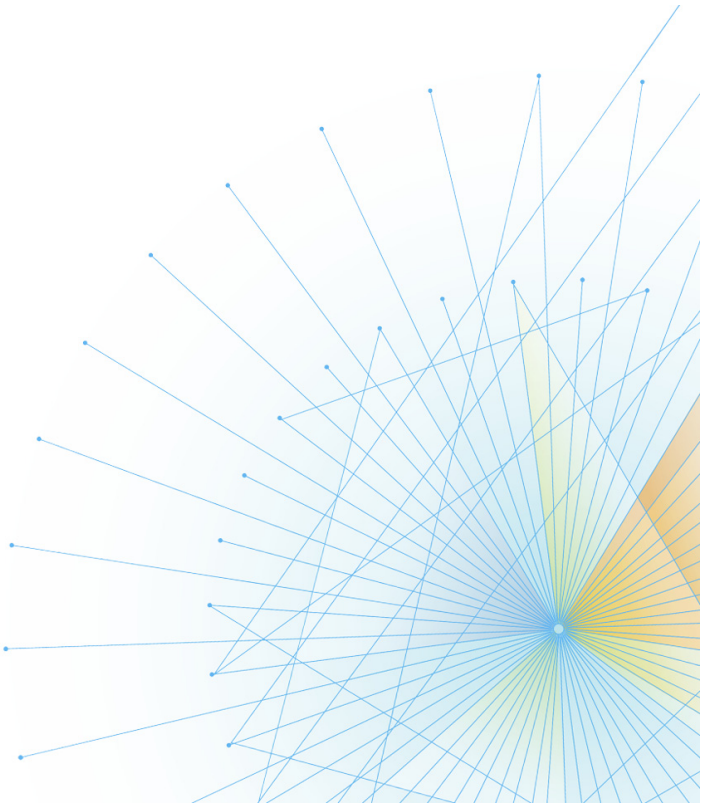
Compuware | The Mainframe Software Partner For The Next 50 Years

Topaz for Enterprise Data Installation and Configuration Guide

Release 19.02



Please direct questions about Topaz for Enterprise Data
or comments on this document to:

Compuware Support Center

https://go.compuware.com/

Doc. OCT2018
October 5, 2018

Contents

Introduction 7
Overview 7
Alerts 7
Additional Resources 7
Related Publications 7
Online Documentation 8

Overview 9
Product Architecture 9

Planning 11
Steps Involved 11
Milestones and Roles 11

Milestone 1: Prerequisites 13
System and Hardware Requirements 13
File-AID/EX Execution Server 13
Hardware Requirements 13
Operating Systems 13
File-AID/EX Enterprise Edition (File-AID/EX Executive) 13
Operating Systems 13
Topaz for Enterprise Data Client 13
Hardware Requirements 13
Operating Systems 13
File-AID Services 14
Hardware Requirements 14
Operating Systems 14
File-AID Rules Engine (FARE) on z/OS UNIX 14
Hardware Requirements 14
Operating Systems 14
Java Runtime Environment 14

Milestone 2: Install File-AID Services (FAS) 15
Task 2.1 Install FAS 15
Task 2.1.1 Install FAS on Windows 15
Task 2.1.2 Install FAS on Linux 16
Task 2.2 Install FAS License 17
Task 2.3 Using the File-AID Services Configuration Utility 17
Task 2.4 Add Database Drivers for FAS 18
Task 2.5 Control FAS 19
Task 2.6 Apply Maintenance to FAS 19

Milestone 3: Install File-AID/EX Execution Server(s) 21

Task 3.1 Install the Execution Server on Windows 21
Task 3.1.1 Install the File-AID/EX Server Edition (if licensed) 21
Task 3.1.2 Install File-AID Rules Engine (FARE) for File-AID/EX Execution Server on Windows 22
Task 3.2 Install on Linux, AIX, Solaris, and HP-UX 22
Task 3.2.1 Install File-AID/EX Components 22
Task 3.2.2 Install a File-AID/EX Server Edition License 23
Task 3.2.3 Install File-AID Rules Engine (FARE) for File-AID Execution Server on UNIX 23
Task 3.3 Configure the File-AID/EX Execution Server 24
Task 3.4 Configure File-AID/EX Execution Server Port Number 24
Task 3.5 Run the File-AID Execution Server in 32 or 64 Bit JVM 25
Task 3.6 Restart and Verify the File-AID/EX Execution Server 26
Task 3.6.1 Start/Stop File-AID/EX Execution Server as Windows Service 27
Task 3.6.2 Start/Stop the File-AID/EX Execution Server on Unix 27
Task 3.7 Configure Third-party JDBC Drivers for Use with File-AID/EX 27
Task 3.7.1 Configure the Driver 28
Examples 29
Uninstall File-AID/EX Execution Server and Rules Engine 30
Maintain the File-AID/EX Execution Server 30

Milestone 4: Install Enterprise Data Companion Components on Mainframe 31
Task 4.1 Install File-AID 31
Task 4.2 Install File-AID/EX Enterprise Edition 31
Task 4.2.1 Install File-AID/EX Enterprise Edition 32
Task 4.2.2 Install File-AID/EX Scheduling Agent 32
Return Code Processing 33
Task 4.3 Install File-AID Rules Engine (FARE) on z/OS Unix 33
Task 4.3.1 Add Database Drivers for File-AID Rules Engine (FARE) 34
Task 4.3.2 Configure Enterprise Data Components on Mainframe 34

Milestone 5: Topaz for Enterprise Data Client Installation 35
Task 5.1 Install Enterprise Data Option on Topaz Workbench 35
Task 5.2 Install File-AID/EX 35
Execution Server Notes 37
Task 5.3 Change the Port Number for the Communication Manager 37
Task 5.4 Set the Location for File-AID Services Server 37
Task 5.5 Enable DB2 JDBC Repository and Database Access Support 38
Task 5.6 Install File-AID Rules Engine (FARE) for Local Execution Server 39
Task 5.7 Configure Enterprise Data Licenses 39
Task 5.8 Configure Enterprise Data Client 39
Task 5.8.1 Perform Basic Setup 39
Task 5.8.2 Create Credentials and Translate Tables 41
Manage Repository Content 41
Manage Projects 42
Silent Installations for File-AID/EX, File-AID Rules Engine, or File-AID Services 43

Milestone 6: Configure Data Privacy Security 47

Role Definitions 47
Task 6.1 Configure Security 49

Troubleshooting 51
Identifying Version of the Installed File-AID Rules Engine 51

File-AID/EX Execution Server Security 53
Securing the Execution Server(s) 53
Execution Server Permissions 53
Launching Execution Servers Under a Domain Account on Windows 53
Launching Execution Servers Under a Domain Account on Linux/Unix 54
Limiting Access to Execution Servers. 54
Limiting Access to Execution Server Configuration Files 55
Limiting Access to Execution of System Commands 55
Secure Communication between File-AID/EX Components 56
Overview of Secure Communication Configuration 56
Regenerating Keys for Secure Communication 57
Using Custom Keys for Secure Communication 57
Assigning Different Sets of Keys to Different Installations of File-AID/EX 58
Sharing Keystore and Truststore Files between Multiple Installations. 58

Checklist of Milestones and Tasks 61

Introduction

This manual provides information about how to install, customize, and maintain Topaz for Enterprise Data.

Overview

This document is intended to guide you through installing/updating, configuring, deploying, and troubleshooting Topaz for Enterprise Data.

Alerts

The alerts found in this guide include:

A note or tip providing additional information.

If a particular milestone or task doesn't apply to your site—or your site is not licensed for a particular option—you can skip ahead to the next milestone or task by clicking the icon.

Information important to remember.

Caution. Failure to follow these instructions can cause problems.

Indicates which skill set is most likely needed to perform the following task(s).

Additional Resources

Refer to these other sources of information on Topaz for Enterprise Data.

Related Publications

- *Compuware Installer Mainframe Products SMP/E Installation Guide*
- *File-AID Advanced Configuration Guide*
- *File-AID Release Notes*
- *File-AID Data Privacy Release Notes*
- *File-AID/EX Release Notes*
- *File-AID Data Privacy online help*

Online Documentation

The Topaz for Enterprise Data product installation package does not include the product documentation. Access the Topaz for Enterprise Data documentation from the Compuware Support Center website at **https://go.compuware.com** in the following electronic formats:

- Product manuals in PDF format
- Product manuals in HTML format

The product documentation is available for viewing or downloading:

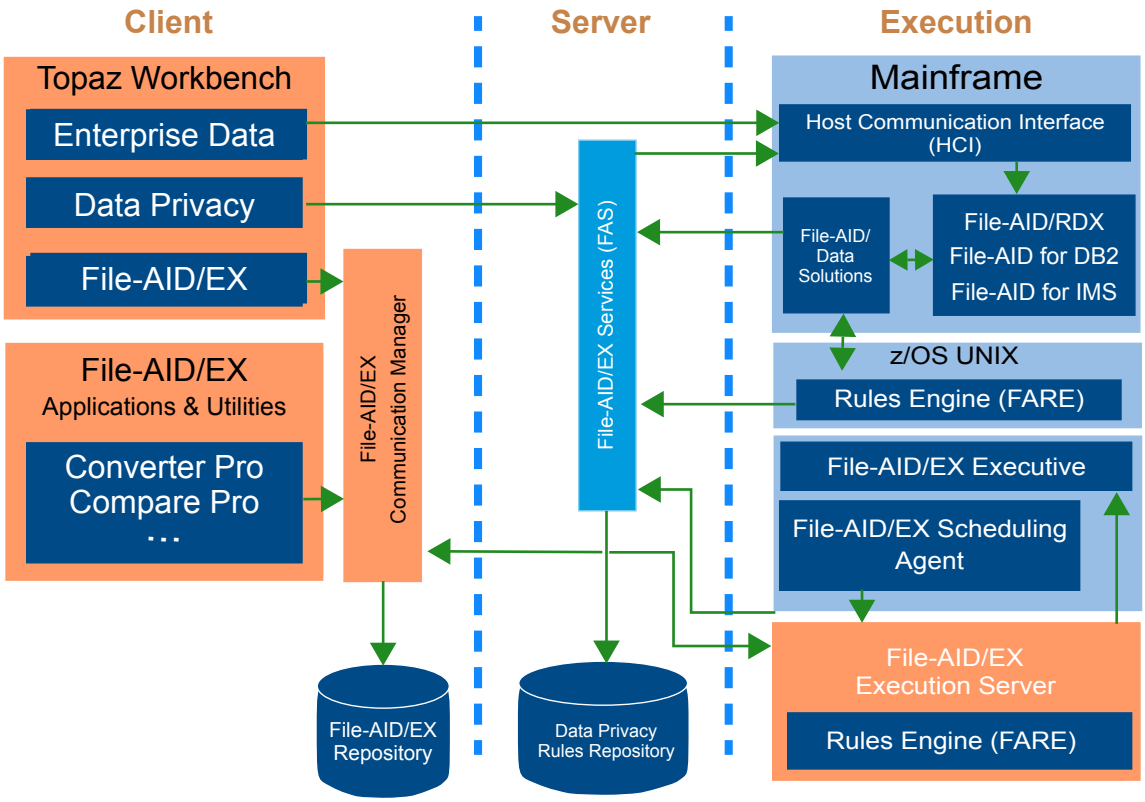
- View PDF files with the free Adobe Reader, available at **http://www.adobe.com**.
- View HTML files with any standard web browser.

Overview

Topaz for Enterprise Data provides a single interface to visualize both mainframe and non-mainframe data in a common, intuitive manner, helping developers and data architects better manage both test and production data and meet the demands of digital business.

Product Architecture

Figure 1. Topaz for Enterprise Data Architecture



Topaz for Enterprise Data is a distributed product, which requires several separate components to be installed, typically on multiple networked computers. These components must then be configured to properly communicate among themselves and with other Compuware products. Figure 1 illustrates the relationships between the various components by breaking them into three logical layers (*Client*, *Server*, and *Execution*), based on their roles in the overall architecture.

Client Layer

The primary users of Topaz for Enterprise Data work directly the applications from the ***Client*** layer. The Client layer contains the Topaz Workbench (with the Topaz for Enterprise Data feature included), and several additional applications and utilities, such as ConverterPro, ComparePro, Homebase, Repository Management Utility, etc.

Server Layer

The ***Server*** layer contains one server application, File-AID Services (FAS). FAS is responsible for management of Data Privacy projects, that include definitions of data elements, privacy rules, etc. Data Privacy Projects and other privacy related artifacts are stored in the Data Privacy Rules Repository. During execution of data processing requests, FAS provides analysis of data layout(s) and detects which fields need to be disguised and which rules should be executed for which fields.

Execution Layer

The ***Execution*** layer contains the components required for execution of data processing requests. Topaz for Enterprise Data supports two types of requests – mainframe and distributed.

The *mainframe* requests typically come from Compuware File-AID mainframe products, such as File-AID/RDX, File-AID for DB2 or File-AID for IMS. To apply Data Privacy rules, the File-AID products launch File-AID Rules Engine (FARE), which runs in IBM Java Runtime Environment. FARE makes calls to FAS for instructions on which rules need to be executed, then applies those rules to certain fields.

The *distributed* requests are handled by **File-AID/EX Execution Servers**, which can be installed on Windows or UNIX/Linux platforms. Every installation of File-AID/EX contains a Local Execution Server, which is launched automatically when the local File-AID/EX needs to communicate with it. Local Execution Servers are typically not recommended for accessing production data, but rather for developing and debugging File-AID/EX specifications. Execution Servers can also be installed as "Remote Execution Servers", in which case they are running as a Windows service or a Unix daemon and can be shared by multiple users. To support data privacy, Execution Servers need to have the File-AID Rules Engine (FARE) installed.

A File-AID/EX Execution Server has the ability to access mainframe data via the (optional) **File-AID/EX Executive** module, which is installed as part of the **File-AID/EX Enterprise Edition**.

File-AID/EX Scheduling Agent can be used for scheduling File-AID/EX (distributed) requests from the mainframe.

The File-AID/EX client applications are installed with a system component **File-AID/EX Communication Manager**, which serves as a proxy in communication with the Execution Servers. It also provides access to the File-AID/EX Repository, which stores definitions of requests and various artifacts that File-AID/EX works with, such as Applications Relationships or Selection Criteria. File-AID Communication Manager is launched automatically, whenever it is required for communicating an execution requests or for browsing repository.

Planning

Steps Involved

1. Order Topaz for Enterprise Data including the latest maintenance, via Compuware's Product Ordering web page or by contacting your Compuware representative.
2. Ensure you satisfy system requirements and prerequisites specified in Milestone 1: Prerequisites.
3. Install File-AID Services on either Windows or Linux by following the appropriate instructions Milestone 2: Install File-AID Services (FAS). You will need to access the FAS installation from either the Topaz for Enterprise Data media or from the download provided with an RFN order.
4. No specific login is required to access the Data Privacy perspective. When the File-AID Data Privacy perspective is selected, the currently active user ID determines the Data Privacy role assignment. All roles are assigned at the server level and all repositories within the same server will have the same role assignments
5. Milestone 3: Install File-AID/EX Execution Server(s) includes the installation of the File-AID/EX Execution Server(s) and the File-AID Rules Engine.
6. Milestone 4: Install Enterprise Data Companion Components on Mainframe includes the installation of File-AID and File-AID Enterprise Edition.
7. Milestone 5: Topaz for Enterprise Data Client Installation includes instructions for installing the client components for Enterprise Data. including Topaz Workbench with the Enterprise Data option, enabling data access support, installing File-AID/EX and various configuration setups.
8. In File-AID Data Privacy, users must be assigned Data Privacy *roles*. Milestone 6: Configure Data Privacy Security discusses how these roles are used and how they are configured.

Milestones and Roles

Installation, configuration, verification, and deployment are accomplished in the milestones listed in Table 1. Each milestone identifies the role or skill set required to perform each milestone.

Table 1. Milestones and Roles

Milestone	Compuware Product Installer
Milestone 1: Prerequisites	various installers
Milestone 2: Install File-AID Services (FAS)	various installers
Milestone 3: Install File-AID/EX Execution Server(s)	various installers
Milestone 4: Install Enterprise Data Companion Components on Mainframe	various installers
Milestone 5: Topaz for Enterprise Data Client Installation	various installers
Milestone 6: Configure Data Privacy Security	Data Privacy administrator

Milestone 1: Prerequisites

System and Hardware Requirements

File-AID/EX Execution Server

Hardware Requirements

- Processor: 3 GHz minimum; multiple cores or CPUs are recommended for better scalability and performance.
- Hard Disk: 700 MB minimum; Additional disk space is required for extracting large sets of data, caching data from translation tables, etc. Fast I/O is critical for performance, so solid-state drives or high-performance RAID-arrays are recommended.
- RAM: 4 GB minimum

Operating Systems

- HP-UX 11iv2 (11.23), 11iv3 (11.31) on Itanium-based machines.
- IBM AIX Enterprise Edition V6.1.0, 7.1.0
- Microsoft Windows 8.1, 10
- Microsoft Windows Server 2012, 2016
- Red Hat Enterprise Linux 6.x, 7.2, 7.3
- Solaris 10 (SPARC processor-based versions only)

File-AID/EX Enterprise Edition (File-AID/EX Executive)

Operating Systems

- IBM z/OS V1.13, 2.1, 2.2, 2.3
- IBM ISPF for the supported z/OS releases

Topaz for Enterprise Data Client

Hardware Requirements

- Distributed Systems:
  - Processor: 3 GHz minimum
  - Hard Disk: 1 GB minimum
  - Memory: 4 GB minimum

Operating Systems

- Microsoft Windows 8.1 Update, 10
- Microsoft Windows Server 2012, 2016

Notes:

- These are the minimum requirements for Topaz Workbench companion products. Visit Compuware Support Center and select the Topaz Workbench product page then select Fixes/Downloads for the latest detailed companion product requirements.
- The File-AID Data Privacy plug-in is not supported in native Eclipse and IBM RDz environments. Topaz Workbench must be installed.
- Compuware requires that all current maintenance be applied to the companion products. In order to use the newest features, any specified PTFs must be applied; otherwise, companion products will operate in toleration mode and new features will be disabled.
- File-AID Data Privacy is an Eclipse-based plug-in distributed with the Topaz Workbench Media or RFN order.

File-AID Services

Hardware Requirements

- Distributed Systems:
  - Processor: 3 GHz minimum
  - Hard Disk: 1 GB (for executables and Derby database)
  - RAM: 4 GB minimum

Operating Systems

- Linux
  - Red Hat Enterprise Linux for Servers 6.x, 7.2, 7.3
- Microsoft Windows (x86, x64 mode)
  - 8.1 Update
  - 10
  - Microsoft Windows Server 2012, 2016

File-AID Rules Engine (FARE) on z/OS UNIX

Hardware Requirements

- Hard Disk: 150 MB (to accommodate the installed files)

Operating Systems

- IBM Mainframe
  - IBM z/OS V2.1, 2.2, 2.3 (z/OS UNIX for File-AID Rules Engine)

Java Runtime Environment

- IBM Java 31-bit SDK V8.0 or higher (only 31-bit Java is supported on z/OS Unix)

Milestone 2: Install File-AID Services (FAS)

Task 2.1 Install FAS

File-AID Services can be installed to either Windows or Linux. You will need to access the FAS installation from either the Topaz for Enterprise Data media or from the download provided with an RFN order. You can download the most current version of the FAS for Windows or Linux installation files from the **Fixes and Downloads** section of the File-AID Data Privacy product pages on the Compuware Support Center web site, FrontLine

When selecting the machine on which to install FAS, you should consider the number of Data Privacy users and then make sure the machine has sufficient capacity in terms of CPU cycles, processor speed, and disk space. In general, Data Privacy has minimal CPU requirements, but does require about 1 GB of disk space to contain FAS software and the default Derby databases. See System and Hardware Requirements for more information.

FAS communicates over the network using the following default open TCP ports: 3081, 4082, 4180, and 5180. Make sure there are no conflicts with these ports on the selected machine. If needed, you can override the default ports, after installation, by using a provided utility as described in Using the File-AID Services Configuration Utility. In addition, when installing FAS, you should be logged in as the *administrator* for the selected server. FAS uses, by default, port 4082 to handle notification messages. This port is dynamic and is controlled by the Topaz Workbench client's notifications callback port preference: **Window > Preferences > Compuware > Notifications**. If needed, you can establish a different master preference port number for this function prior to deployment of the master configurations.

Task 2.1.1 Install FAS on Windows

Access to File-AID Services (FAS) is controlled through Compuware Distributed License Management (DLM) certificates. Before installing the server be sure to order Data Privacy licenses for the latest release of FAS.

1. Select a machine to run FAS and insert or locate the Topaz for Enterprise Data media or the electronic download of FAS installation files from Compuware Support Center. Run `setup.exe` from the media. The media browser appears.
2. When installing from the distribution media, select **Install File-AID Services for Windows**.
3. If installing FAS using the install files downloaded from Compuware Support Center, unzip the self-extracting ZIP file to a directory of your choice. Open the extracted Windows subfolder and run `update.bat`. The InstallAnywhere dialog box appears.
4. Read the introductory text and click **Next**.
5. Read the license agreement and select the **I accept the terms of the License Agreement** button. Click **Next**.
6. Choose a destination folder to install FAS or accept the default value

   ```
   C:\Program Files\Compuware\File-AID Services
   ```

   Click **Next**. Installation setup information is displayed.

7. Select the databases with which you intend to work.

Check all database types that you might access at your site. For each item you select, the installation process automatically installs the appropriate JDBC driver. However, for DB2, you are responsible for providing the location of the folder containing the driver (`db2jcc.jar`) and the corresponding appropriate licenses for accessing DB2 for LUW and/or z/OS.

If you do not choose a database type at install time and later wish to configure a connection to that type of database, you will need to use the Server Configuration utility as described in Add Database Drivers for FAS.

8. If you select **Oracle**, you will be prompted to accept the Oracle license agreement.
9. Confirm the setup information and click **Install**. Once installed, click **Done** to dismiss the InstallAnywhere dialog box. FAS begins running using port 3081 for secure Topaz Workbench client access, port 4180 for Data Privacy execution, and port 5180 for File-AID/Data Solutions interface. If you need to change the default FAS ports for any reason, see Using the File-AID Services Configuration Utility.
10. During installation, the Distributed License Manager (DLM) is installed with a temporary license for FAS. Use the DLM administration tool to activate your permanent FAS license certificate.

    Refer to the *Distributed License Management Installation Guide* for information. To access DLM, click **Start > All Programs > Compuware > Distributed License Management**.

DLM installations default to the C: drive in Windows. Contact Compuware support if you need to install DLM to a different drive letter.

11. Validate that the services are running by using a web browser to view the URL: `http://hostname:4180/versions` where *hostname* is either `localhost` or the machine name; or the IP address where the services are installed. The resulting web page should display with a list of executing bundles.

Task 2.1.2 Install FAS on Linux

Follow these steps to install FAS to a Linux server. It is highly recommended that installation of FAS in Linux be done under the authority of *superuser*.

If the user responsible for the server is not *superuser*, then once installed, File-AID Services should be shutdown, folder ownership and all permissions should be transferred to the user ID/group responsible for the server, and the service should be restarted.

1. Copy the Disk1 folder of either the Linux subfolder from the downloaded extracted Linux File-AID Services install files from the Compuware Support Center or the File-AID media directory `cpwr\FAS\Linux`, to the Linux server or a directory that is mounted on the Linux server.
2. At the command prompt type `which java` to get the location of Java on the Linux server.
3. Set the JAVA_HOME environment variable (`export JAVA_HOME=<location of Java>`).
4. Add the `JAVA_HOME/bin` directory to the PATH environment variable (`export PATH=$JAVA_HOME/bin:$PATH`).
5. Navigate to the directory `Disk1/InstData/NoVM` under the directory where the contents were copied to in step 1.
6. Change the file `install.bin` to be executable (`chmod 777 install.bin`).
7. Before starting the installation, if you intend to do data privacy on IBM DB2, locate the path for the file `db2jcc.jar`.

8. Run the installation (`./install.bin`).
9. Once the install starts follow the prompts:
    a. Read the License Agreement and respond. Accept the agreement to continue with the installation. (If you do not accept the license the install will stop.)
    b. Enter a path in which to install or press *Enter* to accept the default directory as shown (in either case, you must have write access to the chosen path).
    c. Confirm that the path entered is correct.
    d. Select the databases that you intend to disguise using data privacy. (Use the numbers to the left of the database. Multiple databases can be selected by separating them with commas.)
    e. If IBM DB2 was selected, enter the path to the folder containing the `db2jcc.jar` DB2 driver and the appropriate corresponding license files for DB2 UDB on LUW and/or z/OS.
    f. If Oracle was selected, read and accept the license.
    g. Review the install directory and press *Enter* to start the actual installation of the product.
10. When done, validate that the service is running by using a web browser and going to this URL: `http://[hostname]:4180/versions` where *hostname* is the IP address or DNS name of the Linux machine where the server was installed. The resulting web page should display a list of executing bundles.

An alternative way to validate the service is running would be to launch `C:\Users\USERID\Compuware\Topaz` and use the **Test Connection** button in the Server Preference dialog box.

Task 2.2 Install FAS License

To install the license for File-AID Services, license information from Compuware and a license file configured in DLM are needed. Types of licenses include:

- **Temporary:** The default license shipped with the product.
- **Permanent:** A license that gives the user access to the product under the terms of the contract with Compuware.
- **Trial:** A license that enables the user to evaluate the product for 30 days.

Refer to the *Distributed License Management Installation Guide* for instructions on installing a temporary or permanent license. The Distributed License Management online help also provides license installation information.

Note: The DLM configuration tool has to show the licensed feature "dp_server" with the matching version number.

Task 2.3 Using the File-AID Services Configuration Utility

The *File-AID Services Configuration Utility* is provided with FAS to enable you to override the default port assignments. There are three default bi-directional port numbers activated when FAS is installed:

1. Server port: 3081
2. Data Privacy execution port: 4180
3. File-AID/Data Solutions interface port: 5180

User can change the port numbers that were assigned by default. The FAS must be restarted for the port changes to take effect. Also, note that you may need to change the port assignments configured with File-AID/EX and File-AID/Data Solutions (see Task 5.2 Install File-AID/EX and Task 4.3.2

Configure Enterprise Data Components on Mainframe). FAS also uses default port 4082 to handle notification messages. This port is dynamic and is controlled by a Notifications callback port preference: **Window > Preferences > Compuware > Notifications.**

For Windows

1. Use the **Start > Programs > Compuware > Server > Server Configuration** shortcut to invoke the utility. The File-AID Server Configuration Utility dialog box appears.
2. Select the **Communications** tab.
3. Overtype any port numbers you wish to modify.
4. Click **OK**.
5. Stop and restart File-AID Services.

- If changing File-AID Services port (default: 3081), notify users by recording File-AID Services preference information.
- If changing the Data Privacy execution port (default 4180) update the File-AID/EX configuration (Task 5.2 Install File-AID/EX) and Task 4.3.2 Configure Enterprise Data Components on Mainframe).
- If changing the File-AID/Data Solutions port (default 5180) update the File-AID/Data Solutions Data Privacy configuration (see Task 4.3.2 Configure Enterprise Data Components on Mainframe).

For Linux

1. In the directory containing the installed FAS, issue the shell command: `./runServerConfig.sh`
2. Review and change any port numbers you wish to modify.
3. Stop and restart File-AID Services service. See Control FAS on page 19.
4. Be sure to modify the Topaz Workbench configuration, File-AID/EX configuration, and/or File-AID/Data Privacy configurations to match your new port assignments.

Task 2.4 Add Database Drivers for FAS

The *File-AID Services Configuration Utility* is provided with FAS for installing additional database drivers in the event you did not select a database type during the initial installation but now find the need to configure a database.

The following five databases are supported and can have their drivers added via this utility:

- Derby (installed by default and required for Data Privacy security database)
- IBM DB2
- Oracle
- Microsoft SQL Server
- SAP/Sybase

The **Data Privacy** tab on the *File-AID Services Configuration Utility* enables the user to turn on additional databases that were not enabled during the initial installation. In order to apply any changes, FAS service must be restarted. Also, note that if you are adding the IBM DB2 driver you will be requested to supply the location of the folder containing the DB2 JDBC driver file `db2jcc.jar` and the appropriate corresponding license files for DB2 UDB on LUW or z/OS.

For Windows

1. Use the **Start > Programs > Compuware File-AID Services > Configuration** shortcut to invoke the utility.
2. Select the **Data Privacy** tab.
3. Check any database types you need. (For IBM DB2 provide the location of the folder containing the `db2jcc.jar` JDCB driver file and the appropriate corresponding license files for DB2 UDB on LUW or z/OS. For Oracle, accept the license agreement.)
4. Click **OK**.
5. Restart File-AID Services service.

For Linux

1. In the directory containing the installed FAS, issue the shell command `./runServerConfig.sh`
2. Check any database types you need. (For IBM DB2 provide the location of the folder containing the `db2jcc.jar` JDCB driver file and the appropriate corresponding license files for DB2 UDB on LUW or z/OS. For Oracle, accept the license agreement.)
3. Stop and restart File-AID Services service. Refer to Control FAS on page 19.

Task 2.5 Control FAS

For Windows

File-AID Services in Windows can be controlled from the Services Management page, which can be opened by typing `services.msc` in **Windows > Run**. Uninstalling has to be done from the **Add/Remove Programs** management Windows utility.

For Linux

1. Navigate to the subdirectory ~/`MMCServer/eclipse/bin` in the directory where you installed FAS.
   a. To **stop** FAS issue the following command. `./platform.sh stop`
   b. To **restart** FAS issue the following command. `./platform.sh start`
   c. To **uninstall** FAS issue the command. `./platform.sh uninstall`
   d. To **maintain** FAS, see Task 2.6 Apply Maintenance to FAS.

Task 2.6 Apply Maintenance to FAS

Maintenance to File-AID Services is applied by reinstalling the entire File-AID Services with a newer version.

The installer automatically detects that you have an existing installation and preserves your data, repositories, and configurations while applying updates. Updates to File-AID Services will be published to Compuware Support Center in the Fixes/Downloads page of Topaz Workbench product page. Follow the instructions provided to download the maintenance.

Maintaining FAS

Access to File-AID Services is controlled through Compuware Distributed License Management certificates. Before updating the server, be sure to order and install new Data Privacy licenses for the latest release of File-AID Services.

Procedure:

1. After unzipping the downloaded maintenance, execute the `update.bat` file to reinstall/update File-AID Services. The installer application will locate your currently installed version of File-AID Services and backup all data and configurations. You will be warned to make sure that there are no active users before proceeding. Then File-AID Services service will be stopped, uninstalled, and then reinstalled in the same directory. All data and repositories will be preserved. Your rules repository may need to be migrated following an update.

Be sure to use the same login user ID (Administrator) you originally specified.

For Linux installations of FAS, upload the new binary and reinstall to the same location using the same install.bin script you tailored during the initial installation. You will be asked to preserve data — selecting Yes is recommended. It is highly recommended that installation of FAS in Linux be done under the authority of superuser.

2. After installation is complete, FAS service is automatically started.
3. After updating, use Topaz Workbench to access the Data Privacy perspective. If the Data Privacy Explorer repository, File-AID Rules, has a red x icon or cannot otherwise be opened, it may need to be migrated to make it current. To migrate the repository, select Manage Repositories from the **Data Privacy** menu to select the repository and click **Migrate**. Some processing will occur to migrate the repository and then you should be able to open it.

Milestone 3: Install *File-AID/EX Execution Server(s)*

Task 3.1 Install the Execution Server on Windows

The server edition allows units of File-AID/EX work to be routed to remote servers for execution close to the actual data source. Installation of this module requires that a *File-AID/EX execution engine* and a *File-AID Rules Engine* (FARE) be installed on each server where File-AID/EX disguise work is to be routed.

Task 3.1.1 Install the File-AID/EX Server Edition (if licensed)

For Windows Servers, use the **File-AID/EX Client** tab of the media containing File-AID/EX. During the installation, optionally, deselect the File-AID/EX and Repository components but ensure **Execution Server** is selected.

By deselecting the File-AID/EX client, the File-AID/EX Windows Execution Server installs as a Windows service, which automatically starts and runs when the server is booted.

Once your Remote Execution Server is installed and started, launch File-AID/EX Homebase and add this Execution Server to the list of valid Execution Servers.

1. **Configure File-AID/EX for Dynamic Privacy Rules.**
   In order to enable File-AID/EX to specify and execute the Dynamic Privacy Rules (as defined in disguise projects created by File-AID Data Privacy), we need to configure FAS server details.
   a. Start Homebase and select **Tools > Dynamic Data Privacy** option to access the Server Configuration dialog box. In the Server Configuration dialog box, fill in the DNS name or IP address of FAS and the port number (the default port number is 4180). The Server Configuration dialog box can be used to configure all Execution Servers registered to the repository.
   b. Alternatively, the user can also specify FAS location and port by manually editing the `DataPrivacy.properties` file located in `~\ProgramData\Compuware\FAEX\cfg` directory.

The modification to the `DataPrivacy.properties` files must be made to all installations of the File-AID/EX Execution Servers with FARE installed.

2. **Perform this step only if planning on disguising distributed DBMS databases where the Data Privacy project references z/OS files containing shared Translate Tables. If you are not sure about whether you need to install the File-AID/EX Enterprise Edition, defer this step until the use of the Data Privacy plug-in requires it.**
   The File-AID/EX Enterprise edition allows connectivity to mainframe data. Ensure File-AID/EX Enterprise Edition is installed and configured in z/OS.

The current release of File-AID includes the File-AID/EX Enterprise Edition's MVS Access modules. Installation and configuration of File-AID/EX Enterprise Edition's MVS Access modules is described in the *File-AID Installation and Configuration Guide* provided on the Compuware Support Center or on the File-AID EP.

Task 3.1.2 Install *File-AID Rules Engine (FARE)* for *File-AID/EX Execution Server* on Windows

1. From the Topaz for Enterprise Data media or RFN download, select the **File-AID Rules Engine** tab, then select **Install File-AID Rules Engine for Windows**.
2. Click **Next** on Introduction page, then choose the default File-AID/EX installation folder or a separate folder and click **Next**. Please note that the:
   - installation of the FARE for use with File-AID/EX requires the FARE to be installed in the File-AID/EX installation directory.
   - installation into a separate folder is for external API development only and will not be used by File-AID/EX.
3. Click **Install** on the Pre-Installation Summary and click **Done** on the Install Complete screen.

Task 3.2 Install on Linux, AIX, Solaris, and HP-UX

This task describes the File-AID/EX installation setup types and provides installation procedures for File-AID/EX on UNIX.

Task 3.2.1 Install File-AID/EX Components

This subtask describes the steps required to install the File-AID/EX components on Linux, AIX, Solaris, and HP-UX, including the Execution Server and the File-AID Rules Engine (FARE).

Before installing File-AID/EX on UNIX or Linux, Java must be installed. Refer to the System and Hardware Requirements for additional requirements.

To install File-AID/EX (including the Execution Server and Rules Engine)

1. Log on to the UNIX or Linux workstation as a user ID that has the authority to read from the device where the File-AID/EX installation image is mounted and that has the authority to create the directory where File-AID/EX is to be installed.
2. Create an installation *media mount point* directory, if one does not already exist.
3. Insert the installation media containing the File-AID/EX software in the appropriate drive and mount the media device.

   The mount commands vary from platform to platform. The following are examples, where <*media_dev_name*> is the device name and <*media_mount_point*> is the mount point of the device:

   - AIX

     ```
     mount -vr cdrfs <media_dev_name>/<media_mount_point>
     ```

   - HP-UX

     ```
     mount cdfs <media_dev_name>/<media_mount_point>
     ```

   - Solaris (if using Volume Manager, media mounts automatically mount)

     ```
     mount -F hsfs <media_dev_name>/<media_mount_point>
     ```

   - Red Hat Linux

     ```
     mount <media_dev_name>
     ```

     where <*media_dev_name*> matches the device or mount point of the device in the `/etc/fstab` file. Typically, the <*media_dev_name*> is `/dev/cdrom`
4. Navigate to the installation directory for the selected platform.

   Example: `<mount_point>/FileAID_EX_Installer/FG/cpwr/FAEX_Unix/platform/install/`

- For AIX: Install from the FAEX_AIX directory
- For HP-UX: Install from the FAEX_HP-UX directory
- For Solaris: Install from the FAEX_Solaris directory
- For Red Hat Linux: Install from FAEX_Linux directory

5. Make sure the copied files are executable by issuing the command (where <directory> is the directory in the step above:
   `chmod -R 777 <directory>`.
6. Execute `./faexinst.ins`. The **Welcome to the installation for File-AID/EX Server** dialog box appears.
7. Press **Enter**. The default pathname message appears.
8. Type **y** to accept the default or type **n** to specify a different path. Press **Enter**. The copyright message appears, and a prompt to accept the terms appears.
9. Type **y** and press **Enter**. The Java command prompt appears.
10. Do one of the following:
    - Press **Enter** to accept the default Java location.
    - Type the fully qualified path of the Java command and press **Enter**.
11. Type y to install the selected components in the default directory, and press **Enter**. The default installation directory path appears.
12. Do one of the following:
    - Type **y** and press **Enter** to accept the default path.
    - Type the full installation path and directory and press **Enter**.

    Space is validated and then the current settings message appears.
13. Type **y** to continue with the installation and press **Enter**.
14. When the installation completes, a prompt appears asking to view the readme file. Type **y** or **n** and press **Enter**.

The File-AID/EX UNIX components are now installed.

Note: When planning to work with DB2 Databases, make sure that the DB2 JDBC drivers are installed with the Execution Server in the DME directory. See Enable DB2 JDBC Repository and Database Access Support on page 38.

Task 3.2.2 Install a File-AID/EX Server Edition License

To install the license for File-AID/EX Server Edition, license information from Compuware and a license file configured in DLM are needed. There are two types of licenses:

- **Temporary:** The default license shipped with the product.
- **Permanent:** A license that gives the user access to the product under the terms of the contract with Compuware.

Refer to the *Distributed License Management Installation Guide* for instructions on installing a permanent Client license. DLM is automatically installed when File-AID/EX is installed in Unix. The default location is `/usr/faex/dlm`. A temporary license is automatically created. To install a permanent license, use the DLMCV (command line version) utility (`./dlmcv.sh`).

Task 3.2.3 Install *File-AID Rules Engine (FARE)* for *File-AID Execution Server* on UNIX

Perform this step only if you plan to use the File-AID Data Privacy module in a Remote execution server installed on AIX, Linux, Solaris, or HP-UX.

1. Run `setup.exe` on File-AID Services media image downloaded from an electronic distribution order.

The current version of the specific Unix FAREs is also available as a download from the Fixes and Downloads section of the Topaz Workbench product page on the Compuware Support Center. You must synchronize the version of the FARE with the version of the Topaz Workbench client, File-AID Data Privacy plug-in, and File-AID Services (FAS).

2. Select the **File-AID Rules Engine** tab in the media browser and click the link corresponding to your UNIX platform, which opens the folder containing the installation files.
3. Use an FTP tool (for example: WinSCP or PuTTY) to transfer the FARE installer files to the directory of your choice on the UNIX machine.
4. In the UNIX machine, locate the directory path to a current Java Virtual Machine (JVM). The File-AID Rules Engine requires a minimum of Java JRE 1.8 or more current. (For example: `~/usr/compilers/java/java8`). For validation purposes, execute the shell command: *[*`JVM Install directory]/bin/java -version`. For example: `/usr/lpp/java/java8/bin/java -version`).
5. Execute the installer by issuing the shell command: `sh installfare.bin`
6. When prompted, provide the directory path to the current Java Virtual Machine (JVM) you located as part of Step 4.
7. Accept the default installation destination path (`/opt/Compuware/fare`) or specify a path to which you have write access, which should have at least 150MB of free space.

The target directory must not be the same directory where you uploaded `installfare.bin`.

8. If a notification appears indicating that jar files have been found, enter **1** for OK and press **Enter** to continue the install.
9. Press **Enter** again to exit the installer.

Task 3.3 Configure the File-AID/EX Execution Server

Once the Execution Server is installed and started, launch File-AID/EX Homebase and add this execution server to the list of valid execution servers in the default repository or any other repositories that have been configured. Refer to the Default Execution Server topic in the Homebase help.

For production environments, Compuware recommends that users set up a shared repository in an industry-standard RDMS rather than using the local repository created when File-AID/EX is installed. The local repository is not managed or backed up, and is meant only to provide a starting point for small testing scenarios, not production environments.

If the File-AID Rules Engine has been installed, configure the Execution Server for it. Refer to Set the Location for File-AID Services Server on page 37.

Optionally, users can edit the `dataprivacy.properties` file (located by default at `\ProgramData\Compuware\FAEX\Cfg`).

Task 3.4 Configure File-AID/EX Execution Server Port Number

The Execution Server port number can be changed from the default that File-AID/EX originally sets, if desired.

To change to a new port:

1. From the Homebase **Tools** menu, select **Execution Server**. The **File-AID/EX Execution Server** dialog box appears.
2. Click **Stop** and then click **Close** to shut down the currently running engine.

Failure to first stop the execution server will result in having an engine running on both the old port and the new port, and it is then difficult to determine which engine to shut down since there is no port designation to indicate which engine goes with which port.

3. Open the `engine.properties` file, which is located by default at `\ProgramData\Compuware\FAEX\Cfg`
4. Change:

   `port=4900`

   to the desired port number.
5. Save and close the file.
6. From the Homebase **Tools** menu, select **Execution Server**. The **File-AID/EX Execution Server** dialog box appears.
7. Click **Start** and then click **Close**. The new engine is restarted.

Additional information can be found in the `engine.properties` file.

Task 3.5 Run the File-AID Execution Server in 32 or 64 Bit JVM

After installing File-AID/EX, a change must be made to `go.sh` in the `dme` folder to turn on 64-bit mode.

1. In the `go.sh` file, find a line similar to the following:
   `JAVA_PGM="/usr/java/1.x.x/15/bin/java"`
   (where *x.x* refers to the appropriate Java version)
2. Change the Java JRE path to point to a JRE that has 64-bit support.

JREs can be downloaded at http://www.oracle.com/technetwork/java/index.html. Contact your system administrator for assistance in locating and installing an appropriate JRE.

For HP-UX

1. On 64-bit HP-UX, in the `go.sh` file, find the line similar to the following example:

   `JAVA_PGM="/usr/java/1.x.x/08/bin/java"` (where *x.x* is the version)
2. Append the ' -d64' command line parameter to start Java in 64-bit mode. For example:

   `JAVA_PGM="/usr/java/1.x.x/08/bin/java -d64"`
3. To verify that Java is running in 64-bit mode, run it with the '-version' parameter to annotate version information. For example:

   ```
   ->/usr/java/1.x.x/08/bin/java -d64 -version
   java version "1.x.x.08"
   Java(TM) 2 Runtime Environment, Standard Edition (build 1.x.x.08-_04_may_2007_06_31)
   Java HotSpot(TM) 64-Bit Server VM (build 1.x.x.08 jinteg:05.04.07-09:34 PA2.0W
   (aCC_AP), mixed mode)
   ```

   (where *x.x* refers to the appropriate Java version)

"64-Bit Server" indicates that it is running in 64-bit mode.

If the HP-UX Java installation does not support the '-d64' parameter, point to a separate 64-bit Java JRE. Contact your system administrator for assistance in locating such a version of Java.

For AIX

On 64-bit AIX, it is necessary to point to a separate 64-bit Java JRE.

1. To verify that Java is running in 64-bit mode, run it with the '-version' parameter. For example:

```
->/usr/java/1.x.x_64/10/bin/java -version
java version "1.x.x"
Java(TM) 2 Runtime Environment, Standard Edition (build pap64dev-20090707 (SR10))
IBM J9 VM (build 2.3, J2RE 1.x.x IBM J9 2.3 AIX ppc64-64 j9vmap6423-20090707 (JIT
enabled)
J9VM - 20090706_38445_BHdSMr
JIT  - 20090623_1334_r8
GC   - 200906_09)
JCL  - 20090705
```

   (where *x.x* refers to the appropriate Java version)

   The text, ppc64-64, indicates that it is running in 64-bit mode.

2. Update the location of Java in dme/go.sh to point to this 64-bit Java.

For Solaris

1. On 64-bit Solaris, in the go.sh file, fine the line similar to the following:

```
JAVA_PGM="/usr/java/1.x.x/15/bin/java"
```

   (where *x.x* refers to the appropriate Java version)

2. Append the '-d64' command line parameter to Java to start it in 64-bit mode. For example:

```
JAVA_PGM="/usr/java/1.x.x/15/bin/java -d64"
```

3. To verify that Java is running in 64-bit mode, run it with the '-version' parameter. For instance:

```
->/usr/java/1.x.x/15/bin/java -d64 -version
java version "1.x.x_15"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.x.x_15-b04)
Java HotSpot(TM) 64-Bit Server VM (build 1.x.x_15-b04, mixed mode)
```

   (where *x.x* refers to the appropriate Java version)

   The text, 64-Bit Server, indicates that it is running in 64-bit mode.

If the Solaris Java installation does not support the '-d64' parameter, point to a separate 64-bit Java JRE. Contact the system administrator for assistance in locating such a version of Java.

Task 3.6 Restart and Verify the File-AID/EX Execution Server

After this change to dme/go.sh is complete, stop the Execution Server and restart it. When the Execution Server restarts, it should display the following to stdout along with other logging information:

```
sun.arch.data.model: 64
```

If the number displayed is 64, the Execution Server is running in 64-bit mode. If the number displayed is 32, it is still running in 32-bit mode.

Task 3.6.1 Start/Stop *File-AID/EX Execution Server* as Windows Service

Windows services, formerly known as NT services, enable users to create long-running executable applications that run in their own Windows sessions. These services can be automatically started when the computer boots, can be paused and restarted, and do not show any user interface. These features make services ideal for use on a server or whenever there is a need for long-running functionality that does not interfere with other users who are working on the same computer.

The Execution Server as a Service feature was intended to automatically start a remote Execution Server on a machine not used as a workstation. Some users not only want this but additionally want to use the File-AID/EX tools on the same machine. This can be accomplished by doing the following:

1. Use the **Default Execution Server Settings** dialog box to add a new entry defining the system the service is installed on as a remote execution server. Select the new entry as the default execution server. Refer to the *Homebase online help* for instructions.
2. Use the **Shared Repository Connection** dialog box to add a new shared repository using the repository on the system the service is installed on. Make this "shared" repository the default repository. Refer to the *Repository Management Utility online help* for instructions.

Four batch files, located in the `<FAEX_INSTALL_DIR>\dme` folder are supplied to support installing and running the File-AID/EX Execution Server as a Windows Service:

InstallExpressAsService — This batch file will install the File-AID/EX Execution Server Service. After the service is installed, the File-AID/EX Execution Server will be started. On subsequent rebooting of the machine, the File-AID/EX Execution Server will be automatically started. After this batch file is successfully run, the File-AID/EX Execution Server will be listed in the Windows Services dialog window and provides the ability to Start/Restart/Stop the File-AID/EX Execution Server.

UnInstallExpressAsService — This batch file will stop the File-AID/EX Execution Server, then uninstall it as a Windows Service.

StartExpressAsService — If not running, this batch file will start the File-AID/EX Execution Server but will not perform an install.

StopExpressAsService — If running, this batch file will stop the File-AID/EX Execution Server but will not perform an uninstall.

Task 3.6.2 Start/Stop the File-AID/EX Execution Server on Unix

To start the File-AID/EX Execution Server:

The File-AID/EX Execution Server is installed automatically during the installation of File-AID/EX.

To start the Execution Server:

1. Navigate to the `dme` directory where File-AID/EX is installed and enter at the prompt `./go.sh`
2. Press **Enter**. A message appears stating that the engine has compiled or the daemon is waiting for connection.

To stop the File-AID/EX Execution Server perform one of the following, depending on the Unix platform:

- For all platforms except HP-UX, stop (*Ctrl*+C) the terminal session from which the Execution Server was started.
- For HP-UX, it may be necessary to locate the task and KILL it.

Task 3.7 Configure Third-party JDBC Drivers for Use with *File-AID/EX*

Following is an example of how to configure a third-party JDBC driver to use with File-AID/EX. Some third-party JDBC drivers will work with File-AID/EX, but they are not supported by Compuware. This

example is based on a Microsoft-provided MS SQL Server driver, which is considered a third-party driver to File-AID/EX.

- Within ConverterPro, it is possible to configure third-party drivers for use as a SOURCE ONLY. It is not possible to write to these databases. Creating target tables will not work.
- File-AID/EX does not fully support third-party drivers and there is no guarantee that following these steps will be successful.

Task 3.7.1 Configure the Driver

1. From the Homebase **Tools** menu, select **Execution Server**. Click **Stop** to stop the Execution Server.
2. Put the JDBC driver files for the database to be used in the File-AID/EX "drivers" subdirectory.

   Note: The driver may consist of one or more .jar files or a single .zip file. For example, a Microsoft SQL Server driver consists of three files named: Msbase.jar, Mssqlserver.jar, and Msutil.jar.

3. Do one of the following:
   - **To run as a batch job**, edit the BatchEngine.bat file (located in the `Dme` subdirectory). Locate the parameter "FAEX_CLASSPATH" at the top of the file. Using a semicolon delimiter, add the names of the driver file(s) from Step 2 and save your changes.

     For example, for the aforementioned Microsoft SQL Server driver files named: Msbase.jar, Mssqlserver.jar, and Msutil.jar, change:

     ```
     SET FAEX_CLASSPATH=sumatra.jar
     ```

     to:

     ```
     SET FAEX_CLASSPATH=sumatra.jar;Msbase.jar;Mssqlserver.jar;Msutil.jar
     ```

   - **To run via the GUI**, define the driver CLASSPATH by inserting the path and name of the driver .jar file(s) at the front of the Windows System CLASSPATH environment variable.
4. Edit the `engineJDBC.properties` file (located by default at `\ProgramData\Compuware\FAEX\Cfg` and register the driver by appending it using proper syntax. For example, the syntax for driver string "com.microsoft.jdbc.sqlserver.SQLServerDriver" is obtained by unzipping the `Mssqlserver.jar` file and locating the embedded `SqlserverDriver.class` file. The class file path is displayed as

   ```
   com\microsoft\jdbc\sqlserver\
   ```

   The driver string is created by changing the backslash(\) characters to periods (.) and adding the class filename

   Note: The driver string is case-sensitive.

5. Within ConverterPro, use the Connector Type "JDBC Connect String" and enter the proper JDBC URL for the driver of the particular database being accessed. For example:

```
jdbc:microsoft:sqlserver://<server_name>:<port_number>;DATABASENAME=<database_name>
```

Note: The URL is case-sensitive.

Examples

The following list is a compilation of cases were File-AID/EX has successfully connected to the unsupported databases using a third party JDBC driver.

Teradata

Connection String

```
jdbc:teradata://<server_name>
```

See connect string from Teradata driver.

DB2 on AS400

Connection String

```
jdbc:AS400://<server_name>/<schema_name>
```

INFORMIX

Connection String

```
jdbc:informix-sqli://<HOST>:<PORT>/<DB>:INFORMIXSERVER=<SERVER_NAME>
```

Register the Driver for usage within File-AID/EX

Add the following line to the `engineJDBC.properties` file:

```
com.informix.jdbc.IfxDriver
```

.jar Files that Make Up the Driver

```
ifxjdbc.jar
```

```
ifxjdbcx.jar
```

Intersystems Caché

Connection String

```
jdbc:Cache:// <server_name>:1972/SAMPLES
```

User ID: _SYSTEM

Password: sys

Register the Driver for usage within File-AID/EX

Add the following line to the `engineJDBC.properties` file:

```
com.intersys.jdbc.CacheDriver
```

.jar file

```
CacheDB.jar
```

Add to the CLASSPATH system variable

```
C:\InterSystems\Cache\dev\java\lib\JDK15\CacheDB.jar
```

Uninstall File-AID/EX Execution Server and Rules Engine

To remove the File-AID/EX Execution Server and File-AID Rules Engine:

1. Log on to the UNIX or Linux workstation with the same user ID that was used to install File-AID/EX.
2. Make the current working directory one level above the directory into which File-AID/EX was installed.
3. Remove the File-AID/EX installation directory using the `rm` command to first remove the contents of the installation, then use `rmdir` to delete the installation directory itself.

Maintain the File-AID/EX Execution Server

1. Access the Compuware Support Center to get the current maintenance files for the platform. For example, when running Solaris, select `FAEX_SOLARIS_5.xx.x.nnn.tar`. The .tar file contains replacement files for the installed File-AID/EX system.
2. Download the .tar file to the installation directory (which, by default is `/usr/faex`).
3. Copy the FACS script (`faexspxxx.ins`) provided on the Compuware Support Center to the installation directory (where *xxx* is the service pack number).
4. Before installing the service pack, stop the Execution Server (stop the terminal session or, for HP, kill the task).
5. Install the service pack by executing the service pack installation script (`./faexspxxx.ins`).

   Note: The service pack install may reset the port to port 4900. If the port settings for the install were customized as described in Uninstall File-AID/EX Execution Server and Rules Engine on page 30, re-enter the customized port number in the engine.properties file.

6. Restart the Execution Server as described in Restart and Verify the File-AID/EX Execution Server on page 26.

Milestone 4: Install *Enterprise Data* Companion Components on Mainframe

Task 4.1 Install *File-AID*

Refer to the *File-AID Installation and Configuration Guide* for instructions on installing and configuring File-AID.

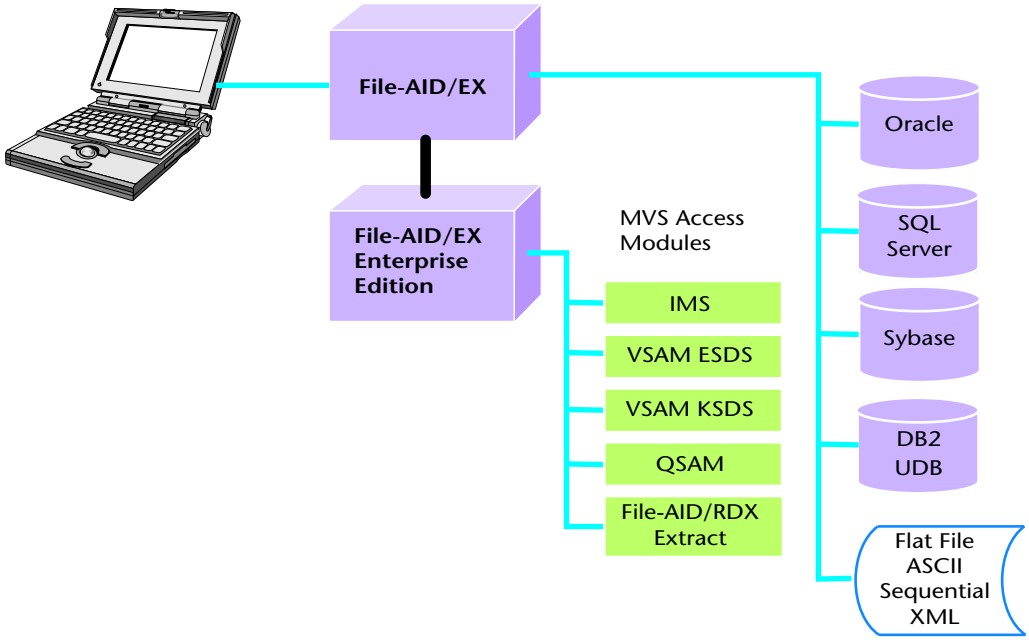
Task 4.2 Install *File-AID/EX Enterprise Edition*

File-AID/EX Enterprise Edition is an optional addition to File-AID/EX. It provides the MVS Access Modules that enable a developer to access mainframe data on z/OS. Sites must set up a license in the License Management System (LMS) license file on the mainframe LPAR before they can use the MVS Access Modules.

The MVS Access Modules supply many z/OS data sources to the File-AID/EX Execution Server. The access modules can accept requests from a File-AID/EX Execution Server running locally or from a remote File-AID/EX Execution Server connected over the network. The MVS Access Modules use TCP/IP connections to communicate over the network. The supported z/OS data sources are: IMS, QSAM, VSAM ESDS, and VSAM KSDS. By moving related DB2 data types to a distributed database, File-AID/RDX extract files are also supported.

Figure 4-1 represents the flow of communication among the facilities of the File-AID/EX Enterprise Edition.

Figure 4-1. File-AID/EX Enterprise Edition Communication Flow



Task 4.2.1 Install File-AID/EX Enterprise Edition

Refer to the *File-AID Installation and Configuration Guide* for instructions on installing and configuring File-AID/EX Enterprise Edition.

Task 4.2.2 Install *File-AID/EX Scheduling Agent*

File-AID/EX can be run through the use of a Scheduler on z/OS. When a conversion completes, a Return Code is sent to the system. The following sections detail the File-AID/EX Scheduling Agent and Return Codes.

File-AID/EX Scheduling Agent

The File-AID/EX Scheduling Agent is named FEAGENT and is automatically installed on z/OS during the File-AID Common installation. FEAGENT provides an interface to the File-AID/EX Execution Server from a Scheduler. Upon initialization, sends a message to an active File-AID/EX Execution Server requesting it to start a File-AID/EX process.

Requirements for calling FEAGENT:

- The selected Execution Server is running in daemon mode.
- Valid specification file of type ConverterPro, Related Extract or Related Load. For assistance in saving specifications as files, refer to the online help for each component.
- The Data Files required to execute the specification reside on the same machine as the Execution Server.

Starting FEAGENT

To execute FEAGENT on the mainframe you must submit JCL that will execute program = 'XVJXIAGT'. This program resides in XVJ load library which must be specified on your STEPLIB DD statement.

The following PARM information is required:

```
PARM='<TCP/IP Address> <IP Address Port> <Specification Type> <File Path> <File Name>'
```

Parameters need to be separated by **space** and enclosed within **single quotes**.

- ***<TCP/IP Address>*** is the TCP/IP address that the Topaz for Enterprise Data Execution Server is running on
- ***<IP Address Port>*** is the port that the File-AID/EX Execution Server is running on
- ***<Specification Type>*** can be ConverterPro, Extract, or Loader
- ***<File Path>*** is the absolute path of the directory where the specification file resides. If the directory path contains spaces, add double quotes around it. Please note that this parameter is optional, and if supplied, the program would look for the specification file in the following location:

  ```
  <File-AID/EX install path>/Conversion/
  ```

- ***<File Name>*** is the name of the specification with its file extension.

Sample JCL:

```
//FEAGENT JOB ('OFABAS9.0.1DEV',M05,1,1),'FEAGENT',
//     CLASS=E,MSGCLASS=X,NOTIFY=&SYSUID,REGION=0M
/*JOBPARM  SYSAFF=CW01
//FEAGENT   EXEC PGM=XVJXIAGT,REGION=0M,

//    PARM='10.10.10.10 4900 ConverterPro c:\MyFolder MyConvProSpec.xml'
//STEPLIB  DD DISP=SHR,DSN=<File-AID Common LOAD LIB>
```

Return Code Processing

When the specification completes, the File-AID/EX Execution Server sends a Return Code to the FEAGENT, which sends the code back to the calling operation and FEAGENT terminates. The following are the Return codes returned by the File-AID/EX Execution Server:

Table 4-1. File-AID/EX Return Code Values

Code Value	Code String
0	"Success: Batch Execution has been successfully completed."
4	"Warning: Warnings have occurred with possible database errors."
8	"Warning: Warnings have occurred with possible database errors." 8 "ABEND:" The message received is ABEND-specific. Examples of this magnitude include: File not found, Parser Exception, Engine could not be started, etc

Task 4.3 Install *File-AID Rules Engine (FARE)* on z/OS Unix

Perform this task only if you plan to use the File-AID Data Privacy plug-in to disguise z/OS data using the Compuware's File-AID mainframe products running on z/OS. A z/OS UNIX console tool (for example, TELNET or OMVS) must be used to install the FARE.

Use the following steps to install the FARE in z/OS UNIX on a target LPAR.

If using OMVS as a console to z/OS UNIX be sure your TSO region size is large enough to run Java. Also, note the FARE requires about 150MB of space — be sure you have sufficient space in the upload and target directories to contain the files.

Installing the FARE in z/OS Unix requires knowledge of z/OS Unix. Your user ID must have a default OMVS segment (or something equivalent) specifying a valid non-zero z/OS Unix user ID (UID), home directory, and shell command. You should have authority to write to at least two directories (install files directory and target FARE files directory), each with sufficient space to contain the installation files or the installed software. Total install time for installing the FARE should be less than 1 hour.

1. Run `setup.exe` on File-AID Services media image downloaded from an electronic distribution order, or from the Topaz for Enterprise Data media.

The current version of the z/OS Unix FARE is also available as a download from the **Fixes and Downloads** section of the Topaz Workbench product page on the Compuware Support Center. *You must synchronize the version of the FARE with the version of the Topaz Workbench client, File-AID Data Privacy plug-in, and also File-AID Services.*

2. Select the **File-AID Rules Engine** tab in the media browser and select the **Install File-AID Rules Engine for z/OS UNIX** button.
3. Use the built in FTP facility to transfer the FARE installer files to z/OS UNIX. Supply the host, user ID, password, and the target path name of an ***existing*** z/OS UNIX directory. Select the **Upload Files to the Mainframe** button to initiate the FTP transfer.

   For example: host LP01 directory `/u/user/userid`

4. In z/OS UNIX, locate the path to a current Java Virtual Machine (JVM). The File-AID Rules Engine requires a minimum of Java JRE 1.8 or more current. (For example: `/usr/lpp/java/java8`). For validation purposes, execute the shell command:

   `[path]/bin/java -version` (where `[path]` is the path name to the JVM —for example: `/usr/lpp/java/java8/bin/java -version`).

5. Edit the uploaded `installfare.sh` file to set the JAVA_HOME environment variable to point to the JVM you located, [*path*].
6. Execute the installer by issuing the shell command: `sh installfare.sh`
7. Accept the default installation destination path (`/opt/Compuware/fare`) or specify a path to which you have write access and has at least 150MB of free space.

The target directory must not be the same directory where you uploaded `installfare.sh`.

Be sure to save the name of the target directory for the FARE and the path name to the JVM — they will be needed to configure File-AID/Data Solutions to enable z/OS disguise executions.

8. Specify whether you will be working with Oracle databases. If you select **Yes**, you will be asked to accept the Oracle license agreement.

Specify whether you will be working with IBM DB2 databases. If you select **Yes**, you will be asked to supply the pathname to the folder containing IBM DB2 JDBC driver file `db2jcc.jar` and the corresponding appropriate license files for DB2 UDB on z/OS.

Task 4.3.1 Add Database Drivers for *File-AID Rules Engine (FARE)*

In the event you did not select a database type during the initial installation but now find the need to configure a database. You just need to rerun the FARE installation (as described in Task 4.3 Install File-AID Rules Engine (FARE) on z/OS Unix), this time making sure you select the drivers you need. If you are using the IBM DB2 driver you will be prompted to supply the location of the folder containing the DB2 JDBC driver file `db2jcc.jar` and the appropriate corresponding license files for DB2 UDB on LUW and/or z/OS.

The following types of database drivers can be installed on the FARE:

- Derby (installed by default and required for Data Privacy security database)
- IBM DB2
- Oracle
- Microsoft SQL Server and Sybase

Task 4.3.2 Configure *Enterprise Data* Components on Mainframe

Refer to the ***File-AID Installation and Configuration Guid*e** sections:

For **New Installations** see section “Configure File-AID Data Privacy Environment”

or

For **Upgrades** see section “Update File-AID Data Privacy Environment”

Then, “Milestone 6: Finalize Configuration” and “Milestone 7: Prepare for Topaz Workbench Integration”

Milestone 5: Topaz for Enterprise Data Client Installation

Task 5.1 Install Enterprise Data Option on Topaz Workbench

See the *Topaz Workbench Installation and Configuration Guide* for information on installing the Topaz Workbench feature packs.

Task 5.2 Install *File-AID/EX*

File-AID/EX executes on Windows operating systems. Administrator privileges are required to install File-AID/EX.

Full installations of File-AID/EX are performed for first-time installations and when upgrading to a later major release. For instance, Compuware recommends running a full install would when going from version 16.00 to version 17.00, while a service pack can be applied to the product for updates of the product within a release. Conversely, applying a service pack would be appropriate when upgrading within a major release, as in an upgrade from 16.03.00 to 16.03.09. Contact Compuware's customer support for guidance if circumstances make it unclear which method to apply.

For a list of other hardware, software, and other requirements necessary to install File-AID/EX, refer to the System and Hardware Requirements. Also listed are database versions and file types for Windows and UNIX that are supported by File-AID/EX.

To use the Oracle Database Client (which is required only if using SQL*Loader or for repositories that were configured in File-AID/CS 4.3 or earlier) ensure the following:

- A `tnsnames.ora` file is present and configured to point to a valid Oracle database.
- The path name for the OCI.dll is added to the PATH. The default location is `c:\oracle\product\10.1.0\Client_1`.
- The TNS_ADMIN environment variable is set to the path to the `tnsnames.ora` file.

When an RFN order for Compuware products includes Topaz for Enterprise Data, a link to the Topaz Workbench and Topaz for Enterprise Data media is provided via email.

To install File-AID/EX:

1. Refer to the System and Hardware Requirements for any installation-related requirements.
2. Preserve any custom configurations to an existing installation of the product. Since the installation program will overwrite the configuration files associated with these user modifications under normal circumstances, preserve these settings as follows:

a. Locate the file(s) that have been modified (for example, the `engine.properties` file if the execution server port number was changed).

b. Copy the file to a safe location outside of the File-AID/EX configuration folder (`C:\Program Data\Compuware\FAEX\cfg` by default).

c. Perform the installation of File-AID/EX.

d. Once the installation is complete. Copy the original files back to the File-AID/EX configuration folder.

3. Close any open applications, including the Execution Server and Communication Manager.
4. Launch the media browser by running `setup.exe` from either the extracted electronically downloaded media image or physical media.
5. On the **Windows Products** tab of the media browser, click **Install File-AID/EX**. A **Preparing to install** dialog box appears.

   – If this is the first time File-AID/EX is installed, the **Welcome to the InstallShield Wizard for Compuware File-AID/EX** dialog box appears.

   – If a prior release of File-AID/EX is already installed, the **Program Maintenance** dialog box appears. Select **Modify** to make changes to the current installation, select **Repair** to fix missing or corrupt files, shortcuts, and registry entries, or select **Remove** to uninstall File-AID/EX. See Uninstall File-AID/EX Execution Server and Rules Engine on page 30 for more information.

6. Click **Next**. The **License Agreement** dialog box appears.
7. Read the license agreement, select **I accept the terms in the license agreement** to accept, and click **Next**. Another license agreement window appears permitting the installation of the Oracle JDBC driver.

Note: The license agreement must be accepted to continue with installation.

8. The Oracle license agreement must be accepted to install the Oracle driver, otherwise the Oracle driver will not be installed. Select whether to install the driver and click **Next**. The **Customer Information** dialog box appears.
9. Type your name and the name of your company, and click **Next**. The **Destination Folder** dialog box appears.
10. Do one of the following:

    – To use the default destination folder, click **Next**.

    – To change the destination folder, click **Change**, navigate to the folder to use, and click **OK**. Then click **Next** on the **Destination Folder** dialog box.

    Note: Do not install File-AID/EX to a network shared drive.

    The **Custom Setup** dialog box appears.

11. Verify features to be installed. By default, File-AID/EX, a repository, and an execution server are installed. File-AID/EX includes Homebase and all of the application components and supporting utility programs of the File-AID/EX suite. The installation can, however, be customized by deselecting features, as follows:

    – Deselect **Repository** if a repository is already set up. This will install only File-AID/EX and the Execution Server. Normally, a user would not select only **Repository** for installation.

      Note: For production environments, Compuware recommends that users set up a shared repository in an industry-standard RDMS rather than using the local repository created when File-AID/EX is installed. The local repository is not managed or backed up, and is meant only to provide a starting point for small testing scenarios, not production environments.

– To install only the Execution Server, deselect **File-AID/EX** and **Repository**. Generally, select only this option when you are installing the Execution Server on a separate server machine. Users would then remotely connect to the Execution Server from their workstations.

To deselect a choice, click the icon next to the option and select **This feature will not be available**. A red X appears beside the deselected option.

12. Click **Next**. The **Ready to Install the Program** dialog box appears.

Note: If making a choice that does not include a repository, a default repository must be set up before using File-AID/EX. When Homebase is first launched, a prompt appears for specifying a default repository.

13. Click **Install** to begin installation. The I**nstalling Compuware File-AID/EX** status window appears showing progress and displaying status messages during installation. It may take several minutes for installation to complete. When the installation is finished, the **InstallShield Wizard Completed** dialog box appears.
14. Click **Finish** to exit the installation window and return to the media browser installation window.
15. Exit the media browser installation window.
16. Reboot to complete the installation.

Execution Server Notes

- The File-AID/EX Execution Server quickly executes complex conversions, extracts, and loads.
- The File-AID/EX Execution Server can be ported to a supported Windows, UNIX, or Linux platform. Note that whenever a remote execution server is installed, it should be configured. Once the Execution Server is installed and started, launch File-AID/EX Homebase and add this Execution Server to the list of valid execution servers in the default repository or any other repositories that have been configured. Refer to the *Default Execution Server* topic in the Homebase help.
- It is desirable for the File-AID/EX Execution Server to reside on the same machine as the source or target data to reduce network traffic. However, using high performance servers is another option. Since transformations are CPU-intensive, this is another benefit to using File-AID/EX when the mapping specifications are complex.
- The File-AID/EX Execution Server can connect directly to a variety of relational data environments and z/OS data types through MVS Access Modules. It enables data conversion between the major z/OS data types, and between mainframe and distributed data types. It can also read existing File-AID/RDX extract files and import record layouts from the extract file.

Task 5.3 Change the Port Number for the Communication Manager

The default Communication Manager port is 4901. The user can change the port by editing the manager.properties file located at `/ProgramData/Compuware/FAEX/Cfg` folder according to the instructions in the manager.properties document.

Task 5.4 Set the Location for File-AID Services Server

This section applies only if the optional File-AID Services Engine for Dynamic Data Privacy is installed.

To use File-AID Data Privacy's dynamic privacy rules with File-AID/EX, the `DataPrivacy.properties` file must be set up. The following steps must be performed for each execution server that will be used for dynamic privacy rules:

1. In Homebase, click  or, from the **Tools** menu, select **Dynamic Data Privacy**. The **Dynamic Data Privacy** dialog box appears.
2. From the **Source Repository** drop-down list, select the source repository that stores the information about the execution server for which to set values. The drop-down list shows all available repositories. *<Local Repository>* is the default.
3. From the **Execution Server** drop-down list, select the execution server for which to set values. The drop-down list shows all available execution servers for the chosen repository.
4. In the **File-AID Services Location** field, enter or modify the value to indicate the server name or IP address of the File-AID Services server.
5. In the **File-AID Services Port** field, enter or modify the value to indicate the port number of the File-AID Services server. The default value is 4180 and valid values are 1 through 65535.
6. Optionally, click **Test** to test the connection. A message indicates success or failure of the connection.
7. Click **Save**. The values are saved in the `DataPrivacy.properties` file, which is located by default at `\ProgramData\Compuware\FAEX\Cfg`

Task 5.5 Enable DB2 JDBC Repository and Database Access Support

DB2 JDBC support is not enabled by default, and JDBC drivers are not provided with the product. Prior to the release of DB2v8, there were no JDBC type 4 drivers. File-AID/EX currently supports JDBC type 2 DB2 drivers as well as JDBC type 4 drivers. As a result, enabling DB2 use requires the following steps.

Note: For Windows, DB2 Client must be installed to use all File-AID/EX features.

DB2 Type 2 Driver

1. If `<db2 installation directory>\IBM\SQLLIB\java12` directory is present, run `java12\usejdbc2.bat`. Copy the resulting `db2java.zip` file to the `<File-AID/EX installation directory>\drivers` directory.
2. If only `<db2 installation directory>\IBM\SQLLIB\`java directory is present, copy the `db2java.zip` file from the `<db2 installation directory>\IBM\SQLLIB\java` to the `<File-AID/EX installation directory>\drivers` directory.
3. Copy the DB2 license file (either `db2jcc_license_cu.jar` or `db2jcc_license_cisuz.jar` depending on platform) to the same directory where the driver was copied.

   Note: This must be done any time the DB2 version is upgraded.

4. Edit the `repositoryJDBC.properties` file (located by default at `\ProgramData\Compuware\FAEX\Cfg` by uncommenting the DB2 driver registration entry `"COM.ibm.db2.jdbc.app.DB2Driver"`.
5. Stop the currently running Communication Manager and Execution Server via Homebase. From the **Tools** menu, select **Communication Manager** or **Execution Server**. Stop, then restart both components. DB2 support should now be enabled.

DB2 Type 4 Driver

1. If `<db2_installation_directory>\IBM\SQLLIB\`java directory is present, copy the `db2jcc.jar` file from the `<db2_installation_directory>\IBM\SQLLIB\java` to the `<File-AID/EX installation directory>\drivers` folder.
2. Copy the DB2 license file (`db2jcc_license_cu.jar` or `db2jcc_license_cisuz.jar` depending on platform) to the same directory where the driver was copied.

   Note: This must be done anytime the DB2 version is upgraded.

3. Edit the `repositoryJDBC.properties` file (located by default at `\ProgramData\Compuware\FAEX\Cfg` and uncomment the DB2 driver registration entry `"COM.ibm.db2.jdbc.app.DB2Driver"`.
4. Stop the currently running Communication Manager and Execution Server via Homebase. From the **Tools** menu, select **Communication Manager** or **Execution Server**. Stop, then restart both components. DB2 support should now be enabled.

Task 5.6 Install File-AID Rules Engine (FARE) for Local Execution Server

1. Install the FARE.
   a. From the Topaz for Enterprise Data media or RFN download, select the **File-AID Rules Engine** tab, then select **Install File-AID Rules Engine for Windows**.
   b. Click **Next** on Introduction page, then choose the default File-AID/EX installation folder or a separate folder and click **Next**. Please note that the:
      - installation of the FARE for use with File-AID/EX requires the FARE to be installed in the File-AID/EX installation directory.
      - installation into a separate folder is for external API development only and will not be used by File-AID/EX.
   c. Click **Install** on the Pre-Installation Summary and click **Done** on the Install Complete screen.

Task 5.7 Configure *Enterprise Data* Licenses

Three client licenses are needed to fully use Topaz for Enterprise Data:

- File-AID Data Privacy
- File-AID/EX
- Topaz for Enterprise Data

To verify that Topaz for Enterprise Data is licensed for use:

1. In Topaz Workbench, from the **Help** menu, select **Topaz Workbench licensing**.
2. If the Topaz for Enterprise Data feature pack is displayed, select the Topaz for Enterprise Data feature pack and select **Check Out**. If the license check out succeeded, the **Lease Begin** and **Lease End** dates will be updated.

Task 5.8 Configure *Enterprise Data* Client

File-AID Data Privacy can be accessed from Topaz Workbench, which is Eclipse-based, allowing you to access data on the mainframe and database management systems (DBMS) from your PC or workstation.

Before you can work with the Data Privacy application you must perform some basic setup. To use translate tables, they must be created and appropriate credentials assigned. To use dynamic privacy rules with Compuware's File-AID products, you must create a project with its associated data elements and project rules.

Task 5.8.1 Perform Basic Setup

The basic setup steps only need to be performed when you first install the Topaz Workbench or if your working environment changes.

1. Start the Topaz Workbench.
2. Set up File-AID Services:

To use Data Privacy, File-AID Services must be installed on a Windows or Linux server by your System Administrator, as described in Milestone 2: Install File-AID Services (FAS).

a. Select **Window > Preferences**, expand **Compuware** and select **File-AID Services**.

b. Type the **URL** for your **File-AID Services**. An example URL is `https://cwsserver.dnsname:3081`.

c. Click **Test Connection**.

d. If you get a Connection Successful message, click **Apply** and **OK**. Click **OK** again. You will return to Topaz Workbench.

3. From the Topaz Workbench **Welcome** window, click the **Data Privacy** icon, or from the Topaz Workbench menu, select **Compuware > File-AID Data Privacy**. This opens the **Data Privacy Explorer** view and shows the available repositories. If your **Data Privacy Explorer** pane is empty, click the **Refresh** icon to list your available repositories.

4. Your Data Privacy Administrator must assign you a user role. The first time you start data privacy, if your role has not yet been assigned, you will receive a "No Roles" error message. Without a role assignment, you will be unable to perform any data privacy tasks. For a description of the default security roles, see “Manage Security” in the Data Privacy online help.

5. If you wish to use a repository other than the default Derby repository that comes with File-AID Services, you must first create it. For instructions on how to do this, see “Manage Data Privacy Repositories” in the Data Privacy online help. To create a new repository, you need to be assigned the Compuware Data Privacy Global Resource Admin role or the Compuware Data Privacy Admin role. Other roles are not permitted to create new repositories.

6. Before you can use data privacy for mainframe data, you must define a mainframe host in Topaz Workbench. For complete details for defining a host, see the **Host Explorer** online help. In general, to configure a new host, you must:

a. Open the **Host Explorer** view.

b. Right-click on **Hosts** and select **Configure > Host Connections on File-AID Services** from the list. The **File-AID Services Connections** dialog box appears.

c. To configure a mainframe host, select the **HCI** tab, and click **Add**. The **File-AID Services Administration** dialog box appears.

d. Enter the **User ID** and P**assword**. Initially, the user ID is `cwadmin` and the password is the same, `cwadmin`. If you are the Administrator, the password should be changed by providing the new password of your choice.

e. Click **OK**. The **Host Connections** dialog box appears.

f. On the **General** tab, enter the **Host**, **Port**, and an optional **Description**.

g. Optionally, select the **Secure connection** check box to enable an encrypted secure HCI connection. Then choose the encrypted protocol your mainframe is configured to use. Selecting **Auto** will cause Host Explorer to check to see what version of TLS or SSL you have.

h. Optionally, select the Credentials tab which enables you to manage any credentials you have saved for this host during Login.

i. Optionally, select the **Advanced** tab to reveal additional parameters:

- **Read/write timeout (seconds)** determines the amount of time Host Explorer will wait for a response from the HCI before timing out.
- **I/O trace level** should only be changed from the default of **None** when directed by Compuware Customer Support.

j. Click **OK**. You will return to the **File-AID Services Connections** dialog box. Your new mainframe host will now appear in the list of hosts.

k. To add a new database connection, click the **JDBC** tab and click **Add**. The **Database Connection** dialog box appears.

l. On the **General** tab, select the database type (IBM DB2 for Linux, Unix, and Windows; IBM DB2 for z/OS; Oracle; SQL Server; Sybase) from the list. Enter the database host, port number, location/SID, and an optional description if desired.

- For Oracle you may also select a **Connection Type** (SID or Service name).
- Optionally, you may select the **Properties** tab to define and manage any additional properties.
- The **Credentials** tab is provided to enable you to manage any login credentials you have saved for this database during Login.

m. Click **OK**. You will return to the **File-AID Services Connections** dialog box. Your database connection will now appear in the database list.

n. Click **OK**. You will return to Topaz Workbench.

o. When you try to access a mainframe host or a database connection in the **Host Explorer** view, a login dialog box appears. Enter your login credentials. For the mainframe, enter your mainframe user ID and password. For a database, enter your database ID and password. You can now access only the information that you are authorized to access. For example, you will only be able to access those files that you can access if you were logged on to the mainframe or your database.

Working with a Project

7. A repository must be opened before you can create or select a Data Privacy project. To open a repository, double-click it or right-click and select **Open Repository**. This provides a list of projects within that repository that you can work with.

   Note: If the repository you expected to see does not appear in the list, click **Refresh**.

   If you click **Refresh**, any open projects will be closed and any changes you have made during this session since the project was last saved will not be saved. A message box appears giving you the option to continue and lose changes or cancel.

8. To create a new project (or your first project), see "Create a New Data Privacy Project" in the Data Privacy online help for complete details.

   Note: Perspectives and views can be opened and closed as desired and windows can be repositioned within the display. When you exit Topaz Workbench, your current perspectives are saved. The next time you start Topaz Workbench, the same perspectives that were open when you exited will reopen.

Task 5.8.2 Create Credentials and Translate Tables

1. Credentials are required at disguise execution time to allow the disguise job to access the values stored in translate tables. For information on how to create new credentials, see "Create New Credentials" in the Data Privacy online help. Translate table definitions require credentials. The credentials can be created prior to defining the translate table or they can be added from within Manage Translate Tables. Credentials are created through **Resource Administration**, and you must be a Data Privacy Administrator or a Data Privacy Global Resource Administrator to create, delete, or modify credentials.
2. Translate tables allow you to use a table of replacement values for data that you want to disguise. For a description of translate tables, see "Manage Translate Tables" in the Data Privacy online help. Translate tables are created through **Resource Administration**, and you must be a Data Privacy Administrator or a Data Privacy Global Resource Administrator to create new translate tables.
3. To return to the **Welcome** window, select **Help > Welcome**.

Manage Repository Content

There are several repository options in the Data Privacy Explorer view. Right-click on a repository to see the following choices:

- **Create New Project**: Right-click on the open repository name and select **Create New Project** to open the **Create New Privacy Project** dialog box. For more information, see "Create a New Data Privacy Project" in the Data Privacy online help.
- **Close Repository**: Right-click on the open repository name and select **Close Repository** to close all open projects and then close the repository.
- **Import Project**: Right-click on the open repository and select **Import Project**. This command allows you to import a project that has been exported using the **Export Project** option available from the project. Only the Data Privacy Administrator can import project XML back into Data Privacy.

The import feature can only import a project that was exported from a repository with the exact same repository version. When this option is selected, a dialog will be displayed where you will specify the location of the project to be imported. You can also optionally specify a new Project Name, Short Name, and Description. This allows you to quickly create a copy of a project and use it to work on variations.

The project ID assigned to the original project will be retained during the import, so any specifications which reference the original project can execute against the imported project as long as the correct repository is specified. If the original project ID is already being used in the repository, a warning message will be displayed and you can choose to import with a new project ID.

If any of the shared resources for credentials, managed keys, translate tables, or custom functions being used in the imported project are already defined in the repository, a warning message will be displayed and you will have the option to import the resources, use the existing resources, or cancel the import.

If the project imported makes use of custom functions, it will be accompanied by a folder with the custom function resources made available in the same location as the XML file. The folder will have the same name as the project XML with the suffix "_CustomFunctionResource". If the root resource folder is missing, or if the respective folder for the custom function resources is missing within that folder, or if the main implementation class is missing, the import process will display a message with that information.

Note: You cannot use **Import project** to import into the Global project; if any global definitions were used in the project being imported, they will be defined as local resources and will not be associated with any global project definitions. The import will bring everything used by the project in together.

- **Edit Data Privacy Repository**: Right-click on the open repository name and select **Edit Data Privacy Repository**. This command allows you to directly edit the project and translate table definitions that are defined in the repository and is useful when host, port, dataset, and schemas must be changed to allow a project to be executed in an environment other than the one where it was defined.

CAUTION: Always create a backup of the repository before using this utility. Use extreme caution when editing.

See "*Editing the Data Privacy Repository*" in the Data Privacy online help for more information on this utility.

Manage Projects

There are several project options in the **Data Privacy Explorer** view. Right-click on a project to see the available actions.

The following action is only available for closed projects:

- **Open Project**: The **Open Project** command is available if the project is not yet open. To open a project from the **Data Privacy Explorer** view, right-click the desired project and select **Open Project** or double-click the project name.

Note: Multiple projects can be open at the same time. To modify a project, it must be open.

The following actions are available for both open and closed projects:

- **Delete Project**: Right-click a project and select **Delete Project** to remove the project from the repository. Once deleted, it will no longer be available and will not appear in the project list.
- **View Project Summary**: Right-click a project and select **View Project Summary**. A project summary provides information about the project, its metadata, data elements, source data identifiers, and rules including rule actions, rule logic, and rule variables.
- **Export Project:** Right-click a project and select **Export Project**. The Save As dialog box appears allowing you to specify where to save the project. This will most often be used if you need to request help from Compuware Customer Support and will save the content of the entire project. A project can be saved to XML whether it is open or closed. If an XML file with the same name exists, a message is displayed and you can choose to either enter a new name or overwrite the existing file. If a custom function resource folder with the same name exists, a message is displayed and you can choose to either overwrite the existing folder or cancel the export (even though the project's XML file would have already been exported at that point).

The following actions are only available for open projects:

- **Lock Project**: If you have used global data elements or global rules in your project, they are normally updated automatically whenever the data elements or rules are updated at their source. If you wish to prevent these updates from occurring automatically in your project, right-click the project and select **Lock Project**. Updates to the global data elements or global rules will no longer be applied to your project. After this, if the global data elements or global rules are updated, you will get a notification message that updates have occurred each time you open the project.
- **Unlock Project**: After a project is locked, you can unlock it by right-clicking the open project and selecting **Unlock**. The changes from updated global datasets or rules will take effect after you click **Refresh** or close and reopen the project.

Silent Installations for File-AID/EX, File-AID Rules Engine, or File-AID Services

To use the silent installer option for File-AID/EX, File-AID Rules Engine, or File-AID Services,

1. A response file needs to be created by running, from the command line, the product's install file with an `-r` flag, and then (*optionally*) create a file pathname where to save the response file. If you do not enter a file pathname for the response file, the file will be named `installer.properties` or `[installername].properties` and it will be created in the same directory as the installer.

   This will create a response file that captures the selections made by the user when stepping through the installer GUI. It can then be used to silently install the product with those selections in place.

2. Recording a response file.

   ```
   c:/install.exe -r c:/temp/installer.properties
   ```

   In the example above, a response file named `installer.properties` will be written to the `c:\temp` directory.

3. Using the recorded response file.

   ```
   c:/install.exe -f c:/temp/installer.properties -i silent
   ```

```
sh ./install.bin -f /install/installer.properties -i console
```

Figure 1,Figure 2, and Figure 3 are examples of recorded response files for File-AID/EX, File-AID Rules Engine, and File-AID Services respectively.

Figure 1. The following is an example of recorded response file for FileAID/EX:

```
# Wed Jun 8 09:00:00 EDT 2018
# Replay feature output
# ---------------------
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.
#true
#----
ORACLE_ACCEPT=true

#Choose Install Set
#------------------

CHOSEN_FEATURE_LIST=Full
CHOSEN_INSTALL_FEATURE_LIST=Full
CHOSEN_INSTALL_SET=Full

#Choose Install Folder
#---------------------
USER_INSTALL_DIR=C:\\Program Files\\Compuware\\File-AID_EX

#Install
#-------
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID_EX\\installdata\\uninstall.lax=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID_EX\\installdata\\resource\\iawin32.dll=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID_EX\\installdata\\resource\\win64_32_x64.exe=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID_EX\\installdata\\resource\\remove.exe=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID_EX\\installdata\\resource\\invoker.exe=Yes
```

Figure 2. An example of recorded response file for FileAID Rules Engine is below.

```
# Wed Jun 8 09:00:00 EDT 2018
# Replay feature output
# ---------------------
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Choose Install Folder
#---------------------
FAEX=1
CUSTOM=0
CUSTOM_USER_INSTALL_DIR=C:\\Program Files\\Compuware\\File-AID_EX\\Dme\\dp
```

Figure 3. An example of recorded response file for FileAID Services is below.

```
# Wed Jun 8 09:00:00 EDT 2018
# Replay feature output
# ---------------------
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

#Choose Install Folder
#---------------------
USER_INSTALL_DIR=C:\\Program Files\\Compuware\\File-AID Services

#Choose Database
#---------------
IBMDB2=0
ORACLE=0
SQLSERVER=1

#Install
#-------
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\ Services\\uninstall\\uninstall.lax=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\uninstall\\resource\\iawin32.dll=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\uninstall\\resource\\win64_32_x64.exe=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\uninstall\\resource\\remove.exe=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\uninstall\\resource\\invoker.exe=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\uninstall\\resource\\iawin64_x64.dll=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\ Services\\MMCServer\\eclipse\\dlm.xml=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\MMCServer\\eclipse\\jre\\bin\\ntlmauth.dll=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\MMCServer\\eclipse\\drivers\\derby.jar=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\MMCServer\\eclipse\\drivers\\derbyclient.jar=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\MMCServer\\eclipse\\drivers\\derbytools.jar=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\MMCServer\\eclipse\\drivers\\derbynet.jar=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\MMCServer\\eclipse\\drivers\\jtds-1.3.1.jar=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\
Services\\Utilities\\ImportUtilityBatch.bat=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\ Services\\ServerConfig.jar=Yes
-fileOverwrite_C\:\\Program\ Files\\Compuware\\File-AID\ Services\\version.xml=Yes
```

Milestone 6: Configure Data Privacy Security

This milestone would typically be performed by a *Data Privacy Administrator*. However, this milestone should be started in order to initially define a *Data Privacy Administrator* user for the purpose of validating the installation of Data Privacy in Topaz Workbench.

In File-AID Data Privacy, users must be assigned Data Privacy *roles*. This step discusses how these roles are used and how they are configured. After the installation of Data Privacy is completed, full configuration would need to be done by users designated with the role of *Data Privacy Administrators*.

No specific login is required to access the Data Privacy perspective. When the File-AID Data Privacy perspective is selected, the currently active user ID determines the Data Privacy role assignment. All roles are assigned at the server level and all repositories within the same server will have the same role assignments.

The following roles prevent users from accessing information that is not available for their role. Information on the mainframe is protected by whatever security the mainframe provides (such as RACF). This means that a Topaz Workbench user cannot access any information on the mainframe that cannot be accessed when logging directly to the mainframe.

Role Definitions

Role definition is the process of mapping user IDs and groups to the roles defined within the product. Each role is associated with a predefined set of permissions within the product functionality.

File-AID Services (FAS) installation includes the installation of a Derby database for the security repository. FAS acts as the roles server, and the mapping of users and groups to the roles used by the product are stored in the security repository.

When any functionality is requested using Data Privacy, the user authorizations are checked to verify that they have the appropriate role to perform the requested function. A user must have at least one Data Privacy role to be allowed to open any project in the Data Privacy application. Data Privacy authorizations are specific to the server being used.

Table 1. File-AID Data Privacy Functionality by Role

Data Privacy Functionality	DP Admin	Project Admin	Global Resource Admin	SME	Privacy Auditor (Only view)
Assign Roles	•				
Create Project	•	•			
Update Project	•	•			
Delete Project	•	• (delete only by owner)			
Change the Project owner	•				
Add Project Metadata	•	•		•	
Manage repositories	•				

Table 1. File-AID Data Privacy Functionality by Role ***(Continued)***

Data Privacy Functionality	DP Admin	Project Admin	Global Resource Admin	SME	Privacy Auditor (Only view)
Create Data Element	•	•			
Update Data Element	•	•			
Delete Data Element	•	•			
Create Rules	•	•			
Update Rules	•	•			
Delete Rules	•	•			
Create rule actions	•	•			
Update rule actions	•	•			
Delete Rule actions	•	•			
Rule Variables	•	•			
Import global Data Elements	•	•			
Import global Rules	•	•			
Expression builder	•	•		•	
Update Global projects	•		•		
Update Global Data Element	•		•		
Update Global Rules	•		•		
Manage Translate tables	•		•		
Manage Encryption keys	•		•		
Manage Credentials	•		•		
Manage Custom Functions	•		•		
Create Data Identifiers	•	•		•	
Update Data Identifiers	•	•		•	
Delete Data Identifiers	•	•		•	
View Coverage	•	•		•	•
Run Coverage Analysis	•	•		•	•
Coverage Report	•	•		•	•

The following is a description of the default roles provided with File-AID Data Privacy:

Data Privacy Administrator

Different roles will have access to different functions within File-AID Data Privacy. The Data Privacy Administrator role has the highest level of authorization giving complete access to all functions within Data Privacy.

When Data Privacy is installed, the role of Data Privacy Administrator is assigned to a temporary default ID. This administrator-level default ID must be used the first time Data Privacy is accessed in order to assign actual user IDs to Data Privacy roles, including other Data Privacy Administrators. Once another user ID is given the role of Data Privacy Administrator, the temporary default ID can be deleted. ***File-AID Data Privacy requires at least one user ID assigned to the Data Privacy Administrator role.*** The Data Privacy Administrator is the only role authorized to manage repositories, set preferences and other definitions that affect the entire Data Privacy installation.

Data Privacy Auditor

The Data Privacy Auditor has the authority to browse and report on all data within all projects. The Data Privacy Auditor cannot change any data.

Data Privacy Global Resource Administrator

The Data Privacy Global Resource Administrator is responsible for defining and managing their sources that are shared by all data privacy projects. This includes global data elements, global rules, managed translation tables, encryption keys, credentials, and custom functions.

Data Privacy Project Administrator

The Data Privacy Project Administrator is responsible for creating projects and managing the definition of privacy within the project. This includes the definition of data elements and rules. Data Privacy Project Administrators can import global definitions into their projects.

Any user assigned to the Data Privacy Project Administrator role is authorized to browse all projects, but they must have the project authorized to be able to edit the project. Because Data Privacy Project Administrators create projects, this role acts as both the project creator and the project owner.

Any Data Privacy Project Administrator can update the project, but only the product owner can delete the project.

Data Privacy SME (Subject Matter Expert)

A user ID assigned the Data Privacy SME role should have knowledge of the application data and thus, is able to create the data element definitions by adding data identifiers to the data elements defined by the project administrator. Users in this role cannot create new data elements. Subject matter experts can use their application knowledge and search the metadata to properly identify the data for each data element.

Task 6.1 Configure Security

Security is configured from within Topaz Workbench. If you have the proper authority, you can set up security from within the Data Privacy perspective.

Following are the steps that allow you to set up your site's default authentication, and manage users, groups, and role mapping.

1. From within Topaz Workbench, select **Compuware > File-AID Data Privacy**. The Data Privacy perspective may also be opened from the **Windows** menu, select **Open Perspective > File-AID Data Privacy**.

When you start Data Privacy for the first time, you will receive an error message "User has no roles". You may ignore this message at this time.

2. Select **Configure > Manage Security**. Supply Administrator credentials with default user ID: `cwsecadmin` and password: `cwsecadmin`. (You should consider changing the password, to limit access to this facility to Data Privacy Administrators only.) The Security Editor Authentication view appears. There are several tabs at the bottom of the screen allowing you to select the different options.
3. **Authentication** is preselected. All fields are filled with defaults provided at installation time, and are disabled and cannot be modified.
4. Select the **User Management** tab. All user IDs previously configured, including the default security user ID, `cwsecadmin` (if not removed by user) appear in the **User Management** tab.
    a. To add a new user, click **Add**.
        1. Enter a domain name and user ID in the **User Name** field in uppercase. The domain name should be followed by a backslash '\' when preceding the user ID (for example: `DOMAINNAME\MYUSERID`). Windows authentication is used to validate user by LAN ID.

2. Click **OK**. The user is now added to the list. Repeat this step until you have added all of the desired users.

b. To modify a user ID's password, select a user ID and click **Edit**. Make your changes and click **OK**.

c. To delete a user, select the user and click **Remove**.

5. Select the **Group Management** tab. The default groups, and any groups that have been added since installation, appear in the **Group Name** list.

a. To modify a group, select a group and click **Edit**. The group name cannot be changed, but you can add users to or delete users from the group. Make your changes and click **OK**.

b. To delete a group, select the group and click **Remove**.

If you are adding multiple users to a new or existing group, you can click **Apply** periodically to save your selections without closing and reopening the dialog box.

c. To add a new group, click **Add**. Enter a group name in the **Group Name** field, and move the users you want to add to the group from the **Available Users** column to the **Selected Users** column. Then click **OK**.

Default Groups are supplied with the Data Privacy plug-in and should be sufficient to control access to Data Privacy plug-ins. In most cases you do not need to add a new Group.

6. Select the **Role Mapping** tab. The default mapped roles, and any roles that have been added since installation, appear in the **Name** list.

a. To map a group to a role, select one of the Application Roles from the list and click **Map Groups**. The Group Selection dialog box appears. Select a group name from the list of groups. If you have many groups, you can search for the desired group, Click **Search**. After you have selected your group, click **OK**. That group will appear in the role mapping list for that role. Repeat this step until you have mapped all of the desired roles.

b. To map a user to a role, select one of the Application Roles from the list and click **Map Users**. The User Selection dialog box appears.

Select a user ID from the list of available users. If you have many user IDs, you can search for the desired user, click **Search**. After you have selected your user, click **OK**. That user ID will appear in the roll mapping list for that role. Repeat this step until you have mapped all of the desired roles.

c. To delete a user or group mapping, select the user or group and click **Remove**.

It is highly recommended to assign at least one user to the Data Privacy Administrator role. That user will be able to access this Manage Security utility, without having to provide any special logon ID or password, whenever they are using the Data Privacy plug-in.

Troubleshooting

Identifying Version of the Installed File-AID Rules Engine

This facility is available only for FARE version 5.0 and above.

For Windows

1. From the install location of the File-AID Rules Engine, modify version.bat to provide the path if JAVA_HOME is not set. The default install location is `../File-AID_EX/Dme/dp`.
2. Run version.bat. A one-line output such as, "Compuware File-AID Rules Engine : 5.0.0", appears indicating the FARE version that is installed.

For Unix Environments

1. From the install location of the File-AID Rules Engine, modify version.sh to add the java path. The default install location is `../usr/faex dme/dp`.
2. Run `version.sh`. A one-line output such as, "Compuware File-AID Rules Engine : 5.0.0", appears indicating the FARE version that is installed.

File-AID/EX Execution Server Security

This section describes the recommended options for configuring Topaz for Enterprise Data components to ensure that they are not exploited for malicious purposes, such as gaining access to sensitive information without proper authorization or installation of malware.

Securing the Execution Server(s)

Execution Server Permissions

Currently, every installation of File-AID/EX includes the installation of Execution Servers. Often these Execution Servers are running under accounts with inappropriate permissions—either being too restrictive, which limits functionality, or too open leaving systems vulnerable.

A full installation of File-AID/EX contains a Local Execution Server, which runs under the account of the user ID who started it explicitly by selecting **Start Execution Server** from a menu or implicitly by launching a client application like ConverterPro.

An Execution Server Only installation on Windows installed by an *administrative* user ID, creates a Windows Service running under that user ID.

A UNIX/Linux-based Execution Server

By default, a Unix/Linux-based Execution Server runs under the account of the user ID that started it. When the Execution Server attempts to access local or network resources, such as files and databases, or to execute external programs or scripts, the local or network security checks access permissions for that user ID. In most cases, local execution servers are less of a security risk, as long as they are secured against remote access and different users, as explained later in this section. For remote execution servers, selection of a user account typically requires analysis and design of how it is to be used.

The recommended approach is to create a specialized domain account for each remote Execution Server, and to give this account appropriate access to all local and network resources that this Execution Server is expected to use.

Typically, one or more shared network locations are selected to contain any source or target files for ConverterPro, target directories for Related Extract, etc. These network locations are configured to be accessible to the domain accounts established for the Execution Servers.

A similar approach can be used for using trusted connections to databases. When trusted access is allowed for the domain user accounts associated with Execution Servers, the File-AID/EX specifications can use the Trusted Connection option when configuring database access rather than providing user IDs and passwords.

Launching Execution Servers Under a Domain Account on Windows

When a File-AID/EX Execution Server is installed on Windows using the *Execution Server Only* installation option, it is automatically registered as a service running under the local system account.

To change the local system account to a domain account:

1. Open **Windows Services**, and select the **Compuware File-AID/EX Execution Server** and its properties.
2. Select the **Log On** tab and change the default Local System account to the domain account.

3. Restart the Execution Server to apply the changes.

When a File-AID/EX Execution Server is installed as a *Local Execution Server* (which is part of the Full Installation mode), there are a few options for launching it under another user account.

The first option is to

1. Create the Execution Server service by launching `InstallExpressAsService.cmd` from the `<Installation_Folder>\Dme` directory (this requires administrative privileges).
2. Follow the steps for the *Execution Server Only* installation. After the installation completes, a *non-administrative* user ID would be able to start and stop this service when needed.

The second option is to

1. Right-click on the `facsexsrvr.exe` filename listed in the `<Installation_Folder>\Dme` directory.
2. Select **Run As Different User** from the pop-up menu.
3. Specify a user ID and password for the domain account designated to run the Execution Server.

The third option is to

1. Launch the Local Execution Server from the command line or from a batch file by issuing the `runas` command, for example

   ```
   runas /user:domain_name\user_name facsexsrvr.exe
   ```

   The password will be requested during the execution of this command.

Launching Execution Servers Under a Domain Account on Linux/Unix

To launch Execution Server on Linux or Unix using a different user account, the `su` or `sudo` commands can be used. A typical example of such command:

```
sudo -u domain_name\\user_name ./go.sh
```

Refer to Linux/UNIX documentation on adding Linux/Unix systems to a domain and on using the `su` and `sudo` commands with a domain account for particular Unix versions and type of shells.

Limiting Access to Execution Servers

When the Execution Server is installed, the default configuration is to allow any user running any File-AID/EX client application to communicate with it—including submitting tasks for execution. This is primarily aimed at simplifying the initial installation and configuration process, and also make the Execution Server sharable with other users in a collaborative environment. It is recommended that as soon as the installation is complete, access to the Execution Server should be limited to only the users that need it. The list of users having access should be monitored and periodically reviewed by the administrators. Monitoring is even more important when the Execution Server runs under a domain account that allows access to databases and restricted network resources.

To configure which users are allowed to send requests to the Execution Server on a system with full installation of File-AID/EX

1. Open the Homebase application and select the **Tools/Execution Server Security** menu item.
2. Specify the port number for the Execution Server (default is 4900). The Execution Server Security Settings dialog box appears.
3. Press the **Remove All** button to remove the default ALL_USER entry from the list, and then use the **Allow...** button to add individual user IDs that should be allowed to submit requests to the Execution Server.

On systems with an Execution Server Only installation, locate the `engineUser_<port_number>.properties` file in the `C:\<ProgramData>\Compuware\FAEX\Security` on Windows or `<InstallDir>/security` on UNIX/Linux directory and populate it with the user IDs

allowed to access the Execution Server. Place one user ID per line, using the format <DomainName>\<NetworkID> format for domain accounts.

Note: The same approach can also be used when the Execution Server is installed as part of a Complete Installation.

If the Execution Server was running, restart it to apply the configuration changes.

Limiting Access to Execution Server Configuration Files

When the Execution Server is configured to be used under a specific domain user account, access to the configuration directories, such as c:\<ProgramData>\Compuware\FAEX\Security and c:\<ProgramData>\Compuware\FAEX\Cfg on Windows and <InstallDir>/security and <InstallDir>/cfg on UNIX/Linux should be secured, to prevent unauthorized users from accessing and possibly modifying the configuration files.

Typically, for the Execution Server Only installation, this access should be limited only to the user ID that the Execution Server runs under and any administrative user IDs that are going to perform system upgrades. For complete installations, such access should be allowed for user IDs launching File-AID/EX client applications. In cases when the local execution server is running under a special domain account using impersonation (as described previously), then access to the configuration directories needs to include that user ID as well.

Limiting Access to Execution of System Commands

File-AID/EX ConverterPro application supports creation of specifications with expressions that can launch system commands during execution. While this is a powerful feature, which is sometimes utilized for copying files and performing other tasks that use the operating system facilities to prepare or transform data, a malicious user can take advantage of this capability by – for example - bringing harmful files to the environment or formatting the hard drive.

The default configuration of File-AID/EX has this capability disabled to prevent its malicious use. When a user needs to make it available, the execution server(s), which are supposed to execute specifications that require this capability, need to be configured to allow it.

To allow execution of system command, open the engine.properties file (located in the <ProgramData>\Compuware\FAEX\Cfg directory on Windows) or <InstallDir>/cfg on UNIX/Linux). If this file has the **AllowSystemCommands** setting, set its value to true (or false, to suppress execution of system commands). If this setting is not present, add a new line with this setting, such as

```
AllowSystemCommands=false
```

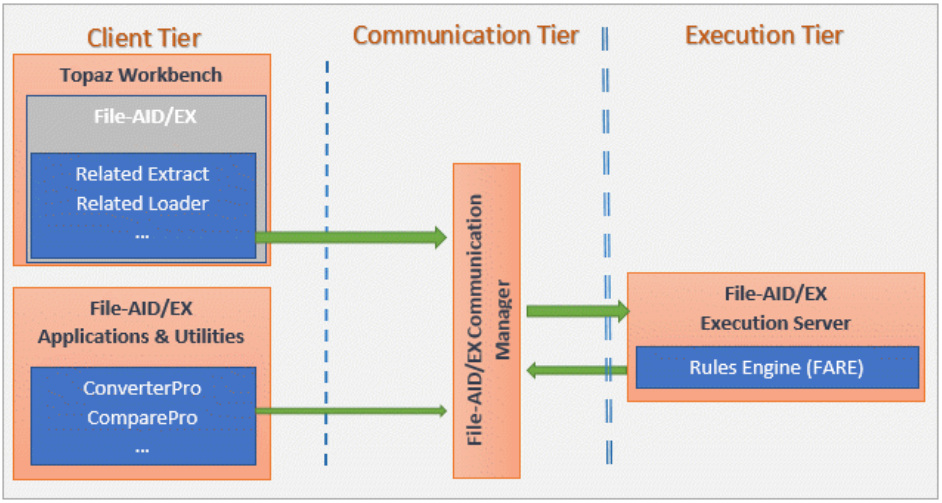
After modifying this file, save it and restart the execution server to apply the changes.

Note: The ability to configure the Execution Server to be able to invoke system commands is another reason for keeping the directories containing the configuration files secure, with only a limited group of users able to modify the settings. See the previous section for more detailed instructions.

Secure Communication between File-AID/EX Components

Overview of Secure Communication Configuration

File-AID/EX is designed as a three-tier solution illustrated on the following diagram.



The Communication Manager is always installed on the same system with the client, but Execution Servers can be accessed both locally and remotely.

The communication between File-AID/EX tiers is implemented based on TCP/IP sockets. To prevent malicious network users from the ability to intercept network traffic and capture the exchange between different File-AID/EX components, starting with File-AID/EX Release 19.01 all communication is being encrypted using the standard Secure Socket Layer (TLS 1.2) mechanism.

This mechanism uses the RSA algorithm with public and private key pairs to establish the SSL handshake and to initiate secure exchange. Those keys are stored in keystore files, one for each tier, located in the in the `<ProgramData>\Compuware\FAEX\Cfg\security` directory (on Windows) or `<InstallDir>/cfg/security` on UNIX/Linux). The names of the keystore files are:

- faexclient.keystore (for the client tier)
- faexcommmgr.keystore (for the communication tier)
- faexexecsvr.keystore (for the execution tier)

In addition to that, each tier is assigned a truststore file, which contains the certificate data of the File-AID/EX components that it can securely communicate with. The names of the truststore files are:

- faexclient.truststore (for the client tier)
  - Configured to trust only the communication tier (Communication Manager)
- faexcommmgr.truststore (for the communication tier)
  - Configured to trust the client and the execution tiers
- faexexecsvr.truststore (for the execution tier)
  - Configured to trust only the communication tier (Communication Manager) and itself (Execution Server

Finally, the main configuration directory (`<ProgramData>\Compuware\FAEX\Cfg` on Windows) or `<InstallDir>/cfg` on UNIX/Linux) contains the following property files, which are defining the location and access to the keystores and truststores:

- clientSecurity.properties (for the client tier)
- managerSecurity.properties (for the communication tier)
- engineSecurity.properties (for the execution tier)

Note: For Execution Server Only installations, only one keystore file (faexexecsvr.keystore), one truststore file (faexexecsvr.truststore), and one security properties file engineSecurity.properties) are included.

The keystore and truststore files can be queried and modified using the keytool.exe utility provided as part of JRE. It can be found, for example, in the jre/bin folder under File-AID/EX installation. See Oracle JRE documentation on the list of supported commands and their formats.

To open these files with keytool.exe (or other keystore management applications), a password is required. The initial (default) passwords for each file are provided below:

- faexclientkey (for the client tier keystore and truststore)
- faexcommmgrkey (for the communication tier keystore and truststore)
- faexexecsvrkey (for the execution tier keystore and truststore)

Note: It is recommended to change all default encryption keys provided with the installation and to change all passwords. The following sections contain detailed information on how it can be done.

Regenerating Keys for Secure Communication

Depending on the company security policies, it may be necessary to perform periodic changes of the keys used for secure communication between File-AID/EX tiers. File-AID/EX provides a tool that makes such a replacement easier.

Open Topaz with File-AID/EX feature and select **File-AID/EX > Administration > Key Management** from the menu. It opens the Key Management Dialog. Refer to *File-AID/EX User Guide* for details on how to use it.

Using the Key Management Dialog, a user can regenerate the keys and create new keystore and truststore files for each tier. It also generates new security properties files that contain encrypted passwords for them.

After the new files are generated, all existing and future installations of File-AID/EX (including Topaz with File-AID/EX feature) need to be updated to include the new keys. All running applications, including local and remote execution servers and the communication managers need to be restarted.

To simplify the step of updating of all installations, see the section Sharing Keystore and Truststore Files between Multiple Installations on page 58.

Using Custom Keys for Secure Communication

While the approach described in the previous section allows to generate new keys, it may still be insufficient for companies that use specific PKI (Public Key Infrastructure) that may require that all keys used for secure communication to be generated by the PKI framework. Another example when use of keys provided externally is required is when company's security policies require that all keys used in secure communication are certified by a trusted CA (Certificate Authority).

To use already existing public/private key pairs and certificates for secure exchange between File-AID/EX tiers, open the Key Management Dialog as described in the previous section. Select the option to not generate the new keys. The tool will then create new empty keystore and truststore files with the specified passwords. After that, the keytool applications included in the JRE can be used to populate the generated keystore and truststore files.

The keystore and truststore files used by File-AID/EX applications follow the PKCS 12 (.p12) format for keystores. If the custom public/private key pairs are not available as a .p12 file, and provided, for example, in .JKS or other forms, other third-party tools may be required to convert them to the .p12 format. One of the popular and powerful options is the OpenSSL toolkit. Consult OpenSSL documentation for details.

After the keystore files are populated with the custom keys, the JRE keytool utility can be used to export the certificates to files and then to import these certificates to the corresponding truststores. Refer to the Overview of Secure Communication Configuration on page 56 for the details on which certificates should be imported to which truststores.

As with regenerated keys, after the keystore and truststore files are populated and tested, all existing and future installations of File-AID/EX (including Topaz with File-AID/EX feature) need to be updated to include the new keys. All running applications, including local and remote execution servers and the communication managers need to be restarted after the update.

To simplify the step of updating of all installations, see the section Sharing Keystore and Truststore Files between Multiple Installations on page 58.

Assigning Different Sets of Keys to Different Installations of File-AID/EX

In some scenarios, it may be beneficial to have different keys assigned to different installations of File-AID/EX.

For example, execution servers running in the production environments may have narrow restrictions on which users or client applications can access them. It is possible to generate separate sets of keys for such execution servers using one of the approaches explained above.

In order to give a certain group of the File-AID/EX client applications access to such remote execution server, use the JRE keytool utility to export its certificate to a file and then import that file to the client's installation Communication Tier truststore (typically – `faexcommmgr.truststore`). Since two-directional certificate validation is performed, in order to establish secure communication, the client installation's communication manager certificate should also be exported from its keystore and then imported to the execution server truststore.

This approach can also be used in another situation, for example – when the company switches to a new set of keys, and some of the client installations still use keystores with old keys. In order to allow such clients to communicate with certain execution servers over a grace period, the new keys certificates can be imported to execution servers' truststores in addition to the old certificates. The execution servers will work with both sets of keys until all users have their keys updated, and then the old certificates can be safely deleted from the execution server truststore.

Sharing Keystore and Truststore Files between Multiple Installations

While by default the keystore and truststore files are placed in the `security` directory under the `cfg` folder, it is possible to place them in any other location accessible to the users under which accounts the applications run. In many scenarios it is beneficial to place them to a shared directory on the network, in which case any updates of the keys will be instantly available to multiple (or all) installations of File-AID/EX.

In order to specify a different location for keystore and truststore files, open the corresponding `*Security.properties` file and modify the `keystore` and `truststore` properties.

For example, the default content of the `engineProperties` file contains the following lines:

```
truststore=security/faexexecsvr.truststore

keystore=security/faexexecsvr.keystore
```

These values provide the path to the keystore and truststore files relative to the `cfg` folder. Modify these values to point to a shared network location that contains the original (default), regenerated or custom files using standard UNC path.

Make sure that the shared directories that contain these files are protected and available only to the users designated to run (and maintain) File-AID/EX applications, and that the keystores and truststores of all remote execution servers are only available to the user accounts associated with those servers and to the administrators performing system maintenance, such as keys and certificates updates.

Checklist of Milestones and Tasks

- ❑ Milestone 1: Prerequisites
- ❑ Milestone 2: Install File-AID Services (FAS)
  - ❑ Task 2.1 Install FAS
    - ❑ **Task 2.1.1 Install FAS on Windows**
    - ❑ **Task 2.1.2 Install FAS on Linux**
  - ❑ Task 2.2 Install FAS License
  - ❑ Task 2.3 Using the File-AID Services Configuration Utility
  - ❑ Task 2.4 Add Database Drivers for FAS
  - ❑ Task 2.5 Control FAS
  - ❑ Task 2.6 Apply Maintenance to FAS
- ❑ Milestone 3: Install File-AID/EX Execution Server(s)
  - ❑ Task 3.1 Install the Execution Server on Windows
    - ❑ **Task 3.1.1 Install the File-AID/EX Server Edition (if licensed)**
    - ❑ **Task 3.1.2 Install File-AID Rules Engine (FARE) for File-AID/EX Execution Server on Windows**
  - ❑ Task 3.2 Install on Linux, AIX, Solaris, and HP-UX
    - ❑ **Task 3.2.1 Install File-AID/EX Components**
    - ❑ **Task 3.2.2 Install a File-AID/EX Server Edition License**
    - ❑ **Task 3.2.3 Install File-AID Rules Engine (FARE) for File-AID Execution Server on UNIX**
  - ❑ Task 3.3 Configure the File-AID/EX Execution Server
  - ❑ Task 3.4 Configure File-AID/EX Execution Server Port Number
  - ❑ Task 3.5 Run the File-AID Execution Server in 32 or 64 Bit JVM
  - ❑ Task 3.6 Restart and Verify the File-AID/EX Execution Server
    - ❑ **Task 3.6.1 Start/Stop File-AID/EX Execution Server as Windows Service**
    - ❑ **Task 3.6.2 Start/Stop the File-AID/EX Execution Server on Unix**

- Task 3.7 Configure Third-party JDBC Drivers for Use with File-AID/EX
  - **Task 3.7.1 Configure the Driver**

- Milestone 4: Install Enterprise Data Companion Components on Mainframe
  - Task 4.1 Install File-AID
  - Task 4.2 Install File-AID/EX Enterprise Edition
    - **Task 4.2.1 Install File-AID/EX Enterprise Edition**
    - **Task 4.2.2 Install File-AID/EX Scheduling Agent**
  - Task 4.3 Install File-AID Rules Engine (FARE) on z/OS Unix
    - **Task 4.3.1 Add Database Drivers for File-AID Rules Engine (FARE)**
    - **Task 4.3.2 Configure Enterprise Data Components on Mainframe**

- Milestone 5: Topaz for Enterprise Data Client Installation
  - Task 5.1 Install Enterprise Data Option on Topaz Workbench
  - Task 5.2 Install File-AID/EX
  - Task 5.3 Change the Port Number for the Communication Manager
  - Task 5.4 Set the Location for File-AID Services Server
  - Task 5.5 Enable DB2 JDBC Repository and Database Access Support
  - Task 5.6 Install File-AID Rules Engine (FARE) for Local Execution Server
  - Task 5.7 Configure Enterprise Data Licenses
  - Task 5.8 Configure Enterprise Data Client
    - **Task 5.8.1 Perform Basic Setup**
    - **Task 5.8.2 Create Credentials and Translate Tables**

- Milestone 6: Configure Data Privacy Security
  - Task 6.1 Configure Security