you click this button, a menu appears and you can select other reports that are contained in the same report definition file.
	Page Break field	Creates a field that inserts a page break.

After you click any of these icons, drag the mouse over the report and the cursor will change into a crosshair. Click and drag to define a space that the new field will occupy, and then release the button to create the new field. If you change your mind, press ESC or click the arrow button to cancel the operation.

You can also add fields by copying and pasting existing fields, or by holding down the control key and dragging a field or group of fields to a new position to create a copy.

To draw a line

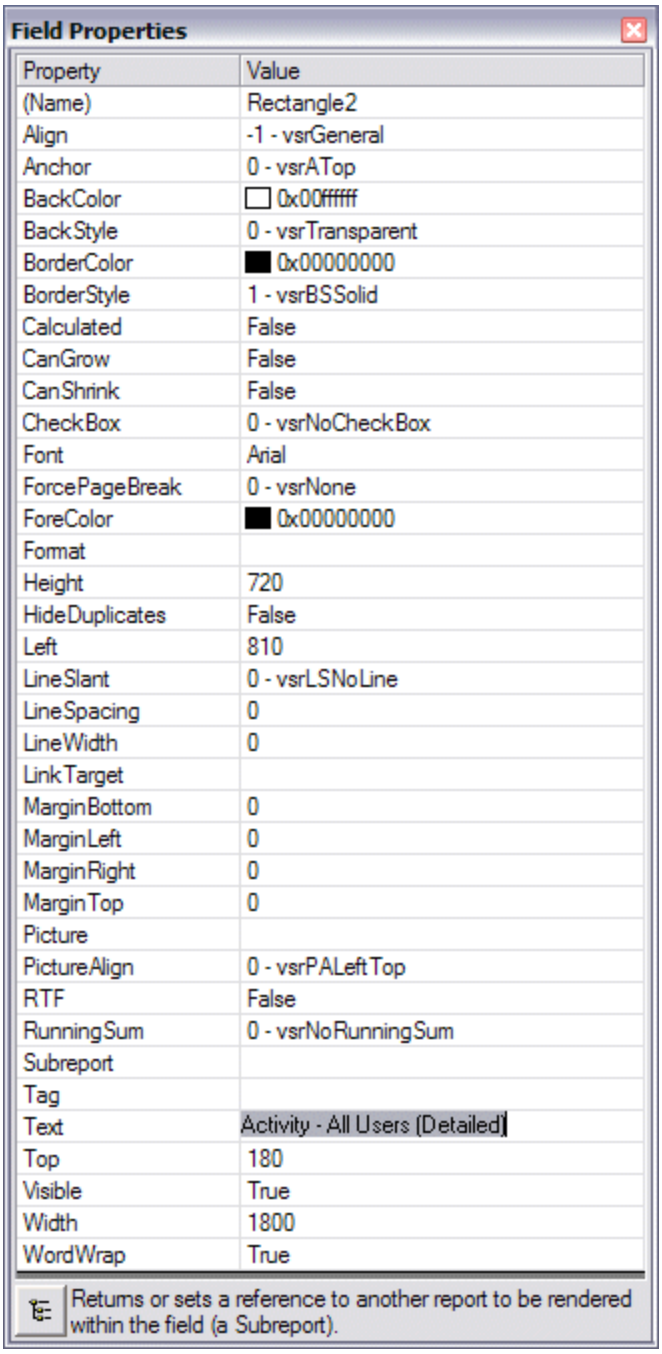
- Click **Line**  , then drag the cursor where you want to draw a line.

To draw a rectangle

- Click **Rectangle**  , then drag the cursor where you want to draw a rectangle.

To add or edit text

1. Insert a rectangle, or double-click or right-click an existing rectangle, and then click **Properties**. The **Field Properties** dialog box appears.



2. Scroll to **Text** in the **Property** column, click the **Value** column, then type the text; press ENTER.

To add labels

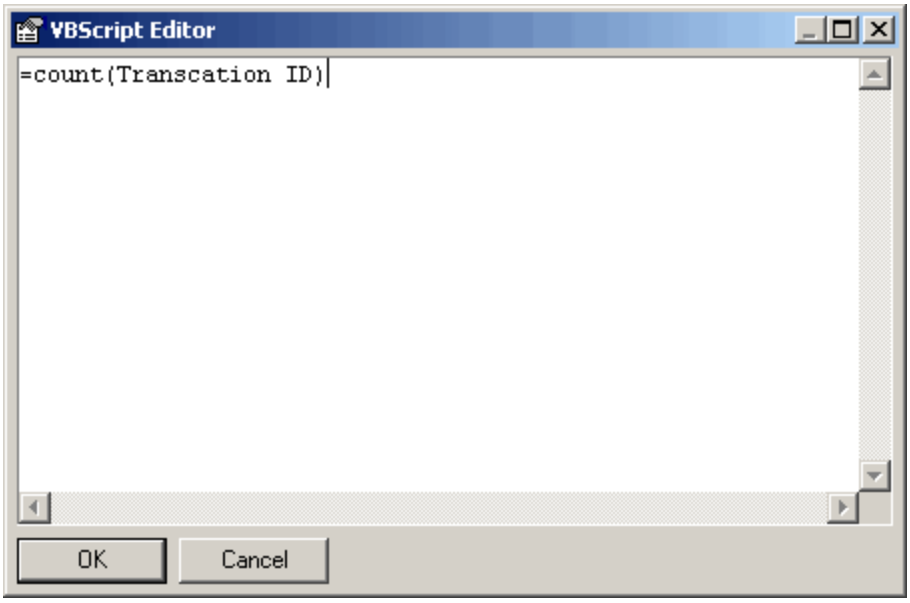
- Click **Label** Aa, then drag the pointer to draw a box in the report at the place you want to add a label. Name the label, then specify its font, color, and other properties. You can click and drag the label to adjust its placement in the report.

To add data fields

- Click **Data field** , then draw a box on the report. Change the properties of the data field by right-clicking it, and then clicking **Properties**.

To create a VBScript expression

1. Click **Calculated field** on the toolbar. The **VBScript Editor** appears.



2. Type the VBScript expression. For example, type:

   ```
   =count (Transaction ID)
   ```

3. Click **OK**.
4. Drag the pointer and place it under the respective field where you want the result to display.
5. Click the **Preview** icon on the toolbar to view the result.

To insert images

1. Click **Picture** . The **Open** dialog box appears.
2. Click an image, and then click **Open**.
3. Drag the cursor to draw a box where you want the image to appear.

To delete fields

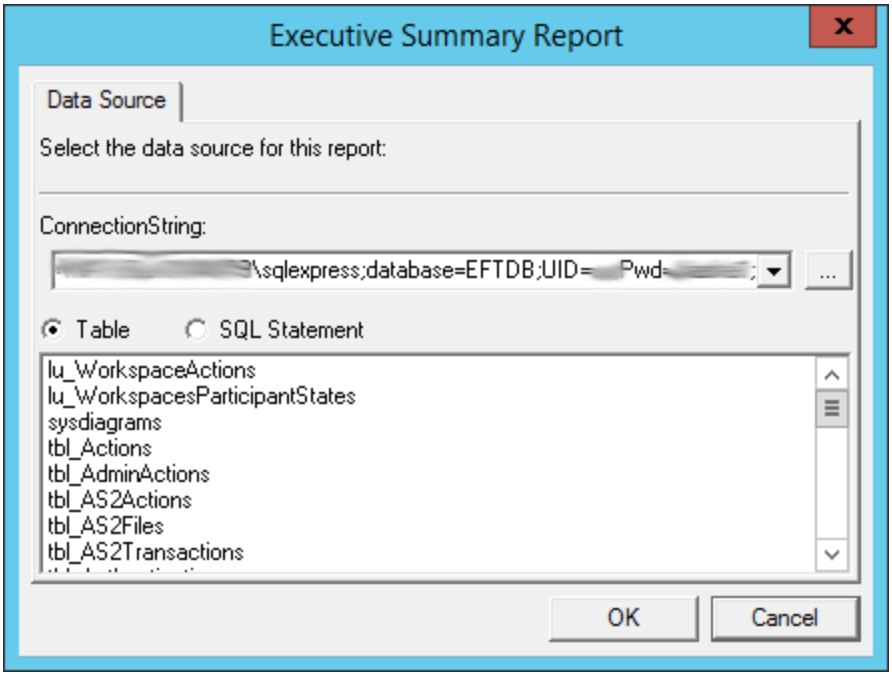
- Click the field, then press DELETE.

Changing the Data Source

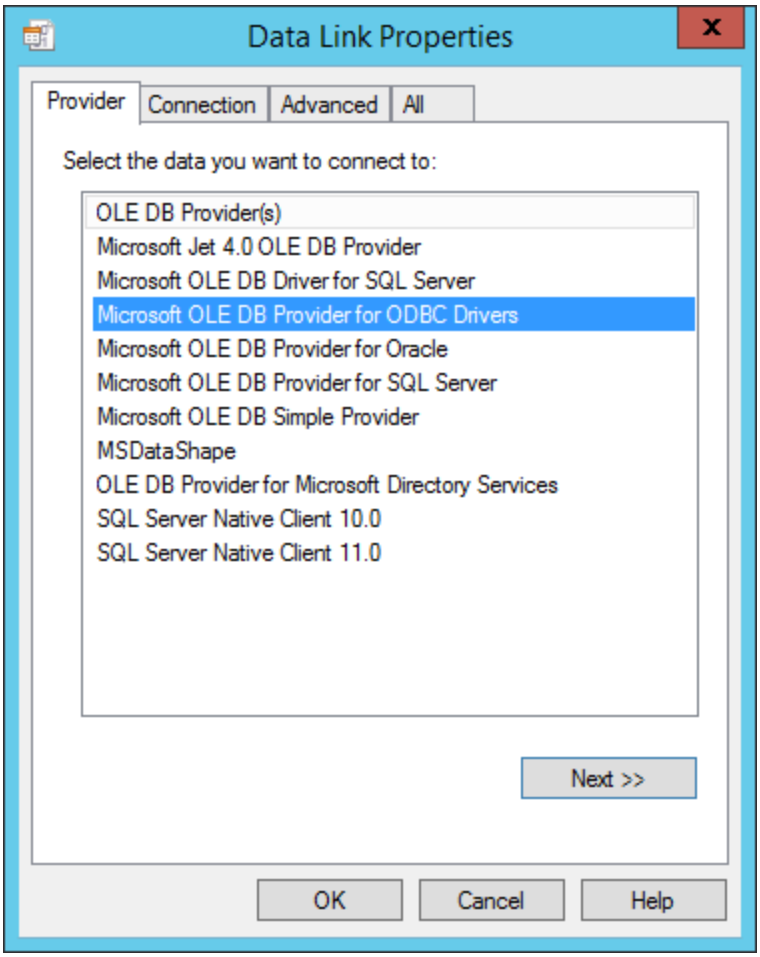
The data source is defined when you installed the ARM database. If you have more than one data source available, you can specify a different source.

To change the data source for a report

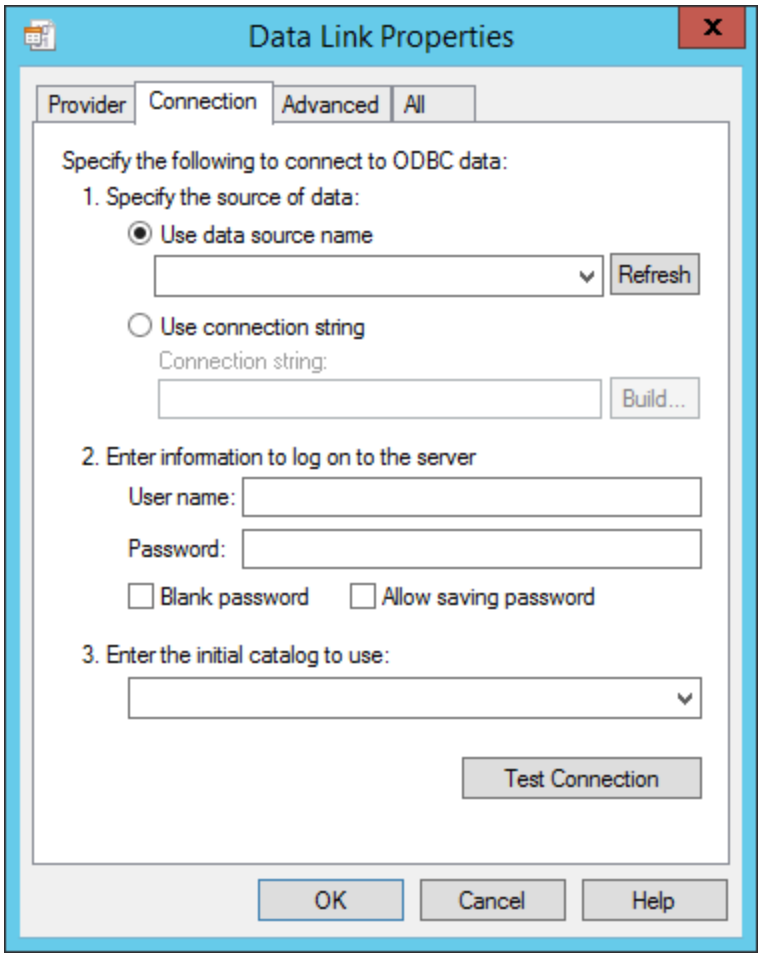
1. View the report in Design mode .
2. Click the **DataSource** icon. The wizard appears.



   - The title bar displays the name of the report.
   - The **ConnectionString** box is populated with the string that was defined when you installed ARM
   - The box below the ConnectionString displays the table or SQL Statement used to populate the report.
3. To specify a different data source, click the browse icon . The **Data Link Properties** dialog box appears.



4. In the **OLE DB Provider(s)** list, click the data source server (for example, **Microsoft OLE DB Provider for ODBC Drivers**), and then click **Next**. The **Connection** tab appears. What appears on the Connection tab depends on the OLE DB Provider selected.



5. In the **Select or enter a server name** box, click the down arrow, and then click the database host\instance name. If the server you want does not appear in the list, click **Refresh**. (If you still do not see the ARM database server, verify EFT's connection to the database on the Server's **Logs** tab.)
6. In the **Enter information to log on to the server** area, do one of the following:
   - Click use **Windows NT Integrated security**. The system will use the logged-in user's account for database connections.
   - Click **Use a specific user name and password**, then specify the username and password.
7. In the **Select the database on the server** box, click the down arrow and select the ARM database name.
8. Click **OK**. The wizard displays the data from the specified source.
9. Click **OK** to close the data source wizard.

Grouping and Sorting Data

After designing the basic layout, you may decide to group the records by certain fields or other criteria to make the report easier to read. Grouping allows you to separate groups of records visually and display introductory and summary data for each group. The group break is based on a grouping expression. This expression is usually based on one or more recordset fields, but it can be as complex as you like.

Groups are also used for sorting the data, even if you do not plan to show the Group Header and Footer sections.

The bar across the top of each section (Page Header, Group Header, Detail) contains some useful tools and information about the section.

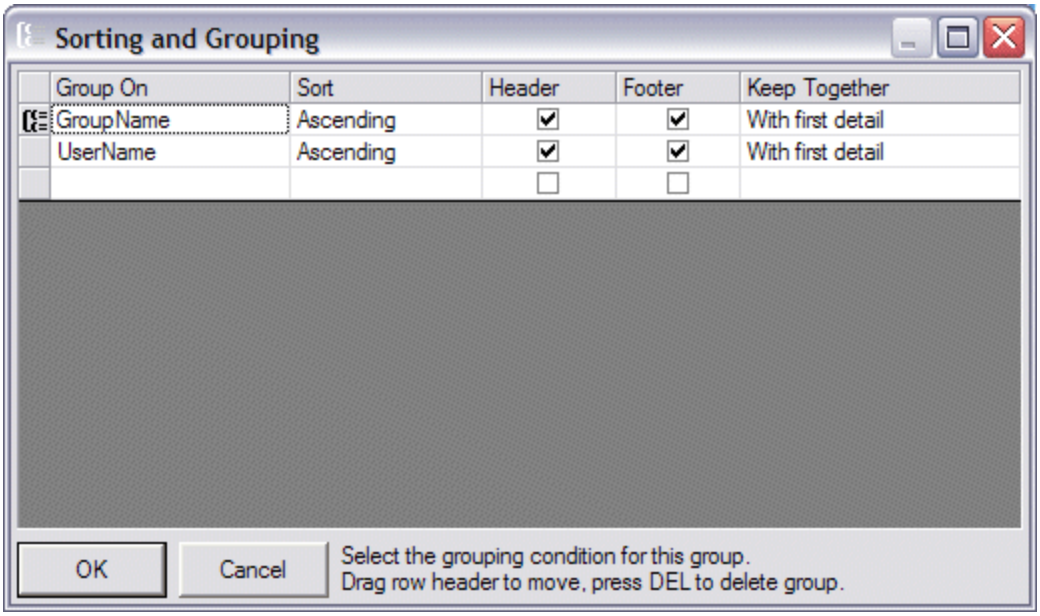
The indented box with a minus sign or a plus sign to the left of the section is used to collapse and expand the section. This feature is useful when you are designing the report to allow you to see a group's header and footer on the same screen without scrolling. Collapsing or expanding a section has no effect on how it is rendered in the report.

- An indented circle indicates that the section currently has zero height. You can drag the divider line down to increase the section's Height property.
- The triangle to the left of **Group Header** indicates the group's sorting order. You can click this icon to open the **Sorting and Grouping** dialog box.
- The labels to the right of the icons are the section name and, for group headers, the value of the group's **GroupBy** property (in this example, **Country**).

To add, edit, reorder, or delete groups in the report

1. Click the **Sorting and Grouping** icon, click **View >Grouping Window**, or click the triangle to the left of the group header. The **Sorting and Grouping** dialog box appears.

2. Use this dialog box to create, edit, reorder, and delete groups.



To create a new grouping condition

1. In the **Group On** column, click an empty row and type a name. For complex grouping, type an expression instead of a simple field name. For example, you could use "Country" to group by country or "Left(Country, 1)" to group by country initial.
2. In the **Sort** column, click the arrow to select the sort order you want to use for grouping the data (**Ascending**, **Descending**, or **None**).
3. In the **Header**, **Footer**, and **Keep Together** columns, specify whether the new group will have visible Header and Footer sections, and whether the group should be rendered together (**No**, **With first detail**, or **Whole Group**) on a page.

   You cannot use memo or binary (object) fields for grouping and sorting. This is a limitation imposed by OLEDB.
4. After you enter some data for the first group, a new blank row is appended to the list, so you can keep creating new groups. If you add more groups, you can change their order by clicking on the left-most gray cell in the row and dragging the row to a new position. This will automatically adjust the position of the Group Header and Footer sections in the report.
5. To delete a field in the group, select it, then press DELETE.
6. Click **OK**. The changes appear in the Designer.

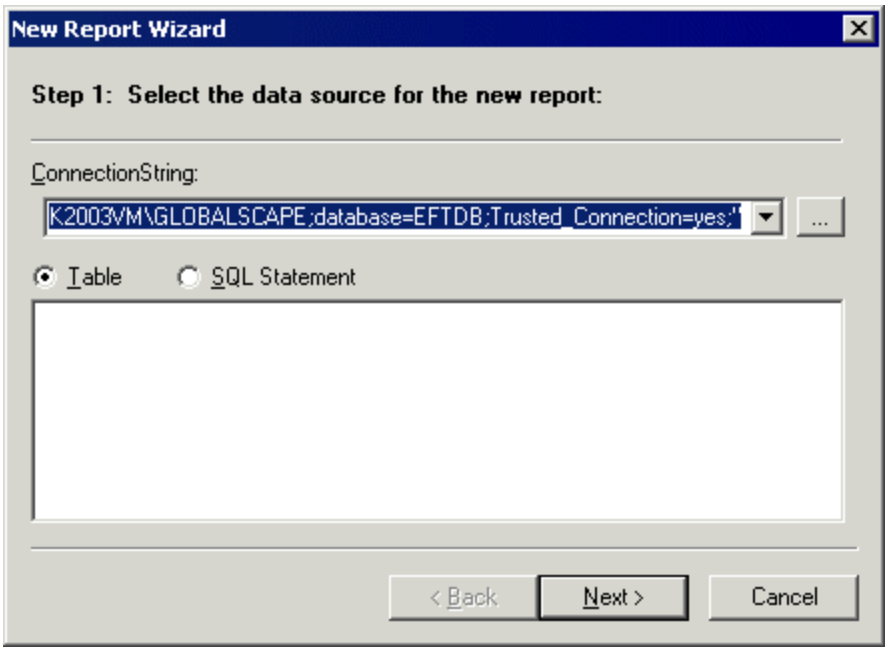
Example: Creating a Custom Report

Below is an example of using the Report Wizard to create a custom administrator Actions report sorted by Site Name. The example assumes you have installed ARM with SQL Server Express and have performed administrator actions in EFT, such as creating users, stopping/starting sites, and so on.

To create the report

1. In the administration interface, connect to EFT, click the Site on which you want to create the report, then do one of the following:
   - On the toolbar, click the click **New Reports** icon .
   - On the main menu, click **Reports >New Report**.
   - Click the **Reports** tab, and then click the **New Report** icon New Report... on the bottom toolbar.

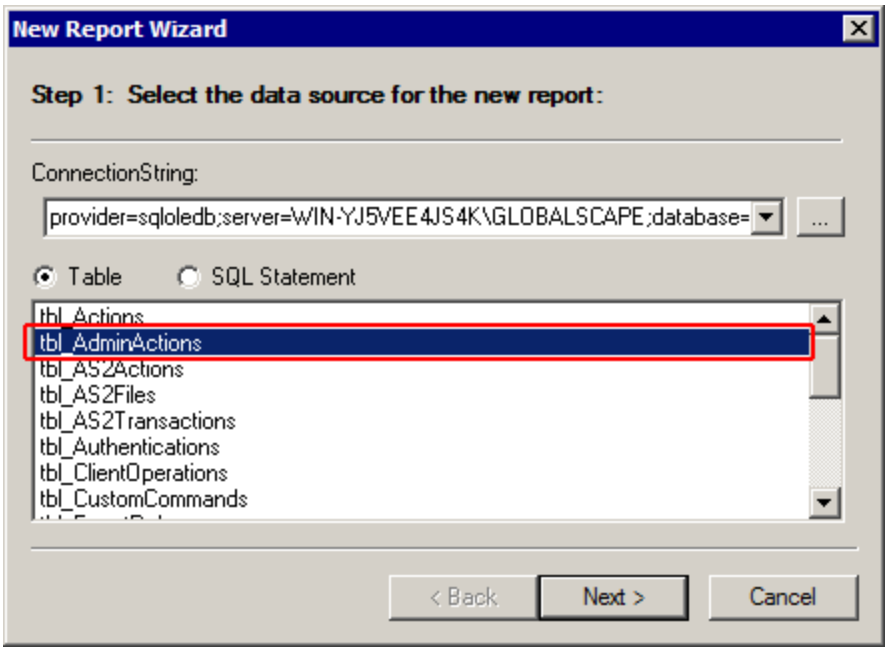
   The **Create New Report** dialog box appears.
2. Type a title for the new report, and then click **Create**. The **Report Designer** appears. So far, all you have done is opened the VSReport Designer, which allows you to open the **New Report Wizard**, which we will do next. You will delete this "template" later.
3. Click **File >New Report** or click the **New Report** icon on the VSReport Designer toolbar. The **New Report Wizard** appears.



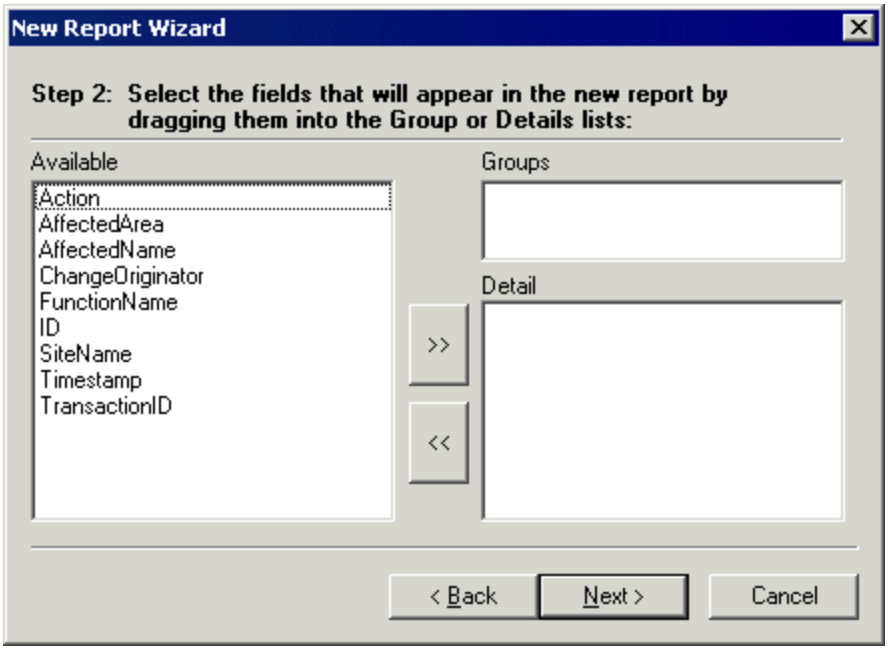
4. By default, the **ConnectionString** box displays information for the database that you specified when you installed the Auditing and Reporting module (for example, **provider=SQLNCLI10;server=localhost\GLOBALSCAPE;database=EFTDB;Trusted_Connection=yes;**). Click **Next** and go to step 5 or, if necessary, you can type a different string that is used to connect to the data source:
    a. Click the ellipsis to define the connection string. The **Data Link Properties** dialog box appears.
    b. On the **Provider** tab, click **Microsoft OLE DB Provider for SQL Server** as the provider to connect to the SQL Server database, and then click **Next**. The **Connection** tab appears.
    c. In **Select or enter a server name**, click the arrow to select or type the name of EFT.
    d. In **Enter information to log on to EFT**, click an authentication option to log on to EFT:
        - **Use Windows NT Integrated security** - Your computer automatically picks up the credentials from your computer and connects you to the database.
        - **Use a specific user name and password** - Specify the user name and the password to be used to log on to EFT. Select the **Allow saving password** check box to save the password in the connection string.

        > NOTE: Select the **Blank password** check box if EFT requires a blank password to log on the database server. Even if you do not type any password when you create a user account on a database server, you can select the **Allow saving password** check box. In this case, EFT takes a dummy password value and saves that value in the connection string. Selecting the **Blank password** check box disables the password field.

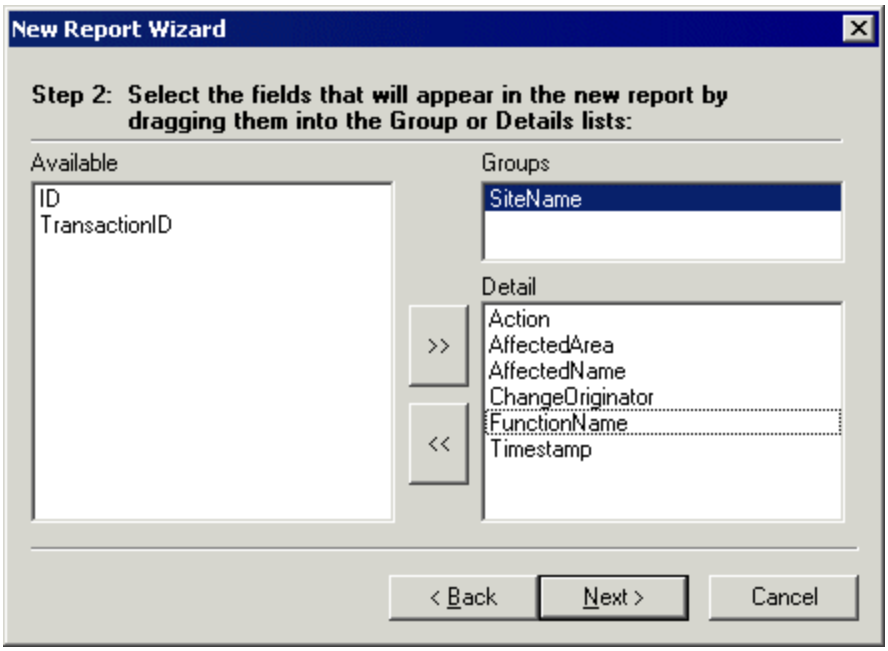
    e. Click one of the following:
        - Select the database on EFT, and then click a database in the list.
        - Attach a database file as a database name - Click the ellipsis icon  to browse for the SQL Server database file (*.mdf). The **Select SQL Server Database File** dialog box appears. Select a file, then click **Open**. The path to the file appears in the **Using the filename** box.
    f. Click **OK** in the **Data Link Properties** dialog box to return to the **New Report Wizard**.
5. Click **Table**, then click **tbl_administratorActions**.



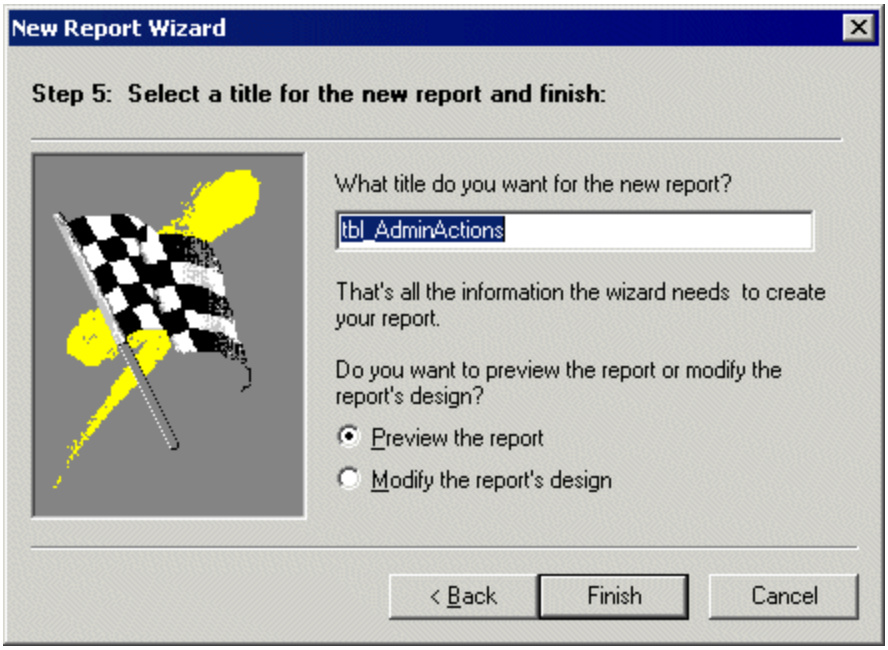
6. Click **Next**. The fields that appear in the **Available** list are from the table you selected in the previous step.



7. Click and drag **SiteName** to the **Groups** field, then click and drag each of the other fields, except **ID** and **TransactionID**, into the **Detail** box. (If you click the right-facing arrows, every field will move to the **Detail** area. Then you can individually move back the fields you do not want.)



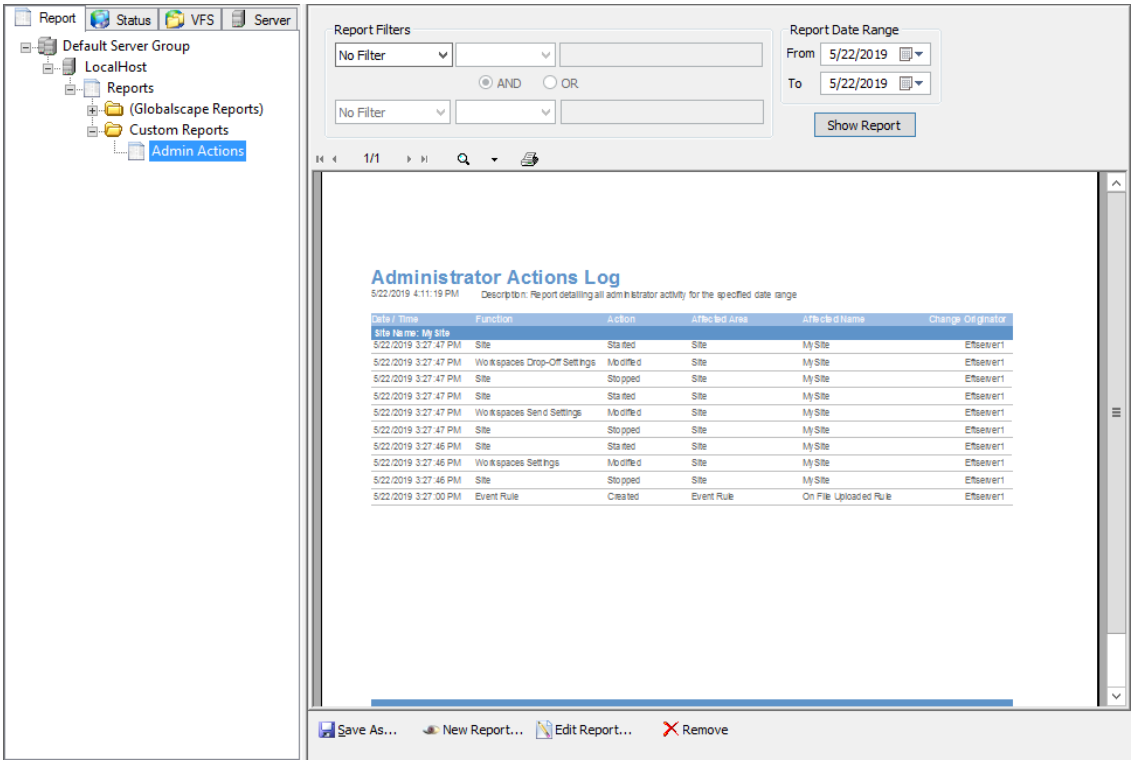
8. Click **Next**. The layout options appear.
9. Keep the default settings and click **Next** on each wizard page until you get to the last step. (For details of using the report wizard to define layout options, refer to Creating a Report with the Report Wizard. For this example, we used the default options.)



10. Type a title for the report, and then click **Finish**.
    - The left pane of the Report Designer displays the report's name (and the report template that was created in step 2).
    - The right pane displays a preview of the report.

- The title bar displays the name of the report and an asterisk, indicating that you have not yet saved the report.

11. Let's get rid of that "new" template that was created when you opened the VSReport Designer. In the left pane, click the name of the template you want to remove, and then click the delete icon on the toolbar. Click **OK** to dismiss the warning message.
12. Click **File > Save** or click the **Save** icon on the toolbar.
13. Click **File > Exit** to close VSReport Designer.
14. On the **Reports** tab, expand the **Custom Reports** node. The new report appears in the tree.
15. In the **Custom Reports** node, click to select the new report.
16. In the right pane, click **Show Report**. The report appears in the preview pane.



You can filter the results, such as show results only for certain Sites, a specific administrator account, or a certain date.

17. Click **Save As** to save the report. The report displays EFT administrator actions sorted by Site Name and Server.

Managing Reports

The topics below provide information regarding managing the reports of EFT activity.

Saving a Report

You can save reports to a file and export them in the following formats: HTML (.htm), VSPrinter (.vp), Portable Document Format (.pdf), Rich-Text Format (RTF), or plain text (.txt). (See Exporting and Publishing Reports in the Report Designer for a description of the various formats.)

To export a report

1. In the administration interface, connect to EFT and the reports database, and click the **Report** tab.
2. With the report displayed in the right pane, click **Save As**.
3. In the **Save as** dialog box, specify the format and location to save the report, then click **Save**.

Exporting Reports in XML Format

You can save (export) EFT reports in XML format, and they can be imported in that format.

To export the report

1. In the administration interface, connect to EFT and click the **Report** tab.
2. In the left pane, click the report.
3. On the main menu, click **Reports >Export Report** or right-click the report and click **Export Report**. The **Save As** dialog box appears.
4. Specify a name (if you want to save it with a different name), location to save the report, and the file type to save it as (XML), and then click **Save**.

Exporting and Publishing Reports in the Report Designer

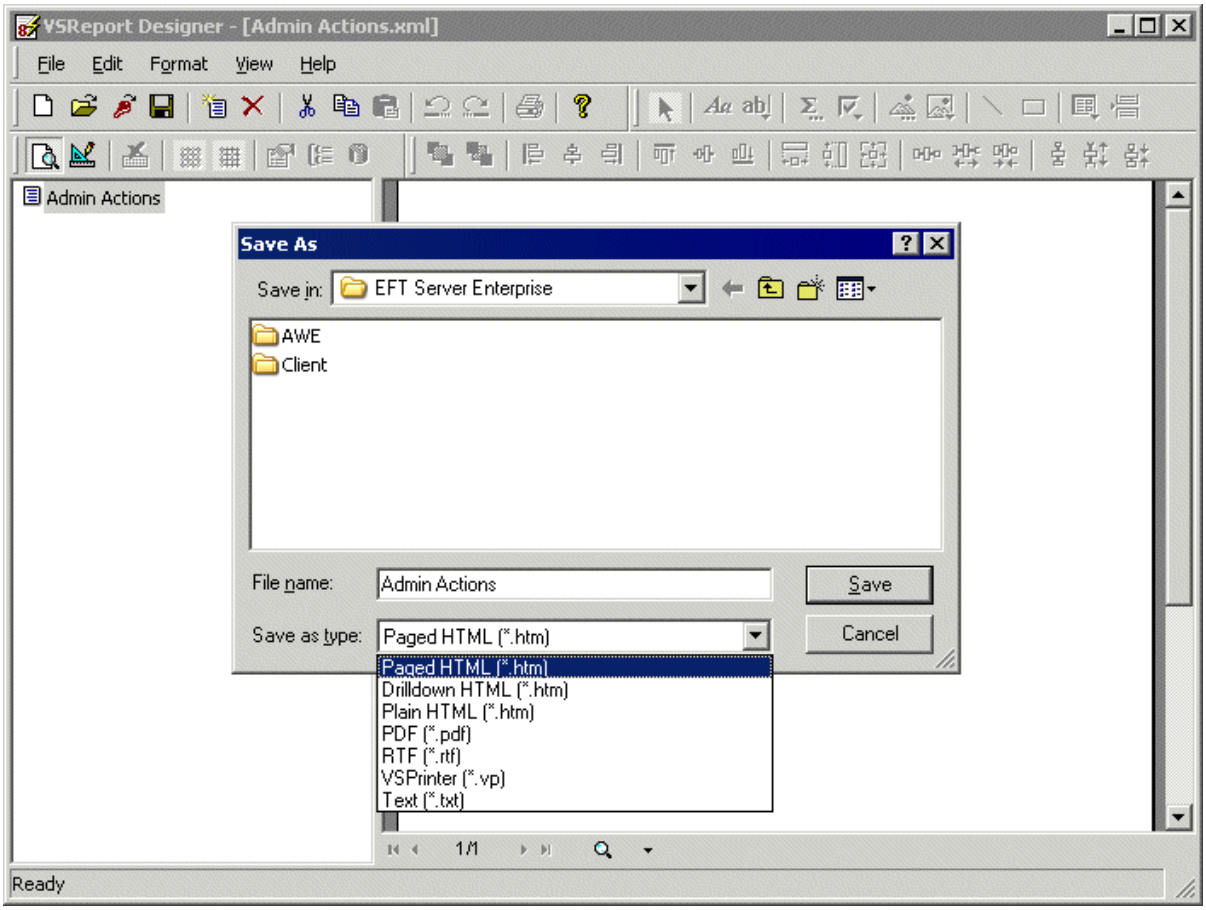
Instead of printing the report, you may want to export it into a file and distribute it electronically to your clients or coworkers. VSReport Designer supports several export formats, listed below:

Format	Description
Paged HTML	Creates one HTML file for each page in the report. The HTML pages contain links that let the user navigate the report.
Drill-Down HTML	Creates a single HTML file with sections that can be collapsed and expanded by the user by clicking on them.
Plain MILT	Creates a single, plain HTML file.

Format	Description
PDF	Creates a PDF file that can be viewed on any computer equipped with Adobe's Acrobat viewer or browser plug-ins.
VSPrinter	Creates a file using the VSPrinter control's native format. The file can be loaded, viewed, and printed from a VSPrinter control within an application or Web page.
Text	Creates a plain text file.

To create an export file

1. In the administration interface, connect to EFT and click the **Report** tab.
2. In the left pane, click the desired report.
3. In the right pane, click **Edit Report**. The report opens in the Report Designer.
4. In the left pane of the Report Designer, click the report that you want to export.
5. Click **File > Export**. The **Save As** dialog box appears.



6. Specify the type of file you want to create, its name (if you want to give it a different name), and its location, then click **Save**.

Importing Reports

You can add reports to EFT by importing the XML reports from the local drive to EFT.

To import reports into EFT

1. In the administration interface, connect to EFT and click the **Report** tab.
2. On the main menu, click **Report >Import** or right-click the **Reports** node and click **Import Report** from the shortcut menu. The **Open** dialog box appears.
3. Click the XML file you want to import, and then click **Open**.
4. The report is added in the left pane under **Reports**.

Deleting a Report

You can delete any reports that you no longer use. You cannot recover the report unless you previously exported and saved it.

To delete reports

1. In the administration interface, connect to EFT and click the **Report** tab.
2. In the left pane, click the report, then do one of the following:
   - On the main menu, click **Reports >Delete Report**.
   - Right-click the report and click **Delete Report**.
   - Click **Remove** .

   A confirmation message appears.
3. Click **Yes** to delete the report. The selected report is deleted and is not recoverable.

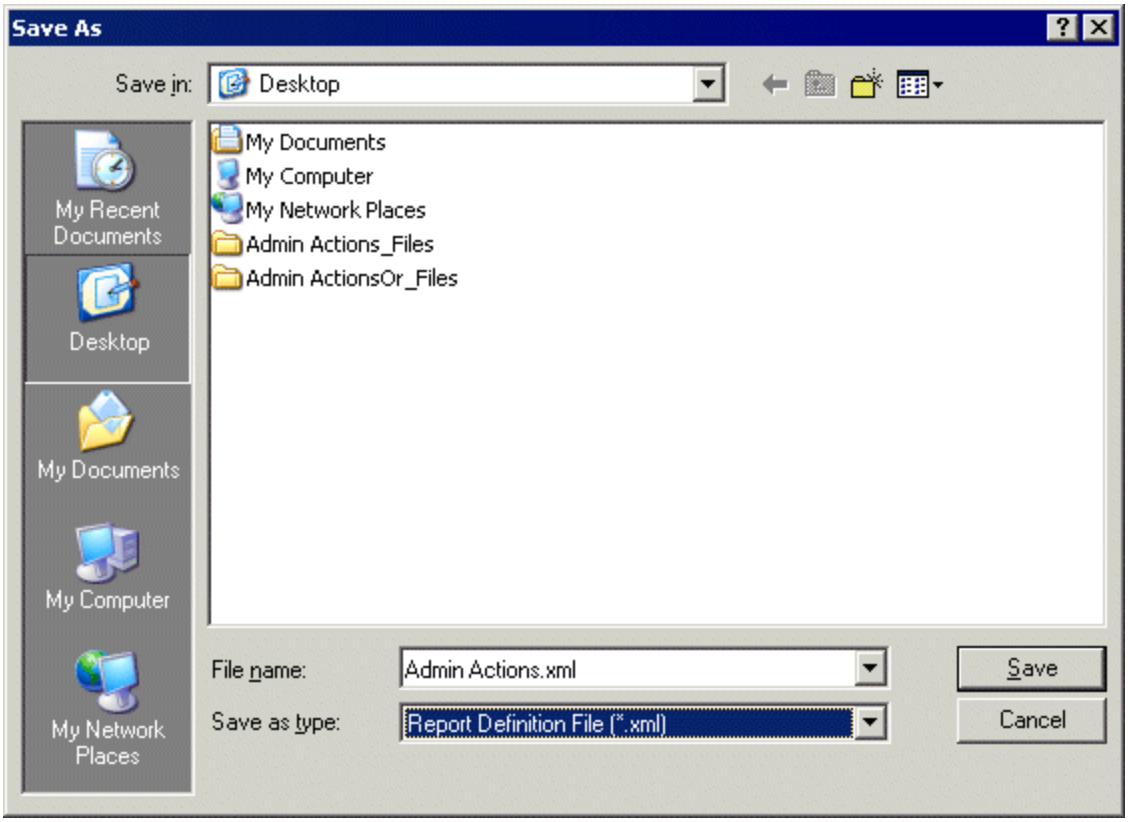
Saving Report Outputs

The report can be saved HTML, PDF, and XML.

To save reports in different formats

1. In the administration interface, connect to EFT and click the **Report** tab.
2. In the left pane, click the report, then do one of the following:
   - On the main menu, click **Reports >Save Report As**.
   - Right-click the report, and then click **Save Report Output As**.

The **Save As** dialog box appears.



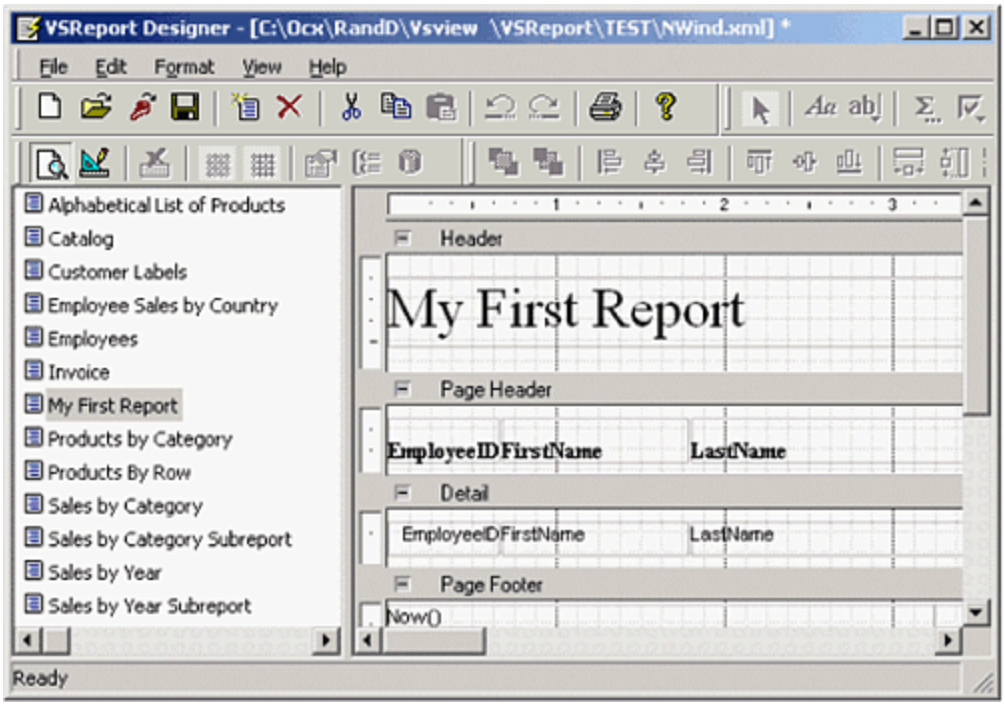
3. Navigate to the folder in which you want to save the report.
4. In the **File name** box, type a name for the report.
5. In the **Save as type** box, click a format, and then click **Save**.

Renaming a Report

You can rename the preconfigured reports and your custom reports, but you can't just type a new name in the tree. You have to open the Report Designer to rename the report.

To rename a report

1. In the administration interface, connect to EFT and click the **Reports** tab.
2. Click the report you want to rename, then click **Edit Report** . The report designer appears.



3. In the left pane of the report designer, click the report name to make it editable, type your changes, then press ENTER or click away from the edit box.
4. On the toolbar, click the **Save** icon, then close the Report Designer.

   The new name does not immediately update in the **Reports** tree of the administration interface. If you click or double-click the report in the tree, the name will update.