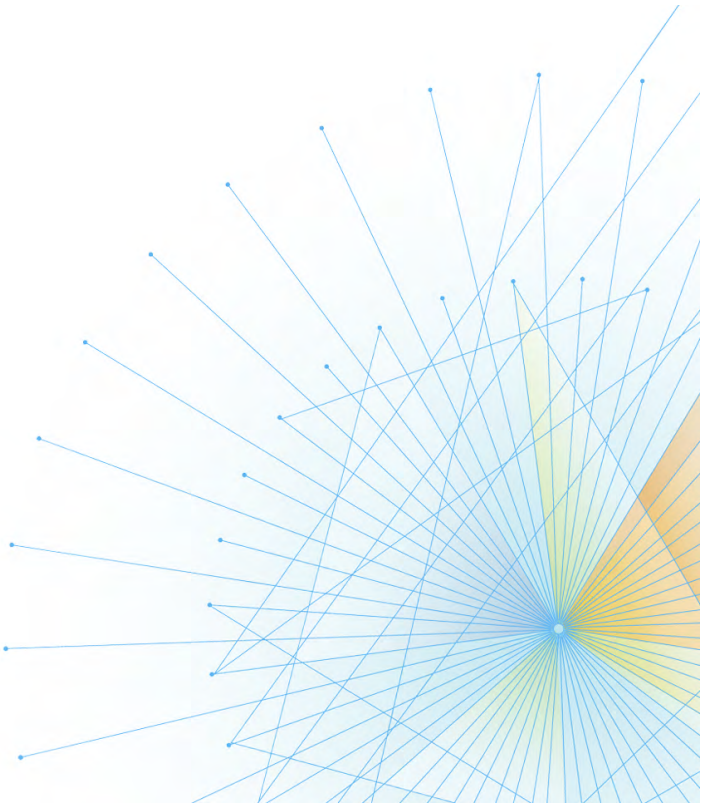
Compuware | The Mainframe Software Partner For The Next 50 Years

File-AID Data Privacy Configuration Guide

Release 18.02



Please direct questions about File-AID Data Privacy
or comments on this document to:

Compuware Customer Support

https://go.compuware.com/

Doc. OCT2017
September 20, 2017

Contents

File-AID Data Privacy

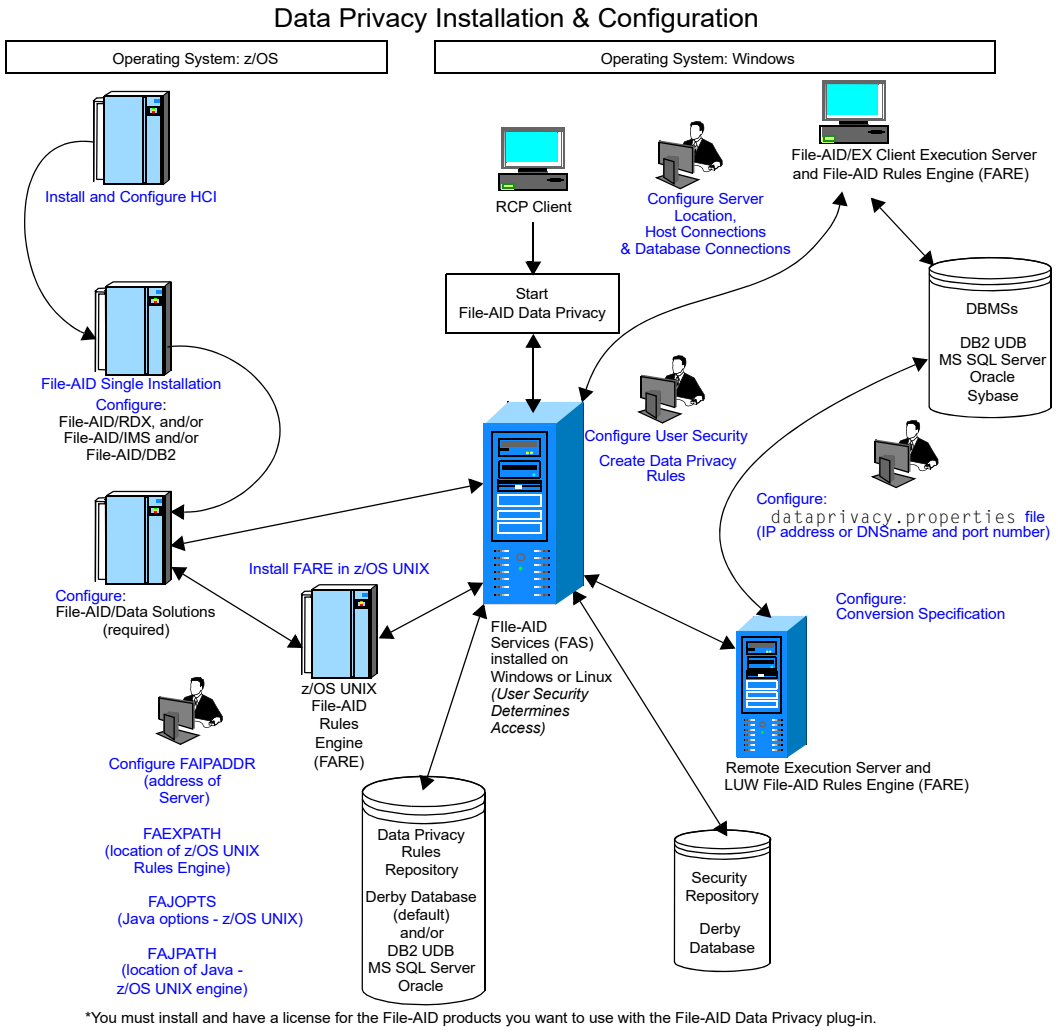
File-AID Data Privacy is used for defining disguise criteria for use in disguising personal identification information in *distributed* test data with File-AID/EX or *mainframe* test data with File-AID z/OS products.

This chapter describes installation requirements to support File-AID Data Privacy. **Following instructions within this chapter are only required if you want to use File-AID Data Privacy**.

Mainframe Data Privacy is only supported on z/OS Release 1.10 or higher.

Figure 1 shows the interaction and dependencies between components required to install and configure File-AID Data Privacy.

Figure 1. File-AID Data Privacy Installation and Configuration



You must install Topaz Workbench with the File-AID Data Privacy feature and File-AID Services (FAS) to use File-AID Data Privacy.

Installing File-AID Data Privacy Summary

The following summary is necessary only if you are planning to use File-AID Data Privacy for mainframe or distributed data disguise.

What you will need to complete this milestone

- An allowance of two hours (estimate) to complete this milestone (depending on the status of the installation of the supporting products). Each product needed for File-AID Data Privacy support has its own configuration process. Typically, it requires two to eight hours to install a File-AID product.

- The File-AID EP and Topaz for Enterprise Data EP media (or equivalent RFN product distributions, including the File-AID/EX and File-AID Services download media image)
- File-AID Services download from FrontLine (Windows or Linux, or via File-AID/EX and File-AID distributed components download)
- Windows or Linux machine to install File-AID Services (FAS). For Windows, this can be the same machine used to install the Topaz Workbench client. By default, File-AID Services uses open TCP ports 3081, 4082, 4180, and 5180 for communication. If needed, you can override the default ports, after installation, by using a provided utility as described in "Changing File-AID Services Port Assignments". Ensure there are no conflicts using those port numbers.
- For the z/OS UNIX installation of the File-AID Rules Engine (FARE):
  - Two directories, each with at least 80MB of available disk space
  - An expert knowledge of the z/OS UNIX system, with privileges to create a directory and knowledge of editing scripts
  - The path name of the location of Java on z/OS UNIX is required
  - The FARE installation requires about 2 hours.
- Also required is the location of a local or LAN directory containing the DB2 database driver (`db2jcc.jar`) and license files in case DB2 will be used as a disguise target, rules repository or translate table repository.

Procedure

The following steps are a summary of the descriptions in Figure 1.

1. Install File-AID Services as described in "Step 1. Install File-AID Services (FAS).".
2. (*Only if planning on disguising distributed RDBMS databases.*) Verify File-AID/EX 5.3 or higher is installed and configured for File-AID Data Privacy as discussed in "Step 2. Install File-AID/EX". When you configured Dynamic Privacy you verified that the Execution Server and File-AID Rules Engine were installed on your target execution platform(s).
3. Install the File-AID Rules Engine in z/OS UNIX as described in "Step 3a. Install the File-AID Rules Engine (FARE) on z/OS UNIX".
4. Install File-AID Data Solutions 4.4 or higher and configure for File-AID Data Privacy as discussed in "Step 4. Configure File-AID/Data Solutions". Verify File-AID/Data Solutions configuration.
5. Ensure File-AID/Common Components 2.1 or higher is installed as discussed in "Step 5. Install File-AID/Common Components".
6. Complete "Step 6. Install Additional File-AID Mainframe Products as Needed".
7. Be sure to modify the CXSS0000 (STASK) proc to reference the required File-AID dataset names. The CXSS0000 Proc was specified in the HCI00 Parameter File. Refer to the *Enterprise Common Components Installation and Configuration Guide* for STASK.
8. Perform step 12 of "Step 1. Install File-AID Services (FAS)." (optionally, including the configuration of Database connections). Be sure to redefine all host connections on File-AID Services.
9. Complete the configuration of Data Privacy security as described in "Step 7. Data Privacy Security Configuration".

10. Verify Data Privacy is communicating. Use the Compuware menu to launch the Data Privacy perspective and the Data Privacy Explorer view. You should be able to see the File-AID Rules repository listed in the view.

If the repository, File-AID Rules, has a red x icon or cannot be opened, it may need to be migrated to make it current. Use the **Data Privacy** menu option **Manage Repositories** to select the repository and click **Migrate**. Some processing will occur to migrate the repository and then you should be able to open it and create a new project.

Step 1. Install File-AID Services (FAS).

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.

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 Windows or Linux version of FAS installation files from the **Fixes and Downloads** section of the File-AID Data Privacy product pages on FrontLine (https://go.compuware.com).

During installation of the Topaz Workbench client, it is recommended that you copy the Topaz Workbench media to a central file share. Note that FAS may be installed on the central file share machine. 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 1GB of disk space to contain FAS software and the default Derby databases.

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 "Changing File-AID Services Port Assignments". 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.

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 FrontLine. Run `setup.exe` from the media. The media browser appears.
2. When installing from the distribution media do the following: To install FAS in Windows, select the **Install File-AID Services for Windows** button.
3. If installing FAS using the install files downloaded from FrontLine, unzip the self-extracting ZIP file to a directory of your choice. For Windows, open the extracted Windows subfolder and run `update.bat`. (For Linux see "Installing File-AID Services to Linux"). 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` or `C:\Program Files(x86)\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 "Adding File-AID Services Database Drivers".

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 "Changing File-AID Services Port Assignments".
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 IP address where the services are installed. The resulting web page should display with a list of executing bundles.
12. Configure FAS in Topaz Workbench
    a. Run the Topaz Workbench client.
13. Access **Window > Preferences > Compuware > File-AID Services** to establish the location and port of the installed FAS. Use the **Test Connection** button in the Preference dialog box to verify that the address is correct.

Note: The default File-AID Services port to connect to is 3081. For example: `https://DWSserver:3081`.

Be sure to include the 's' in *https* for your connection string.

To access metadata for Distributed RDBMS databases and Host Connections, you must first configure a connection to each desired instance using the Configure facility in Host Explorer. Refer to the online help for the ***Host Explorer User Guide*** for details. In general, the procedure to configure a remote host database is:

1. In Host Explorer, right-click **Hosts** and select **Configure**, then choose **Host Connections defined in File-AID Services** from the cascade menu list.
2. Use the HCI or JDBC tab to add a new host connection or JDBC database connection respectively.
3. Supply Administrator credentials (default is user ID: `cwadmin`, password: `cwadmin`). (You should consider changing the password to limit access to this facility to server administrators only.)
4. Complete the connection information in the Database Connection dialog box. Click **OK**.

Step 2. Install File-AID/EX

This step is optional if you plan on privatizing only mainframe data.

1. **File-AID/EX Windows Client**

   A copy of the File-AID/EX client will need to be installed for each user machine. Install the current release of File-AID/EX (see the Topaz Workbench Release Notes for current release information).

   An Execution Server is installed by default with the installation of the File-AID/EX client. For more information refer to the *File-AID/EX Installation Guide* provided with the distribution media or on Compuware FrontLine.

2. **File-AID/EX Server Edition (if licensed)**.

   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.

   a. For Unix servers, use the **File-AID/EX Execution Servers** tab of the media containing File-AID/EX to access files needed to install Execution Servers for AIX, HP-UX, Linux, or Solaris.

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

      By de-selecting 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. For more information refer to the *File-AID/EX Installation Guide* provided with the File-AID/EX distribution media or at Compuware FrontLine.

3. 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.

4. **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.

5. **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 Single Install Image Installation and Configuration Guide* provided on Compuware FrontLine or on the File-AID EP and Topaz for Enterprise Data EP media.

Step 3a. Install the File-AID Rules Engine (FARE) on z/OS UNIX

Perform this Step 3. only if you plan to use the File-AID Data Privacy plug-in to disguise z/OS data using the Compuware's File-AID products (File-AID/Data Solutions, etc.) running on z/OS. A z/OS UNIX console tool (for example, TELNET or OMVS) must be used to install the FARE. Follow these 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 EP 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 FrontLine. *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.
9. 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.

Step 3b. Install the File-AID Rules Engine (FARE) on UNIX (AIX, Linux, Solaris, HP-UX)

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 FrontLine. 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.

Step 4. Configure File-AID/Data Solutions

1. For File-AID Data Solutions:

   Use configuration task **2** (DB2/IMS/DPR Environment) and select **Option 3 (Data Privacy)** to configure Data Solutions customization module XVJOPDPR to work with File-AID Data Privacy and to provide information about the following:

   – FAS location (machine name or IP address)

   – FAS port assignments

   – Mainframe (z/OS UNIX) FARE (Java path and installation directory).

For more information refer to the *File-AID Single Install Image Installation and Customization Guide*.

For File-AID/Data Solutions 4.4:

Be sure to use the Installation Customization Option **5 - Data Privacy** to provide Privacy configuration information. Also, be sure to run Customization task **7**, DATA PRIVACY - Configure Dynamic Privacy Rules (DPR), to request that File-AID/Data Solutions generate an additional dataset (JAVAINFO). This dataset contains values you established, which are used to invoke the FARE whenever a disguise execution of a File-AID Data Privacy plug-in project is requested from the mainframe (z/OS) File-AID products.

For more information refer to the *File-AID/Data Solutions Installation Guide* provided with the product media.

2. Follow the Installation Verification for File-AID Data Privacy process described in the *installation guide* to verify operation of File-AID Data Solutions.

Step 5. Install File-AID/Common Components

File-AID/Common Components functionality is automatically installed as part of the File-AID Single Install image installation; be sure to include just the File-AID customization library (CXVJLOAD) and the authorized load library (SXVJAUTH) in the STEPLIB concatenation of the STASK.

For File-AID products prior to 10.1: Install File-AID/Common Components 2.1. File-AID/Common Components is distributed on the File-AID EP media and also on the Topaz for Enterprise Data EP media or RFN distribution. Installation documentation is provided on the media or on Compuware Go/FrontLine.

File-AID/Common Components is also required for File-AID Data Editor. Skip this step if File-AID/Common Components has already been installed for File-AID Data Editor.

Be sure to include the File-AID/Common Components Authorized load libraries (MXVJnnn.SXVJAUTH, and MXVJnnn.CXVJAUTH) in the STEPLIB concatenation of the STASK.

Step 6. Install Additional File-AID Mainframe Products as Needed

During the File-AID install, all of the File-AID products are automatically installed. User access to these File-AID products is controlled by licensing with Compuware. Refer to the Topaz Workbench Release Notes for minimum requirements.

- File-AID/RDX 5.0 and higher is distributed on the Topaz for Enterprise Data EP media or RFN order. Installation documentation is provided on the media.
- File-AID for IMS 7.7and higher is provided on the File-AID EP media or RFN order.
- File-AID for DB2 6.3 and higher is provided on the File-AID EP media or RFN order.
- Apply all current maintenance to the z/OS versions of File-AID family of applications (used to disguise data using the new File-AID Data Privacy facility).

Step 7. Data Privacy Security Configuration

This step is typically performed by a *Data Privacy Administrator*. But this Step 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 was completed, full configuration would be typically 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, and additional roles you create for your site, 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

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	•				
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	•	•		•	

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)
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.

Map Security Roles

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.

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. The User Management view appears. The default user names, and any users who have been added since installation, appear in the **User Name** list.
   a. To add a new user, click **Add**. The Add Users dialog box appears. 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`). You may optionally supply a password for this user. It is not required or used at this time. Instead, Windows authentication is used to validate users by LAN ID. Then 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 or password, select a user 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 Group Management view appears. 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**. The Add Groups dialog box appears. 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 Role Mapping view appears. 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.

   c. 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.

   d. 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.

Appendix A.
File-AID Services Ancillary Procedures

Changing File-AID Services Port Assignments

A 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

When the utility is run, it reads the current port assignments and allows you to change them. In order for the changes to become effective, FAS service must be stopped and restarted.

Also, note that you may need to change the port assignments configured with File-AID/EX and File-AID/Data Solutions (see "Step 2. Install File-AID/EX" and "Step 4. Configure File-AID/Data Solutions"). 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.**

Executing the Server Configuration Utility

For Windows

1. Use the **Start > Programs > Compuware > Server > Server Configuration** shortcut to invoke the utility.
2. Overtype any port numbers you wish to modify.
3. Click **OK**.
4. Stop and restart File-AID Services.
5. If changing File-AID Services port (default: 3081), notify users by recording File-AID Services preference information.
6. If changing the Data Privacy execution port (default 4180) update the File-AID/EX configuration ("Step 2. Install File-AID/EX") and the File-AID/Data Solutions Data Privacy configuration (see "Step 4. Configure File-AID/Data Solutions").
7. If changing the File-AID/Data Solutions port (default 5180) update the File-AID/Data Solutions Data Privacy configuration (see "Step 4. Configure File-AID/Data Solutions").

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 "Controlling File-AID Services in Linux".
4. Be sure to modify theTopaz Workbench configuration, File-AID/EX configuration, and/or File-AID/Data Privacy configurations to match your new port assignments (see steps 5, 6, 7 in "For Windows").

Adding File-AID Services Database Drivers

A 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.

There are four types of database drivers that can be installed on FAS:

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

When the utility runs, a **Data Privacy** tab is provided for specifying additional database types. 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 and/or z/OS.

Executing the Server Configuration Utility

For Windows

1. Use the **Start > Programs > Compuware > Server > Server 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 and/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 and/or z/OS. For Oracle, accept the license agreement.)
3. Stop and restart File-AID Services service. Refer to “Controlling File-AID Services in Linux”.

Adding File-AID Rules Engine 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. You just need to rerun the FARE installation (as described in “Step 3a. Install the File-AID Rules Engine (FARE) on z/OS UNIX”), this time making sure you select the drivers you need. Note that 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.

Four 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

Installing File-AID Services to 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 Compuware FrontLine 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:\Program Files (x86)\Compuware\Topaz Workbench` or `C:\Program Files\Compuware\Topaz Workbench` and use the **Test Connection** button in the Server Preference dialog box.

Controlling File-AID Services in Linux

Navigate to the subdirectory ~/ `MMCServer/eclipse/bin` in the directory where you installed FAS.

To stop FAS issue the following command. `./platform.sh stop`

To restart FAS issue the following command. `./platform.sh start`

To uninstall FAS issue the command. `./platform.sh uninstall`

To maintain FAS, see “Applying Maintenance to File-AID Services”.

Applying Maintenance to File-AID Services

Maintenance to File-AID Services is implemented 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 FrontLine (https://go.compuware.com) in the Fixes/Downloads page of Topaz Workbench product page. Follow the instructions provided to download the maintenance.

Maintaining File-AID Services

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 FileAID 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 (see step 3 on page D-3).

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.

Maintaining the File-AID Rules Engine (FARE)

When installing an update, you will be warned that an update is about to proceed. For z/OS UNIX, be sure no disguise jobs are executing. For File-AID/EX, be sure to stop the execution server for the FARE you are updating. When ready, select OK to proceed with the update.

For z/OS UNIX (Mainframe Data Privacy only): When Compuware provides an updated `installfare.jar` file, binary transfer the file to z/OS UNIX and replace the original `installfare.jar` you uploaded from the media image. Then, re-invoke the `installfare.sh` installation script and specify the same target directory and database usage you originally chose for the FARE (See “Step 3a.

Install the File-AID Rules Engine (FARE) on z/OS UNIX”). The new version will install and replace the current version of the FARE.

For File-AID/EX (Distributed Data Privacy): Beginning with File-AID/EX 5.2.1, the FARE may be updated independently from the File-AID/EX Execution Server.

When a new release of the FARE is made available on Compuware FrontLine or via new media, the installed FARE(s) should be updated for all File-AID/EX Execution Servers (local Windows installation of File-AID/EX as well as any installed remote execution servers in Windows or UNIX).

Please refer to the *File-AID/EX Installation Guide* for complete information on installing updates to the FARE in Windows or UNIX.