

ibiTM Open Data Hub for Mainframe Connectors

Installation and User Guide

Version 1.0.7 | November 2024

Contents

Contents	2
Introducing ibi Open Data Hub for Mainframe	8
Open Data Hub for Mainframe Benefits	9
Open Data Hub for Mainframe Components	11
Open Data Hub for Mainframe Users	12
Open Data Hub for Mainframe ODBC Connector	13
What Is Open Database Connectivity?	14
What Is an ODBC Driver?	15
ODBC Application Components	16
Open Data Hub for Mainframe ODBC Connector Components	17
Installing the Open Data Hub for Mainframe ODBC Connector on Windows	18
Installing and Configuring the Open Data Hub for Mainframe ODBC Connector on Windows	19
Install and Configure the Open Data Hub for Mainframe ODBC Connector on Windows	20
Add Data Sources on Windows	24
Remove Data Sources on Windows	28
Configure Data Sources on Windows	29

Test the ODBC Driver With Microsoft Excel	31
Set Advanced Options for Data Sources	33
Installation for z/OS	36
Information You Need Prior to Installation on z/OS	36
z/OS Installation Requirements	37
JVM Requirements for Java Services (Server Installations Only)	38
Installation for ZFS and PDS	39
Choosing How to Deploy	39
File Locations	42
Supplied Files Location (EDAHOME)	43
Configuration Files Location (EDACONF)	44
Profile Files Location	45
Administration Files Location	45
Application Files Location (APPROOT)	46
Step-By-Step Installation Overview	48
ZFS/USS Deployment Installation Details	49
Installing New on ZFS	49
Set Up User IDs	50
Collect Required Information for Adapters	64
Download and Process the Distribution File from eDelivery	68
Run isetup to Install and Configure a New Server	69
Run isetup to Add an Additional Configuration Instance	72
Run isetup to Upgrade an Existing Installation to a Newer Release	77
Testing the New or Upgraded Installation/Configuration	81
Configure Security	82
Starting and Stopping the ibi WebFOCUS Reporting Server for ZFS	91
Starting and Stopping the ibi WebFOCUS Reporting Server Using a Batch Job	91
Starting and Stopping the ibi WebFOCUS Reporting Server Using a Started Task	92
Sample IWAYS Started Task	92
Sample IWAYP Started Task	93

ibi WebFOCUS Reporting Server Operations Using MVS Operator Commands	94
Enabling HTTPS Security on the HTTP Listener for ZFS	94
Defining the ICSF Dataset Key Label for ZFS to Use Pervasive Encryption	97
Db2 Security Exit Configuration for ZFS	100
Changing DSN3SATH for RACF and eTrust CA-Top Secret Sites	100
Changing DSN3SATH for eTrust CA-ACF2 Sites	102
Modifying the Link JCL for DSN3SATH	103
Upgrading From a Release Prior to 8207.27 to Release 8207.27 or Higher	105
Reconfigure Security	106
Preventing Unsecured Starts After Upgrades	107
Reconfigure Adapters	108
Accounting for ZFS - SMF Records	108
Enable Accounting	109
Set the Accounting Field	110
Report From SMF Data	110
SMF RECTYPES	111
SMF Record Format for RECTYPES 1 and 4	112
SMF Record Format for RECTYPES 2 and 5	114
Accounting for Db2 in an ibi WebFOCUS Reporting Server Task	118
Enabling Use of the zIIP Specialty Engine	118
What Is a zIIP Specialty Engine?	119
Steps to zIIP Enablement	119
Activating a zIIP Environment or Projecting zIIP Usage	120
Activate the zIIP Enablement Feature	120
How the ibi WebFOCUS Reporting Server Takes Advantage of the zIIP Processor	123
Evaluating zIIP Usage	124
Performance Considerations for ZFS	125
Running the ibi WebFOCUS Reporting Server in a Non-Swappable Address Space ...	125
Workload Manager	126
Troubleshooting for ZFS	129
Problem: The ibi WebFOCUS Reporting Server Abends With a U4039 Code	129

Problem: INSUFFICIENT AUTHORITY TO GETPSENT messages in JESLOG	130
Problem: Request fails, and JVM not found messages written to edaprint.log	130
Secured ibi WebFOCUS Reporting Server Starts Unsecured or Does not Start After Upgrade	131
Generate a Trace	131
Generate a System Dump	132
Add JCL Allocations to a Running ibi WebFOCUS Reporting Server	133
Allocate a Data set From the z/OS System Console	133
Free Data sets Allocated to the ibi WebFOCUS Reporting Server	134
Free a Data set From the MVS System Console	134
Freeing an Allocated Data Set	135
PDS Deployment	135
Installation Requirements for PDS	135
Installing New on PDS	141
Starting and Stopping the ibi WebFOCUS Reporting Server for PDS	161
Enabling HTTPS Security on the HTTP Listener for PDS	163
Defining the ICSF Dataset Key Label for PDS to Use Pervasive Encryption	165
Db2 Security Exit Configuration for PDS	168
MSODDX: DDNAME Translation for User Subroutines	172
Overriding the Time Zone Setting	172
Adding a Configuration Instance for PDS	172
Upgrading the Release of your PDS-Deployed ibi WebFOCUS Reporting Server	179
Accounting for PDS - SMF Records	181
Enabling Use of the zIIP Specialty Engine	191
Performance Considerations for PDS	198
General Information for a z/OS PDS Installation	205
Third-Party Software and Licenses	208
Troubleshooting for PDS	208
Security Providers	221
Using Applications	222
Using the Open Data Hub for Mainframe ODBC Connector	223

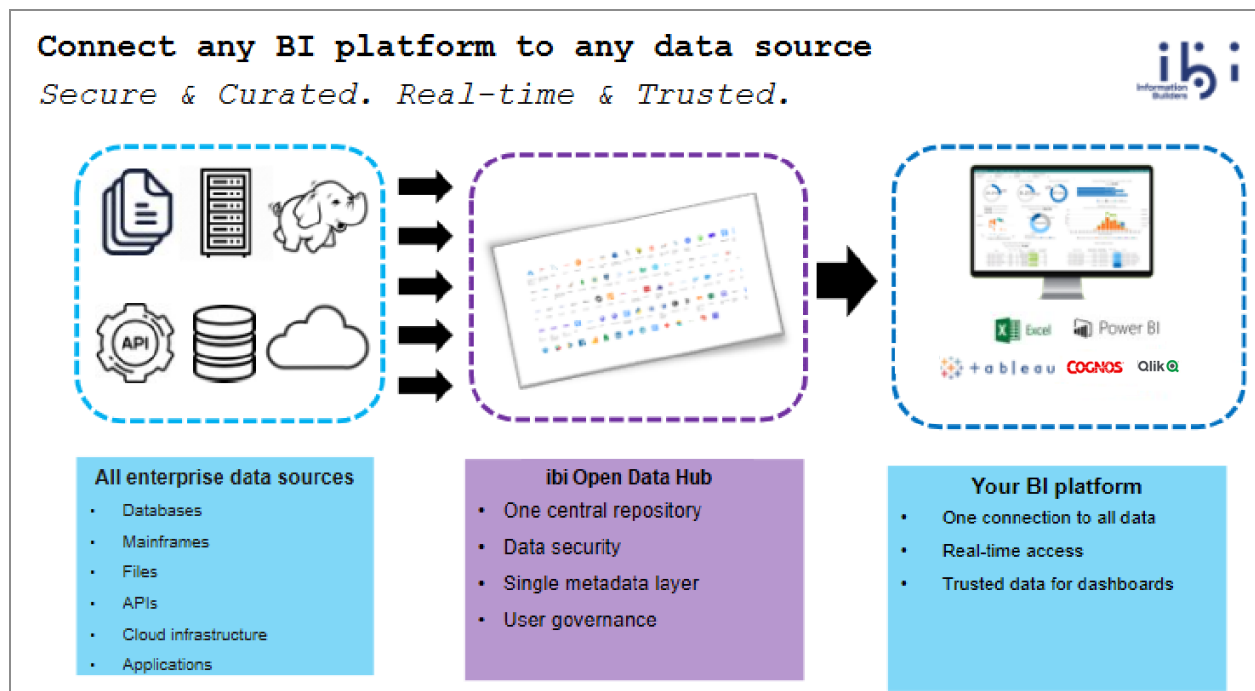
Open Data Hub for Mainframe ODBC Connector from Microsoft Excel	224
Use the ODBC Connector from Microsoft Excel	225
Open Data Hub for Mainframe ODBC Connector from Microsoft Power BI	229
Use the ODBC Connector from Microsoft Power BI Import	230
Use the ODBC Connector from Microsoft Power BI Direct Query	231
Open Data Hub for Mainframe ODBC Connector from Tableau	233
Use the ODBC Connector from Tableau	234
Using ODBC Escape Clauses	235
Using ODBC Escape Clauses to Run Remote Procedures	236
Invoking Remote Procedures Using Shorthand Syntax	237
Using ODBC Escape Clauses for Dates, Times, and Timestamps	238
Issuing Your Own SQL Statement	239
Open Data Hub for Mainframe JDBC Connector	241
Using the Open Data Hub for Mainframe JDBC Connector	242
Use the Open Data Hub for Mainframe JDBC Connector With sqlline	243
Connect to a Server Using a URL	244
Use the Open Data Hub for Mainframe JDBC Connector With Squirrel SQL	246
Create an Alias	251
ibi Documentation and Support Services	257

Legal and Third-Party Notices	258
--------------------------------------------	------------

Introducing ibi Open Data Hub for Mainframe

ibi™ Open Data Hub for Mainframe is a data virtualization solution that easily connects your existing BI platform to virtually any database, file format, application, or web service in your Enterprise. In addition, these connections are made in a curated, secure, real-time, trusted manner.

The ibi Open Data Hub for Mainframe environment is shown in the following image.



Open Data Hub for Mainframe Benefits

The benefits of Open Data Hub for Mainframe include the following:

- **Install once and configure at scale.** Install and configure multiple data connections on one central server with little data preparation effort.
 - **Access to almost any data source.** Our data adapters use native database APIs, whenever possible, and ODBC and JDBC when required, as well as providing access to flat, delimited files, XML or JSON documents, and RESTful Web Services.
- **Easily establish secure data management and architecture standards.** Take control of your data without undertaking a large data mastering project.
 - **Robust metadata.** Create a single, robust metadata layer for database tables and file sources.
 - **Folder functionality.** Classify metadata into folders to group related sources together.
 - **User authorization for security.** Categorize users with permission levels for data access.
 - **Control data access.** Administrator can control access to individual columns by user or data values.
 - **Usage reports.** Access reports that show what data assets are being used and who is using them.
- **Power up your dashboards with integrated data.** Cross-database joins allow you to query and treat multiple data sources as one.
 - **Data federation.** Make all data sources, regardless of source, appear as one. The server queries the underlying data sources and returns a single answer set.
 - **Virtualization abilities.** Gain access to virtually any database, column store, file format, or web service, without the requirement to copy or prepare the data.
 - **Data preparation features.** Simplify or augment data, all built into the product.

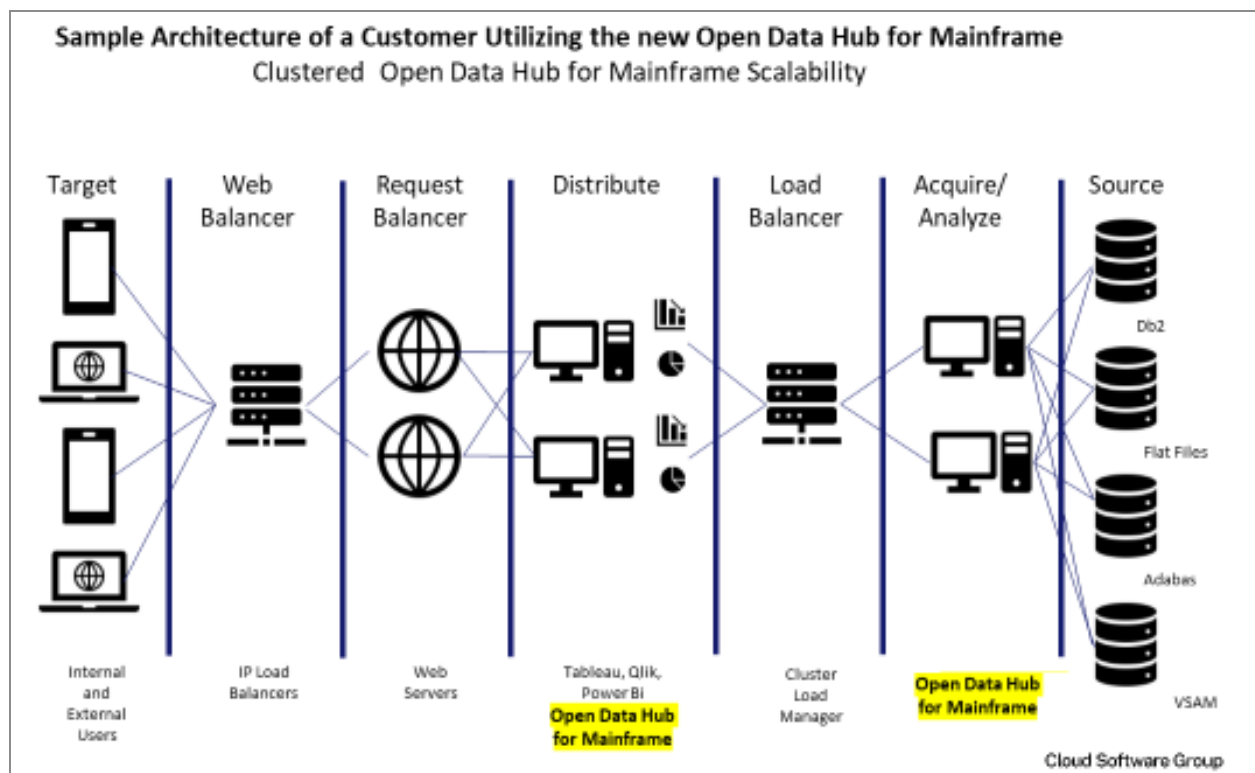
- **Resource usage reports.** See which users accessed which data sources.
- **Make it easy for end users.** Provide a native and single connection to trusted data with real-time access.
 - **JDBC and ODBC Connectors.** Connectors installed on each user machine to connect to an Open Data Hub for Mainframe Server natively within your BI platform.
 - **Direct pipes.** Direct connection to enterprise data sources ensures real-time access and no latency for users.
 - **Ready made and trusted data.** Since all data is curated within Open Data Hub for Mainframe, users can use the data as-is within their BI tool.

Open Data Hub for Mainframe Components

The following are the components of Open Data Hub for Mainframe:

- ODBC and JDBC Connectors to provide access to data from any visualization tool.
- Open Data Hub for Mainframe Server to provide web configuration for data virtualization, data preparation, usage reporting, and optimized SQL generation.
- Adapters to data sources to provide access to almost any database, column store, file, and web service.

The Open Data Hub for Mainframe architecture is shown in the following image.



Open Data Hub for Mainframe Users

The following are user types for Open Data Hub for Mainframe:

- **Business Analyst.** Uses an analytics or visualization tool, such as IBM® Cognos®, Qlik®, Tableau™, Microsoft Excel, and Microsoft Power BI. The ODBC and JDBC Connectors provide access to curated data sources.
- **Data Administrator.** Uses Open Data Hub for Mainframe to configure Adapters and connections to data sources. Creates metadata for tables and other data so they can be used by the Business Analyst. May also classify, augment, and secure data.

Open Data Hub for Mainframe ODBC Connector

The Open Data Hub for Mainframe ODBC Connector provides ODBC-enabled applications with transparent access to local and remote data sources.

What Is Open Database Connectivity?

Open Database Connectivity (ODBC) is the database access component of the Windows Open System Architecture (WOSA). It is a remote database specification based on the SQL Access Group (SAG) and the X/Open Call Level Interface specification.

The specification attempts to define all calls required for application interaction with a data source. The format of the call and expected data return for connect, query, define, and data manipulation are standardized. This enables front-end applications to access multiple, heterogeneous relational and non-relational DBMSs, while eliminating the need to develop a specific interface for each one.

What Is an ODBC Driver?

An ODBC driver represents the layer of software that maps the ODBC specification to proprietary API specification of the DBMS. These drivers are recognized and managed by the ODBC Driver Manager. Applications make database access calls to the Driver Manager, and the Driver Manager calls the appropriate ODBC driver.

To call the Driver Manager and to use the ODBC calls for the connection and retrieval of data, an application must be ODBC-compliant. Also, the ODBC drivers must conform to these calls. The drivers must return data and messages to the application, according to the ODBC specification.

ODBC Application Components

The following components are used when an ODBC application queries a data source:

- **ODBC API.** An open API designed to provide a standard set of calls that multiple applications can use to access remote data sources.
- **ODBC-enabled application.** An application that uses the ODBC API to access remote data. For example, Microsoft applications, such as Excel, or visualization tools, such as Cognos, Qlik, and Tableau.
- **ODBC Driver Manager.** Stores information on the installed ODBC drivers and the associated data source names. An ODBC-enabled application can request a list of drivers and available data sources from the Driver Manager. Once a connect request is made for a data source, the Driver Manager loads the relevant driver and passes the ODBC requests from the application to that driver. The ODBC Administration utilities are used to record information about drivers, data sources, and data source configurations. These utilities are also used to add new data sources.

Note: While Windows includes an ODBC Driver Manager, other operating systems require that you install one.

Open Data Hub for Mainframe ODBC Connector Components

The Open Data Hub for Mainframe ODBC Connector is an ODBC driver that provides access to a server. This driver receives incoming ODBC calls (requests) from an ODBC application through the Driver Manager. It converts the calls into the appropriate API commands. The SQL statement is sent to the server in the form passed from the application.

Installing the Open Data Hub for Mainframe ODBC Connector on Windows

The following procedures describe how to install and configure the Open Data Hub for Mainframe ODBC Connector on Windows platforms.

Installing and Configuring the Open Data Hub for Mainframe ODBC Connector on Windows

The following procedures describe how to install, configure, test, and enable traces for the Open Data Hub ODBC Connector on Windows.

Install and Configure the Open Data Hub for Mainframe ODBC Connector on Windows

Procedure

1. Exit all programs before continuing.
2. Execute the following executable from the location in which you extracted the software (IBI_odh-mf-cnct_1.x.x_windows.zip):

```
setup_odbc_client.exe
```

i Note: If a User Access Control (UAC) security prompt appears, click **yes**.

The Choose Setup Language window opens.

3. Select the language to be used during installation and click **Next**.

The License Agreement window opens.

4. Read the License Agreement and click **Yes** to accept the terms.

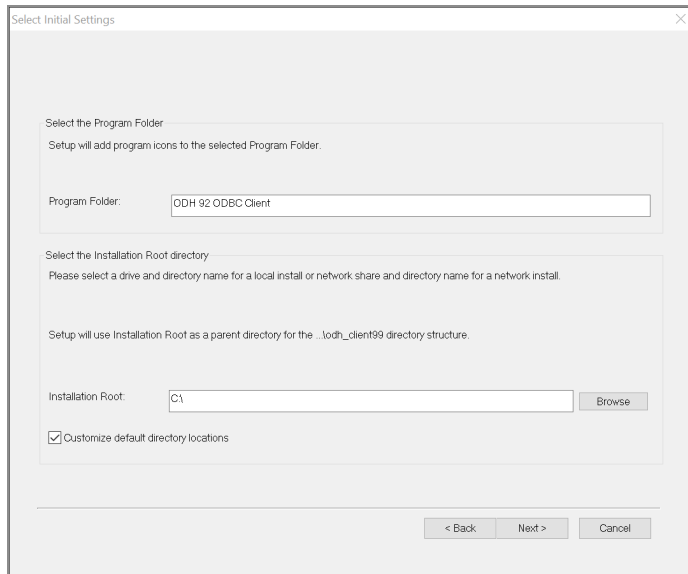
If a prior installation was found, the Prior Installs Found: Choose an Action window opens.

You can choose to upgrade a selected installation or to create a new installation.

If you choose to create a new installation/configuration, choose between a new installation or adding a configuration. If *add configuration* is chosen, the software is not installed, but the highlighted entry from the prior screen is used as a base for adding an additional configuration. Choosing a new installation gives a separate complete new installation and initial configuration, but in this instance, and when adding a new configuration, it is appropriate to not use the default installation paths and server name to avoid overwriting a prior installation or configuration location.

5. Click **Next**.

The Select Initial Settings dialog box opens, as shown in the following image.

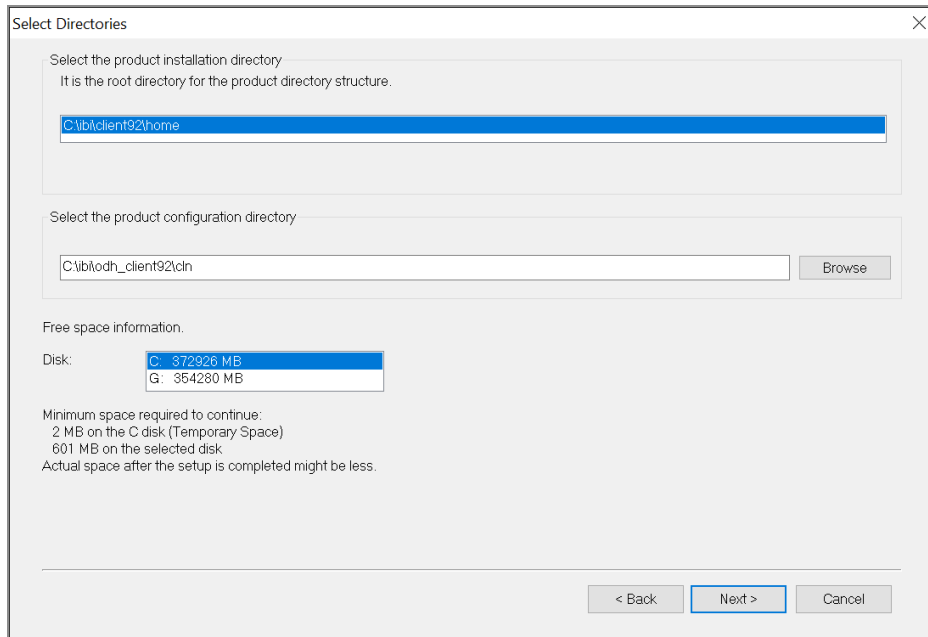


6. You can accept the default values or edit the following settings.

- **Program Folder.** By default, this is named **ODH 92 ODBC Client**.
- **Installation Root.** By default, this is C:\. You can browse to or type another location.
- **Customize default directory locations.** Select this check box if you want to customize the directory locations. For example, if you are configuring an additional instance of the server, some of the locations, such as EDAHOME and EDACONF, must be customized. One way to customize the directories is to just use a different installation root and keep the default location names under that root.

7. Click **Next**.

If you selected this checkbox to customize the default directories, the Select Directories dialog opens, as shown in the following image.



8. Specify the following locations, or accept the default values:

- a. **Product installation directory.** This contains the executable files. This location is referred to as EDACONF. It must conform to the pattern:

```
C:\ibi\client9x\home
```

If you are performing a new installation, accept the default directory, or specify a different directory. The new software will be placed in this directory.

If you are configuring an additional instance, using your existing software, accept the default EDACONF directory. If several 9x installation directories exist, select the one that corresponds to the software home directory for which you are configuring a new instance.

- b. **Product configuration directory.** This contains configuration information for the instance. This location is referred to as EDACONF.

If you changed the EDACONF value, the default EDACONF value changes to conform to EDACONF.

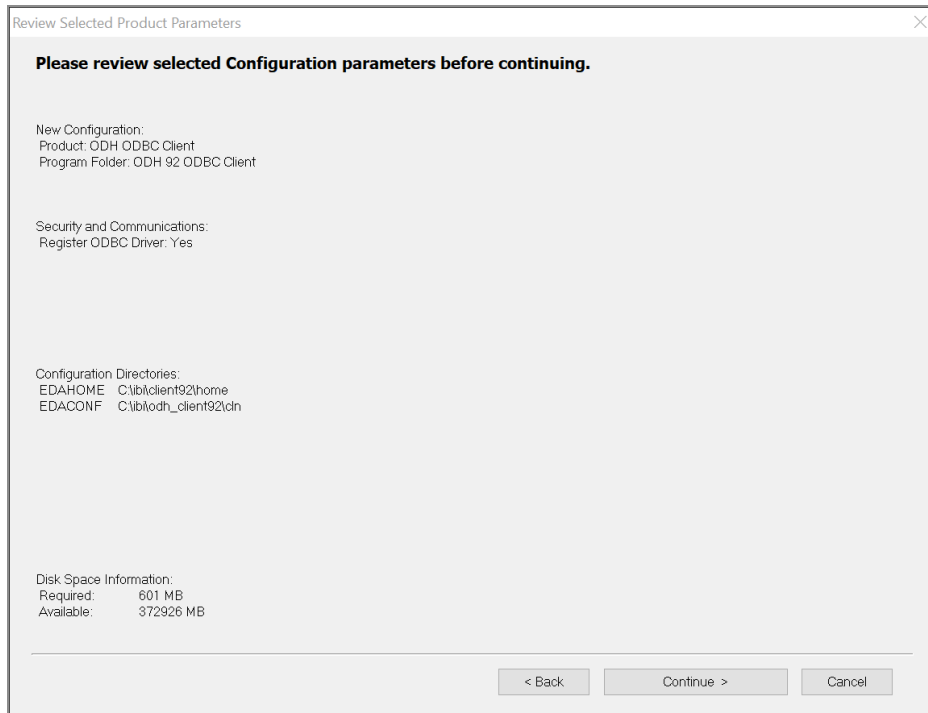
For example:

```
C:\ibi\client9x\cln
```

Accept the default value, or click **Browse**, or type a name to specify a different directory.

9. Click **Next**.

The review selected Configuration parameters dialog box opens showing all of the selections you have made, as shown in the following image.



On the Review Selected Product Parameters dialog box, ensure that the Register ODBC Driver parameter is set to Yes.

10. Click **Continue**.

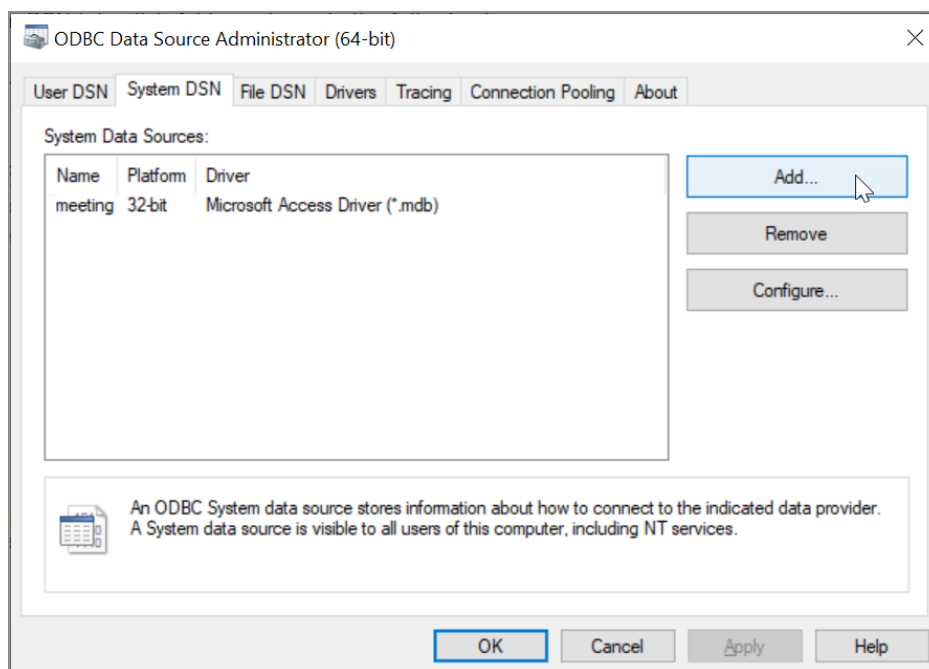
11. When the setup is complete, click **Finish**.

Add Data Sources on Windows

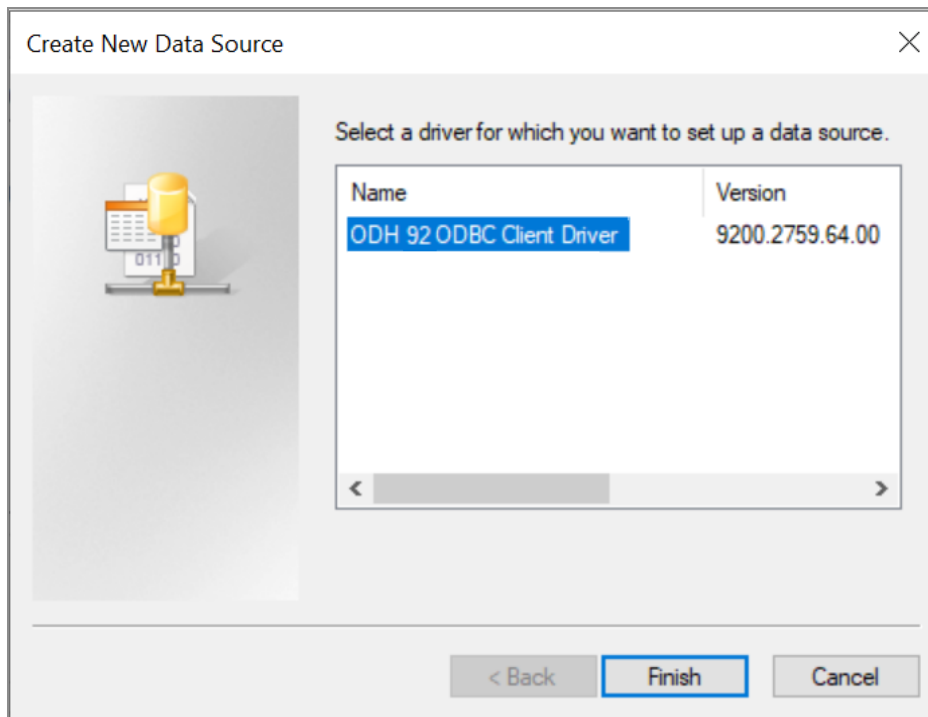
You can add data sources from the Connector after installation is completed.

Procedure

1. From the Start menu, type **ODBC** in the search box.
2. Select **ODBC Data Sources (64-bit)**.
The ODBC Data Source Administrator (64-bit) dialog opens.
3. Select the **System DSN** tab.
4. From the System DSN tab, click **Add**, as shown in the following image.



The **Create New Data Source** dialog opens, as shown in the following image.



5. Select **ODH 92 ODBC Client Driver** and click **Finish**.

The ibi ODBC Driver Configuration dialog opens, as shown in the following image.

ibi™ ODBC Driver Configuration

ODBC Connector

Connection Parameters

Data Source Name:

Description:

TCP/IP Server: Port:

Security: Explicit ▾ Test

User:

Password:

Advanced >> OK Cancel

6. Enter the following information:

Data Source Name. Type a name for the server. The default value is IBISERVE.

Description. Type a description for the server.

TCP/IP Server. Type the host name for the Open Data Hub for Mainframe Server. This can be a name on your system, a fully-qualified domain name, or an IPv4 address.

Port. Type the TCP Port Number. This number is one less than the port number used to connect to the server from a web browser. The default value is 8120, other common values are 8100 and 8116. It must be the port number that the Open Data Hub for Mainframe Server is listening on. Contact your server administrator if you do not know this number.

Security. Select *Explicit* to indicate that the user ID and password are explicitly specified for each connection to the Open Data Hub for Mainframe Server at connection time, for authentication. Select *Kerberos* to indicate that the Kerberos

security protocol authenticates the service requests between two or more trusted hosts across an untrusted network.

User and Password. Optionally, type a user ID and Password to connect to the server. Some ODBC Client tools may use these credentials to connect to the server.

Note: The ODBC Driver Manager stores credentials in the Windows Registry in plain text, so do not enter a password if your PC is not secured.

7. Optionally, you can test your connection by clicking **Test**. You should receive a "Connection Succeeded" message. If not, correct your entries and try again.
8. Click **OK** to save your connection.

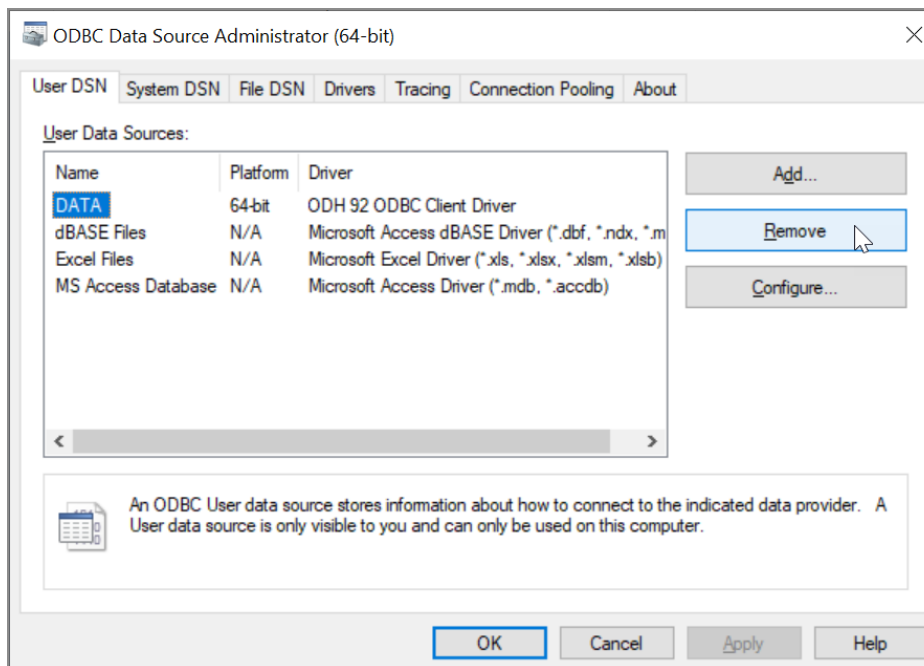
Note: You can click **Advanced** to specify advanced settings for the connection. For more information, see [Set Advanced Options for Data Sources](#).

Remove Data Sources on Windows

You can remove data sources from the Connector after installation is completed.

Procedure

1. From the Start menu, type **ODBC** in the search box.
2. Select **ODBC Data Sources (64-bit)**.
The ODBC Data Source Administrator (64-bit) dialog opens.
3. Select the **System DSN** tab.
4. From the System DSN tab, select the System data source to which you want to add a data source and click **Remove**, as shown in the following image.

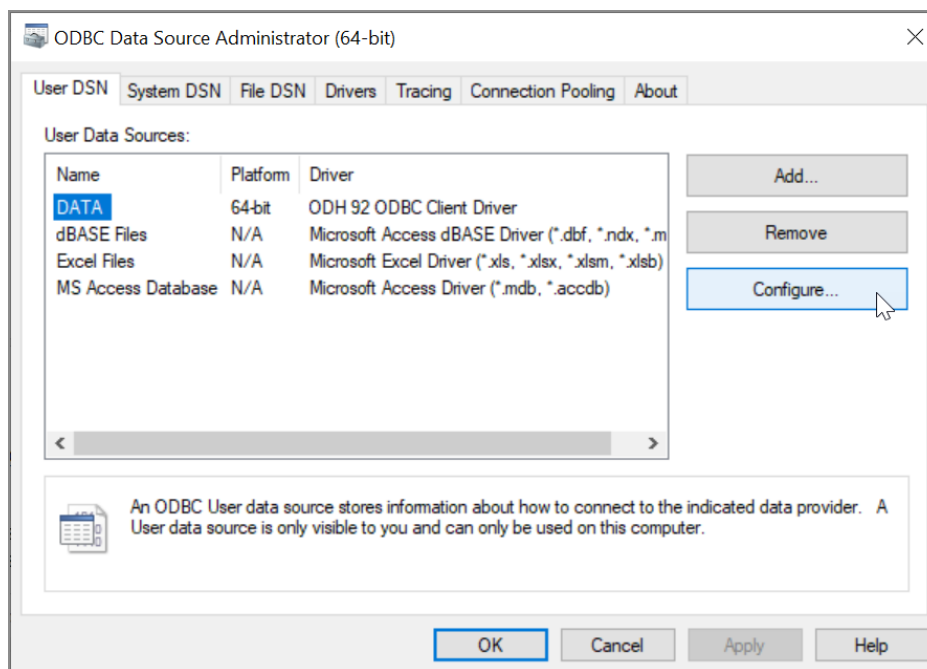


Configure Data Sources on Windows

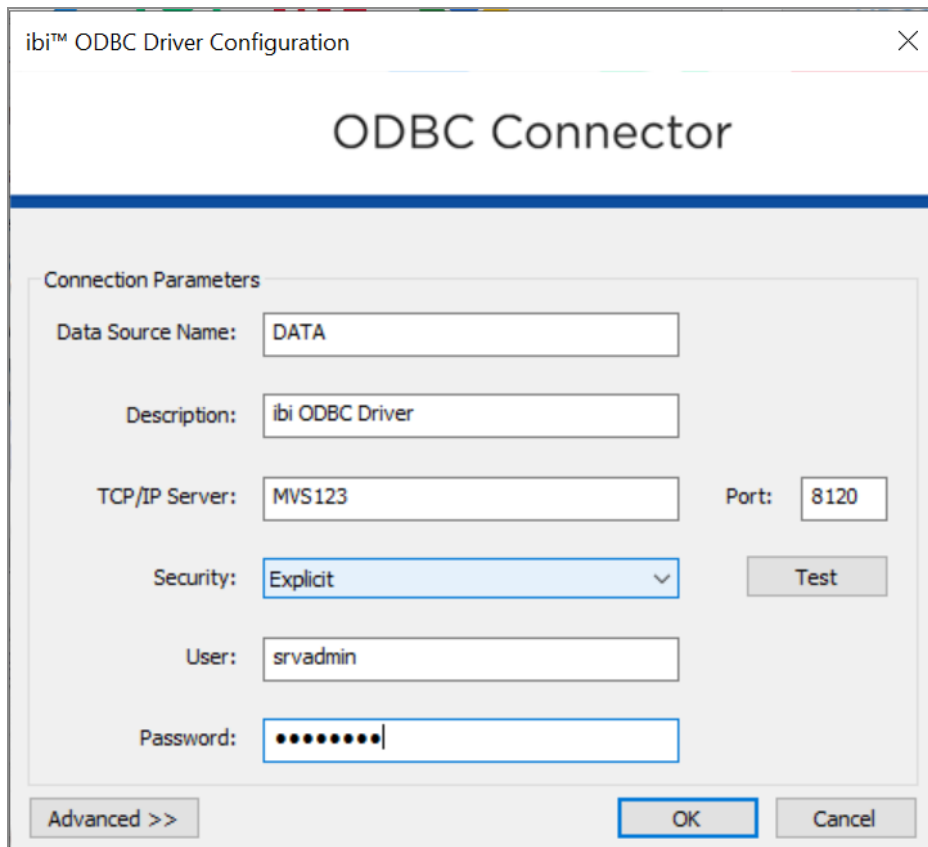
You can configure data sources from the Connector, if you need to change any of the parameters.

Procedure

1. From the Start menu, type **ODBC** in the search box.
2. Select **ODBC Data Sources (64-bit)**.
The ODBC Data Source Administrator (64-bit) dialog opens.
3. Select the **System DSN** tab.
4. From the System DSN tab, select the System data source to which you want to add a data source and click **Configure**, as shown in the following image.



The ibi ODBC Driver Configuration dialog opens, as shown in the following image.



The screenshot shows the 'ibi™ ODBC Driver Configuration' window. The title bar includes the text 'ibi™ ODBC Driver Configuration' and a close button. The main heading is 'ODBC Connector'. Below this is a section titled 'Connection Parameters' which contains several input fields: 'Data Source Name' with the value 'DATA', 'Description' with 'ibi ODBC Driver', 'TCP/IP Server' with 'MVS123', 'Port' with '8120', 'Security' with a dropdown menu set to 'Explicit', 'User' with 'srvadmin', and 'Password' with masked characters. A 'Test' button is located to the right of the 'Security' dropdown. At the bottom of the window are three buttons: 'Advanced >>', 'OK', and 'Cancel'.

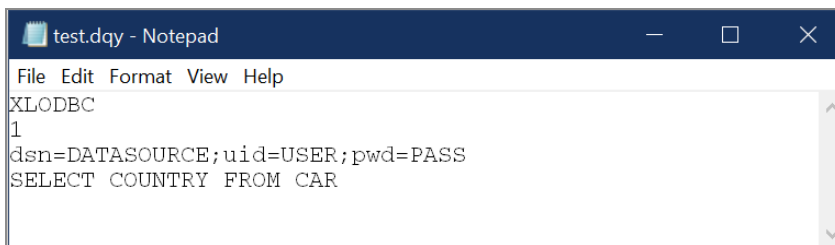
5. Make any necessary changes or add new information as needed, and then click **OK**. For more information, see [Add Data Sources on Windows](#).

Test the ODBC Driver With Microsoft Excel

If you have Microsoft Excel installed on your Windows PC, you can also test the ODBC Driver using the following procedure.

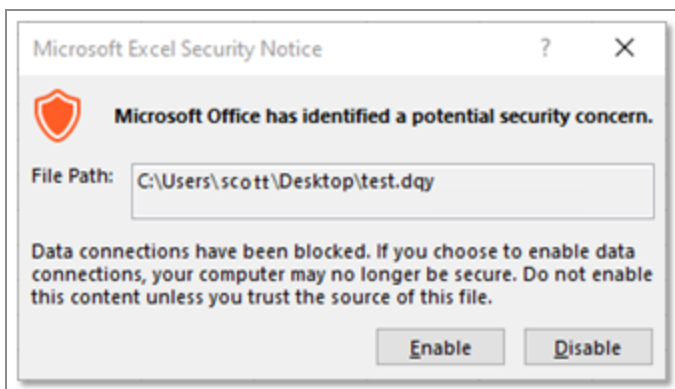
Procedure

1. Create a text file with a .dqy extension. Include your DATASOURCE, USER, and PASS values, in addition to your SQL request, as shown in the following image.



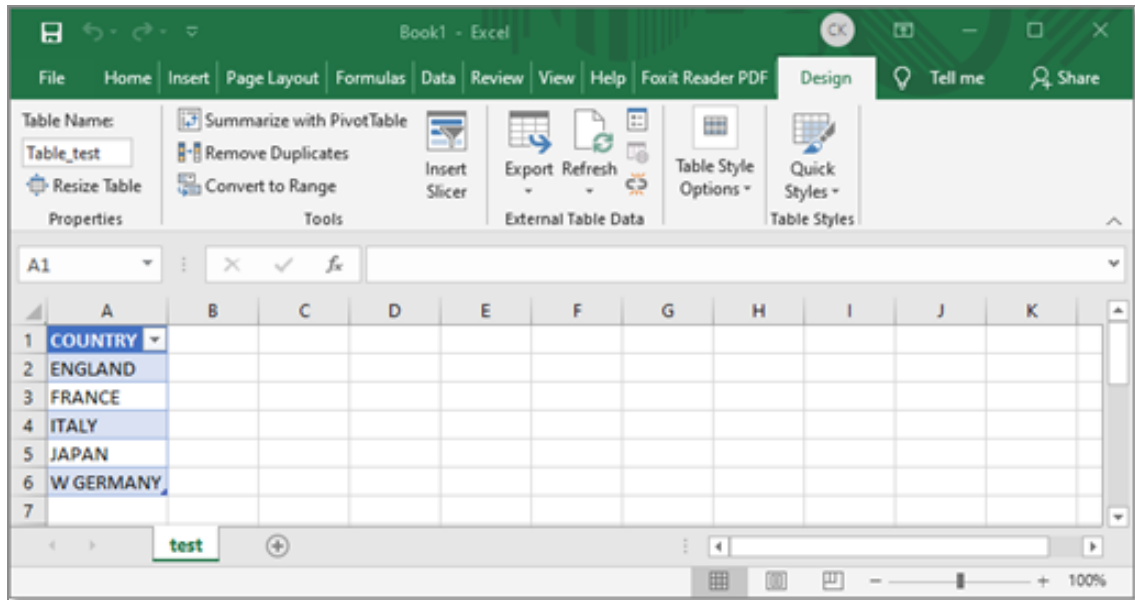
Note: Replace the SELECT COUNTRY FROM CAR statement with a SELECT statement for a table that exists on your server.

2. Save the file.
3. Double-click the file to run.
4. On the Security Notice dialog, click **Enable**, as shown in the following image.



5. If the server has security enabled, type the user ID and password to connect and click **OK**.

The values from the SQL request display, as shown in the following image.

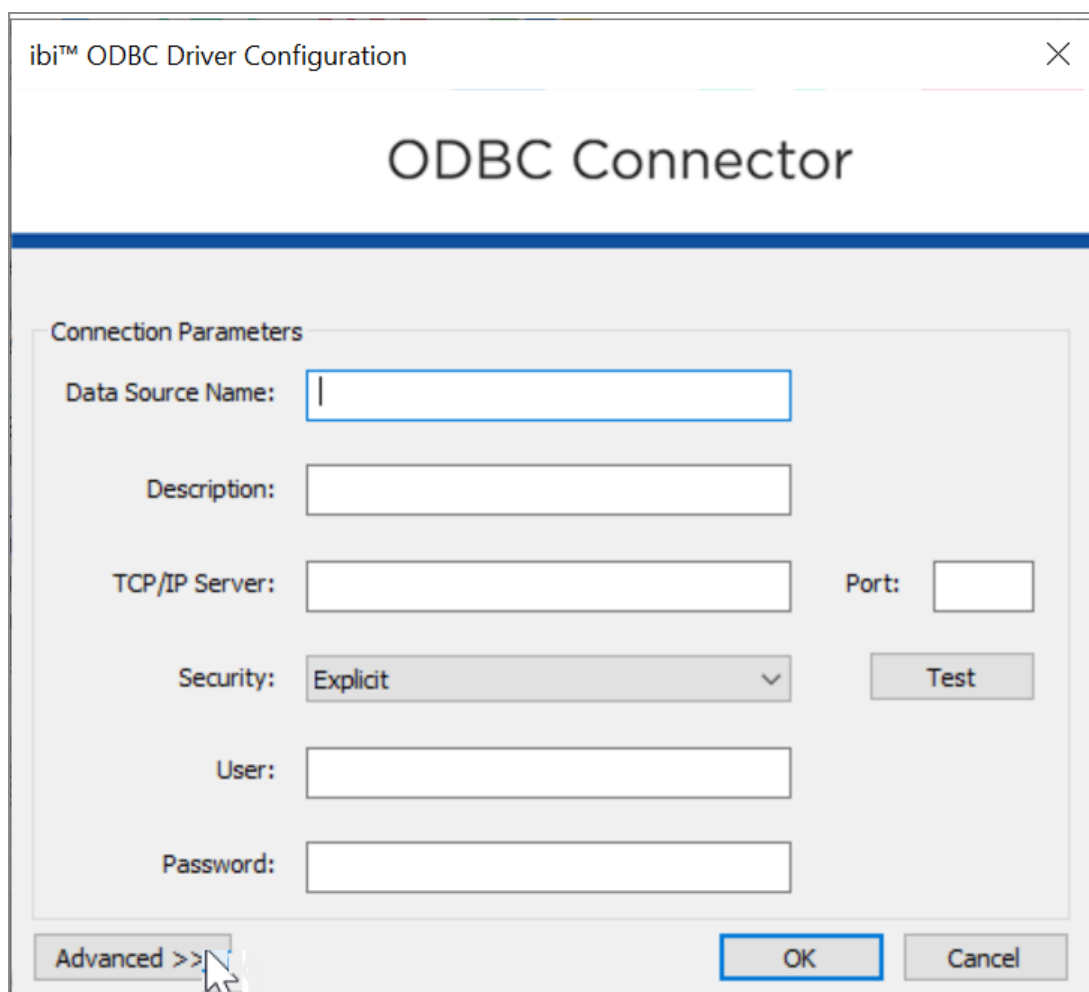


Set Advanced Options for Data Sources

The ODBC Connector environment can be configured from the ODBC Administrator on the Advanced panel.

Procedure

1. To access the advanced settings, click **Advanced**, as shown in the following image.



The Data source and Global settings options appear, as shown in the following image.

The screenshot shows a 'Data source' configuration window. It contains the following elements:

- Data source section:**
 - Service:** A text input field.
 - Schemas:** A dropdown menu with a downward arrow.
 - Cluster connection:** A checkbox.
 - Cluster Name (optional):** A text input field.
- Global section:**
 - Enable tracing:** A checked checkbox.
- Buttons:** 'Advanced <<' (highlighted with a blue border), 'OK', and 'Cancel'.

2. In the Data source settings section:

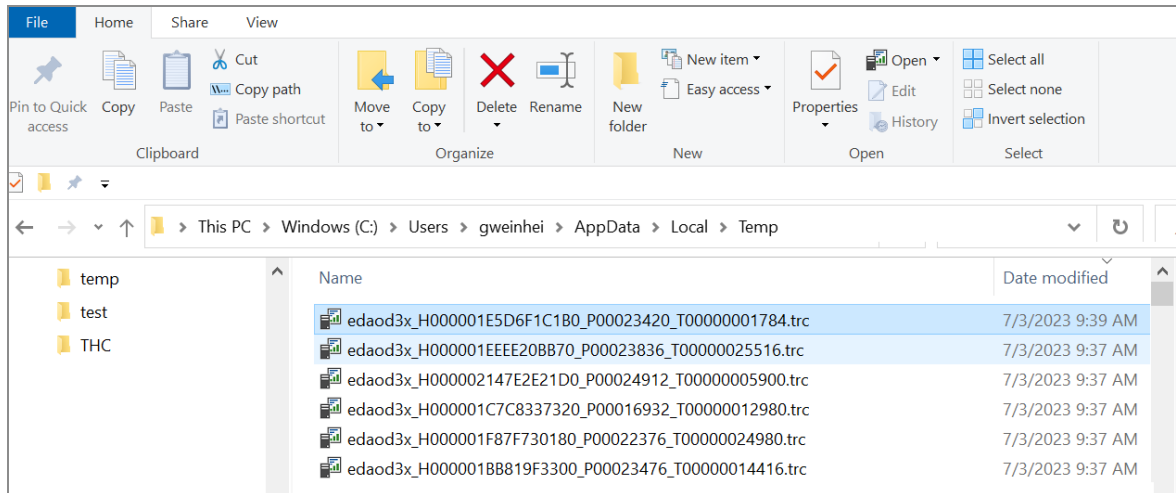
- **Service.** Type the Service name of a configured service on your reporting server, which may be the server included in Open Data Hub for Mainframe or an ibi™ WebFOCUS® Reporting Server. When multiple services are configured on your reporting server, you can specify the server to connect to for each DSN.

i Note: Service names are case sensitive.

- **Schemas.** From the drop-down menu, select **Folders** to indicate that the application folder names on the server should be used or select **EDADBA** to indicate that the name EDADBA should be used.
- **Cluster connection.** Select this check box to access data from multiple Open Data Hub for Mainframe Servers combined in clusters using the ODBC or JDBC connection.
- **Cluster Name (optional).** Type the name of the cluster on the Open Data Hub for Mainframe Server. In this case, the Data Source Name on the Configuration screen should be a node name of a cluster from the `odin.cfg` CLM to which you are connecting.

i Note: By default, for Microsoft Excel, Microsoft Power BI, and Tableau, the default application folder names on the server are used. For other applications, the name EDADBA is used.

3. In the Global settings section, which applies to all connections, select the **Enable tracing** checkbox if you want to enable tracing. When enabled, trace files are written to the user's %TEMP% directory, as shown in the following image.



Installation for z/OS

The unified software for z/OS provides a choice of deployment environments, either:

- z/OS Distributed File Service zSeries File System (ZFS) files on UNIX System Services.
- Partitioned data set (PDS) libraries.

To compare their benefits, see [Choosing How to Deploy](#).

Information You Need Prior to Installation on z/OS

The Open Data Hub for Mainframe server is installed by downloading the installation file from the eDelivery site at:

<https://edelivery.tibco.com/storefront/index.ep>

Once the desired file is downloaded, and if necessary, transferred to the actual machine where the installation will occur and into a temporary working directory, untar the .tar file.

More specifically, change directory (cd) to the temporary directory and issue the following command, where the actual .tar file name is the full file name that was downloaded.

```
tar -xvf IBI_wf-rs_*.tar
```

After extraction, proceed with the instructions in the following topics.

The process for a full download is similar. A main directory is created on the desktop with multiple directories and subdirectories. Simply find the applicable IBI_wf-rs_*.tar file from the download, transfer, and extract, as previously noted.

You need a server administrator user ID, referred to as *iadmin* in the remainder of this chapter.

- The operating system ID you use when installing the server owns the server files and is the default server administrator for OPSYS mode. You can create a new operating

system ID to run and own the server files, or use any ordinary (non-superuser) ID. However, you should not install the server as root.

The server has an email notification feature that requires SMTP mail server information. You can enter these parameters either during installation, or later using the WebFOCUS® Reporting Server browser interface Administration tool.

z/OS Installation Requirements

Before you install, review the following requirements.

Type	Description
Operating System	<p>z/OS 2.1 or higher</p> <p>The <i>ibi™ Release Notes</i> maintains a current list of supported operating systems and levels.</p>
Disk Space	<p>For USS Deployment, approximately 6 GB, however, about double the space is needed during installation.</p> <p>For PDS Deployment, approximately 1555 cylinders of 3390 disk for HOME data sets.</p>
IP Ports	<p>Up to six consecutive IP ports (two in reserve for typical extra features).</p> <p>Additional Java Listeners (post-installation option) require additional ports (beyond basic reserve).</p>
Java	<p>Java JRE or Java SDK (also known as JDK) 8 or higher.</p> <p>Used for Java-based adapters, server-side graphics, XBRL, or user-written CALLJAVA applications. For additional information, see JVM Requirements for Java Services (Server Installations Only).</p> <p>Note: Java 8 and Java 11 are explicitly tested and certified to be compatible with Open Data Hub for Mainframe. Other Java releases may be compatible with the Open Data Hub for Mainframe. If you use an untested Java release, you must self-certify its compatibility with the Open Data Hub for Mainframe and accept responsibility for using an untested release.</p>

Type	Description
Memory	Per Agent 20 MB
Common framework plus per agent memory.	Common Framework 500 MB
Web Browser	<p>Needed for using the WebFOCUS Reporting Server browser interface.</p> <p>Microsoft Edge</p> <p>Mozilla Firefox® 59 or higher.</p> <p>Google Chrome® 65 or higher.</p>

JVM Requirements for Java Services (Server Installations Only)

The minimum Java JVM release level is 8 or higher, due to required internal components of the server. As already noted, only Java release 8 and release 11 are explicitly tested, and use of any other release must be self-certified by the customer if they choose to not use release 8 or release 11. The Java Listener will not start properly (and will show errors in the edaprint.log file) if 8 (or higher) is not in use.

When a server starts, it adds search directories based on JDK_HOME or JAVA_HOME variables. If JVM is found with the correct bit size and level (8+), the Java Listener will start, send a *start* message to the edaprint.log file, and no further configuration is needed.

If JVM loading fails, the server will start, but should be corrected by setting JDK_HOME or JAVA_HOME to a respective home directory for a Java that matches the required bit size and release level. If both values are declared, JDK_HOME will be used. Set the environment variable in the server EDAENV environment file.

For example:

```
JDK_HOME=/usr/java/64/jdk1.8.0_381
```

Installation for ZFS and PDS

Before installing, read the topics in this section for:

- Guidance on choosing how to deploy on ZFS in UNIX System Services or PDS.
- Configuration information common to both deployments, such as the location of different types of server files.
- An overview of which steps you will need to perform to install your server.

Choosing How to Deploy

z/OS provides you with the following deployment environment: a choice of deployment environments. You can deploy using either:

- **The z/OS File System (ZFS)** on UNIX System Services (USS). The ZFS-deployed software stores executable code and user data on the ZFS. Security is provided by UNIX file security and by your z/OS security package, such as RACF, eTrust CA-Top Secret®, or eTrust CA-ACF2®. You install from ISPF and start it using JCL. All other processes occur under USS.
- **Partitioned data sets (PDS)** which deploys software in partitioned data sets. The PDS-deployed software provides most features of the ZFS-deployed software, but removes the requirement for interaction with UNIX System Services at installation time and run time. Administration of the software, from a systems perspective, has been streamlined to match that of the classic MVS version of the server (also known as the SSCTL server).

The PDS deployment environment is designed to support legacy applications and features. New server features that require some ZFS footprint, such as .xlsx support, file uploads, and the stress tool on the WebFOCUS Reporting Server browser interface, will not be available.

To take advantage of these features, you can either deploy the ZFS version or, alternatively, have a mixed environment, where you create a PDS instance for your legacy applications, and have a small ZFS instance just for the administrator to access the WebFOCUS Reporting Server browser interface features missing in PDS. Both server instances can have a shared mapped application to exchange data seamlessly.

The following table compares the benefits of each way of deploying on z/OS.

Feature	ZFS / USS	PDS
File Management: Server run-time and configuration files	In the UNIX ZFS file system.	In partitioned data sets (PDSs).
File Management: User data, metadata, and procedures	In the UNIX ZFS and, optionally, in a PDS.	In a PDS and, optionally, in the UNIX ZFS.
Security	<p>Standard security packages are supported (RACF, eTrust, CA-ACF2®, and eTrust CA-Top Secret).</p> <p>All directories and files must have their user/group/world attributes correctly set.</p> <p>A user ID with a UID of 0 (that is, a superuser) is required when running the server with security set to OPSYS or a special UNIXPRIV user ID can be used.</p>	<p>Standard security packages are supported (RACF, eTrust CA-ACF2, and eTrust CA-Top Secret). No additional security is required.</p>
User IDs	<p>A UID of 0 (that is, a superuser) can install, but not administer or connect to, the server.</p> <p>Each user ID that will install, administer, or connect to the server requires a ZFS segment with sufficient space and appropriate file permissions for</p>	<p>Any user ID can install, administer, and connect to the server.</p>

Feature	ZFS / USS	PDS
	the tasks that the ID will perform.	
Adapters	Use a mixture of USS-based and MVS-based libraries/APIs.	Use MVS-based libraries/APIs. The exception is DBMSs that support only USS-based libraries/APIs, such as Db2 CLI and Java-based adapters, such as Microsoft SQL Server, which use vendor libraries/APIs residing in the hierarchical file system.
Traces and Server Log	Accessible from the WebFOCUS Reporting Server browser interface.	These are available on the JES output of the server job.
WebFOCUS Reporting Server browser interface Stress Tool	Available from the WebFOCUS Reporting Server browser interface.	Feature not available.
Format XLSX and PPTX	Supported	Not Supported Note: As a workaround, you can SET EXCELSERVURL to point to a ibi™ WebFOCUS® apps context root.
Adobe Flex	Supported	Not Supported
RACF TEMPDSN class	Supported	Supported, except for the FOCCACHE app.
DFM reports stored in approot app	Supported	Not Supported Use standard DFM data sets instead.
Native ! (bang)	Supported	Not Supported

Feature	ZFS / USS	PDS
USS Operating System commands in applications		
Adapter Flat File via FTP Server	Supported	Not Supported
WebFOCUS Reporting Server browser interface Upload file tool	Supported	Not Supported

PDS deployment also requires each user of the server to be identified to USS by means of a default segment definition. For more information, see [Security Providers](#).

File Locations

The software includes several groups of files used for installation, configuration, and administration. These groups are implemented differently in USS and PDS deployments:

- **Supplied files (EDAHOME)**, which contains programs and related files. For more information, see [Supplied Files Location \(EDAHOME\)](#).
- **Configuration (EDACONF)**, which contains the files that control the behavior of each configured instance. For more information, see [Configuration Files Location \(EDACONF\)](#).
- **Applications (APPROOT)**, which is the default location for storing applications. For more information, see [Application Files Location \(APPROOT\)](#).
- **Profiles**, which contains user and group profiles. For more information, see [Profile Files Location](#).
- **Administration**, which includes a file that specifies server administrators. For more information, see [Administration Files Location](#).

Supplied Files Location (EDAHOME)

The programs and related files are stored in a location referred to as EDAHOME. The installation process copies the software into EDAHOME.

- In **USS** deployment, EDAHOME defaults to the following directory and several subdirectories:

```
ibi/srv/home
```

- In **PDS** deployment, EDAHOME defaults to the following partitioned data sets:

```
high_level_qualifier.P.HOME.WFS
```

where:

high_level_qualifier

Is the high-level qualifier for HOME.DATA and for all other data sets that the installation procedure allocates. We recommend that the high-level qualifier reflect the release of the software (for example, IADMIN.SRV). However, you can use any site-specific value.

component_type

Designates the type of server component. The values are:

Type of Component	Description
ETC	Script and text files.
BIN	Binary-based object files.
ACX	Server Access Files.

Type of Component	Description
MAS	Server Master Files.
FEX	Server procedure (FOCEXEC) files.
ERR	Error files.
LOAD	Load library.

Configuration Files Location (EDACONF)

The configuration files are stored in a location referred to as EDACONF. Each configured instance has its own EDACONF, which controls the behavior of that instance.

- In **USS** deployment, EDACONF defaults to the following directory and several subdirectories:

```
ibi/srv/wfs
```

- In **PDS** deployment, EDACONF defaults to the following partitioned data sets:

```
high_level_qualifier.WFS.CONF.config_type
```

where:

high_level_qualifier

Is the high-level qualifier for HOME.DATA and for all other data sets that the installation procedure allocates. We recommend that the high-level qualifier reflect the release of the software (for example, IADMIN.SRV). However, you can use any site-specific value.

config_type

Designates the type of configuration file.

The primary configuration file is CFG.

The WebFOCUS Reporting Server deferred execution configuration files are DEL, RPE, RPF, RPO, RQD, RQF, RQO, and RQP.

Profile Files Location

Server profiles are stored in the following location:

- In **USS** deployment, the location is specified in the environment variable EDAPRFU, and defaults to the following directory:

```
ibi\profiles
```

- In **PDS** deployment, the location is the following partitioned data set

```
high_level_qualifier.WFS.CONF.PRF
```

where:

high_level_qualifier

Is the high-level qualifier for HOME.DATA and for all other data sets that the installation procedure allocates. We recommend that the high-level qualifier reflect the release of the software (for example, IADMIN.SRV92). However, you can use any site-specific value.

This PDS is allocated in ddname EDAPROF in the server JCL.

Administration Files Location

The file that specifies server administrators is located in:

- In **USS** deployment, the location is specified in the environment variable EDAPRFU, and defaults to the following directory:

```
ibi\profiles
```

- In **PDS** deployment, the location is member ADMIN of the following partitioned data set

```
high_level_qualifier.WFS.CONF.CFG
```

where:

high_level_qualifier

Is the high-level qualifier for HOME.DATA and for all other data sets that the installation procedure allocates. We recommend that the high-level qualifier reflect the release of the software (for example, IADMIN.SRV92). However, you can use any site-specific value.

This PDS is allocated to ddname EDACFG in the server JCL.

Application Files Location (APPROOT)

The server application files are stored in a location referred to as APPROOT. APPROOT may be shared by multiple applications.

- In **USS** deployment, APPROOT defaults to the following directory:

```
ibi/apps
```

- In **PDS** deployment, APPROOT defaults to the following partitioned data sets:

```
approot.appname.type.DATA
```

where:

approot

Designates the root qualifier for the server applications.

appname

Designates the name of the application. There will be one *appname* qualifier for each application.

type

Designates the type of application component. The values are:

Type	Description
ACCESS	Access Files.
ETG	ibi™ Data Migrator flow information.
FOCEXEC	Procedure files.
FTM	Temporary files.
GIF	Image files (both GIF and JPG).
HTML	HTML files.
MAINTAIN	Maintain files.
MASTER	Master Files.
WINFORMS	Forms.
DTD	XML DTD files.

Type	Description
FOCCOMP	FOCCOMP files.
FOCSTYLE	Stylesheet files.
SQL	SQL files.
XML	XML files.
XSD	XML XSD files.
FOCUS	ibi™ FOCUS® data files.

Two applications are generated automatically during installation: IBISAMP and BASEAPP, a default application space.

Step-By-Step Installation Overview

The installation process differs somewhat, depending on how you are deploying the software for z/OS. To deploy using:

- **ZFS/USS:**

1. Installation Requirements for HFS
2. Installing New on HFS
3. Starting and Stopping a Server for HFS
4. DB2 Security Exit Configuration for HFS
5. MSODDX for DD Translation for User Subroutines

6. Overriding the Time Zone Setting
7. Adding a Configuration Instance for HFS
8. Upgrading Your Server Release for HFS
9. Performance Considerations for HFS
10. General Information for a z/OS HFS Installation
11. Troubleshooting for HFS

- **PDS:**

1. Installation Requirements for PDS
2. Installing a New Server for PDS
3. Starting and Stopping a Server for PDS
4. DB2 Security Exit Configuration for PDS
5. MSODDX: DDNAME Translation for User Subroutines
6. Overriding the Time Zone Setting
7. Adding a Configuration Instance for PDS
8. Upgrading Your Server Release for PDS
9. Performance Considerations for PDS
10. General Information for a z/OS PDS Installation
11. Troubleshooting for PDS

ZFS/USS Deployment Installation Details

The topics in this section describe how to install your software in a ZFS environment on UNIX System Services.

Installing New on ZFS

To install on z/OS deployed using the ZFS File System and UNIX System Services (USS), perform the following steps.

Set Up User IDs

To install and run the software, the following types of user IDs are required:

- Server installation ID (*iinstal*).
- OPSYS server administrator ID (*iadmin*).
- PTH administrator ID (*srvadmin*).
- Server system ID (*iserver*).
- General IDs (for connecting users).

The number of IDs and their names depend on the needs and configuration of your site.

Software Installation ID (*iinstal*)

An ID is required to unload the software installation from tape and to create PDSs and ZFS directories. Many sites already have a suitable ID that they use for installing vendor software.

The sample ID name *iinstal* is used throughout the installation procedure to refer to this ID, but you can choose any name. (We have omitted the second "l" from "install" due to a seven-character length restriction in some RACF and eTrust CA-Top Secret® environments.) To define *iinstal*, see [Define the Software Installation ID](#).

OPSYS Server Administrator ID (*iadmin*)

An ID is required to administer the server. It owns and has full access to server files installed in the ZFS directory that you specify during installation. This ID should be available only to users who require administrative server privileges such as :

- Starting and stopping the server
- Adding adapters
- Changing run-time parameters

The sample ID name *iadmin* and group *isrvgrp* are used throughout the installation procedure to refer to this ID, but you can choose any names.

To define *iadmin*, if you are using:

- **RACF**, see [Define the OPSYS Administrator ID With RACF](#).
- **CA-ACF2**, see [Define the OPSYS Administrator ID With CA-ACF2](#).
- **CA-Top Secret**, see [Define the OPSYS Administrator ID With CA-Top Secret](#).

PTH Administrator ID

An ID is required to administer the server immediately after initial installation. This ID is defined and maintained solely in the realm of the server.

For more information about running the server in secure mode, see [Configure Security](#).

ibi WebFOCUS Reporting Server System ID (iserver)

If you plan to run the server with security provider OPSYS, you must create a user ID for internal use by the server. The server will use this server system ID when it needs superuser privileges. For example, it will use it to impersonate a connected user when the server agent is created.

This ID does not need TSO logon privileges. All IDs require an OMVS segment. Be sure never to delete this ID. Doing so would cause server administration problems.

The sample ID name *iserver* is used throughout the installation procedure to refer to this ID, but you can choose any name.

You can define this server system ID as either:

- **A superuser ID.** This is an ID whose security definition specifies UID(0), authorizing it to perform all z/OS UNIX functions without restriction.

To define *iserver* using a superuser ID, if you are using:

RACF, see [Define the System User ID With RACF](#).

CA-ACF2, see [Define the System User ID With CA-ACF2](#).

CA-Top Secret, see [Define the System User ID With CA-Top Secret](#).

- **An ID employing profiles with UNIXPRIV for authorization**, which is necessary for certain superuser privileges.

By granting limited superuser privileges with a high degree of granularity to an ID that does not have superuser authority, you minimize the number of assignments of superuser authority at your installation and reduce your security risk.

This is supported for sites using RACF, eTrust CA-ACF2®, and eTrust CA-Top Secret. Note that global access checking is not used for authorization checking to UNIXPRIV resources.

To define the iserver using UNIXPRIV profiles, see [Define the System User ID With UNIXPRIV Profiles](#).

General IDs (for Connecting Users)

Any user requiring access to the server must have a non-superuser ID (that is, it must have a unique UID other than 0) and have an OMVS segment. For information about this, see [Add the OMVS Segment to General User IDs](#).

User ID Installation Scenarios

There are two user ID installation scenarios:

- **Installation and administrator IDs are the same.**

The user ID must have a unique non-zero UID. It cannot be a superuser. For this scenario, logon to TSO with this ID and do not change the default administrator ID that is presented on the first full panel of the ISETUP installation process.

- **Installation and administrator IDs are different.**

The *installation ID* can be a superuser or non-superuser, and must have authority over the administrator ID so that it can change ownership of the server directory structure from the installation ID to the administrator ID. The command issued during the installation process to change ownership is shown.

The *administrator ID* must have a unique non-0 UID. It cannot be a superuser.

Define the Software Installation ID

When defining the software installation ID:

- The installation ID requires read access to the BPX.FILEATTR.APF facility class.
- The installation ID requires an OMVS segment.
- The installation ID can be any existing user ID. If it is the same as the administrator ID (iadmin), see one of the following topics for a sample definition. If you are using:

- **RACF**, see [Define the OPSYS Administrator ID With RACF](#).
- **CA-ACF2**, see [Define the OPSYS Administrator ID With CA-ACF2](#).
- **CA-Top Secret**, see [Define the OPSYS Administrator ID With CA-Top Secret](#).

Define the OPSYS Administrator ID With RACF

The server administrator ID requires an OMVS segment.

To define the server administrator ID with RACF:

1. Have the Security Administrator issue the following RACF commands:

```
ADDUSER iadmin PASSW(XXXX)

DFLTGRP(ISRVGRP)

OMVS(UID(8) HOME('/u/iadmin') PROGRAM('/bin/sh'))

TSO(ACCTNUM(12345) PROC(PROC01))
```

2. Verify that the ADDUSER command completed successfully by issuing the following command, and be sure that the command is available to the iadmin ID:

```
[TSO] LISTUSER iadmin OMVS NORACF
```

You should receive the following response:

```
USER=iadmin

OMVS INFORMATION

-----

UID=0000000008

HOME=/u/iadmin

PROGRAM=/bin/sh
```

3. A Security Administrator must update the Facility classes of RACF, using the following commands issued with ISPF Option 6:

```
RDEFINE FACILITY BPX.FILEATTR.APF UACC(NONE)

PERMIT BPX.FILEATTR.APF CL(FACILITY) ID(iadmin) ACCESS(READ)
```

4. Refresh the RACF Facility class so that these commands will take effect.

```
SETROPTS RACLIST(FACILITY) REFRESH
```

5. Continue by verifying the server administrator ID, as described in [Verify the OPSYS Administrator ID](#).

Define the OPSYS Administrator ID With CA-ACF2

The server administrator ID requires an OMVS segment.

To define the server administrator ID with eTrust CA-ACF2:

1. To define the ID that will administer the server, issue the following commands:

```
SET LID

INSERT iadmin GROUP(admin) PASSWORD(pass) STC

SET PROFILE(USER) DIV(OMVS)

INSERT iadmin UID(n) HOME(/) OMVSPGM(/bin/sh)
```

where:

iadmin

Is the ID you are creating to administer the server.

admin

Is the group in which iadmin will reside.

pass

Is the password for iadmin.

n

Is the UID.

2. Continue by verifying the server administrator ID, as described in [Verify the OPSYS Administrator ID](#).

Define the OPSYS Administrator ID With CA-Top Secret

The server administrator ID requires an OMVS segment.

To define the server administrator ID with eTrust CA-Top Secret:

1. Create a department ID for everyone defined to eTrust CA-Top Secret who will be using the server, by issuing the command

```
TSS CRE(dept) TYPE(DEPT) NAME('formal department name')
```

where:

dept

Is the name of the department you are creating.

formal department name

Is the label you want to associate with the new department.

2. For users within the department you just created for the server, you can define resource access within a group. To define an ID for that group, issue the following command

```
TSS CRE(deptgrp) NAME('dept group') DEPT(dept) TYPE(GROUP) GID(n)
```

where:

deptgrp

Is the name of the group you are creating.

dept group

Is the label you want to associate with the new group.

dept

Is the name of the department you created.

n

Is the number you want to assign to the new group.

3. Create the iadmin ID and attach it to the new department by issuing the following commands:

```
TSS CRE(iadmin) NAME('iadmin id')
TYPE(USER) DEPT(dept) PASSWORD(pass)
GROUP(deptgrp) DFLTGRP(deptgrp)
```

where:

iadmin

Is the ID you are creating to administer the server.

iadmin id

Is the label you want to associate with the new ID.

dept

Is the name of the department that you created.

pass

Is the password for the ID you are creating.

deptgrp

Is the group you created.

4. Issue the following command to define the user's USS shell program (using OMVSPGM), facility access (using FAC), and, optionally, the initial directory (using HOME).

The OMVS segment of the ACID defines the ACID's UID, the user's home directory, and the initial program that the user will run. The initial program is generally the shell program that the user invokes.

```
TSS ADD(iadmin) UID(n) [HOME(/u/dir)] OMVSPGM(/bin/sh) FAC
```



```
(BATCH,TSO)
```

where:

iadmin

Is the ID you created to administer the server.

n

Is the UID. It cannot be 0 (zero).

HOME

Defines the initial directory path name. If it is omitted, USS sets the user's initial directory to the root directory.

dir

Is the ID home directory.

5. Issue the following command

```
TSS PER(iadmin) IBMFAC(BPX.FILEATTR.APF) ACC(READ)
```

where:

iadmin

Is the ID you created to administer the server.

6. Continue by verifying the server administrator ID, as described in [Verify the OPSYS Administrator ID](#).

Verify the OPSYS Administrator ID

To verify the server administrator ID:

Procedure

1. Verify that the home directory of the server administrator ID is correct by logging on to the server administrator ID (if not already logged on) and issuing the following command from ISPF option 6:

```
OSHELL pwd
```

You should receive the following response:

```
/u/iadmin
```

This directory should be the home directory specified in the UID definition for iadmin.

2. For a second confirmation, issue the following command:

```
OSHELL echo $HOME
```

You should receive the following response:

```
/u/iadmin
```

3. Verify that the server administrator ID has a unique UID and the correct GID defined by issuing the following command and pressing Enter:

```
OSHELL id
```

You should receive the following response:

```
uid=8(IADMIN) gid=50(ISRVGRP)
```

This UID and GID should match what is defined in the OMVS segment.

Define the System User ID With RACF

The RACF commands in this procedure must be issued by the Security Administrator. The server system user ID does not require logon authority.

To define the server system user ID with RACF:

1. Issue the following RACF command

```
ADDUSER iserver DFLTGRP(OMVSGRP) OMVS(UID(0)) NOPASSWORD
```

where:

iserver

Is the account you use for the system server ID.

2. Verify that the above ADDUSER command completed successfully by issuing the following command:

```
[TSO] LISTUSER iserver OMVS NORACF
```

You should receive the following output:

```
USER=iserver

OMVS INFORMATION

-----

UID=0000000000

HOME=/u/iserver

PROGRAM=/bin/sh
```

Define the System User ID With CA-ACF2

To define the server system user ID with eTrust CA-ACF2, issue the following commands:

```
SET LID

INSERT iserver NAME(iserverID) GROUP(pgm)

SET PROFILE(USER) DIV(omvs)

INSERT iserver UID(0) HOME(/) PROGRAM(/bin/sh)

SET PROFILE(GROUP) DIV(omvs)

INSERT pgm GID(n)
```

where:

iserver

Is the ID you are defining for the server system ID.

iserverID

Is the description you want to associate with the system server ID.

pgm

Is the ID group.

omvs

Is the name of your OMVS division.

n

Is the group ID.

Define the System User ID With CA-Top Secret

To define the server system user ID with eTrust CA-Top Secret:

1. Issue the following commands:

```
TSS CRE(iserver) TYPE(USER) NAME('server system ID')  
DEPT(dept) PASS(pass,0) SOURCE(INTRDR)
```

where:

iserver

Is the name you wish to assign to the server system ID you are defining.

dept

Is the name of the department you created in step 2b.

server system ID

Is the label you want to associate with the new ID.

pass

Is the ID password.

This password never expires.

Note that the SOURCE(INTRDR) setting prevents this ACID from logging on.

2. Define the required access for the server system ID by issuing the following command

```
TSS ADD(iserver) UID(0) HOME(/) OMVSPGM(/bin/sh) GROUP(deptgrp)
DFLTGRP(deptgrp)
```

where:

iserver

Is the server system ID.

deptgrp

Is the name of the group you created in step 2b.

3. You can choose to audit the server system ID. Each time the ACID is used, an audit record will be written to the eTrust CA-Top Secret audit tracking file. To set this option, issue the following command

```
TSS ADD(iserver) AUDIT
```

where:

iserver

Is the server system ID.

Define the System User ID With UNIXPRIV Profiles

Resource names in the UNIXPRIV class are associated with z/OS UNIX privileges. In order to use authorization to grant z/OS UNIX privileges, you must define profiles in the UNIXPRIV class protecting these resources. The UNIXPRIV class must be active. If you are using RACF, SETROPTS RACLIST must be in effect for the UNIXPRIV class.

To use profiles in the UNIXPRIV class to grant authorization for superuser privileges to a server system ID that does not have superuser authority (UID=0), you must assign:

READ access for SUPERUSER.FILESYS.CHOWN

CONTROL access for SUPERUSER.FILESYS

i Note:

- It is strongly recommended that you do not assign TSO privileges to the UNIXPRIV user ID. This can be done by adding the keyword NOPASSWORD to the RACF command ADDUSER.
- The installation routine ISETUP will ask for the server system ID (default ISERVER). It checks if the supplied userid has a UID of 0. If it does not, UNIXPRIV authorization is assumed. This results in an entry in the ibi/srv93/WFS/bin/edaserve.cfg file as follows:

```
server_system_id = ISERVER3/PRIV
```

rather than

```
server_system_id = ISERVER
```

If you installed the software with the server system ID pointing to a superuser ID (UID=0), and then decide to use the UNIXPRIV user ID, the value in the edaserve.cfg file must reflect the /PRIV syntax. Edit the file manually or by using the WebFOCUS Reporting Server browser interface, click **Workspace, Configuration/Monitor**. Open the **Configuration Files** folder, double-click **Workspace**, and change the server_system_id value before starting the server.

For more information about UNIXPRIV authorization, for:

- **RACF**, see the *IBM Security Server RACF Security Administrator's Guide*.
- **ACF2**, see the *eTrust CA-ACF2 Security Cookbook*.
- **Top Secret**, see the *eTrust CA-Top Secret Security Cookbook*.

System User ID With UNIXPRIV

The server system ID requires different authorities in order to be used with UNIXPRIV. The following RACF example lists the authorities for a system server ID with UNIXPRIV authorization, named ISERVER3. Authorizations for your site may differ.

Occurrences of ISERVER3

In standard access list of general resource profile UNIXMAP U100122

In standard access list of general resource profile TSOAUTH RECOVER

In standard access list of general resource profile TSOAUTH JCL

In standard access list of general resource profile ACCTNUM EDA

In standard access list of general resource profile UNIXPRIV

SUPERUSER.FILESYS.CHOWN

In standard access list of general resource profile UNIXPRIV

SUPERUSER.FILESYS

Owner of profile ISERVR3.* (G)

First qualifier of profile ISERVR3.* (G)

In access list of group EDA

User entry exists

Add the OMVS Segment to General User IDs

To add the OMVS segment to general user IDs:

1. For all users connecting to servers, ensure that each user ID has an OMVS segment (or is set up to use a default user ID as documented in the IBM manual *UNIX System Services Planning*).

For example, to modify an existing RACF TSO user ID profile, from ISPF Option 6, issue the following command

```
ALTUSER user_ID OMVS(UID(nnn) HOME('/u/user_ID') PROGRAM
('/bin/sh'))
```

where:

user_ID

Is the user ID you are modifying.

Collect Required Information for Adapters

For current information about which adapters are supported, see the *ibi™ WebFOCUS® Adapter Administration* manual.

You must provide information to configure the adapters that you want to install. The installation procedure automatically prompts you for this information. When you are prompted for an optional steplib, ddname, or environment variable, the installation procedure will indicate this with an OPT> prompt.

If you are using non-APF-authorized DBMS libraries, you must allocate the libraries to the ddname TASKLIB in IRUNJCL. The installation routine collects the information and allocates the required libraries in STEPLIB.

After you have installed and configured the server, you will be able to further configure your adapters using a web-based server configuration tool called the WebFOCUS Reporting Server browser interface.

The following table describes what information you need to provide for each adapter that you have. (If an adapter is not listed, no information needs to be provided for it.) Note that the table refers to:

- **EDAENV.** This file contains environment variables and values set at server startup
- **IRUNJCL.** This procedure starts the server.

Both files are members of the edaconfliB PDS. You will be prompted for the name of this PDS at installation time.

Adapter	Information you must provide
Adabas	<p>Provide the data set name for the following STEPLIB allocation:</p> <ul style="list-style-type: none"> • load library <p>This is required only for the synonym creation process. For example, in a production environment in which all synonyms already exist, you can omit this.</p> <p>When you configure the adapter, you will need to provide the name of the Adabas source library and the associated data set name.</p>
CA-	Provide the data set names for the following STEPLIB allocations:

Adapter	Information you must provide
DATACOM	<ul style="list-style-type: none"> • CUSLIB load library • CAILIB load library • utility library • URT library
CA- IDMS (both DB and SQL)	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • load library • DBA load library <p>Provide the data set names to which the following ddnames are allocated:</p> <ul style="list-style-type: none"> • SYSIDMS. Check with your CA-IDMS DBA regarding this ddname. • SYSCTL. Is the library corresponding to the central version you want to use.
Call Java	<p>You must have the JDK installed.</p> <p>Provide a value for the following environment variables:</p> <ul style="list-style-type: none"> • CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. • This adapter requires configuration of the JSCOM3 listener. The path to JVM must be provided using either JDK_HOME or JAVA_HOME. The installation will prompt for it.
CICS Transaction	<p>Provide the data set name for the following STEPLIB allocation:</p> <ul style="list-style-type: none"> • CICS EXCI load library
Db2 CAF	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • SDSNLOAD load library <p>For security information, see Db2 Security Exit Configuration for ZFS.</p> <ul style="list-style-type: none"> • SDSNEXIT load library (optional)
Db2 CLI	<p>Provide the data set names for the following STEPLIB allocations:</p>

Adapter	Information you must provide
	<ul style="list-style-type: none"> • SDSNLOAD load library For security information, see Db2 Security Exit Configuration for ZFS. • SDSNLOD2 load library • SDSNEXIT load library (optional; this is needed only for an explicit connection). <p>Provide a value for the following environment variable:</p> <ul style="list-style-type: none"> • DSNAOINI, which contains the full path and file name of the Db2 CLI .ini file.
EJB	<p>You must have the JDK installed.</p> <p>Provide a value for the following environment variables:</p> <ul style="list-style-type: none"> • CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. <p>If you are deploying the adapter to access an EJB on a:</p> <ul style="list-style-type: none"> ◦ WebLogic server, specify the following path: <div data-bbox="591 1087 1412 1173" data-label="Text"> <pre>/pathspec/weblogic.jar</pre> </div> ◦ WebSphere server, specify the following paths: <div data-bbox="591 1249 1412 1404" data-label="Text"> <pre>/pathspec/websphere.jar /pathspec/ejbcontainer.jar</pre> </div> <p>(one for each EJB container)</p> • This adapter requires configuration of the JSCOM3 listener. The path to JVM must be provided using either JDK_HOME or JAVA_HOME. The installation will prompt for it.
IMS	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • DFSPZP load library (optional; not needed if PZP modules are stored

Adapter	Information you must provide
	<p>in the DFSRESLB library)</p> <ul style="list-style-type: none"> • DFSRESLB load library
JDBC	<p>You must have the JDK installed.</p> <p>Provide a value for the following environment variables:</p> <ul style="list-style-type: none"> • CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. • This adapter requires configuration of the JSCOM3 listener. The path to JVM must be provided using either JDK_HOME or JAVA_HOME. The installation prompts for it.
Microsoft SQL Server	<p>Select the Call Java adapter, in addition to the Microsoft SQL Server adapter.</p> <p>Provide a value for the following environment variables:</p> <ul style="list-style-type: none"> • CLASSPATH. Provide the paths to the following files. These paths will be appended to CLASSPATH. <ul style="list-style-type: none"> ◦ msbase.jar ◦ mssqlserver.jar ◦ msutil.jar • This adapter requires configuration of the JSCOM3 listener. The path to JVM must be provided using either JDK_HOME or JAVA_HOME. The installation prompts for it.
Millennium	<p>Provide the data set name for the following STEPLIB allocation:</p> <ul style="list-style-type: none"> • load library
Model 204	<p>Provide the data set name for the following STEPLIB allocation:</p> <ul style="list-style-type: none"> • load library
MQSeries	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • SCSQLOAD load library

Adapter	Information you must provide
	<ul style="list-style-type: none"> • SCSQAUTH load library
NATURAL Batch	Provide the data set name for the following STEPLIB allocation: <ul style="list-style-type: none"> • NATURAL load library
SAP (SQL)	Provide values for the following environment variables: <ul style="list-style-type: none"> • LIBPATH, which contains the path to SAP RFC SDK. • SAP_CODEPAGE=0126, or the correct SAP code page for your language environment.
SAP BW	Provide values for the following environment variables: <ul style="list-style-type: none"> • LIBPATH, which contains the path to SAP RFC SDK.SAP_CODEPAGE=0126, or the correct SAP code page for your language environment.
Supra	Provide the data set name for the following STEPLIB allocations: <ul style="list-style-type: none"> • LINKLIB load library. • INTERFLM load library. • ENVLIB load library.

Download and Process the Distribution File from eDelivery

1. Download the `*zos_zseries.run` file for the selected release from eDelivery.tibco.com.
2. Upload the file, binary, to a USS directory on your z/OS system.
3. Log in to USS using the `iadmin` userid.
4. Change to the directory containing the uploaded `*zos_zseries.run` file.
5. Run the run file by using the following command:

```
sh *zos_zseries.fun
```

This extracts all files to a 'temp' subdirectory under your current directory.

Run isetup to Install and Configure a New Server

Follow the steps mentioned below to run isetup to Install and Configure a New Server.

1. Log in to USS by using the iadmin user ID.
2. Change to the temp directory created when you processed the run file.
3. Run the isetup program. Enter **1** on the Welcome screen.

```

Welcome to the Product Set Up Facility
Please respond to the prompts or enter Q to quit at any prompt.

-----
ISETUP: Installing ibi WebFOCUS 9.3 Server
-----

Select an option:

1. Install and Configure
2. Add Additional Configuration Instance
3. Refresh Installation (Reinstall, Keep Configurations)

Enter a selection (Default=1) : 1

```

4. Provide the full path name of the media for the product or press Enter to accept the default.

```

Please enter the full path name of the media for the product
(Default=/u/pgmlaw/temp/iserver.tar)

Please supply media or <Enter> :

```

5. Enter the z/OS Userid for Server administration or press Enter to accept the default. For more information, see [OPSYs Server Administrator ID \(iadmin\)](#).

```

Enter z/OS Userid for Server administration, or hit ENTER to accept the default
(Default=PGMLAW) :

```

6. Enter the Server Administration ID and password. The password, which does not display, is stored in encrypted form. For more information, see [PTH Administrator ID](#).

```
Enter credentials for the server's internal security
provider (PTH), the server's default start up mode.
```

```
Enter the Server Administrator ID
```

```
(Default=srvadmin) : █
```

7. Enter the Server System Support userid or press Enter to accept the default. For more information, see [ibi WebFOCUS Reporting Server System ID \(iserver\)](#).

```
Enter the z/OS USS Userid for Server System Support, or hit ENTER to accept the
default
```

```
(Default=ISERVER) : █
```

8. You are now shown the default values of the server environment variables and port number.

```
Please review the default settings.
```

```
EDAHOME = /u/pgmlaw/ibi/srv99/home
EDACONF = /u/pgmlaw/ibi/srv99/wfs
EDAPRFU = /u/pgmlaw/ibi/profiles
APPROOT = /u/pgmlaw/ibi/apps
HOMEAPPS = /u/pgmlaw/ibi/homeapps
EDAHOMELIB = PGMLAW.SRV99.HOME.LOAD
EDAHOMELIB_UNIT = SYSDA
EDACONFLIB = PGMLAW.SRV99.WFS.DATA
EDACONFLIB_UNIT = SYSDA
HTTP_BASE_PORT = 8121
```

```
If you are satisfied with the default settings you may proceed to
final confirmation else you will be prompted for individual values.
Proceed with defaults? (Y/N Default=Y) : █
```

9. If you do not want to accept the default values, skip to the next step. If you do accept the default values, you still have to respond to two more prompts:
 - a. If you are unsure where your `libjvm.so` is installed, contact your System Administrator.

```
Supply the USS directory name where the product will look for lib/server/libjvm.so.
This location is also known as JDK_HOME, and is required for Java Services and certain adapters.
```

```
(Default=none) : █
```

- b. Contact ibi Customer Support to receive your site's Customer ID.

```
Please supply Customer ID : █
```

Now proceed to step 11.

10. Select N to change any properties that you wish.

Name	Description
EDAHOME PDS name	Fully qualified name of a PDS that contains executable modules necessary for running the WebFOCUS Reporting Server.
EDAHOME unit	UNIT value for EDAHOME PDS.
EDAHOME volume	VOLUME value for EDAHOME PDS.
EDAHOME SMS rule	SMS allocation rule for EDAHOME PDS.
CICSLIB PDS name	Fully qualified name of a PDS that contains executable modules necessary for running the CICS adapter.
EDACONF PDS name	Fully qualified name of a PDS that contains configuration data files.
EDAPRFU path	The location on the disk where the product looks for the user profiles and the admin.cfg file.
APPROOT path	The location on the disk where the product looks for applications.
HOMEAPPS path	The location on the disk where the product looks for the use of home applications.
JDK_HOME path	Full USS path name to your Java installation. This variable and value is stored in edaenv.cfg. Server startup logic looks for lib/server/libjvm.so under this directory. If it is not found, the Server's jscom listener does not start, and certain java-based adapters do not run.
	Note: If you do not know this location, contact your system administrator.
Customer ID	The customer ID provided with your WebFOCUS software.

Name	Description
HTTP Listener port	<p>The HTTP Listener port.</p> <p>Default: 8101.</p> <p>This is the second of the seven consecutive port numbers that must be open and available for the server's IP based services.</p>

11. All installation and configuration options are displayed. One last prompt asks you to Accept and Proceed, Start Over, or Quit.
12. After a successful installation, you receive this last prompt:

```
Would you like to start the Server Workspace (Y/N Default=Y)? : █
```

You can start the Server, for initial testing purposes, by responding Y, but for production Servers, it is recommended that you start via submitting `istart` from your EDACONF PDS.

Run isetup to Add an Additional Configuration Instance

Follow the steps mentioned below to run `isetup` to add an Additional Configuration Instance.

1. Log in to USS by using the iadmin user ID.
2. Change to the temp directory created when you processed the run file.
3. Run the `isetup` program. Select option **2** on the initial screen:


```

Welcome to the Product Set Up Facility
Please respond to the prompts or enter Q to quit at any prompt.

-----

ISETUP: Installing ibi WebFOCUS 93 Server

-----

Select an option:

1. Install and Configure
2. Add Additional Configuration Instance
3. Refresh Installation (Reinstall, Keep Configurations)

Enter a selection (Default=1) : 2

-----

Enter z/OS Userid for Server administration, or hit ENTER to accept the default
(Default=PGMASW) :

```

4. Enter z/OS Userid for Server administration, PTH Administrator ID, and password. Press Enter to accept the defaults. For more information, see [OPSY Server Administrator ID \(iadmin\)](#).

```

Enter z/OS Userid for Server administration, or hit ENTER to accept the default
(Default=PGMASW) :
Enter credentials for the server's internal security
provider (PTH), the server's default start up mode.

Enter the Server Administrator ID

(Default=srvadmin) :
Enter the Administrator Password :

```

5. Enter, or accept the default value for the z/OS Server System Support ID. For more information, see [ibi WebFOCUS Reporting Server System ID \(iserver\)](#).

```

Use the WebConsole Access Control option to configure alternate
or additional security providers, such as OPSYS, LDAP or others.

Enter the z/OS USS Userid for Server System Support, or hit ENTER to accept the
default

(Default=ISERVER) : █

```

6. You are presented with the default settings and asked whether to proceed. Type N. Specify values for EDACONF, EDACONFLIB and HTTP_BASE_PORT that do not conflict with your existing configuration.

```

-----
Please review the default settings.

EDAHOME = /u/pgmasw/ibi/srv93/home
EDACONF = /u/pgmasw/ibi/srv93/wfs  (*EXISTS, owner PGMASW *)
EDAPRFU = /u/pgmasw/ibi/profiles
APPROOT = /u/pgmasw/ibi/apps
HOMEAPPS = /u/pgmasw/ibi/homeapps
EDACONFLIB = PGMASW.SRV93.WFS.DATA
EDACONFLIB_UNIT = SYSDA
HTTP_BASE_PORT = 8121

WARNING: Directories marked as existing will be deleted and recreated!

If you are satisfied with the default settings you may proceed to
final confirmation else you will be prompted for individual values.
Proceed with defaults? (Y/N Default=Y) : N
-----

```

7. Accept the EDAHOME location.

```

-----
Enter the EDAHOME directory where the product was installed
(Default=/u/pgmasw/ibi/srv93/home)

Please supply location or <Enter>:
-----

```

8. Provide a new EDACONF location. Typically this location simply adds a suffix to the existing EDACONF, such as ../wfs_test.

```

-----
Supply the location on disk in which to configure the software.
This location is also known as EDACONF.

(Default=/u/pgmasw/ibi/srv93/wfs)

Please supply location or <Enter>: /u/pgmasw/ibi/srv93/wfs02
-----

```

9. In the next prompts for EDACONFLIB and EDAPFRU, the proposed value uses the same suffix. Accept it or edit as appropriate.

```

-----
Enter fully qualified EDACONF PDS name, or hit ENTER to accept the default
(Default=PGMASW.SRV93.WFS02.DATA)

Please supply EDACONFLIB or <Enter>:

-----

Supply the location on disk where the product will look for user profiles
and the admin.cfg file. This location is also known as EDAPRFU.

(Default=/u/pgmasw/ibi/srv93/profiles02)

Please supply location or <Enter>:

-----

```

10. Continue through the remaining prompts for APPROOT, HOMEAPPS, and JDK_HOME.

```

-----

Supply the location on disk where the product will look for applications.
This location is also known as APPROOT.

(Default=/u/pgmasw/ibi/apps)

Please supply location or <Enter>:

-----

Supply the location on disk where the product will look for user home
applications. This location is also known as HOMEAPPS.

(Default=/u/pgmasw/ibi/homeapps)

Please supply location or <Enter>:

-----

Supply the USS directory name where the product will look for lib/server/libjvm
.so.
This location is also known as JDK_HOME, and is required for Java Services and
certain adapters.

(Default=none) :

-----

```

11. Enter the Customer ID. It is provided with your WebFOCUS software.

```

Please supply Customer ID : 9999█

```

12. At the HTTP Listener Port prompt, enter a new value. If you accept the default value,

you cannot run your old and new configurations at the same time. Also enter the SMTP Mail Server if required.

```
-----
Enter HTTP Listener Port (HTTP_BASE_PORT). This is the second of
seven consecutive port numbers that must be open and available for
the server's IP based services. For HTTPS (SSL), use WebConsole
HTTP Listener Properties page to configure.

(Default=8121) :

Enter SMTP Mail Server (Optional) :

-----
```

13. Review the configuration options and enter Y to Accept and Proceed.

```
The following selections have been made for ...

Configure Options ...
  EDACONF = /u/pgmasw/ibi/srv93/wfs
  EDACONFLIB = PGMASW.SRV93.WFS.DATA
  EDACONFLIB_UNIT = SYSDA
  EDAHOME = /u/pgmasw/ibi/srv93/home
  PRODUCT = server
  EDAPRFU = /u/pgmasw/ibi/profiles
  HOMEAPPS = /u/pgmasw/ibi/homeapps
  WORKSPACE_MANAGER_NAME = "WebFOCUS 93 Server"
  APPROOT = /u/pgmasw/ibi/apps
  SERVER_TYPE = ffs
  SERVER_SYSTEM_ID = ISERVER
  SERVER_ADMIN_ID = PGMASW
  PTH_USER = srvadmin
  PTH_PASSWORD = {AES}09E2F90C6B37E5EA4DAB41B9274A731B
  HTTP_BASE_PORT = 8121
  POPULATE_EDACONFLIB = Y
  CUSTOMER_ID = 9999
Please confirm these values with one of the following responses ...

  Y = Accept and Proceed
  N = Start Over
  Q = Quit

Please supply confirmation: Y
```

14. You are prompted to review the selections and accept and proceed, start over, or quit. Type Y to accept and proceed.
15. After a successful creation of a new configuration, you receive this last prompt:

```
ISSETUP: Configuration Step completed
```

```
-----  
Would you like to start the Server Workspace (Y/N Default=Y)? : █
```

For initial testing purpose, you can start the Server by entering Y. However, for production Servers, it is recommended that you start by submitting `istart` from your new EDACONF PDS.

Run isetup to Upgrade an Existing Installation to a Newer Release

Use this option to upgrade a server to a new maintenance level within the same major release. A major release is indicated by the first two digits of the release number.

Server upgrade consists of a series of ISPF panels, which gather information for the upgrade. After the panel dialog is complete, JCL is created and submitted (if required) to upgrade the server on z/OS. This JCL job retrieves the remainder of the MVS libraries and ZFS files from the media.



Caution: Ensure that all server processes are stopped before you upgrade.

Follow the below mentioned steps to run `isetup` to Upgrade an Existing Installation to a Newer Release.

1. Log in to USS by using the `iadmin` user ID.
2. Change to the temp directory created when you processed the run file
3. Run the `isetup` program. Select option **3** on the initial screen:

```

-----
                        Welcome to the Product Set Up Facility
                Please respond to the prompts or enter Q to quit at any prompt.
-----

      ISETUP: Installing ibi WebFOCUS 93 Server
-----

Select an option:

      1. Install and Configure
      2. Add Additional Configuration Instance
      3. Refresh Installation (Reinstall, Keep Configurations)

Enter a selection (Default=1) :    3
-----

```

4. Enter the default value for the path of the media file or press Enter to accept the default.

```

-----
Please enter the full path name of the media for the product
(Default=/u/pgmasw/temp/iserver.tar)
Please supply media or <Enter> :
-----

```

5. Enter, or accept the default value for the z/OS Server administrator userid.

```

-----
Enter z/OS Userid for Server administration, or hit ENTER to accept the default
(Default=PGMASW) :
-----

```

6. Enter the full path to the existing EDAHOME location where you wish to upgrade.

```

-----
Enter the EDAHOME directory where the product was installed
(Default=/u/pgmasw/ibi/srv93/home)
Please supply location or <Enter>:
-----

```

7. Enter the default fully qualified name for EDAHOME PDS or press Enter to accept the default.

```
-----
Enter fully qualified name for EDAHOME PDS, or hit ENTER to accept the default
(Default=PGMASW.SRV93.HOME.LOAD) :
-----
```

8. One at a time, enter the UNIT value, VOLUME for EDAHOME PDS or press enter to accept the default.

```
-----
Enter UNIT value for EDAHOME PDS, or hit ENTER to accept the default
(Default=SYSDA) :

-----
Enter VOLUME value for EDAHOME PDS, or hit ENTER to accept the default
(Default=none) :
-----
```

9. Enter the SMS Allocation Rule for EDAHOME PDS or press Enter to accept the default.

```
-----
Enter the SMS Allocation Rule for EDAHOME PDS, or hit ENTER to accept the default
(Default=none) :
-----
```

10. One by one enter the full path to each configuration to be modified and press Enter. Or if your list is complete, type C to continue.

```
-----
During the upgrade process, each active configuration has to be updated with the
Customer ID.

Type the full path to each configuration to be modified and press Enter
or if your list is complete, type C to Continue :C
```

11. A summary of selection you made is displayed. Enter Y to proceed. Your old EDAHOME locations on both USS and PDS are removed and replaced with the new release.

```

The following selections have been made for ...

Refresh Options ...
  media release name = M729300D
  media gen number = 2961 06/17/2024 09:32:27
  INSTALLATION_DEVICE = /u/pgmasw/temp/iserver.tar
  PRODUCT = server
  EDAHOME = /u/pgmasw/ibi/srv93/home
  EDAHOMELIB = PGMASW.SRV93.HOME.LOAD
  EDAHOMELIB_UNIT = SYSDA
  CREATE_EDAHOMELIB = Y
  SERVER_ADMIN_ID = PGMASW

Replacing
  release name = M729300D
  gen number = 2961 06/17/2024 09:32:27

This option will remove and recreate EDAHOME removing all prior contents
including debuggables that may have been installed. It does not touch the
contents of any configuration directories outside the EDAHOME directory.

If you have any site_specific files under the EDAHOME location that need
to be retained then they must be backed up before proceeding!

Please confirm these values with one of the following responses ...

  Y = Accept and Proceed
  N = Start Over
  Q = Quit

Please supply confirmation: Y

```

12. After a successful refresh installation, "Installation step completed" message is displayed.

```

Please wait while we are reinstalling the product ...

ISETUP: Installation Step completed
$ █

```

13. You are prompted to start the Server Workspace. For initial testing purposes, you can start the server by responding Y, but for production servers, it is recommended that you start via submitting istart from your EDACONF PDS.

```

Would you like to start the Server Workspace (Y/N Default=Y)? : █

```

i Note: To upgrade from a release prior to 8207.27 to Release 8207.27 or higher, see [Upgrading From a Release Prior to 8207.27 to Release 8207.27 or Higher](#).

Testing the New or Upgraded Installation/Configuration

Procedure

1. Log in to TSO as iadmin.
2. Submit the ISTART JCL from the appropriate configuration dataset. This executes the IRUNJCL proc.
3. Check the job output for errors. Look for the EDAPRINT message:

```
(EDA13023) ALL INITIAL SERVERS STARTED
```

4. Start the WebFOCUS Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

```
http://host:port
```

where:

host

Is the name of the machine on which the server is installed.

port

Is the http port number specified during installation.

The WebFOCUS Reporting Server browser interface opens.

5. If the WebFOCUS Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree. The server may be further data tested (if desired).
6. Continue with adapter configuration, as described in the *ibi™ WebFOCUS® Adapter Administration* manual.

Result

When you are finished using the server, you can use the WebFOCUS Reporting Server browser interface to stop the server by going to the WebFOCUS Reporting Server browser

interface menu bar, selecting **Workspace**, and then **Stop**.

If you experience problems at start-up, examine the job output for more information.

Configure Security

If you will be configuring your server with an OPSYS security provider, you must perform the instructions in the following topics. (For PTH, DBMS, and LDAP security providers, skip these topics.)

- [Configure Security With All Security Products](#), regardless of which security product you use.
- [Configure Security With eTrust CA-ACF2](#) if you use eTrust CA-ACF2.
- [Configure Security With eTrust CA-Top Secret](#) if you use eTrust CA-Top Secret.

You can see a full description of all server security providers in the WebFOCUS Reporting Server browser interface help, and also in the *WebFOCUS Reporting Server Administration* manual. To see it in the WebFOCUS Reporting Server browser interface:

1. From the WebFOCUS Reporting Server browser interface menu bar, select **Help**, then **Contents and Search**.

The WebFOCUS Reporting Server browser interface Help window opens.

2. In the left pane, expand **Server Administration**.

Security Providers

The default security provider for a new installation is the internal security provider, PTH. The PTH provider implements security using user IDs, passwords, and group memberships stored in the `admin.cfg` configuration file.

After the initial installation, the Server Administrator that was configured during the installation can start the server and use the Reporting Server browser interface to further customize security settings, for example, to configure alternate or additional security providers, create additional PTH IDs, and register groups and users in a security role. For more information about security providers, see the *Server Security* chapter in the *ibi™ WebFOCUS® Reporting Server Administration* guide.

Satisfy Security Provider OPSYS Requirements

To run a server with security provider OPSYS, you must perform the following steps. You must do this once after installing and after each refresh of the server with fixes.

Set up tscom300.out as a root-owned SUID program:

Procedure

1. If the server is running, bring it down.
2. Log on to the system as root, or issue the su root command.
3. Change your current directory to the bin directory of the home directory created during the installation procedure.

For example, type the following command:

```
cd /home/iadmin/ibi/srv93/home/bin
```

4. Change file ownership and permissions by typing the following commands:

```
chown root tscom300.out
```

```
chmod 4555 tscom300.out
```

5. Verify your changes by issuing the following command:

```
ls -l tscom300.out
```

The output should be similar to the following:

```
-r-sr-xr-x 1 root iadmin 123503 Aug 23 04:45 tscom300.out
```

Note the permissions and ownerships.

Result

When you start the server, it will now run with security provider OPSYS.

The chmod and chown steps will need to be repeated after any server upgrade since the tscom300.out file is replaced during an upgrade and the attributes are lost.

Note: The server issues RACROUTE REQUEST=VERIFY calls to authenticate users, so all users must have access to APPL MSO, which identifies our server.

Note: If this Security Provider OPSYS step has been configured and the site later decides to switch to Security OFF, special steps must be taken to ensure the mode remains after a full server shutdown (where edastart -start is used to restart the server). The steps are:

1. After the server recycles from the change to OFF, use the WebFOCUS Reporting Server browser interface to open the environment configuration file of the server by clicking **Workspace** and expanding the **Configuration Files** folder, followed by the **Miscellaneous** folder.
2. Double-click **Environment - edaenv.cfg** to edit the file and add the `EDAEXTSEC=OFF` variable.
3. Save your work.

After the next full server shutdown, be sure to do an edastart -cleardir before restarting the server. This will clear any root-owned files that would prevent a security OFF server from starting.

Preventing Unsecured Starts After Upgrades

If the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the edaprint log.

This feature prevents an unsecured starting of the server after a software upgrade if any of the required post-upgrade reauthorization steps are missed on a UNIX, IBM i, or z/OS ZFS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server edaenv.cfg environment configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
Configured security is 'ON' as set by EDAEXTSEC variable.
```

```
Server has no root privilege.
```

```
Workspace initialization aborted.
```

```
(EDA13171) UNABLE TO START SERVER
```

Configure Security With All Security Products

To configure server security with RACF, eTrust CA-ACF2, or eTrust CA-Top Secret:

Procedure

1. Log on to TSO using an ID with read access to the BPX.FILEATTR.APF facility class.
2. Using the name of the actual EDAHOME directory, change file attributes by entering the following TSO commands in ISPF Command Shell (option 6):

```
OSHELL extattr +a /u/iadmin/ibi/srv93/home/bin/tscom300.out
OSHELL extattr +a /u/iadmin/ibi/srv93/home/bin/tsqprx.out
```

3. Verify your changes by issuing the following commands:

```
OSHELL ls -E /u/iadmin/ibi/srv93/home/bin/tscom300.out
OSHELL ls -E /u/iadmin/ibi/srv93/home/bin/tsqprx.out
```

The extended attributes portion of the output should be a-s-.

4. The libraries allocated to STEPLIB in IRUNJCL must be APF-authorized. Any non-APF-authorized libraries must be allocated to the TASKLIB DDNAME.
5. Test server security by repeating the process described in [Testing the New or Upgraded Installation/Configuration](#).

Configure Security With eTrust CA-ACF2

If you are installing the server to run with eTrust CA-ACF2 security package, you may have to apply fix number QO71149 for eTrust CA-ACF2 6.4 or QO51462 for eTrust CA-ACF2 6.5. If you are installing the server under z/OS 2.1 or higher to run with eTrust CA-ACF2 14.0, PTF RO24848 may have to be applied if server USS user IDs are to be defined using the USS

default segment. For more information about these fixes, contact Computer Associates.

The MVS address space must have access to those system resources that are required by each user. eTrust CA-ACF2 will check for job-level access as well as user-level access. Therefore, the job-level user ID must have access to all data sets. For example, this can be done by setting the MAINT attribute on the eTrust CA-ACF2 record for the job-level user ID. Refer to eTrust CA-ACF2 technical reference guides for further information.

The job-level user ID of the server should have the Multiple User, Single Address Space (MUSSAS) attribute set to on. If the server is run as a started task, you must enable the started task attribute for the job-level user ID. You must also use the Reporting Server browser interface to define this user ID with OPER authority. For more information, see the *ibi™ WebFOCUS® Reporting Server Administration* manual.

Each user ID must be defined to eTrust CA-ACF2.

To create the necessary logon IDs and profile records, issue the following commands:

```
ACF
SET LID
INSERT OMVS GROUP(OMVSGRP) STC UID(0)
INSERT INETD GROUP(OMVSGRP) STC UID(0) HOME(/) OMVSPGM(/bin/sh)
INSERT TCPIP GROUP(OMVSGRP) STC UID(0)
```

For more information, see the following sections in the Computer Associates *eTrust CA-ACF2 Security for z/OS and OS/390 Cookbook*:

- *Defining USS Users*
- *Superusers*
- *HTTP Server*
- *Installation Steps*

Configure Security With eTrust CA-Top Secret

If you use Computer Associates eTrust CA-Top Secret, follow these guidelines and refer to the security vendor manual for implementing user-level security.

The TSS PERMIT command for BPX.FILEATTR.APF facility class access is:

```
TSS PER(user_acid) IBMFAC(BPX.FILEATTR.APF) ACC(READ)
```

This allows users to turn on the APF-authorized attribute for a ZFS file. Refer to *z/OS UNIX System Services Support* in the *eTrust CA-Top Secret Security Cookbook* for more information.

To use eTrust CA-Top Secret, perform the following steps:

1. Create an eTrust CA-Top Secret facility entry for the server security module, *PATHNAM.

This is an example of a facility entry defining the server to eTrust CA-Top Secret:

```
FACILITY DISPLAY

PGM=*PATHNAM ID=9 TYPE=26

ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,ASUBM,TENV,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),NOPSEUDO,INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,MENU,NOAUDIT,RES,NOMRO,WARNPW,NOTSOC
ATTRIBUTES=NOTRACE,NOLAB,NODORMPW,NONPWR,NOIMSXTND

MODE=IMPL

LOGGING=ACCESS,INIT,SMF,MSG,SEC9

UIDACID=8 LOCKTIME=000 DEFACID=*NONE* KEY=8
```

For more information, see *How to Define z/OS UNIX System Services Users* in the Computer Associates *eTrust CA-Top Secret Security for OS/390 and z/OS Cookbook*.

2. Within this entry, include eTrust CA-Top Secret parameters to establish the proper operating characteristics.

The ISERVER and IADMIN ACIDs must have authority to the facility you have defined for the server and to the resources within the facility:

```
TSS ADD(region_acid) MASTFAC(facility) <- defines the facility to CA-Top Secret
```

```
TSS ADD(user_acid) FAC(facility) <- adds it to users requiring server access
```

3. Each user of the server must be defined to eTrust CA-Top Secret and given access to the appropriate system resources, including the facility you have defined for the server.

Each user requires an OMVS segment and ZFS directories.

4. If you are operating with eTrust CA-Top Secret HFSSEC=ON, continue with Step 5. Otherwise, skip to Step 7.
5. In the definitions for IADMIN and ISERVER ACIDs (shown in the previous examples), set up the following security authorization:

```
XA HFSSEC = /U.IADMIN
ACCESS = ALL
```

6. eTrust CA-Top Secret provides superuser granularity with separate definitions for the following resource names:

```
SUPERUSER.FILESYS.FILE (CONTROL access)
SUPERUSER.FILESYS.CHOWN
SUPERUSER.FILESYS.MOUNT
SUPERUSER.FILESYS.PFSCTL
SUPERUSER.FILESYS.VREGISTER
SUPERUSER.IPC.RMID
SUPERUSER.PROCESS.GETPSENT
SUPERUSER.PROCESS.KILL
SUPERUSER.PROCESS.PTRACE
SUPERUSER.SETPRIORITY
```

Ensure that the server system ID, ISERVER, which has UID=0, is granted full access to all these resources. Grant access to the superuser-listed resources by means of the UNIXPRIV resource class. For example:

```
TSS ADD(owning_acid) UNIXPRIV(SUPERUSE)
TSS PER(acid) UNIXPRIV(SUPERUSER.FILESYS.FILE) ACC(CONTROL)
```

For details see the *Superuser Granularity* topic in the Computer Associates eTrust CA-

Top Secret Security for OS/390 and z/OS Cookbook.

7. After you create a new user ID or change a user UID or GID, you must issue the following command to reflect the updates in Top Secret's in-storage tables:

```
TSS MOD(OMVSTABS)
```

The following commands can also be used to list all UIDs, GIDs and their owners:

```
TSS WHOOWNS UID(*)
```

```
TSS WHOOWNS GID(*)
```

This information can be used for diagnostic purposes.

For more information, see the Computer Associates *eTrust CA-Top Secret Security for OS/390 and z/OS Cookbook*.

Facility Entry Defining the Server to CA-Top Secret

The following is an example of a facility entry that defines the server to eTrust CA-Top Secret:

```
FACILITY DISPLAY
PGM=*PATHNAM ID=9 TYPE=26
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,ASUBM,TENV,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),NOPSEUDO,INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,MENU,NOAUDIT,RES,NOMRO,WARNPW,NOTSOC
ATTRIBUTES=NOTRACE,NOLAB,NODORMPW,NONPWR,NOIMSXTND
MODE=IMPL
LOGGING=ACCESS,INIT,SMF,MSG,SEC9
UIDACID=8 LOCKTIME=000 DEFACID=*NONE* KEY=8
```

ISERVER ACID Definition for CA-Top Secret

The following is an example of an ISERVER ACID definition for eTrust CA-Top Secret. Note that:

- UID is zero.
- The facility of the server is set to IWAY as an example; it can differ at your site.
- The SOURCE = INTRDR setting prevents this ACID from logging in.

```
TSS LIST(ISERVER) DATA(ALL,PROFILE)

ACCESSORID = ISERVER          NAME = IWAY ID
TYPE        = USER           SIZE = 512 BYTES
SOURCE      = INTRDR
DEPT ACID   = IWAY            DEPARTMENT = IWAY DEPT
DIV ACID    = IWAYDIV         DIVISION = IWAYDIV
GROUPS      = IWAYGRP
DFLTGRP     = IWAYGRP
----- SEGMENT OMVS
HOME        = /
OMVSPGM     = /bin/sh
UID         = 0000000000
```

IADMIN ACID Definition for CA-Top Secret

The following is an example of an IADMIN ACID definition for eTrust CA-Top Secret. Note that the UID is *not* zero.

```
TSS LIST(IADMIN) DATA(ALL,PROFILE)

ACCESSORID = IADMIN          NAME = IWAY ADMIN ID
```

```

TYPE          = USER                      SIZE = 512 BYTES
FACILITY      = TSO
FACILITY      = BATCH
DEPT ACID     = IWAY                      DEPARTMENT = IWAY DEPT
DIV ACID      = IWAYDIV                  DIVISION   = IWAY DIVISION
GROUPS        = IWAYGRP
DFLTGRP       = IWAYGRP
----- SEGMENT OMVS
HOME          = /u/iadmin
OMVSPGM       = /bin/sh
UID           = 00000000008

```

Starting and Stopping the ibi WebFOCUS Reporting Server for ZFS

This section provides information on the operation and use of the server. Additional information on the server and how to configure adapters is available in the WebFOCUS Reporting Server browser interface help. The WebFOCUS Reporting Server browser interface help is also available in the *ibi™ WebFOCUS® Reporting Server Administration* manual.

Starting and Stopping the ibi WebFOCUS Reporting Server Using a Batch Job

To start the server, submit the ISTART member of the MVS configuration library (*high_level_qualifier.WFS.DATA*).

To stop a server, submit the ISTOP member of the MVS configuration library or use the WebFOCUS Reporting Server browser interface. For information about using the WebFOCUS Reporting Server browser interface, see the *ibi™ WebFOCUS® Reporting Server Administration* manual.

Starting and Stopping the ibi WebFOCUS Reporting Server Using a Started Task

ISSETUP creates a started task JCL to start and stop the server. These started task members of the MVS configuration library are:

- **IWAYS**, which starts the server.
- **IWAYP**, which stops the server.

In order to execute the started tasks, you must:

- **Copy them** into SYS1.PROCLIB or any other JES2 Proclib data set.
- **Satisfy security requirements.** All external security-related permissions must exist for both the data sets and the started tasks. In order to issue the started tasks, the user must satisfy both of the following requirements:
 - Have at least OPERATOR authority defined within the WebFOCUS Reporting Server browser interface.
 - Be in the same security group, or associated with the same security group, as the owner of the server directory structure (for example, as iadmin).

To submit the started tasks from the MVS console, issue the following command:

```
S IWAYS
```

```
S IWAYP
```

You can add the started tasks to any automation product that you run.

Sample IWAYS Started Task

This is an example of IWAYS, the started task that starts the server:

```
//IWAYS      PROC

//TSCOM300    EXEC  PGM=TSCOM300,

//          PARM=' ENVAR("_EDC_UMASK_DFLT=0022") / '

//STEPLIB     DD    DSN=IADMIN.SRV93.HOME.LOAD,DISP=SHR

//EDAPRINT    DD    SYSOUT=A

//SYSPRINT    DD    SYSOUT=A

//SYSOUT      DD    SYSOUT=A

//EDAPARM     DD    DUMMY

//EDAENV      DD    DSN=IADMIN.SRV93.WFS.DATA(EDAENV),DISP=SHR
```

Sample IWAYP Started Task

This following is an example of IWAYP, the started task that stops the server.

```
//IWAYP      PROC

//TSCOM300    EXEC  PGM=TSCOM300

//STEPLIB     DD    DSN=IADMIN.SRV93.HOME.LOAD,DISP=SHR

//EDAPRINT    DD    SYSOUT=A

//SYSPRINT    DD    SYSOUT=A

//SYSOUT      DD    SYSOUT=A

//EDAPARM     DD    DSN=IADMIN.SRV93.WFS.DATA(EDAPRMP),DISP=SHR

//EDAENV      DD    DSN=IADMIN.SRV93.WFS.DATA(EDAENV),DISP=SHR
```

ibi WebFOCUS Reporting Server Operations

Using MVS Operator Commands

On MVS, you can issue operator MODIFY commands against the server job from either the MVS Console or SDSF. You can use MODIFY commands to pass options to an already running job:

Use MVS Operator MODIFY commands in the following format:

```
F jobname, parameters
```

For instance:

```
F IWAY93,-SHOW
```



Note: If the server job is canceled or it abends, submit the ICLEAR job in the configuration data set before restarting the server.

Enabling HTTPS Security on the HTTP Listener for ZFS

If you are using RACF, a private key *must be* generated together with the certificate. The generated key must be type RSA. The supported private key size is up to 4096 bits.

Generating the Certificate and Key

- **Generating the Certificate.** You can generate the certificate using the TSO RACDCERT command with options GENCERT (generate certificate) or GENREQ (generate certificate request). For example:

```
RACDCERT GENCERT SUBJECTSDN(CN('Workspace Manager')) -  
OU('IOD') -
```

```

O('IBI') -
C('US')) -
SIZE(2048) -
NOTAFTER(DATE(2026-12-01)) -
ID(ISERVER) -
RSA -
WITHLABEL('IBIcert')

SETOPTS RACLIST(DIGTCERT) REFRESH

```

- **Creating the Key Ring.** You can create the key ring using the RACDCERT ADDRING command. For example:

```
RACDCERT ADDRING(IBIring1) ID(ISERVER)
```

- **Connecting the Certificate to the Key Ring.** You can connect the certificate to a ring using the RACDCERT CONNECT command. For example:

```

RACDCERT CONNECT(LABEL('IBIcert') DEFAULT RING(IBIring1)) -
ID(ISERVER)

```

The ID owner of all objects is the same. It must be ISERVER.

The following JCL shows how to run the RACDCERT command in a batch:

```

//*** JOB CARD *****

//*****

//STEP1 EXEC PGM=IKJEFT01

//SYSTSPRT DD SYSOUT=*

//SYSTSIN DD *

```

```
RACDCERT LIST ID(ISERVER)
```

For detailed information and options of the RACDCERT command, see the IBM document *z/OS Security Server RACF Command Language Reference*.

TLS 1.3 SSL Protocol Requirements

The TLS 1.3 protocol requires additional RACF permissions be given to users and/or groups connecting to the WebFOCUS Reporting Server. READ permission must be given to CSFOWH CL(CSFSESV).

If you do not plan to use the default of TLS 1.3, you can force the WebFOCUS Reporting Server to use TLS 1.2 by adding the following parameter to the edaserve.cfg file:

```
ssl_protocol = tls_1_2
```

Enabling HTTPS

After the key ring and label are created, to enable HTTPS:

1. Go to the WebFOCUS Reporting Server browser interface Workspace page.
2. Expand **Special Services and Listeners**.
3. Right-click TCP/HTTP and click **Properties of HTTP**.
The Listener Configuration page opens.
4. Expand the Security section.
5. In the Enable HTTPS drop-down list, select **Yes**.

Additional fields open in which you can enter the certificate label and keyring values you defined using the RACDCERT commands.

```
SSL_CERTIFICATE = keyring
```

```
SSL_LABEL = certificate
```

6. Click **Save and Restart Server**.

Defining the ICSF Dataset Key Label for ZFS to Use Pervasive Encryption

In the following sample JCL, values are shown for clarity. These are the current IBM defaults.

```
SYMEXPORTABLE(BYANY) and ASYMUSAGE(HANDSHAKE SECUREEXPORT)
```

In the following sample PERMIT statement, ID contains only group names, not user ID names. During installation, you can choose which name to use or to use a combination of both.



Note: PGMYMG, PGM, QCS, EDA, and CSD in the sample code are arbitrary users and groups.

```
//TSOBATCH EXEC PGM=IKJEFT01

//SYSTSPRT DD SYSOUT=*

//SYSTSIN DD *

RDEF CSFKEYS DATASET.PGMYMG.ENCRYPTKEY.001 OWNER(SYS1) UACC(NONE) -

ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES)-

SYMEXPORTABLE(BYANY) ASYMUSAGE(HANDSHAKE SECUREEXPORT))

PERMIT DATASET.PGMYMG.ENCRYPTKEY.001 CLASS(CSFKEYS) ACCESS(READ) -

ID(PGM QCS EDA CSD)

SETOPTS RACLIST(CSFKEYS) REFRESH

/*

//
```

ICSF Panels

1. Select option 5, **UTILITY**, as shown in the following image, and press Enter.

```

HCR77D0 ----- Integrated Cryptographic Service Facility --
OPTION ==> _
System Name:  IBI1                      Crypto Domain: 0
Enter the number of the desired option.

 1 COPROCESSOR MGMT - Management of Cryptographic Coprocessors
 2 KDS MANAGEMENT  - Master key set or change, KDS Processing
 3 OPSTAT           - Installation options
 4 ADMINCTL         - Administrative Control Functions
 5 UTILITY          - ICSF Utilities
 6 PPINIT           - Pass Phrase Master Key/KDS Initialization
 7 TKE              - TKE PKA Direct Key Load
 8 KGUP             - Key Generator Utility processes
 9 UDX MGMT         - Management of User Defined Extensions

```

2. Select option 5, **CKDS KEYS**, as shown in the following image, and press Enter.

```

----- ICSF - Utilities -----
OPTION ==> _
Enter the number of the desired option.

 1 ENCODE           - Encode data
 2 DECODE           - Decode data
 3 RANDOM           - Generate a random number
 4 CHECKSUM         - Generate a checksum and verification patterns
 5 CKDS KEYS        - Manage keys in the CKDS
 6 PKDS KEYS        - Manage keys in the PKDS

```

3. Select option 7, **Generate AES DATA keys**, as shown in the following image, and press Enter.

```

----- ICSF - CKDS KEYS -----
OPTION ==> 7
Active CKDS:  IBI1.CSF.SCSFCKDS                      Keys: 4
Enter the number of the desired option.
 1 List and manage all records
 2 List and manage records with label key type _____ leave blank for
                                                                list, see help
 3 List and manage records that are _____ (ACTIVE, INACTIVE, ARCHIVED)
 4 List and manage records that contain unsupported CCA keys
 5 Display the key attributes and record metadata for a record
 6 Delete a record
 7 Generate AES DATA keys
Full or partial record label
==> _____
The label may contain up to seven wild cards (*)
Number of labels to display ==> 100 (Maximum 100)
Press ENTER to go to the selected option.
Press END to exit to the previous menu.

```

4. Type the CKDS record label for the new key and select the AES key bit length, as shown in the following image, and press Enter.

```
----- ICSF - CKDS Generate Key -----  
COMMAND ==>  
  
Active CKDS: IBI1.CSF.SCSFCKDS  
  
Enter the CKDS record label for the new AES DATA key  
==> DATASET.PGMYMG.ENCRYPTKEY.001  
  
AES key bit length: 128 192 s 256
```

If the operation was successful, Key Generated is returned at the upper-right corner of the screen, as shown in the following image.

```
- ICSF - CKDS Generate Key ----- KEY GENERATED
```

Db2 Security Exit Configuration for ZFS

Customize the Db2 security exit to allow the Adapter for Db2 to run with user-level security enabled. If you do so, users will connect to Db2 with the authorization of the user ID with which they logged on to the server. The server must also be running with security turned on.

If you do not customize the Db2 security exit, all users will be assigned the connection ID to Db2 that is associated with the region, job submitter, or started task.


For the Adapter for Db2 CLI, the connection to Db2 must be configured as *trusted* for the exit to be invoked.

The changes that must be made to the IBM Db2 sign-on exit, DSN3SATH, differ for RACF and eTrust CA-Top Secret sites and eTrust CA-ACF2 sites.

The following sections show an example for each security package.


The highlighted text and comments shown in the examples indicate the lines containing the recommended modification of DSN3SATH, which calls the module FOCDN3 the supplied exit.

After you finish the edits, assemble the exit into an object file. This object file is input to the link JCL found in one of the examples that follow.

-  **Note:**
- The positioning of these lines is approximate, assuming that no other changes or additions have already been made to DSN3SATH. If any changes have been made, you should decide on the most appropriate location for this call to FOCDN3.
 - FOCDN3 is used to set the proper primary (individual user ID) authorization.
 - Another program, FOCDN4, is used to set the proper secondary (group ID) authorization for RACF and eTrust CA-Top Secret. FOCDN4 is not needed with eTrust CA-ACF2; the secondary authorization ID(s) will be set correctly without it.

Changing DSN3SATH for RACF and eTrust CA-Top Secret Sites

1. Search for the **SATH001 label** - add two lines (FOCDN3):

 **Caution:** Code snippets in the PDF can have undesired line breaks because of space constraints. Before directly copying and running them in your program, they must be verified.

```
SATH001  DS      0H
        USING  WORKAREA,R11      ESTABLISH DATA AREA ADDRESSABILITY
        ST     R2,FREMFLAG        SAVE FREEMAIN INDICATOR
        XC     SAVEAREA(72),SAVEAREA CLEAR REGISTER SAVE AREA
        .
        .
        .
*****SECTION 1:  DETERMINE THE PRIMARY AUTHORIZATION ID *****
*
*  IF THE INPUT AUTHID IS NULL OR BLANKS, CHANGE IT TO THE AUTHID  *
```

```
* IN EITHER THE JCT OR THE FIELD POINTED TO BY ASCBJBNS. *
* THE CODE IN THIS SECTION IS AN ASSEMBLER LANGUAGE VERSION OF *
* THE DEFAULT IDENTIFY AUTHORIZATION EXIT. IT IS EXECUTED ONLY *
* IF THE FIELD ASXBUSER IS NULL UPON RETURN FROM THE RACROUTE *
* SERVICE. FOR EXAMPLE, IT DETERMINES THE PRIMARY AUTH ID FOR *
* ENVIRONMENTS WITH NO SECURITY SYSTEM INSTALLED AND ACTIVE. *
* *
*****
SPACE
    LA    R1,AIDLPRIM      LOAD PARM REG1          <--ADD
    CALL  FOCDSN3          GO GET THE IBI EXIT      <--ADD
    CLI   AIDLPRIM,BLANK    IS THE INPUT PRIMARY AUTHID NULL
    BH    SATH020          SKIP IF A PRIMARY AUTH ID EXISTS
```

2. Search for the SATH020 label - add a comment box, add one line, and comment out four lines:

```
SATH020 DS    0H          BRANCH TO HERE IF PRIMARY EXISTS
*****OPTIONAL CHANGE @CHAR7:  FALLBACK TO SEVEN CHAR PRIMARY AUTHID***
*
* IF YOUR INSTALLATION REQUIRES ONLY SEVEN CHARACTER PRIMARY *
* AUTHORIZATION IDS (POSSIBLY TRUNCATED) DUE TO DB2 PRIVILEGES *
* GRANTED TO TRUNCATED AUTHORIZATION IDS, THEN YOU MUST BLANK OUT *
* COLUMN 1 OF THE ASSEMBLER STATEMENT IMMEDIATELY FOLLOWING THIS *
* BLOCK COMMENT. THEN ASSEMBLE THIS PROGRAM AND LINK-EDIT IT INTO *
* THE APPROPRIATE DB2 LOAD LIBRARY AS EXPLAINED IN AN APPENDIX *
* OF "THE DB2 ADMINISTRATION GUIDE". *
* *
* OTHERWISE, YOU NEED DO NOTHING. *
* *
* @KYD0271*
*****
*      MVI   AIDLPRIM+7,BLANK    BLANK OUT EIGHTH CHARACTER
*      SPACE
*      .
*      .
*      .
* RACF IS ACTIVE ON THIS MVS
***** <--ADD
* * <--ADD
* The logic was modified because in DB2 V8 AIDLACEE is always not* <--ADD
* NULL. We used to honor AIDLACEE first, FOCDSN4 second and then * <--ADD
* AS ACEE. Now we honor FOCDSN4 first, AIDLACEE second and then * <--ADD
* AS ACEE. * <--ADD
* * <--ADD
* 03/11/05   ASK0 * <--ADD
***** <--ADD
    USING ACEE,R6          ESTABLISH BASE FOR ACEE      @KYL0108
    L      R6,AIDLACEE      Get => caller ACEE if any    <--ADD
* ICM     R6,B'1111',AIDLACEE CALLER PASSED ACEE ADDRESS? @KYL0108 <-COMMENT
* BZ      SATH024          NO, USE ADDRESS SPACE ACEE    @KYL0108 <-COMMENT
* CLC     ACEEACEE,EYEACEE  IS IT REALLY AN ACEE?         @KYL0108 <-COMMENT
```

```
* BE      SATH027          YES, PROCEED NORMALLY      @KYL0108  <--COMMENT
      SPACE 1
SATH024  DS      0H          USE ADDRESS SPACE ACEE      @KYL0108
.
.
.
```

3. Search for the SATH025 label - replace sath025 and add sath026 (FOCDSN4):

```
SATH025  DS      0H


      CALL  FOCDSN4          GO GET THE IBI EXIT (4=GROUP AUTH) <--ADD
      LTR   R6,R6          DOES AN ACEE EXIST?  IF NOT,      <--ADD
      BZ    SATH026        CHECK ACEE IN ADDRESS SPACE      <--ADD
      CLC   ACEEACEE,EYEACEE DOES IT LOOK LIKE AN ACEE?      <--ADD
      BE    SATH027        YES, GO DO GROUPS                <--ADD
SATH026  DS      0H          <--ADD
.
.
.
```

```
SATH027  DS      0H          CHECK LIST OF GROUPS OPTION
      TM    RCVTOPTX,RCVTLGRP IS LIST OF GROUPS CHECKING ACTIVE
      BZ    SATH040        SKIP TO SINGLE GROUP COPY IF NOT
      DROP  R7            DROP RCVT BASE REG
      SPACE 1
* RACF LIST OF GROUPS OPTION IS ACTIVE
      EJECT
.
.
.
```

Changing DSN3SATH for eTrust CA-ACF2 Sites

*DSN3SATH source is provided by ACF2.

1. Search for PRIMARY AUTHORIZATION ID - add two lines (FOCDSN3):

 **Caution:** Code snippets in the PDF can have undesired line breaks because of space constraints. Before directly copying and running them in your program, they must be verified.

```
*****
*                                     *
*          PRIMARY AUTHORIZATION ID          *
```

```

*
*****
*
*      IF THE PRIMARY AUTHORIZATION ID IS NULL OR BLANKS      *
*      IF CA-ACF2 IS AVAILABLE                                  *
*      SET PRIMARY ID FROM ACFASVT (ASVLID)                    *
*      ELSE                                                    *
*      IF TSO FOREGROUND USER                                  *
*      SET PRIMARY ID FROM TSO LOGON ID (ASCBJBNS)             *
*      ELSE                                                    *
*      SET PRIMARY ID FROM JOB USER (JCTUSER)                  *
*
*****
SPACE 2                                04260000
LA R1,AIDLPRIM LOAD PARM REG1          <--ADD
CALL FOCDSN3 GO GET THE IBI EXIT        <--ADD
CLI  AIDLPRIM,C' ' PRIMARY AUTHID THERE ? 04270000
BH   PRIMWTO ..YES, EVERYTHINGS OK HERE 04280000
L    R3,PSAAOLD-PSA(0) CURRENT ASCB ADDRESS 04290000
USING ASCB,R3 ASCB ADDRESSABILITY 04300000
SPACE 2                                04310000

```

Modifying the Link JCL for DSN3SATH

This is a sample link JCL for the IBM exit DSN3SATH. Modify the JCL to link the modules into the Db2 security exit as follows.

```

//LKED EXEC PGM=IEWL,PARM='LIST,XREF,LET,RENT,AMODE=31'
//OBJECT DD DSN=db2pref.SDSNSAMP.OBJ,DISP=SHR <--OUTPUT OF ASSEMBLE
STEP
//EDAMOD DD DSN=high_level_qualifier.HOME.LOAD,DISP=SHR
//SYSLMOD DD DSN=db2pref.DSNEXIT,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSUT1 DD UNIT=SYSDA,SPACE=(100,(50,50))
//SYSLIN DD *
INCLUDE EDAMOD(FOCDN3)
*****
*** Omit the following line for eTrust CA-ACF2
*****
INCLUDE EDAMOD(FOCDN4)
ENTRY DSN3@ATH
NAME DSN3@ATH(R)
/*

```

where:

db2pref

Is the prefix for the Db2 data sets.

high_level_qualifier

Is the high-level qualifier for the data sets.

Once this job finishes successfully, you must recycle the Db2 subsystem in order for the changes to take effect.

Upgrading From a Release Prior to 8207.27 to Release 8207.27 or Higher

If you are upgrading from a release that did not support the Golden Key (in which you needed to supply a license key in order to install the server) to a release that supports the Golden Key (in which you do not need a license key in order to install the server), you may need to perform a one-time prerequisite step.

In Release 8207.27 and higher, the only type of server that can be installed is a WebFOCUS Reporting Server. This server provides all of the functionality that was available in prior releases for a Full Function Server or ibi Data Migrator Server. A WebFOCUS Reporting Server requires a configuration directory named `wfs` directly under the server installation root directory.

If you install an ibi Data Migrator Server, you have a directory named `dm` instead of `wfs`. If you installed a Full Function Server, you have a directory named `ffs` instead of `wfs`.

1. In TSO, edit member `EDAENV` that is in your current configuration directory (either `ffs` or `dm`), for example:

```
srvhlq.FFS.DATA(EDAENV)
```

or

```
srvhlq.DM.DATA(EDAENV)
```

where:

srvhlq

Is the high-level qualifier for your server installation directory, for example, `IBI.SERVER.SRV93`.

Change the configuration directory path. For example, assume your `EDAENV` member has the following entry

```
EDACONF=/ibi/server/srv93/ffs
```

or

```
EDACONF=/ibi/server/srv93/dm
```

Change ffs or dm to wfs and save the file.

```
EDACONF=/ibi/server/srv93/wfs
```

2. Exit TSO, and go to your server installation directory under USS. You can issue the OMVS command to enter the USS environment.

For example, if your server installation directory is /ibi/server/srv93, issue the following command:

```
cd /ibi/server/srv93
```

3. Copy your existing configuration directory to a new configuration directory named wfs, using the following command.

For a Full Function Server:

```
cp -R ffs wfs
```

For an ibi Data Migrator Server:

```
cp -R dm wfs
```

After you have completed and tested the upgrade, you can delete the original ffs or dm directory.

Reconfigure Security

For information about configuring server security, see [Configure Security](#).

To reconfigure server security to OPSYS provider only:

1. Log on to TSO using an ID with read access to the BPX.FILEATTR.APF facility class.
2. Using the name of the actual EDAHOME directory, change file attributes by entering the following TSO commands in ISPF Command Shell (option 6):

```
OSHELL extattr +a /u/iadmin/ibi/srv93/home/bin/tscom300.out
```

```
OSHELL extattr +a /u/iadmin/ibi/srv93/home/bin/tsqprx.out
```

3. Verify your changes by issuing the following commands:

```
OSHELL ls -E /u/iadmin/ibi/srv93/home/bin/tscom300.out
```

```
OSHELL ls -E /u/iadmin/ibi/srv93/home/bin/tsqprx.out
```

The extended attributes portion of the output should be a-s-.

4. The libraries allocated to STEPLIB in IRUNJCL must be APF-authorized. Any non-APF-authorized libraries must be allocated the TASKLIB DDNAME.
5. Test server security by repeating the process described in Test the Installation.

This step will need to be repeated after any server upgrade since these files are replaced during an upgrade.

Preventing Unsecured Starts After Upgrades

If the security provider is set to OPSYS in the configuration file and, additionally, the explicit environment variable EDAEXTSEC is set to OPSYS (or ON), and the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the edaprint log.

This feature prevents an unsecured server start after a software upgrade if any of the required post-upgrade reauthorization steps are missed on a UNIX, IBM i, or z/OS USS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server edaenv.cfg configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
I Configured primary security is 'OPSYS' as set in configuration file
```

```
E Server security explicitly set to OPSYS, but lacks authority!
```

```
Workspace initialization aborted.
```

```
(EDA13171) UNABLE TO START SERVER
```

Reconfigure Adapters

While most adapters do not require additional steps after updating binary files, the following table notes the adapters that do require some consideration.

Adapter	Steps After Updating Binaries
Adabas	<ul style="list-style-type: none"> • Re-enable the module containing SVC using the WebFOCUS Reporting Server browser interface adapter configuration page. • Test the adapter from the adapter page before running your applications.
Db2 CAF	<ul style="list-style-type: none"> • Rebind the Db2 plan using the WebFOCUS Reporting Server browser interface adapter configuration page. • Test the adapter from the adapter page before running your applications.

Accounting for ZFS - SMF Records

The server provides an optional facility to use for accounting purposes that enables you to log resource utilization on a per-user basis. This facility enables the server to generate SMF records for query-level and user-level accounting.

Server accounting requires that the server STEPLIB data sets be APF-authorized. When SMF records are generated, they contain:

- The logon ID and security ID of the user.
- The CPU time and EXCPs consumed.
- Data based on the type of record written.

You can process the SMF records using the accounting programs that exist at your site. Examples of SMF records are provided in [SMF Record Format for RECTYPES 1 and 4](#).

In order to write SMF records, the server must be running APF authorized.

Two sample Master Files (SMFVSAM and SMFFIX) are provided for accessing accounting statistics. They reside under the catalog subdirectory in the EDAHOME location. Their difference is that SMFVSAM can be used to report directly from the system-live SYS1.MANx records, while SMFFIX can be used to report from a sequential file produced from running the SMFDUMP utility. These Master Files enable you to interpret the SMF records generated by the accounting facility using reporting requests or store procedures. Both Master Files are for logoff records only, as indicated by ALIAS=2 on the RECTYPE field entry.

A sample procedure report to query the SMF data is also provided under the same location. It is called smfman1.fex.

Enable Accounting

To enable accounting, insert the following statement into the server configuration file (edaserve.cfg):

```
smf_recno=smfnumber
```

where:

smfnumber

Is an integer in a range from 128 to 255, inclusive. This number represents the SMF number used by the accounting facility when it sends records to the SMF system.

By default, both RECTYPE pairs will be created when accounting is enabled. You can override the default by coding the following parameter on edaserve.cfg:

```
smf_subtype = {all|logon|query}
```

where:

all

Cuts all records. This is the default.

logon

Cuts logon records only (RECTYPE pair 1 and 2).

query

Cuts query records only (RECTYPE pair 4 and 5).

Set the Accounting Field

Up to 40 characters can be supplied that appear in the SMF records field SMFOFA40. The SET BILLCODE command can be used in any support server profile to provide the account field information. The syntax is

```
SET BILLCODE=value
```

where:

value

Is the 1–40 characters to be used on each SMF record produced.

This information can also be set dynamically from a client application by coding an RPC with the SET command and executing it with the value as a parameter. WebFOCUS users can send the SET command to the server.

Report From SMF Data

To report from SMF data, execute the sample procedure **smfman1.fex**, provided under home/catalog (DDNAME EDAHFEX for a PDS Deployment server).

You will be prompted for the DSN of the SMF VSAM data set from which you want to report, and the **smf_recno** value used to produce the SMF records.

The following is a listing of smfman1.fex

```
DYNAM ALLOC FI SMFVSAM DSN &SMFDSN.Please provide SMF VSAM DSN. SHR REU

DEFINE FILE SMFVSAM

CPU/D8.2 = SMFOFCPU / 100 ;

USER/A20 = SMFOFUID ;
```

```

EXCPS/I6 = SMFOFEXC ;

TIME/D9.2 = SMFOFLTM / 100 ;

HR/I2 = SMFOFTME / 360000 ;

MIN/I2 = (SMFOFTME - (HR*360000)) / 6000 ;

TOD/A5 = EDIT(HR) | ':' | EDIT(MIN) ;

END

TABLE FILE SMFVSAM

PRINT USER CPU EXCPS TIME TOD

WHERE SMFOFRTY EQ &SMFNUM.Please provide SMF number(type) for report.

END

```

SMF RECTYPES

There are four RECTYPE values defined to produce SMF records:

RECTYPE	Description
1	Indicates a start of task record. When included in a report, these statistics tell when a task initiation occurred, and are of no particular use in chargeback. By pairing start and end of task records for all tasks within a time period, statistics, such as average active time, peak task count, and average task count, can be determined. These values can be used for future capacity planning activities for the server.
2	Indicates the start of a task record. When included in a report, these statistics tell when a task termination occurred. These records are cut for both publicly and privately deployed services and contain statistics for the subtask as a whole. For privately deployed services, RECTYPE (2) records contain statistics associated with a single user connection.

RECTYPE	Description
4	Begin query. Record layout is the same as RECTYPE (1).
5	End query. Record layout is the same as RECTYPE (2).

SMF Record Format for RECTYPES 1 and 4

The record format for RECTYPES 1 and 4 of the SMF records written by the server is defined below. The format is provided in the System 390 assembler DSECT form.

```

SMFON      DSECT

          SPACE

*-----*

*  USAGE ACCOUNTING SMF RECORD LAYOUT FOR LOGON RECORDS.          *

*                                                                    *

*  THIS IS THE DSECT DESCRIBING THE SMF RECORD WHICH IS PASSED TO  *

*  YOUR EXIT ON AT USER LOGON TIME.  IT IS COMPLETELY READY TO BE  *

*  WRITTEN WHEN YOUR EXIT RECEIVES CONTROL.                        *

*-----*

          SPACE

```

```

*-----*

*  THE FIRST TWENTY FOUR BYTES OF THE RECORD ARE THE SMF HEADER.    *

*  THESE FIELDS ARE REQUIRED IN ALL SMF RECORDS (18 BYTES FOR RECORDS *

*  WITHOUT SUBTYPES; WE USE SUBTYPES, THE HEADER IS 24 BYTES).      *

          SPACE

```


SMFONLEN DS	H'116'	RECORD LENGTH
SMFONSEG DS	XL2'0000'	SEGMENT DESCRIPTOR (0 UNLESS SPANNED)
SMFONFLG DS	XL1	SYSTEM INDICATOR
SMFONRTY DS	XL1	RECORD TYPE
SMFONTME DS	XL4	TIME, IN HUNDREDTHS OF A SECOND
SMFONDTE DS	PL4	DATE, 00CYYDDDF, WHERE F IS THE SIGN
SMFONSID DS	CL4	SYSTEM IDENTIFICATION
SMFONSBS DS	CL4	SUBSYSTEM IDENTIFICATION
SMFONSBT DS	XL2'0001'	SUBTYPE OF RECORD - X'0001' INDICATES X THIS IS A LOGON RECORD

SPACE

* THE NEXT FIELDS ARE THOSE PRESENT IN THE LOGON *

* RECORD FOR THE START OF A USER SESSION. *

SPACE

SMFONMSO DS	CL8	JOBNAME
SMFONJID DS	CL8	JOBID (FROM SSIBJBID)
SMFONASI DS	Y	ASID
SMFONRV1 DS	XL2	RESERVED
SMFONUID DS	CL20	SECURITY USERID
SMFONLID DS	CL20	USERID PRESENTED AT LOGON (SAME AS X SMFONSID UNLESS CHANGED VIA MSIDTR X

			SECURITY EXIT)
SMFONRSV	DS	XL8	RESERVED FOR FUTURE EXPANSION
SMFONCTI	DS	XL4	RESERVED FOR FUTURE EXPANSION
SMFONSRV	DS	CL8	SERVICE NAME FROM SERVICE BLOCK
SMFONRS0	DS	XL4	RESERVED FOR FUTURE EXPANSION
SMFONCNT	DS	XL1	CONNECTION TYPE
	SPACE		
SMFONTSO	EQU	1	CONNECTION VIA TSO
SMFONCIC	EQU	2	CONNECTION VIA CICS
SMFONVTM	EQU	4	CONNECTION VIA VTAM
SMFONPSR	EQU	8	
	SPACE		
SMFONRS1	DS	XL3	RESERVED
SMFONID1	DS	F	SYSPLEX ID 1
SMFONID2	DS	F	SYSPLEX ID 2
SMFOFPID	DS	XL20	POOLED USER ID
SMFONRS2	DS	XL12	RESERVED
SMFONL	EQU	*-SMFON	LENGTH OF THE SMF LOGON RECORD

SMF Record Format for RECTYPES 2 and 5

The record format for RECTYPES 2 and 5 of the SMF records written by the server is defined below. The format is provided in the system 390 assembler DSECT form.

SMFOFSBS DS	CL4	SUBSYSTEM IDENTIFICATION
SMFOFSBT DS	XL2'0002'	SUBTYPE OF RECORD - X'0002' INDICATES X THIS IS A LOGOFF RECORD
SPACE		

```

*-----*
*  THE NEXT FIELDS ARE THOSE PRESENT IN THE LOGOFF                      *
*  RECORD FOR THE END OF A USER SESSION.                                *
*-----*

```

SPACE		
SMFOFMSO DS	CL8	JOBNAME
SMFOFJID DS	CL8	JOBID (FROM SSIBJBID)
SMFOFASI DS	Y	ASID
SMFOFRV1 DS	XL2	RESERVED
SMFOFUID DS	CL20	SECURITY USERID
SMFOFLID DS	CL20	USERID PRESENTED AT LOGON (SAME AS X SMFOFSID UNLESS CHANGED VIA MSIDTR X SECURITY EXIT)
SMFMEMA DS	XL4	MEMORY ABOVE THE LINE (IN KILOBYTES)
SMFMEMB DS	XL4	MEMORY BELOW THE LINE (IN KILOBYTES)
SMFZIIP DS	XL4	ZIIP CPU NORMALIZED (HUNDREDTHS OF A SEC)
SMFOFSRV DS	CL8	SERVICE NAME FROM THE SERVICE BLOCK
SMFZPOCP DS	XL4	ZIIP ON CP (HUNDREDTHS OF A SEC)

SMFOFCNT	DS	XL1	CONNECTION TYPE	
		SPACE		
SMFOFTSO	EQU	1	CONNECTION VIA TSO	
SMFOFCIC	EQU	2	CONNECTION VIA CICS	
SMFOFVTM	EQU	4	CONNECTION VIA VTAM	
SMFOFPSR	EQU	8		
SMFOFCC	DS	XL3	COMPLETION CODE FOR THE TASK	
SMFOFACT	DS	CL8	USER ACCOUNTING INFORMATION; THIS FIELD CURRENTLY PASSED AS LOW VALUE	X
SMFOFCPU	DS	XL4	CPU TIME IN HUNDREDTHS OF A SECOND	
SMFOFEXC	DS	XL4	COUNT OF EXCP'S	
SMFOFLTM	DS	FL4	LOGON DURATION IN HUNDREDTHS OF A SECOND	X
SMFPRTY	DS	XL1	PRIORITY	
SMFCOMPL	DS	XL1	COMPLETION TYPE	
	DS	XL2	RESERVED	
SMFOFID1	DS	F	SYSPLEX ID 1	
SMFOFID2	DS	F	SYSPLEX ID 2	
SMFOPID	DS	XL20	POOLED USERID	
SMFOFA40	DS	CL40	FULL 40-BYTE ACCOUNTING FIELD	
		SPACE		
SMFOFL	EQU	*-SMFOF	LENGTH OF THE SMF LOGOFF RECORD	

Accounting for Db2 in an ibi WebFOCUS Reporting Server Task

When using a server to access Db2 data, certain processing takes place within the Db2 address space and is governed by the Db2 chargeback system. If a user requests data from Db2, the server passes the request to the Db2 subsystem. The Db2 subsystem then processes the request, performing such tasks as retrieving rows and aggregating the data. It generates the answer set, and passes the output back to the server. The server then performs any joins and formatting which have not been performed by Db2 to satisfy the original request.

Charges incurred while the request was being processed by the Db2 subsystem are added to the charges accumulated in the server task that originated the request for processing. If the server accounting is enabled, these charges are associated with the user logon and security IDs in the SMF records described earlier.

Enabling Use of the zIIP Specialty Engine

If your site has a zIIP (System **z** Integrated Information **P**rocessor) specialty engine from IBM, you can offload specific categories of workload from the Central Processors to the zIIP.

The zIIP engine is a restricted version of a Central Processor (CP), also referred to as a General Processor (GP). The capacity of the zIIP engine does not count toward the overall MIPS rating of the mainframe image, so the CPU usage incurred on the zIIP is effectively free. Central Processors are often configured to run at speeds below their maximum rating for cost saving and capacity planning purposes. For Central Processors, *100% capacity* typically refers to the maximum MIPS that the processor is allowed to generate at that installation, in accordance with your contract with IBM. In contrast, the zIIP engine always runs at true 100 percent of capacity.

As much as 80 percent of server processing is enabled to run on the zIIP engine. Typical workloads are expected to offload 30 to 80 percent of CPU processing to the zIIP engine.

To make use of the zIIP enablement feature, the server must run in an authorized state.

What Is a zIIP Specialty Engine?

Though physically identical to a central processor, the zIIP engine is microcoded at installation time to run specific types of workloads. The central processor continues to handle the operating system, I/O interrupts and timer interrupts, job initiations, and user interactions with the operating system. The zIIP concentrates on CPU intensive workloads, leaving the central processor more time to absorb otherwise queued workloads, thereby achieving some overall performance improvement across all mainframe activity.

Steps to zIIP Enablement

This section describes steps and requirements for the server use of the zIIP processor.

The steps to server zIIP enablement are:

1. Obtain APF authorization for the server load library.
2. Activate the zIIP feature using the SET ZIIP=ON or SET ZIIP=ON/SIMMAXZIIP command. For instructions, see [Activating a zIIP Environment or Projecting zIIP Usage](#).

Usage Notes for Use of the zIIP Processor

- Maximize the block sizes of data sources that are read or written by the server to reduce the number of I/Os required to access the file. This will reduce the number of switches to non-zIIP mode that the server agents have to make, thus permitting a greater percentage of zIIP contribution to the request.
- Move or rewrite functions developed at your site since the server must switch to non-zIIP mode for each call to such routines. You may be able to use one of the following possible solutions:
 - Move the routines from DEFINES to COMPUTEs to reduce the number of times they are referenced. This tactic must be applied carefully, and only when report results would not change.
 - Rewrite the routines using DEFINE FUNCTION, which executes on the zIIP processor.

- Confine the routine to a pre-step run with ZIIP=OFF which collects its calculated results, then use those calculations in the next step with ZIIP=ON.

Activating a zIIP Environment or Projecting zIIP Usage

The last step in zIIP enablement is to activate the use of the zIIP processor in the server. zIIP enablement is activated by the SET ZIIP command.

The SET ZIIP command has three options:

- **OFF.** This setting prevents the server from offloading its processing to a zIIP.
- **ON.** This setting causes the server to offload processing to a zIIP engine if you have a zIIP processor and the environment is properly APF-authorized.
- **ON/SIMMAXZIIP.** This setting enables you to project zIIP processing in two different environments:
 - **You do not have a zIIP processor.** Using this setting along with the PROJECTCPU parameter, you can project how much server workload would have been offloaded to a zIIP.
 - **You do have a zIIP processor.** Using this setting you can project how much advantage you would achieve by offloading 100% of eligible server processing to the zIIP.

Activate the zIIP Enablement Feature

You can issue the SET ZIIP command in a server profile or in a particular FOCEXEC.

```
SET ZIIP={ON[/SIMMAXZIIP] | OFF}
```

where:

ON

Configures the server to offload processing to the zIIP engine.

This setting:

- Determines if the zIIP processor is accessible to the LPAR in which a job is running.
- Determines if the server environment has been properly authorized to run a zIIP workload.

i Note: If the server determines that the zIIP processor is not accessible or that the environment has not been authorized correctly, it issues a message describing the reason and continues in ZIIP=OFF mode, which forwards all subsequent work to the central processor.

ON/SIMMAXZIIP

Configures the server to either:

- Project what the zIIP usage would be if the server could offload processing to a zIIP, when the server is operating in an LPAR without a zIIP. This requires that the PROJECTCPU parameter be set to YES.

The SYS1.PARMLIB member IEAOPTxx contains the PROJECTCPU statement. Activating the PROJECTCPU parameter projects zIIP consumption when a zIIP processor is not yet defined to the LPAR. SMF type 30 records will show the potential calculated zIIP time, so that you can accurately project zIIP usage. This enables you to evaluate the effect of configuring a zIIP processor to be available for server usage. The Systems Programmer for your site will have access to this data. Use this option for simulation purposes only.

Since the zIIP engine is actually not present, all zIIP-eligible workload will be diverted to the central processor. Thus, all of that CPU utilization will be recorded in a server variable called &FOCZIIPONCP. This is the amount of workload that would have run on the zIIP engine, and would have appeared in &FOCZIIPCPU, had the zIIP been present and accessible to server work. This information is also recorded in the server job statistics as well as in IBM SMF type 30 records.

To use this option, insert the following parameter in SYS1.PARMLIB for your LPAR, and also issue the SET ZIIP=ON/SIMMAXZIIP command:

```
PROJECTCPU=YES
```

This setting:

- Determines if the PROJECTCPU=YES command has been set in the LPAR.
- Determines if the server environment has been properly authorized to run a zIIP workload.
- Projects zIIP utilization if 100% of eligible server processing could be offloaded to the zIIP, when the server is running in an LPAR with a zIIP. This lets you determine what you would gain by configuring Workload Manager to give the server a bigger share of zIIP processing.

IBM Workload Manager (WLM) prioritizes workloads among the central processors and zIIP processors at your site based on a complex set of goals and rules established by the system administrator. These rules apply to all workloads from all sources, not just the server. These goals combine to influence the decision to direct server requests to the zIIP engine at any particular moment.

Utilizing this setting with a zIIP present can help you determine how much advantage you would get if the server had more of a share of the zIIP processor. To see the difference in actual and projected zIIP usage, run the same job with SET ZIIP=ON and then with SET ZIIP=ON/SIMMAXZIIP and compare the results. For more information about evaluating zIIP usage, see [Evaluating zIIP Usage](#).

This setting:

- Determines if the zIIP processor is accessible to the LPAR in which a job is running.
- Determines if the server environment has been properly authorized to run a zIIP workload.

i Note: If the server determines that the environment has not been authorized correctly, it issues a message describing the reason and continues in ZIIP=OFF mode, which forwards all subsequent work to the central processor.

OFF

Configures the server not to offload processing to the zIIP engine. OFF is the default value.

i Note: Turn off zIIP enablement only when you know for sure that a job will not gain any advantage from using the zIIP processor or if the system operator or administrator requires that you turn it off.

Setting the PROJECTCPU Parameter in SYS1.PARMLIB Member IEAOPTxx

Use the following sample as a guide for setting the PROJECTCPU parameter in SYS1.PARMLIB(IEAOPTxx):

```
/* ***** */
/*          SYS1.PARMLIB(IEAOPTxx)          */
/* ***** */

PROJECTCPU=YES
```

How the ibi WebFOCUS Reporting Server Takes Advantage of the zIIP Processor

The server diverts eligible workload to the zIIP engine by switching from TCB (Task Control Block) mode for workloads that can run only on a Central Processor to SRB (Service Request Block) mode for execution of enabled workloads on the zIIP engine.

Types of server processing that are offloaded to the zIIP engine include:

- Computations
- Aggregation
- Screening
- Sorting
- Report formatting and styling
- Transaction Processing

The server zIIP Monitor detects situations in which the overhead cost of zIIP usage is exceeding the CPU benefits gained. When this threshold is reached, the server may decide to suspend use of the zIIP for the duration of a logical phase of the server request. When it does so, it places a message to that effect in the JES log. It then resets to make the zIIP processor accessible to the next logical phase of the server request.

TABLE, MATCH, MODIFY, and MORE requests may suspend and resume more than once as they progress through the logical phases of execution.

In every case, the server attempts to optimize the use of the zIIP and minimize chargeable CPU costs.

Applications that perform significant database I/O, high-volume sorting, or the use of third-party tools or user functions during processing require switching out of SRB (zIIP) mode into TCB (non-zIIP) mode to communicate, and then back again to continue processing. Although each switch is minuscule, the cumulative effect can absorb measurable amounts of CPU time on both the zIIP engine and the Central Processor.

In order to diminish this effect, the server buffers the collection of records passed to the system sort utility and some adapters rather than passing one record at a time, thus reducing the number of switches between TCB and SRB modes.

These third-party products may themselves be zIIP enabled and may offload some or all of their processing to the zIIP engine independent of the server. The server always calls these products from the Central Processor because it cannot know whether they will perform any processing that is prohibited on the zIIP.

Even though zIIP usage occurs more frequently on non-optimized requests to a relational data source, optimized requests are still inherently more efficient and, therefore, may incur less CPU time. Being zIIP enabled, Db2 may also take advantage of the zIIP processor for server requests based on the local configuration of Db2 relative to the server.

Requests against some types of data sources whose I/O can be buffered gain a lot of advantages from zIIP enablement. Data sources that gain the most benefit from zIIP processing due to buffered I/O include:

- Blocked flat files
- FOCUS
- XFOCUS
- VSAM
- Db2

Evaluating zIIP Usage

In order to evaluate server zIIP processing in a session, you can query three Dialogue Manager variables that accumulate statistics about CPU processing:

- &FOCCPU accumulates the time spent on a Central Processor. This is an existing variable that precedes zIIP enablement.
- &FOCZIIPCPU accumulates the time actually spent on the zIIP processor (in SRB mode). This is the normalized CPU value using the same scale as &FOCCPU.
- &FOCZIIPONCP accumulates the time that processing could have been offloaded to the zIIP processor but was diverted to the Central Processor by the system.

**Note:**

- &FOCCPU includes the value of &FOCZIIPONCP.
- The sum of &FOCZIIPCPU and &FOCCPU represents the total CPU utilized by the server agent.
- If you set ZIIP=OFF, the zIIP variables do not accumulate further but are not reset to zero. If you later set ZIIP=ON, they resume accumulating statistics.

The RM (Resource Manager) that monitors server usage also captures zIIP statistics.

Performance Considerations for ZFS

There are several ways in which you can improve the server performance:

- **Non-swappable address space.** We recommend that you run the server in a non-swappable address space. For more information, see [Running the ibi WebFOCUS Reporting Server in a Non-Swappable Address Space](#).
- **Workload Manager (WLM).** You can balance server workload by using Workload Manager. For more information, see [Workload Manager](#).

Running the ibi WebFOCUS Reporting Server in a Non-Swappable Address Space

We recommend that you run the server in a non-swappable address space. In order to make the server address space permanently non-swappable, add the following entry to SYS1.PARMLIB(SCHEDxx):

PPT PGMNAME(TSCOM300)	/* PROGRAM NAME */
NOSWAP	/* NON-SWAPPABLE */
CANCEL	/* CAN BE CANCELLED */

Do not use the KEY 0 parameter, or any other parameter (such as NOPASS), unless the system programmer completely understands the consequences of adding the parameter.

All local spawn transactions are performed in the mode of the server. For example, if the server address space is non-swappable, all local spawn transactions execute as non-swappable.

The server executes limited non-local spawn, such as when the user executes a UNIX system command. Non-local spawn execute as swappable.

The server never executes a fork subroutine. (A fork subroutine creates a new process. The new process, called the child process, is an almost exact copy of the calling process, which is called the parent process.)

Workload Manager

Although the server may run in a specific performance group, transactions submitted by server agents may perform differently than the server by adding the following keyword to edaserve.cfg:

```
wlm_enclave_trname = WLM_transaction_name
```

where:

WLM_transaction_name

Can be up to 8 characters.

This is a service-level keyword.

Using this setting, the task will join a Workload Manager (WLM) enclave when a request starts, and leave the enclave when the request finishes. This gives WLM control of the dispatching priority of the task. The transaction rules defined on WLM will determine the default service class assigned to this transaction, and that service class will determine how the request runs.

This feature helps to balance a workload so that a long request will not affect a short request. This can be achieved through WLM rules designed to lower the priority of a long request after a certain period of time. Without this feature, all requests share the region priority.

The transaction name passed in this keyword must match one defined in the WLM Classification Rules for the Job Entry Subsystem (JES). A corresponding WLM Service Class pointed to by this rule will then be associated with this service.

The classification rules for JES must be used even if the server is started as a started task. The subtasks are always run under JES.

For example, you would include the following in edaserve.cfg:

```
SERVICE = DEFAULT

BEGIN

wlm_enclave_trname = IWAYFAST

.

.

.

END
```

The WLM definition is:

```
Subsystem Type JES - Batch Jobs

Classification:

Default service class is PRDBATLO

There is no default report class.
```

Qualifier	Qualifier	Starting	Service	Report
-----------	-----------	----------	---------	--------

#	type	name	position	Class	Class

1	TN	IWAYFAST		EDAQRYHI	

WLM subrules (levels 2 and above) are supported. For a server request to join an enclave in a particular service class, the names of all rule qualifiers below our transaction name are checked.

For example, consider the following WLM definition:

Subsystem Type JES - Batch Jobs

Classification:

Default service class is PRDBATLO

There is no default report class.

Qualifier	Qualifier	Starting Service	Report
#	type	name	position Class Class

1	SSC	PRDMVS	PRDDFLT
2	. TN	. IWAYFAST	EDAQRYHI

In this particular case, the qualifier 1 type is SSC (Subsystem Collection), and a server request will only join the enclave IWAYFAST if it is running on a particular LPAR in the SYSPLEX. This qualifier (PRDMVS) must match the XCF group definition: issue \$DMASDEF (for JES2) and check the value of XCFGRPNM field.

You can handle WLM scheduling environments by defining them to WLM and then adding the JOB statement parameter SCHENV=xxxxx to the ISTART JCL.

Troubleshooting for ZFS

To troubleshoot an installation problem, identify your problem in the following list, and follow the link to a description of the solution.

If you cannot find your problem described in the list, and cannot resolve it yourself, contact Customer Support . In addition, supply the following information to Customer Support:

- Server trace (see [Generate a Trace](#)).
- JCL for IRUNJCL.
- Job output.
- System dump, if needed (see [Generate a System Dump](#)).
- Any additional information regarding how the problem occurred.

Problems:

- The server abends with a U4039 code.
For details, see [Problem: The ibi WebFOCUS Reporting Server Abends With a U4039 Code](#).
- INSUFFICIENT AUTHORITY TO GETSPENT messages appear in JESLOG.
For details, see [Problem: INSUFFICIENT AUTHORITY TO GETPSENT messages in JESLOG](#).
- The request fails, and *JVM not found* messages are written to edaprint.log.
For details, see [Problem: Request fails, and JVM not found messages written to edaprint.log](#).

Problem: The ibi WebFOCUS Reporting Server Abends With a U4039 Code

Problem: The server abends with a U4039 code.

Cause: This is a generic abend.

Solution: Find out what caused the abend by checking the edaprint.log file, SYSOUT ddname, and the MVS system log.

Problem: INSUFFICIENT AUTHORITY TO GETPSENT messages in JESLOG

Problem: INSUFFICIENT AUTHORITY TO GETPSENT messages appearing in JESLOG.

Cause: See IBM APAR II11813.

Solution: The APAR recommends issuing one of the following RACF commands:

```
SETROPTS LOGOPTIONS (NEVER(PROCACT))  
SETOPTS LOGOPTIONS (DEFAULT(PROCACT))
```

However, when a non-superuser in the OMVS shell issues the command `ps -ef`, the following security message is repeated in SYSLOG:

```
ICH408I USER(default) GROUP(dgltgrp) NAME(bpxdefaultuser) 060  
CL(PROCACT) INSUFFICIENT AUTHORITY TO GETPSENT
```

This does not indicate an error. It is an informational message issued because of RACF LOGOPTIONS settings. The `ps -ef` command is a request to show all processes that the requester is authorized to see, but a non-superuser is allowed to see only his or her own processes.

Problem: Request fails, and *JVM not found* messages written to edaprint.log

Problem: The request fails, and *JVM not found* messages are written to edaprint.log.

Cause: If the server cannot find the Java Virtual Machine (JVM), the JSCOM Listener will not be able to start, and messages will be written to the server log stating that the JVM cannot be found.

Solution: Specify the location of the JVM in JDK_HOME or JAVA_HOME. For more information, see [JVM Requirements for Java Services \(Server Installations Only\)](#).

Secured ibi WebFOCUS Reporting Server Starts Unsecured or Does not Start After Upgrade

A server will implicitly attempt to start unsecured if proper authorization steps have not been completed. Starting the server normally clears edatemp. If prior edatemp files exist (and authorization has not been done), start-up will fail due to an inability to clear the directory. However, if an edastart -cleardir command was issued just before the upgrade, there is nothing to clear, no error occurs, and the server starts. If the server starts and is not inspected after the initial start-up, the server being in the wrong mode may go unnoticed.

The proper solution is to add proper authorizations after an upgrade, as described in [Reconfigure Security](#), and restart the server. A new safety measure has also been added. If the environment variable EDAEXTSEC is set to OPSYS explicitly, and a server lacks authorization, it will not start (see [Preventing Unsecured Starts After Upgrades](#) for details).

Generate a Trace

To generate a server trace:

Procedure

1. Turn tracing by going to the WebFOCUS Reporting Server browser interface menu bar, selecting **Workspace**, and then **Diagnostics**, or by running the ITRCON JCL member.
2. Reproduce the problem.
3. Submit the ISAVEDIA member to produce the diagnostic information.

A directory called `sdnnnnnn` is created under your configuration directory (for example, `/ibi/srv/ffs/sd123456`). Diagnostic information is placed in this directory. Make sure you have access to this directory.

Result

Do not change anything in the EDAENV member. Changes could prevent the correct information from being copied to your directory.

Generate a System Dump

To generate a system dump:

Procedure

1. Allocate DDNAME SYSMDUMP pointing to the data set with the following DCB parameters:

```
RECFM=FB,LRECL=4160,BLKSIZE=4160
```

2. To get the first dump, add the parameter FREE=CLOSE to your DD statement. The DD statement should appear as follows:

```
//SYSMDUMP DD DISP=SHR,DSN=MYID.EDAPTH.SYSMDUMP,FREE=CLOSE
```

3. To get the last dump, the statement should appear as follows:

```
//SYSMDUMP DD DISP=SHR,DSN=MYID.EDAPTH.SYSMDUMP
```

Only two IDs must have privileges to write into this data set: ISERVER and IADMIN. General server users DO NOT need read or write access to the SYSMDUMP data set.

4. To prevent Abend-AID from intercepting the dump, add:

```
//ABNLIGNR DD DUMMY
```

5. To prevent the Language Environment from intercepting the dump, specify:

```
EDADUMPOPT=UAIMM in EDAENV DD
```

This enables you to get more accurate information reflecting the moment the abend actually occurs.

6. Save the entire job output for the server (including JES logs), and send it to Customer Support.

Result

Instead of using JCL allocations to add SYSMDUMP, the procedure described below can be used alternatively.

Add JCL Allocations to a Running ibi WebFOCUS Reporting Server

A z/OS operator can issue modify commands from the z/OS system console to allocate DDNAMES to the server without restarting it. This procedure is useful if you need to reallocate a file that was freed to allow a batch overnight utility to run, or perhaps to add SYSMDUMP allocation to a running server.

Allocate a Data set From the z/OS System Console

```
F <iway_server_jobname/started task>,DYNAM ALLOC FI <ddname> DA <dsname>
<optional dynam parameters>
```

Allocating a VSAM Data set

```
F IWAY2,DYNAM ALLOC F VSAMFILE DA VSAM.FILEA.CLUSTER SHR
```

Allocating a SYSMDUMP Data set With FREE=CLOSE Option

```
F IWAY2,DYNAM ALLOC FILE SYSMDUMP DA PROD2.SYSMDUMP.DATA SHR CLOSE
```



Note: The examples above assume IWAY2 is the jobname/started task ID for the server.

All valid DYNAM ALLOC syntaxes are supported. For more information on the DYNAM command, refer to the *ibi™ WebFOCUS® Reporting Server Stored Procedure and Subroutine Reference for 3GL Languages* guide.

The following message will be issued in the server JESMSG LG indicating if the command was processed successfully or not.

Success:

```
+DYNAM COMMAND SUCCESSFULLY PROCESSED Rc=0
```

Failure:

```
+DYNAM ERROR: IKJ56225I DATA SET IWAY.TEST ALREADY IN USE, TRY LATER
```

Free Data sets Allocated to the ibi WebFOCUS Reporting Server

A z/OS operator can issue modify commands from the z/OS system console to free DDNAMEs or DSNAMES allocated to the server. Both global allocations (made at the server ISTART JCL) and local ones (DYNAM ALLOC commands issued by user tasks) can be freed. This procedure is useful if you need to free an allocation to run a batch utility overnight, without restarting the server.

Free a Data set From the MVS System Console

To free a single DDNAME:

```
F <iway_server_jobname/started task>,DYNAM FREE FI <ddname>
```

To free a single DSNAMES (all occurrences in the server):

```
F <iway_server_jobname/started task>,DYNAM FREE DS <dsname>
```

To free multiple DDNAMEs, passing a pattern (free all DDNAMEs starting with AB):

```
F <iway_server_jobname/started task>,DYNAM FREE FI AB*
```

To free multiple DSNAMES (all occurrences in the server), passing a pattern (free all allocations of data sets starting with IWAY.VSAM):

```
F <iway_server_jobname/started task>,DYNAM FREE DA IWAY.VSAM*
```

A message will be issued in the iway_server JESMSG LG indicating if the command was processed successfully or not, as follows.

Success:

```
+DYNAM COMMAND SUCCESSFULLY PROCESSED Rc=0
```

Failure:

```
+DYNAM ERROR: IKJ56225I DATA SET IWAY.TEST ALREADY IN USE, TRY LATER
```

Freeing an Allocated Data Set

Suppose ISTART JCL (jobname IWAY2) has the following allocation:

```
//VSAMFILE DD DISP=SHR,DSN=VSAM.FILEA.CLUSTER
```

The operator can free this file using the command (from the MVS console):

```
F IWAY2,DYNAM FREE FI VSAMFILE
```

PDS Deployment

The topics in this section describe how to install your server in a Partitioned Data Set (PDS) environment.

Installation Requirements for PDS

Before beginning server installation, review all requirements.

Operating System Requirements

The server runs on any supported release of z/OS. For current information about supported releases, see the *ibi™ WebFOCUS® Release Notes*.

In general, the operating system should have the latest cumulative patch levels applied.

Confirm that your server installation software is labeled for your operating system level.

IP Port Number Requirements

The installation process prompts for two IP port numbers: the TCP Listener and HTTP Listener. It also uses the next two consecutive ports after the supplied HTTP Listener port for FDS use. This results in a total of four IP ports.

The supplied IP port numbers must be above the IANA registered well-known reserve range (numbers under 1024) and not over the maximum legal number (65535). Do not use IP port numbers already used by other applications or products. Netstat, or netstat like commands, should reveal what actual ports are in use.

Browser Requirements

The WebFOCUS Reporting Server browser interface requires one of the following web browsers:

- Microsoft Edge.
- Mozilla Firefox® 59 or higher.
- Google Chrome® 65 or higher.

Disk Space Requirements

The server disk space requirements are:

Supplied (EDAHOME) Data Sets	3390 Cylinders
<i>high_level_qualifier.P.HOME.ACX</i>	2
<i>high_level_qualifier.P.HOME.BIN</i>	1100

Supplied (EDAHOME) Data Sets	3390 Cylinders
<i>high_level_qualifier.P.HOME.CICS.LOAD</i>	10
<i>high_level_qualifier.P.HOME.ERR</i>	500
<i>high_level_qualifier.P.HOME.ETC</i>	100
<i>high_level_qualifier.P.HOME.FEX</i>	25
<i>high_level_qualifier.P.HOME.LOAD</i>	750
<i>high_level_qualifier.P.HOME.MAS</i>	4

Configuration (EDACONF) Data Sets	3390 Cylinders
<i>high_level_qualifier.WFS.CONF.ACX</i>	2
<i>high_level_qualifier.WFS.CONF.CFG</i>	2
<i>high_level_qualifier.WFS.CONF.MAS</i>	2
<i>high_level_qualifier.WFS.CONF.PRF</i>	2

Installation Data Sets	3390 Cylinders
<i>high_level_qualifier.HOME.DATA</i>	10
<i>high_level_qualifier.WFS.DATA</i>	2

Application Data Sets	3390 Cylinders
<i>aproot.IBISAMP.type.DATA</i>	38 (across 14 data sets)
<i>aproot.BASEAPP.type.DATA</i>	56 (14 data sets using 4 cylinders per file)

Deferred Execution Data Sets (Optional)	3390 Cylinders
<i>high_level_qualifier.WFS.CONF.DFM.DEL</i>	5
<i>high_level_qualifier.WFS.CONF.DFM.RPE</i>	5
<i>high_level_qualifier.WFS.CONF.DFM.RPF</i>	5
<i>high_level_qualifier.WFS.CONF.DFM.RPO</i>	100
<i>high_level_qualifier.WFS.CONF.DFM.RQD</i>	5
<i>high_level_qualifier.WFS.CONF.DFM.RQF</i>	5
<i>high_level_qualifier.WFS.CONF.DFM.RQO</i>	5
<i>high_level_qualifier.WFS.CONF.DFM.RQP</i>	5



Note: Deferred Execution Datasets are not created by the installation procedure. They are created when the Scheduler/Deferred service starts. By default, the Scheduler/Deferred service auto starts at server startup. To disable the feature, enter `dfm_autostart = n` in the EDASERVE administration control file.

Supplementary Data Sets	3390 Cylinders
<i>high_level_qualifier.WFS.SYSRPC.FOCUS</i>	1
<i>high_level_qualifier.WFS.ETLLOG.FOCUS</i>	1
<i>high_level_qualifier.WFS.ETLSTATS.FOCUS</i>	1
<i>high_level_qualifier.WFS.CONF.SMARTLIB.DATA</i>	1

high_level_qualifier

Is the high-level qualifier to be used for all output libraries. This is the same high-level qualifier, which you specify during server installation.

approot

Is the default location for storing applications. You specify approot during server installation, as described in [Run isetup](#)

Memory Requirements

Memory usage of a configured environment consists of the following elements:

- Workspace Manager
- Listeners
- Concurrently running application agents

Actual memory usage depends on application features, and varies depending on the application. The SHRLIBRGNSIZE parameter (defined on SYS1.PARMLIB, member BPXPRMxx) can affect the amount of memory that the server address space will allocate. For SHRLIBRGNSIZE, we recommend the default MVS installation value of 64Mb:

```
SHRLIBRGNSIZE(67108864)
```

Server memory usage:

- The workspace (including Listeners) uses 200 megabytes.
- Each pre-started agent requires 4 megabytes.

The minimum amount of memory for a newly installed server with no workload is 250Mb. However, depending on usage, workload, and configuration options, 500Mb is recommended to start, to be adjusted as needed.

Communication Requirements

You need four TCP/IP ports for each server instance that you configure. Three of these ports must be consecutive. You specify these port numbers during installation. You may require additional ports depending on which options you configure later.

The server supports only IBM TCP/IP. It does not support Interlink or any other third-party TCP/IP.

USS Segment Requirements

PDS deployment requires each user of the server to be identified to USS by means of a default segment definition. This default OMVS segment is defined when USS is installed as a part of z/OS. Refer to your IBM UNIX System Services documentation for more information about this subject.

ZFS Home and Configuration Directory Requirements

Libraries and the APIs supporting them must reside in the ZFS file system to enable the following features:

- Server-side graphics

They are also required for the following Java-based and SAP-based adapters:

- Call Java
- EJB
- JDBC
- Microsoft SQL Server
- SQL SAP
- SAP BWB

At installation time, a panel with a list of adapters to be configured will be displayed. If any of the above adapters are selected, the installation will require the path for two ZFS locations as follows:

- **edahome_dir**. Provide the edahome path for the dll modules that interface with Java/SAP and must reside in ZFS. The directory will be created with 755 permissions, if it does not exist.
- **edaconf_dir**. Provide the edaconf path to be used for both configuration files (such as codepage files), as well as the root location for temporary files (such as traces and logs), that must reside in ZFS. If it does not exist, the directory will be created with 755 permissions.

If no data adapters were selected, the next panel will allow an optional configuration for the JSCOM3 listener. If server-side graphics support is desired, the listener must be configured and all three paths are required (edahome_dir, edaconf_dir, plus the path to Java passed to either JDK_HOME or JAVA_HOME).

If `edahome_dir` is not defined at installation time, it will not be possible to configure it later using the WebFOCUS Reporting Server browser interface. The server will have to be re-installed, configuring the JSCOM3 listener.

Installing New on PDS

To install a new Server for z/OS deployed using partitioned data set (PDS) libraries, perform the following steps.

Installing ibi WebFOCUS Reporting Server With ISETUP

WebFOCUS Reporting Server includes an automated installation and maintenance procedure named ISETUP. Use this procedure to install or apply maintenance to WebFOCUS Reporting Server.

There are aspects of the installation process that are not handled by ISETUP. These are detailed in this document and require manual intervention.

ISETUP asks you for the high-level qualifier for your WebFOCUS Reporting Server data sets. Based on this qualifier and a list of all of the standard data set names (low-level qualifiers), ISETUP installs all the necessary WebFOCUS Reporting Server libraries.

About the ISETUP Procedure

The ISETUP procedure is an interactive process that uses ISPF panels.



Important: You must use the version of ISETUP that comes with your WebFOCUS Reporting Server release to install WebFOCUS Reporting Server.

Installing without the use of ISETUP is no longer supported. Additionally, you cannot use previous versions of your installatio JCL to install Release 1.0.7.

You must run ISETUP from the ISPF command shell.

You should not use ISETUP to overwrite your current production WebFOCUS Reporting Server data sets with new versions.

Overview of the ISETUP Procedure

This topic provides a high-level overview of the installation procedure and the steps that may be needed after running the installation procedure.

Overview of the Electronic Download Process

The following is a high-level summary of how to receive the WebFOCUS Reporting Server release or maintenance electronically:

1. Download the appropriate `*mvs_zseries.run` file from [eDelivery](#).
2. Upload the file to a USS directory on your z/OS system.
3. Log in to USS.
4. Run this command to extract all the files and transfer them to PDS: `sh *mvs_zseries.run`
5. You are prompted to enter a PDS High-Level Qualifier (hlq).
6. Log in to TSO/ISPF.
7. Start the installation via this command in ISPF 6: EX 'hlq.P.HOME.DATA(ISETUP)'
8. After successful testing of the WebFOCUS Reporting Server release or maintenance, move the test environment to production according to the standards of your site.

Installing ibi WebFOCUS Reporting Server Using ISETUP

The ISETUP panels consist of **input** fields in which you can enter information and **display** fields in which you cannot enter information. Input fields have a red background and display fields have a white background.

After the ISETUP procedure has executed, all of your HOME libraries will have names of the form **new_hlq**.P.HOME.**suffix**, where **new_hlq** is the high-level qualifier you specify on the ISETUP panels. For example, if you specify the high-level qualifier `WFRS.nnnn`, ISETUP creates a data set called `WFRS.nnnn.P.HOME.LOAD`.

The installation procedure builds and, optionally, runs the JCL needed to install WebFOCUS Reporting Server.

Note that when a screen opens, its input fields may be populated with the values from a previous install. When you change any values, you must press **Enter** once to register the changes and then press **Enter** again to proceed to the next panel.

If you decide you are not satisfied with the values you entered and you want to change them, press **PF3** to return to the previous panel.

Set Up User IDs

You can use any user ID to install and run the server. Whichever ID you use becomes the first server administrator ID (sometimes referred to as iadmin).

Collect Required Information for Adapters

For current information about which adapters are supported, see the *ibi™ WebFOCUS® Adapter Administration* manual.

You must provide information to configure the adapters that you want to install. The installation procedure automatically prompts you for this information. When you are prompted for an optional steplib, ddname, or environment variable, the installation procedure will indicate this with an OPT> prompt.

After you have installed and configured the server, you can further configure your adapters using a web-based server configuration tool called the WebFOCUS Reporting Server browser interface.

The following table describes what information you need to provide for each adapter that you have. (If an adapter is not listed, no information needs to be provided for it.)

Note that the table refers to:

- **IRUNJCL.** This procedure contains the JCL procedure for the server, and is a member of the configuration library

```
high_level_qualifier.PDS.WFS.DATA
```

where:

high_level_qualifier

Is the high-level qualifier to be used for all output libraries. This is the same high-level qualifier, which you specify during server installation.

Adapter	Information you must provide
Adabas	<p>Provide the data set name for the following STEPLIB allocation:</p> <ul style="list-style-type: none"> • load library <p>This is required only for the synonym creation process. For example, in a production environment in which all synonyms already exist, you can omit this.</p> <p>When you configure the adapter, you will need to provide the name of the Adabas source library and the associated data set name.</p>
CA-DATACOM	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • CUSLIB load library • CALIB load library • utility library • URT library
CA- IDMS (both DB and SQL)	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • load library • DBA load library <p>Provide the data set names to which the following ddnames are allocated:</p> <ul style="list-style-type: none"> • SYSIDMS. Check with your CA-IDMS DBA for this ddname. • SYSCTL. Is the library corresponding to the central version you want to use.
CICS Transaction	<p>Provide the data set name for the following STEPLIB allocation:</p> <ul style="list-style-type: none"> • CICS EXCI load library
Call Java	<p>You must have the JDK installed.</p> <p>Provide a value for the following environment variables:</p>

Adapter	Information you must provide
	<ul style="list-style-type: none"> • CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. <p>This adapter requires configuration of the JSCOM3 listener. Provide three required paths:</p> <ul style="list-style-type: none"> • The path to JVM using either JDK_HOME or JAVA_HOME, as described in Installation Requirements for PDS. • The paths to edahome_dir and edaconf_dir, as described in ZFS Home and Configuration Directory Requirements.
EJB	<p>You must have the JDK installed.</p> <p>Provide a value for the following environment variables:</p> <ul style="list-style-type: none"> • CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. <p>If you are deploying the adapter to access an EJB on a:</p> <ul style="list-style-type: none"> • WebLogic server, specify the following path: <div data-bbox="511 1045 1412 1129" data-label="Text"> <pre>/pathspec/weblogic.jar</pre> </div> • WebSphere server, specify the following paths: <div data-bbox="511 1207 1412 1291" data-label="Text"> <pre>/pathspec/websphere.jar</pre> </div> <div data-bbox="511 1323 1412 1360" data-label="Text"> <pre>/pathspec/ejbcontainer.jar (one for each EJB container)</pre> </div> <p>This adapter requires configuration of the JSCOM3 listener. Provide three required paths:</p> <ul style="list-style-type: none"> • The path to JVM using either JDK_HOME or JAVA_HOME, as described in Installation Requirements for PDS. • The paths to edahome_dir and edaconf_dir, as described in ZFS Home and Configuration Directory Requirements.
JDBC	<p>You must have the JDK installed.</p>

Adapter	Information you must provide
	<p>Provide a value for the following environment variables:</p> <ul style="list-style-type: none"> • CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. <p>This adapter requires configuration of the JSCOM3 listener. Provide three required paths:</p> <ul style="list-style-type: none"> • The path to JVM using either JDK_HOME or JAVA_HOME, as described in Installation Requirements for PDS. • The paths to edahome_dir and edaconf_dir, as described in ZFS Home and Configuration Directory Requirements.
Microsoft SQL Server	<p>You must select the Call Java adapter in addition to the Microsoft SQL Server adapter.</p> <p>Provide a value for the following environment variables:</p> <ul style="list-style-type: none"> • CLASSPATH. Provide the paths to the following files; these paths will be appended to CLASSPATH. <ul style="list-style-type: none"> ◦ msbase.jar ◦ mssqlserver.jar ◦ msutil.jar <p>This adapter requires configuration of the JSCOM3 listener. Provide three required paths:</p> <ul style="list-style-type: none"> • The path to JVM using either JDK_HOME or JAVA_HOME, as described in Installation Requirements for PDS. • The paths to edahome_dir and edaconf_dir, as described in ZFS Home and Configuration Directory Requirements.
Db2 CAF	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • SDSNLOAD load library <p>For security information, see DB2 Security Exit Configuration for PDS.</p> <ul style="list-style-type: none"> • SDSNEXIT load library (optional)

Adapter	Information you must provide
Db2 CLI	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • SDSNLOAD load library <p>For security information, see DB2 Security Exit Configuration for PDS.</p> <ul style="list-style-type: none"> • SDSNLOD2 load library • SDSNEXIT load library (optional; this is needed only for an explicit connection). <p>Provide the data set name (including member name if applicable) for the following DDname:</p> <ul style="list-style-type: none"> • DSNAOINI, which contains the Db2 CLI ini file.
IMS	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • DFSPZP load library (optional; not needed if PZP modules are stored in the DFSRESLB library) • DFSRESLB load library
Millennium	<p>Provide the data set name for the following STEPLIB allocation:</p> <ul style="list-style-type: none"> • load library
Model 204	<p>Provide the data set name for the following STEPLIB allocation:</p> <ul style="list-style-type: none"> • load library
MQSeries	<p>Provide the data set names for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • SCSQLOAD load library • SCSQAUTH load library
NATURAL Batch	<p>Provide the data set name for the following STEPLIB allocation:</p> <ul style="list-style-type: none"> • NATURAL load library
SAP (SQL)	<p>Provide values for the following environment variables:</p> <ul style="list-style-type: none"> • LIBPATH, which contains the path to SAP RFC SDK.

Adapter	Information you must provide
	<ul style="list-style-type: none"> • SAP_CODEPAGE=0126, or the correct SAP code page for your language environment. <p>This adapter requires configuration of two required paths:</p> <ul style="list-style-type: none"> • The paths to edahome_dir and edaconf_dir, as described in ZFS Home and Configuration Directory Requirements <p>It is recommended that the code page conversion tables be created under the edaconf_dir directory.</p>
SAP BW	<p>Provide values for the following environment variables:</p> <ul style="list-style-type: none"> • LIBPATH, which contains the path to SAP RFC SDK.SAP_CODEPAGE=0126, or the correct SAP code page for your language environment. <p>This adapter requires configuration of two required paths:</p> <ul style="list-style-type: none"> • The paths to edahome_dir and edaconf_dir, as described in ZFS Home and Configuration Directory Requirements. <p>Is recommended that the code page conversion tables be created under the edaconf_dir directory.</p>
Supra	<p>Provide the data set name for the following STEPLIB allocations:</p> <ul style="list-style-type: none"> • LINKLIB load library. • INTERFLM load library. • ENVLIB load library.

Optional Low-Level Qualifier Changes

We recommend retaining the default low-level qualifiers that are supplied for the installation libraries. However, if you need to change any of them (for example, to conform to site-specific naming conventions), you can do so by editing them in member PDSSNAME of *high_level_qualifier*.HOME.DATA. You can see a list of the qualifiers in [Default Low-Level Qualifiers](#).



Caution: If you change any low-level qualifiers and do not reflect those changes exactly in PDSSNAME, you will experience problems with the server installation and operation.

Do not change the value of &CONFTYPE.

Once you have finished changing any names, continue with [Run isetup](#).

Default Low-Level Qualifiers

The following low-level qualifiers are set in *high_level_qualifier*.HOME.DATA(PDSSNAME):

//	SET	EDALOAD='P.HOME.LOAD'	Load Library
//	SET	EDAHETC='P.HOME.ETC'	Server html and text files
//	SET	EDAHACX='P.HOME.ACX'	Access files
//	SET	EDAHFEX='P.HOME.FEX'	RPCs
//	SET	EDAHMAS='P.HOME.MAS'	Master files
//	SET	EDAHBIN='P.HOME.BIN'	Server binary files
//	SET	EDAERR='P.HOME.ERR'	Server NLS and error files
//	SET	EDACICS='P.HOME.CICS.LOAD'	CICS Load Library
//	SET	PDSWFSD='PDS.WFS.DATA'	WebFocus Reporting server

Run isetup

Server installation consists of a series of ISPF panels, which gather the required information. After the panel dialog is complete, JCL is created and optionally submitted to install and configure the server.

1. Execute the isetup member of your *high_level_qualifier*.HOME.DATA using ISPF option 6.

The first Installation and Configuration panel opens.

```

ibi                                Installation and Configuration    z/OS PDS Deployment    D1
Command ====>

Please select one of the following options:

    1. Install and Configure
    2. Add Additional Configuration Instance

Enter selection (Default=1) ====> 1
Installation Userid          ====> PGMASW                Logged on Userid
PTH Administrator Userid     ====> srvadmin              Server install only
PTH Administrator Password   ====>                      Retype ====>
Customer ID                  ====>

Enter Job Card information                                Override JOB name checking ====> N
====> // JOB (ACCT INFO),
====> // *
====> // *
Press Enter to continue, PF3 to END
F1=HELP      F2=SPLIT    F3=END      F4=RETURN   F5=RFIND    F6=RCHANGE
F7=UP        F8=DOWN     F9=SWAP    F10=LEFT    F11=RIGHT   F12=RETRIEVE

```

Complete the panel as follows.

Field	Instructions
Enter selection	Accept the default value 1, Install and Configure , for a new installation. For option 2, Add Additional Configuration Instance , see Adding a Configuration Instance for PDS .
Installation Userid	Shows the current logon ID. It cannot be changed.
PTH Administrator Userid	An ID is required to administer the server immediately after initial installation. This ID is defined and maintained solely in the realm of the server. It defaults to srvadmin , and it can be changed here. For more information about running the server in secure mode, see Configure Security .
PTH Administrator Password	Password for the PTH Administrator ID. It cannot be left blank and must be matched at the Retype field.

Field	Instructions
Customer ID	Enter the Customer ID that was provided to you with your WebFOCUS software.
Enter Job Card information	To provide JOB card information for submitting jobs to the JES queue, provide a valid job name (a maximum of seven characters following the 2 forward slashes // on the first JCL line), which defaults to the user ID that you are currently using. This job name is used for multiple submissions (for example, jobnameA, jobnameB, jobnameC, and so on) in the JCL that is generated by the installation procedure.
Override JOB name checking	To provide your own JOB card information, including JOB name, enter Y and provide valid JOB card information in the Enter Job Card information field. The JOB card information that you enter is used for each job that is submitted.

2. Press Enter to continue to the next panel.

The following panel opens.

```

ibi                               Installation and Configuration  z/OS PDS Deployment
Command ==>                                                                D8

                               New Installation

Please enter the following information for WebFocus Reporting Server

  EDAHOME Libraries HLQ      ==> PGMASW.SRV932

  EDACONF Libraries HLQ      ==> PGMASW.SRV932.P
  EDACONF Libraries Attributes Unit ==> SYSDA      Volume ==>

Configuration options
  HTTP Listener Port        ==> PLEASE SUPPLY VALUE      (21 Characters max)
                           ==> 8121      TCP Listener Port ==> 8120
  Installation JCL Library  ==> PGMASW.SRV932.P.PDS.WFS.DATA

Press Enter to continue, PF3 to return to previous menu

```

In this and some later panels, you can see a field's default value (if one exists) by blanking out the field and pressing Enter. Complete the panel as follows.

Field	Instructions
EDAHOME Libraries HLQ (EDAHOME)	Enter the same HLQ value you provided when you processed the .run file.
EDACONF Libraries HLQ	EDAHOME libraries HLQ with additional qualifier .P.
EDACONF Libraries Attributes Unit	Follow your site's rules. For most sites, Unit is SYSDA and Volume is left blank.
HTTP Listener Port	<p>This is the port number that the server uses for HTTP. It is the first of three connection ports that must be available to the server.</p> <p>For example, if you choose port 8101, then ports 8101, 8102, and 8103 are used by the server. Ensure that you choose ports that are not currently being used.</p>
TCP Listener Port	<p>This is the port number of the TCP Listener.</p> <p>The default is one less than the port specified for the HTTP Listener, but it can be any port number other than the three reserved for HTTP.</p>
Installation JCL Library	Data set where installation JCL and other files are written.

3. Press Enter to continue to the next panel. The Data Adapters panel opens. It lists adapters that require the allocation of MVS libraries in IRUNJCL or environment variables in the EDAENV member. To select specific adapters:
 - a. Type **Y** next to the required adapters and press Enter.
 - b. Supply the requested information, which is described in [Collect Required Information for Adapters](#).

After you have finished installing and configuring the server, you can use the WebFOCUS Reporting Server browser interface to finish configuring these adapters, and to configure adapters that do not have MVS JCL requirements.


```

ibi                                     Installation and Configuration  z/OS PDS Deployment
Command ==> _                                                                    PB

                                     Data Adapters

Will you be configuring for any of the following adapters ?

ADABAS          ==> N      CA-DATACOM      ==> N      CA-IDMS          ==> N
CICS TRAN       ==> N      DB2 CAF        ==> N      DB2 CLI         ==> N
CALL JAVA       ==> N      JDBC         ==> N      IMS            ==> N
MILLENNIUM      ==> N      MODEL 204    ==> N      SUPRA          ==> N
MSSQL SERVER    ==> N      NATURAL BATCH ==> N      SAP            ==> N
BWB             ==> N

Note: Use the Web Console for the completion of adapter configuration
Press Enter to continue, PF3 to return to previous menu

```

4. Press Enter to continue to the next panel.

The JSCOM3 Listener configuration panel opens.

- a. This panel prompts for a value for JDK_HOME. For more information see [Installation Requirements for PDS](#). It also prompts for values for edahome_dir and edaconfi_dir, as described in [ZFS Home and Configuration Directory Requirements](#).
- b. Configuration of the JSCOM3 Listener is either optional or mandatory depending on which adapters were selected. If any Java-based adapters were selected (EJB, Call Java, JDBC, Microsoft SQL Server), the configuration of all three paths listed above is mandatory. If SAP-based adapters were selected (SAP or SAP BW), only edahome_dir and edaconf_dir are required.
- c. If no Java-based or SAP-based adapters were selected, this configuration might still be desirable to enable the server-side graphics feature. To skip the configuration, leave the path blank.

```

ibi                                Installation and Configuration    z/OS PDS Deployment
Command ===>                                                                DB

                                Optional JSCOM3 Listener

Enables JAVA-based data adapters and server-side graphics support
      (Blank values to skip configuration)

Please enter   JDK_HOME   path:

JDK_HOME     ===> /usr/lpp/java/j11.0_64

Please enter path to install modules that interface with JVM/SAP:
      (Blank values to skip configuration)

edahome_dir  ===> /ibi/eda/edamr/ibi/z/srv93/home

edacnf_dir   ===> /ibi/eda/edamr/z/ibi/z/srv93/wfs

Press Enter to process, PF3 to return to previous menu

```

5. Press Enter to continue to the next panel.

The Confirmation panel opens.

```

ibi                                Installation and Configuration    z/OS PDS Deployment
Command ===>                                                                D9

                                New Installation

Please confirm the following information for WebFocus Reporting Server

  EDASW Libraries HLQ      ===> PGMASW.SRV932

Product Configuration parameters

  EDACNF Libraries HLQ      ===> PGMASW.SRV932.P
  EDACNF Libraries Attributes Unit===> SYSDA      Volume ===>

  Approot value             ===>PGMASW.WFRS93.P
  HTTP Listener Port        ===> 8121      TCP Listener Port ===> 8120
  PTH Administrator userid  ===> srvadmin

  Installation JCL Library  ===> PGMASW.SRV932.P.PDS.WFS.DATA
  Review output allocations ===> N          (Y or N)

Continue ? (N)o, (C)reate JCL only, (S)ubmit JCL ===> N  (Enter N, C or S)
Press Enter to process, PF3 to return to previous menu

```

6. Ensure that all values on the Confirmation panel are correct, then select one of the following options

- **N** to return to the initial panel so that you can change installation values.
- **C** to create JCL which you can submit at a later time. The JCL is placed in your *high_level_qualifier*.PDS.WFS.DATA configuration library.

- **S** to create JCL in *high_level_qualifier*.PDS.WFS.DATA, and submit the job immediately.

where:

high_level_qualifier

Is the high-level qualifier to be used for all output libraries. This is the same high-level qualifier, which you specify during server installation.

7. As the job is processed, in SDSF, check JESLOG for errors and return codes.

The following is a table of the jobs created. All members are created in the configuration library.

Job	Description
ISSETUPJ1	Main JCL Job stream that is used to install the server.
ISOPTS1	Options used to install.

All the following members call the IRUNJCL procedure, which is the main server JCL. If you need to change the server JCL, change member IRUNJCL.

Member	Description
ISTART	Starts the server.
ISAVEDIA	JCL to print a copy of configuration files for diagnostic purposes.
ITRCON	Starts the server with traces on.

The following members contain batch JCL for auxiliary functions, and are created in the configuration library.

Member	Description
CMRUN	JCL to run ibi Data Migrator batch jobs.
DB2VverPR	Db2 DBRM, where <i>ver</i> is your supported

Member	Description
	version of Db2 referenced in GENDB2 JCL.
GENDB2	JCL to bind the Db2/CAF plan.
IRDAAPPC	Example CLIST to run RDAAPP Client test tool.
IRDAAPPJ	Example JCL to run RDAAPP Client test tool.

The following members contain sample started task JCL, and are created in the configuration library.

Member	Description
IWAYS	A started task that starts the server.
EDAENV	A parameter file used by the server. It contains all required environment variables.

Overview of Manual Steps Following isetup

The following features are not installed by isetup. For these features, follow the instructions in the WebFOCUS Reporting Server Installation Guide for your current production version of WebFOCUS Reporting Server:

- Data Adapters (Interfaces, for example, Db2 or ADABAS).



Important: All data adapter files are included and allocated in WebFOCUS Reporting Server after you run ISETUP. However, using the instructions in the relevant Installation Guides for those data adapters, you must reinstall every data adapter to which you want to have access in the installed version of WebFOCUS Reporting Server.

If you run WebFOCUS Reporting Server out of LPA libraries, perform the following steps:

1. Copy all the reentrant modules back into FOCLIB.LOAD from FOCLPA.LOAD. (Use JOB JFSCPBACK.)
2. Run isetup.
3. Copy the reentrant modules from FOCLIB.LOAD back into FOCLPA.LOAD. (Repeat JOB JFSCPLPA.)
4. Delete the reentrant modules FROM FOCLIB.LOAD. (Repeat JOB JFSDELPA.)

ISETUP Processing Flow

The installation job should complete with 0 return codes for all steps, and additional libraries should be created under the high-level qualifier you entered on the ISETUP screen.

The following physical HOME libraries should exist.

SYSADMIN1.P.HOME.BIN	USERM1
SYSADMIN1.P.HOME.FEX	USERM1
SYSADMIN1.P.HOME.ACX	USERM1
SYSADMIN1.P.HOME.LOAD	USERM1
SYSADMIN1.P.HOME.ERR	USERM1
SYSADMIN1.P.HOME.ETC	USERM1
SYSADMIN1.P.HOME.DATA	USERM1
SYSADMIN1.P.HOME.MAS	USERM1
SYSADMIN1.P.HOME.CICS.LOAD	USERM1

The following physical CONF libraries should exist.

SYSADMIN1.CONF.ACX	USERM1
SYSADMIN1.CONF.CFG	USERM1
SYSADMIN1.CONF.DATA	USERM1
SYSADMIN1.CONF.SQL	USERM1
SYSADMIN1.CONF.MAS	USERM1
SYSADMIN1.CONF.PRF	USERM1

Test the Installation

To test the server installation:

1. Log on to TSO as iadmin.

2. Submit the ISTART JCL from the configuration library to start the server. This executes the IRUNJCL proc. The configuration library is

```
high_level_qualifier.PDS.WFS.DATA
```

where:

high_level_qualifier

Is the high-level qualifier to be used for all output libraries. This is the same high-level qualifier, which you specify during server installation.

3. Check the job output for errors. Look for the EDAPRINT message:

```
(EDA13023) ALL INITIAL SERVERS STARTED
```

4. Start the WebFOCUS Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

```
http://host:port
```

where:

host

Is the name of the machine on which the product is installed.

port

Is the value you specified as HTTP Listener Port in ISETUP.

The WebFOCUS Reporting Server browser interface opens.

5. If the WebFOCUS Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree.
6. Continue with adapter configuration, as described in the *ibi™ WebFOCUS® Adapter Administration* manual.

When you are finished using the server, you can use the WebFOCUS Reporting Server browser interface to stop the server by going to the WebFOCUS Reporting Server browser interface menu bar, selecting **Workspace**, and then **Stop**.

If you experience problems at start-up, examine the job output for more information.

Configure Security

If you plan to configure security provider OPSYS, perform the instructions in [Configure Security With All Security Products](#), regardless of which security product you use. (For security providers PTH, DBMS, and LDAP, skip these topics.)

For a full description of all security providers:

1. From the WebFOCUS Reporting Server browser interface menu bar, select **Help**, then **Contents and Search**.

The WebFOCUS Reporting Server browser interface Help window opens.

2. In the left pane, expand **Server Administration**.

Alternatively, see the *ibi™ WebFOCUS® Reporting Server Administration* guide.

Security Providers

The default security provider for a new installation is the internal security provider, PTH. The PTH provider implements security using user IDs, passwords, and group memberships stored in the `admin.cfg` configuration file.

After the initial installation, the Server Administrator that was configured during the installation can start the server and use the Reporting Server browser interface to further customize security settings, for example, to configure alternate or additional security providers, create additional PTH IDs, and register groups and users in a security role. For more information about security providers, see the *Server Security* chapter in the *ibi™ WebFOCUS® Reporting Server Administration* guide.

Preventing Unsecured ibi WebFOCUS Reporting Server Starts After Upgrades

If the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the `edaprint` log.

This feature prevents an unsecured starting of the server after a software upgrade if any of the required post-upgrade reauthorization steps are missed on a UNIX, IBM i, or z/OS USS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server `edaenv.cfg` environment configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
Configured security is 'ON' as set by EDAEXTSEC variable.
```

```
Server has no root privilege.
```

```
Workspace initialization aborted.
```

```
(EDA13171) UNABLE TO START SERVER
```

Configure Security With All Security Products

To configure security with RACF, eTrust CA-ACF2, or eTrust CA-Top Secret:

Procedure

1. Log on to TSO using the ID used to install the server.
2. The libraries allocated to STEPLIB in IRUNJCL must be APF-authorized. Any non-APF-authorized libraries must be allocated to the TASKLIB DDNAME.
3. Restart the server.

Result

i Note: If you want to use eTrust CA-ACF2 or eTrust CA-Top Secret, contact Customer Support.

Configure Security With eTrust CA-Top Secret

To use eTrust CA-Top Secret security, perform the following step:

- Create an eTrust CA-Top Secret facility entry for the server security module, R1SEC. The only need for permissions is for the RACROUTE call from the R1SEC program.

Facility Entry Defining the Server to CA-Top Secret

The following is an example of a facility entry that defines the server to eTrust CA-Top Secret:

```
PGM=R1SEC ID=1 TYPE=099

ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF

ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT

ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFTRANS

ATTRIBUTES=NOMSGLC,NOTRACE,NOEODINIT,IJU,NODORMPW,ONPWR

ATTRIBUTES=LUUPD MODE=FAIL DOWN=GLOBAL LOGGING=ACCESS,INIT

UIDACID=8 LOCKTIME=000 DEFACID=*NONE* KEY=8

MAXUSER=03000 PRFT=003
```

Starting and Stopping the ibi WebFOCUS Reporting Server for PDS

This section provides information on the operation and use of the server. Additional information on the server and how to configure adapters is available in the WebFOCUS Reporting Server browser interface help. The WebFOCUS Reporting Server browser interface help is also available in the *ibi™ WebFOCUS® Reporting Server Administration* guide.

Starting the ibi WebFOCUS Reporting Server Using a Batch Job

To start the server, submit the ISTART member of the MVS configuration library (*high_level_qualifier.WFS.DATA*) for your server.

Starting the ibi WebFOCUS Reporting Server Using a Started Task

ISSETUP creates started task JCL to start the server. This started task is a member of the MVS configuration library IWAYS.

To execute the started task:

- **Copy it** into SYS1.PROCLIB or any other JES2 Proclib data set.
- **Satisfy security requirements.** All external security-related permissions must exist for both the data sets and the started tasks. In order to issue the started tasks, the user must satisfy both of the following requirements:
 - Have at least OPERATOR authority defined within the WebFOCUS Reporting Server browser interface.
 - Be in the same security group, or associated with the same security group, as the owner of the server directory structure (for example, as iadmin).

To submit the started task from the MVS console, issue the following command:

```
S IWAYS
```

You can add the started task to any automation product that you run.

Stopping the ibi WebFOCUS Reporting Server

You can stop the server using any of the following methods:

- **WebFOCUS Reporting Server browser interface.** From the WebFOCUS Reporting Server browser interface menu bar, select **Workspace** and then **Stop**.
- **MVS operator command.** On the MVS Console or SDSF, issue the following operator MODIFY command:

```
F jobname, -stop
```

where:

jobname

Is the job under which the server is running.

- **Cancel the server job.** In SDSF, cancel the job.

Enabling HTTPS Security on the HTTP Listener for PDS

If you are using RACF, a private key *must be* generated together with the certificate. The generated key must be type RSA. The supported private key size is up to 4096 bits.

Generating the Certificate and Key

- **Generating the Certificate.** You can generate the certificate using the TSO RACDCERT command with options GENCERT (generate certificate) or GENREQ (generate certificate request).

For example:

```
RACDCERT GENCERT SUBJECTSDN(CN('Workspace Manager') -
OU('IOD') -
O('IBI') -
C('US')) -
SIZE(2048) -
NOTAFTER(DATE(2026-12-01)) -
ID(JOBOWNID) -
RSA -
WITHLABEL('IBIcert')

SETROPTS RACLIST(DIGTCERT) REFRESH
```

- **Creating the Key Ring.** You can create the key ring using the RACDCERT ADDRING command. For example:

```
RACDCERT ADDRING(IBIring1) ID(JOBOWNID)
```

- **Connecting the Certificate to the Key Ring.** You can connect the certificate to a ring using the RACDCERT CONNECT command. For example:

```
RACDCERT CONNECT(LABEL('IBIcert') DEFAULT RING(IBIring1)) -
ID(JOBOWNID)
```

The ID owner of all objects is the same. It must be the owner ID of the server job. In these examples, the value JOBOWNID is used arbitrarily.

The following JCL shows how to run the RACDCERT command in a batch:

```
//*** JOB CARD *****

//*****

//STEP1 EXEC PGM=IKJEFT01

//SYSTSPRT DD SYSOUT=*

//SYSTSIN DD *

RACDCERT LIST ID(JOBOWNID)
```

For detailed information and options of the RACDCERT command, see the IBM document *z/OS Security Server RACF Command Language Reference*.

TLS 1.3 SSL Protocol Requirements

The TLS 1.3 protocol requires additional RACF permissions to be given to users and/or groups connecting to the WebFOCUS Reporting Server. READ permission must be given to CSFOWH CL(CSFSESV).

If you do not plan to use the default of TLS 1.3, you can force the WebFOCUS Reporting Server to use TLS 1.2 by adding the following parameter to the edaserve.cfg file:

```
ssl_protocol = tls_1_2
```

Enabling HTTPS

After the key ring and label are created, to enable HTTPS:

1. Go to the WebFOCUS Reporting Server browser interface Workspace page.
2. Expand **Special Services and Listeners**.
3. Right-click TCP/HTTP and click **Properties of HTTP**.

The Listener Configuration page opens.

4. Expand the Security section.
5. In the Enable HTTPS drop-down list, select **Yes**.

Additional fields open in which you can enter the certificate label and keyring values you defined using the RACDCERT commands.

```
SSL_CERTIFICATE = keyring
SSL_LABEL = certificate
```

6. Click **Save and Restart Server**.

Defining the ICSF Dataset Key Label for PDS to Use Pervasive Encryption

In the following sample JCL, values are shown for clarity. These are the current IBM defaults.

```
SYMEXPORTABLE(BYANY) and ASYMUSAGE(HANDSHAKE SECUREEXPORT)
```

In the following sample PERMIT statement, ID contains only group names, not user ID names. During installation, you can choose which name to use or to use a combination of both.

i Note: PGMYMG, PGM, QCS, EDA, and CSD in the sample code are arbitrary users and groups.

```
//TSOBATCH EXEC PGM=IKJEFT01

//SYSTSPRT DD SYSOUT=*

//SYSTSIN DD *

RDEF CSFKEYS DATASET.PGMYMG.ENCRYPTKEY.001 OWNER(SYS1) UACC(NONE) -

ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES)-
```

```

SYMEXPORTABLE(BYANY) ASYMUSAGE(HANDSHAKE SECUREEXPORT))

PERMIT DATASET.PGMYMG.ENCRYPTKEY.001 CLASS(CSFKEYS) ACCESS(READ) -

ID(PGM QCS EDA CSD)

SETROPTS RACLIST(CSFKEYS) REFRESH

/*

//

```

ICSF Panels

1. Select option 5, **UTILITY**, as shown in the following image, and press Enter.

```

HCR77D0 ----- Integrated Cryptographic Service Facility -----
OPTION ==>
System Name: IBI1 Crypto Domain: 0
Enter the number of the desired option.

 1 COPROCESSOR MGMT - Management of Cryptographic Coprocessors
 2 KDS MANAGEMENT  - Master key set or change, KDS Processing
 3 OPSTAT           - Installation options
 4 ADMINCNTRL       - Administrative Control Functions
 5 UTILITY          - ICSF Utilities
 6 PPINIT           - Pass Phrase Master Key/KDS Initialization
 7 TKE              - TKE PKA Direct Key Load
 8 KGUP             - Key Generator Utility processes
 9 UDX MGMT         - Management of User Defined Extensions

```

2. Select option 5, **CKDS KEYS**, as shown in the following image, and press Enter.

```

----- ICSF - Utilities -----
OPTION ==>
Enter the number of the desired option.

 1 ENCODE          - Encode data
 2 DECODE          - Decode data
 3 RANDOM          - Generate a random number
 4 CHECKSUM        - Generate a checksum and verification patterns
 5 CKDS KEYS       - Manage keys in the CKDS
 6 PKDS KEYS       - Manage keys in the PKDS

```

3. Select option 7, **Generate AES DATA keys**, as shown in the following image, and press Enter.

```

----- ICSF - CKDS KEYS -----
OPTION ==> 7

Active CKDS: IBI1.CSF.SCSFCKDS                      Keys: 4

Enter the number of the desired option.
 1 List and manage all records
 2 List and manage records with label key type _____ leave blank for
                                     list, see help
 3 List and manage records that are _____ (ACTIVE, INACTIVE, ARCHIVED)
 4 List and manage records that contain unsupported CCA keys
 5 Display the key attributes and record metadata for a record
 6 Delete a record
 7 Generate AES DATA keys

Full or partial record label
==>
The label may contain up to seven wild cards (*)

Number of labels to display ==> 100 (Maximum 100)

Press ENTER to go to the selected option.
Press END to exit to the previous menu.

```

4. Type the CKDS record label for the new key and select the AES key bit length, as shown in the following image, and press Enter.

```

----- ICSF - CKDS Generate Key -----
COMMAND ==>

Active CKDS: IBI1.CSF.SCSFCKDS

Enter the CKDS record label for the new AES DATA key
==> DATASET.PGMYMG.ENCRYPTKEY.001

AES key bit length: _ 128 _ 192 s 256

```

If the operation was successful, Key Generated is returned at the upper-right corner of the screen, as shown in the following image.

```

- ICSF - CKDS Generate Key ----- KEY GENERATED

```

Db2 Security Exit Configuration for PDS

Customize the Db2 security exit to allow the Adapter for Db2 to run with user-level security enabled. If you do so, users will connect to Db2 with the authorization of the user ID with which they logged on to the server. The server must also be running with security turned on.

If you do not customize the Db2 security exit, all users will be assigned the connection ID to Db2 that is associated with the region, job submitter, or started task.


For the Adapter for Db2 CLI, the connection to Db2 must be configured as *trusted* for the exit to be invoked.

The changes that must be made to the IBM Db2 sign-on exit, DSN3SATH, differ for RACF and eTrust CA-Top Secret sites and eTrust CA-ACF2 sites.

An example of each is shown in the following sections.

The highlighted text and comments shown in the examples indicate the lines containing the recommended modification of DSN3SATH, which calls the module FOCDN3, the supplied exit.

After you finish the edits, assemble the exit into an object file. This object file is given as an input to the link that JCL found in one of the examples that follow.

- 

Note:
 - The positioning of these lines is approximate, assuming that no other changes or additions have already been made to DSN3SATH. If any changes have been made, you should decide on the most appropriate location for this call to FOCDN3.
 - FOCDN3 is used to set the proper primary (individual user ID) authorization.
 - Another program, FOCDN4, is used to set the proper secondary (group ID) authorization for RACF and eTrust CA-Top Secret. FOCDN4 is not needed with eTrust CA-ACF2. The secondary authorization ID(s) will be set correctly without it.

Changing DSN3SATH for RACF and eTrust CA-Top Secret Sites

1. Search for the **SATH001 label** - add two lines (FOCDN3):

```
SATH001  DS      0H
        USING WORKAREA,R11      ESTABLISH DATA AREA ADDRESSABILITY
        ST      R2,FREMFLAG      SAVE FREEMAIN INDICATOR
        XC      SAVEAREA(72),SAVEAREA CLEAR REGISTER SAVE AREA
        .
        .
        .
*****SECTION 1:  DETERMINE THE PRIMARY AUTHORIZATION ID *****
*
*  IF THE INPUT AUTHID IS NULL OR BLANKS, CHANGE IT TO THE AUTHID
*  IN EITHER THE JCT OR THE FIELD POINTED TO BY ASCBJBNS.
*  THE CODE IN THIS SECTION IS AN ASSEMBLER LANGUAGE VERSION OF
*  THE DEFAULT IDENTIFY AUTHORIZATION EXIT.  IT IS EXECUTED ONLY
*  IF THE FIELD ASXBUSER IS NULL UPON RETURN FROM THE RACROUTE
*  SERVICE.  FOR EXAMPLE, IT DETERMINES THE PRIMARY AUTH ID FOR
*  ENVIRONMENTS WITH NO SECURITY SYSTEM INSTALLED AND ACTIVE.
*
```


3. Search for the **SATH025 label** - replace sath025 and add sath026 (FOCDSN4):

```
SATH025  DS      0H

      CALL  FOCDSN4          GO GET THE IBI EXIT (4=GROUP AUTH) <--ADD
      LTR   R6,R6            DOES AN ACEE EXIST?  IF NOT,      <--ADD
      BZ    SATH026          CHECK ACEE IN ADDRESS SPACE      <--ADD
      CLC   ACEEACEE,EYEACEE DOES IT LOOK LIKE AN ACEE?      <--ADD
      BE    SATH027          YES, GO DO GROUPS                <--ADD
SATH026  DS      0H      <--ADD
      .
      .
      .

SATH027  DS      0H      CHECK LIST OF GROUPS OPTION
      TM    RCVTOPTX,RCVTLGRP IS LIST OF GROUPS CHECKING ACTIVE
      BZ    SATH040          SKIP TO SINGLE GROUP COPY IF NOT
      DROP  R7              DROP RCVT BASE REG
      SPACE 1
* RACF LIST OF GROUPS OPTION IS ACTIVE
EJECT
      .
      .
      .
```

Changing DSN3SATH for eTrust CA-ACF2 Sites

*DSN3SATH source is provided by ACF2.

1. Search for **PRIMARY AUTHORIZATION ID** - add two lines (FOCDSN3):

```
*****
*
*          PRIMARY AUTHORIZATION ID
*
*****
*
*  IF THE PRIMARY AUTHORIZATION ID IS NULL OR BLANKS
*  IF CA-ACF2 IS AVAILABLE
*  SET PRIMARY ID FROM ACFASVT (ASVLID)
*  ELSE
*  IF TSO FOREGROUND USER
*  SET PRIMARY ID FROM TSO LOGON ID (ASCBJBNS)
*  ELSE
*  SET PRIMARY ID FROM JOB USER (JCTUSER)
*
*****
      SPACE 2                                04260000
```

```
LA R1,AIDLPRIM LOAD PARM REG1          <--ADD
CALL FOCDSN3 GO GET THE IBI EXIT        <--ADD
CLI  AIDLPRIM,C' '      PRIMARY AUTHID THERE ?    04270000
BH   PRIMWTO           ..YES, EVERYTHINGS OK HERE 04280000
L    R3,PSAAOLD-PSA(0)  CURRENT ASCB ADDRESS      04290000
USING ASCB,R3          ASCB ADDRESSABILITY        04300000
SPACE 2               04310000
```

Modifying the Link JCL for DSN3SATH

This is a sample link JCL for the IBM exit DSN3SATH. Modify the JCL to link the modules into the Db2 security exit as follows.

```
//LKED EXEC PGM=IEWL,PARM='LIST,XREF,LET,RENT,AMODE=31'
//OBJECT DD DSN=db2pref.SDSNSAMP.OBJ,DISP=SHR <--OUTPUT OF ASSEMBLE
STEP
//EDAMOD DD DSN=high_level_qualifier.HOME.LOAD,DISP=SHR
//SYSLMOD DD DSN=db2pref.DSNEXIT,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSUT1 DD UNIT=SYSDA,SPACE=(100,(50,50))
//SYSLIN DD *
INCLUDE EDAMOD(FOCDSN3)
*****
*** Omit the following line for eTrust CA-ACF2
*****
INCLUDE EDAMOD(FOCDSN4)
ENTRY DSN3@ATH
NAME DSN3@ATH(R)
/*
```

where:

db2pref

Is the prefix for the Db2 data sets.

high_level_qualifier

Is the high-level qualifier for the data sets.

After this job finishes successfully, you must recycle the Db2 subsystem in order for the changes to take effect.

MSODDX: DDNAME Translation for User Subroutines

On z/OS, you can incorporate an additional routine called MSODDX into a user-written subroutine that needs to access ddnames allocated to a WebFOCUS Reporting Server. MSODDX provides ddname translation services that enable external programs to access files under the ddname used by the WebFOCUS Reporting Server.

For details, see the *Stored Procedures* chapter in the *ibi™ WebFOCUS® Administration* manual.

Overriding the Time Zone Setting

By default, the server uses the value set by the system for Time Zone. This can be overridden by setting the TZ in the EDAENV member of the server configuration library.

```
TZ = valid tz string
```

For more information about time zone values, see the *IBM UNIX System Services Command Reference* and search for TZ.

Adding a Configuration Instance for PDS

Adding a configuration instance allows you to run different server configuration instances using the same server binaries. You can add up to nine additional servers.

Run ISETUP

To add a configuration instance, perform the following steps.

1. From ISPF 6, run the following command.

```
EX 'high_level_qualifier.HOME..DATA(ISETUP)'
```



Note: If this PDS is not available, re-process the .run file you downloaded from eDelivery.

The first Installation and Configuration panel opens.

```

1b1 Installation and Configuration z/OS PDS Deployment 01
Command ===>

Please select one of the following options:

1. Install and Configure
2. Add Additional Configuration Instance

Enter selection (Default=1) ===> 1
Installation Userid ===> EDAHR Logged on Userid
PTH Administrator Userid ===> srvadmin Server install only
PTH Administrator Password ===> Retype ===>
Customer ID ===>

Enter Job Card information Override JOB name checking ===> N
===> // EDAHR JOB 'EDAHR',CLASS=T,MSGCLASS=Q
===> // *
===> // *
Press Enter to continue, PF3 to END

```

Field	Instructions
Enter selection	Choose option 2, Add Additional Configuration Instance .
Installation Userid	Shows the current login ID. It cannot be changed.
PTH Administrator Userid	An ID is required to administer the server immediately after initial installation. This ID is defined and maintained solely in the realm of the server. It defaults to srvadmin , and it can be changed here. For more information about running the server in secure mode, see Configure Security .
PTH Administrator Password	Password for the PTH Administrator ID. It cannot be left blank and must be matched at Retype field.
Customer ID	The Customer ID provided with your WebFOCUS software.
Enter Job Card information	To provide JOB card information for submitting jobs to the JES queue, provide a valid job name (a maximum of seven characters following the // on the first JCL line), which defaults to the user ID that you are currently using.

Field	Instructions
	This job name is used for multiple submissions (for example, <i>jobnameA</i> , <i>jobnameB</i> , <i>jobnameC</i> , and so on) in the JCL generated by the installation procedure.
Override JOB name checking	To provide your own JOB card information, including JOB name, enter Y and provide valid JOB card information in the Enter Job Card information field. The JOB card information that you enter is used for each job that is submitted.

2. Press Enter to continue to the next panel.

The following panel opens.

```

1bi Installation and Configuration z/OS PDS Deployment DG
Command ===>

Add Configuration

Please enter the following information for WebFocus Reporting Server

Product Configuration Parameters

EDAHOME Libraries HLQ      ===> EDAMR.I932

Press Enter to continue, PF3 to return to previous menu

```

3. Enter the current base high-level qualifier used for EDAHOME.

This indicates where to install the configuration (EDACONF) and where the HOME data sets were previously installed. The installation procedure checks whether the required set of HOME data sets exist. If the test fails, you receive a message indicating the failure and available options.

4. Press Enter to continue to the next panel.

```

ib1                               Installation and Configuration  z/OS PDS Deployment
Command ==>                       DI

                                Add additional Configurations

Please enter the following information for WebFocus Reporting Server

Using the following existing information
Current base HLQ                  ==> EDAMR.I932
Base Install Library              ==> EDAMR.I932.P.PDS.WFS.DATA

Current configurations            ==> WFS

Configuration Options (blank any field for default)

Approot value                     ==> EDAMR.WFRS9.P
EDACONF suffix ( WFS plus)       ==> 1           or string suffix ==>
EDACONF Libraries Attributes     Unit==> SYSDA      Volume ==>
HTTP Listener Port               ==> 8121        TCP Listener Port ==> 8120 _

Installation JCL Library          ==> EDAMR.I932.P.PDS.WFS1.DATA

Press Enter to continue, PF3 to return to previous menu

```

5. Complete the configuration parameters on the panel as follows.

Field	Instructions
Approot value	<p>Indicates where application components reside for this configuration. The default value is based on the value specified for <i>Current Base HLQ</i> (<i>EDAHOME</i>) on the previous panel. To specify a different location for application components, change the value of this field.</p> <p>Different configurations which use the same base HLQ (high-level qualifier) libraries (<i>EDAHOME</i>) can share the same approot value (that is, the same application files). They can also use different approot values to have different sets of application files.</p> <p>If you specify the approot value of an existing server configuration, the installation process recreates the server supplementary data sets and sample files (see Disk Space Requirements). If you do not want them to be recreated, provide a different value for approot.</p>
EDACONF suffix	<p>Each instance must have its own set of configuration libraries. To guarantee this, and to prevent a new set of configuration libraries from overwriting an existing set, the specified suffix is appended to the name of the WFS qualifier. For example, if you configure the second instance of a WebFOCUS Reporting Server, you can specify a suffix of "1", to make the EDACONF high-level qualifier:</p>

Field	Instructions
	<div>IADMIN.SRV93.PDS.WFS1.DATA</div> <p>You can add the new configuration as a numeric or string suffix to the base product type. If you supply a string, the installation procedure ignores any numeric suffix. For a:</p> <ul style="list-style-type: none"> • Numeric suffix. Enter a digit between 1 and 9. This suffix is added to the product type in the directory name and library name to distinguish it from other configuration instances. • String suffix. Enter a one to five-character string (for example, TEST, PROD, or DEV) that does not contain embedded spaces. <p>You can also use the string suffix to extend the numeric numbering past 9 by supplying a number greater than 9. If you change the suffix value and press Enter, the panel refreshes with a new value for the EDACONF Library.</p>
HTTP Listener Port	<p>This indicates the port number that the server uses for HTTP. It is the first of three connection ports that must be available to the server.</p> <p>For example, if you choose port 8101, then ports 8101, 8102, and 8103 are used by the server. Ensure that you choose ports that are not currently being used by existing WebFOCUS Reporting Server configurations, or for any other applications.</p>
TCP Listener Port	<p>This is the port number of the TCP Listener.</p> <p>The default is one less than the port specified for the HTTP Listener, but it can be any port number other than the three reserved for HTTP.</p>

6. Press Enter to continue to the next panel.

The Data Adapters panel may open before the confirmation panel. If the Data Adapters panel opens, continue with Step 9; otherwise, skip to Step 10.

7. The Data Adapters panel lists adapters that require the allocation of libraries in IRUNJCL or environment variables in the EDAENV member. To select specific adapters:

- a. Type **Y** next to the required adapters and press Enter.
- b. Supply the requested information, which is described in [Collect Required Information for Adapters](#).

After you have finished installing and configuring the server, you can use the WebFOCUS Reporting Server browser interface to finish configuring these adapters, and to configure adapters that do not have JCL requirements.

8. Press Enter to continue to the next panel.

The JSCOM3 Listener configuration panel opens.

- a. The panel prompts for the path to the Java environment to be passed to either JDK_HOME or JAVA_HOME, as described in [Installation Requirements for PDS](#), and it also prompt for edahome_dir and edaconf_dir, as described in [ZFS Home and Configuration Directory Requirements](#).
- b. Configuration of the JSCOM3 Listener is either optional or mandatory depending on which adapters were selected. If any Java-based adapters were selected (EJB, Call Java, JDBC, Microsoft SQL Server), the configuration of all three paths listed above is mandatory. If SAP-based adapters were selected (SAP or SAP BW), only edahome_dir and edaconf_dir are required.
- c. If no Java-based or SAP-based adapters were selected, this configuration might still be desirable to enable the server-side graphics feature. To skip the configuration, leave the path blank.

9. Press Enter to continue to the next panel.

The confirmation panel opens.

10. Ensure that all values on the Confirmation panel are correct, then select one of the following options:

- **N** to return to the initial panel so that you can change installation values.
- **C** to create JCL which you can submit at a later time. The JCL is placed in your configuration library.
- **S** to create JCL and submit the job immediately.

11. As the job is processed, validate the installation as described in [Test the New Configuration Instance](#).

Test the New Configuration Instance

To test the configuration instance that you just added:

1. Log on to TSO as iadmin.
2. Submit the ISTART JCL from the configuration library to start the server. This executes the IRUNJCL proc. The configuration library is

```
high_level_qualifier.PDS.WFS[suffix].DATA
```

where:

high_level_qualifier

Is the high-level qualifier to be used for all output libraries. This is the same high-level qualifier, which you specified during server installation.

suffix

If you are testing an additional instance, the new configuration library product type qualifier has a suffix (for example, WFS1 or WFSDEV). The suffix distinguishes the new configuration library from the original one.

3. Check the job output for errors. Look for the EDAPRINT message:

```
(EDA13023) ALL INITIAL SERVERS STARTED
```

4. Start the WebFOCUS Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

```
http://host:port
```

where:

host

Is the name of the machine on which the server is installed.

port

Is the HTTP Port Number specified during configuration.

The WebFOCUS Reporting Server browser interface opens.

5. If the WebFOCUS Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree.

6. Continue with adapter configuration, as described in the *ibi™ WebFOCUS® Adapter Administration* manual.

Upgrading the Release of your PDS-Deployed ibi WebFOCUS Reporting Server

You can upgrade your currently installed WebFOCUS Reporting Server by specifying the `high_level_qualifier` of your existing HOME data sets when prompted during execution of the `.run` file. The content of all HOME data sets are refreshed, but no changes are made to any Configuration or Application data set names or contents.

It is a good practice to back up your existing HOME data sets before refreshing them.

Step 3. Test the Installation

To test the installation:

1. Log on to TSO as iadmin.
2. Using a test server, replace all the EDAHOME libraries referenced in IRUNJCL with the new set.
3. Submit the ISTART JCL to start the server.
4. Check the job output for errors. Look for the EDAPRINT message:

```
(EDA13023) ALL INITIAL SERVERS STARTED
```

5. Start the WebFOCUS Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

```
http://host:port
```

where:

host

Is the name of the machine on which the server is installed.

port

Is the HTTP port number specified during installation.

The WebFOCUS Reporting Server browser interface opens.

6. If the WebFOCUS Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree.

When you are finished using the server, you can use the WebFOCUS Reporting Server browser interface to stop the server by going to the WebFOCUS Reporting Server browser interface menu bar, selecting **Workspace**, and then **Stop**.

If you experience problems at start-up, examine the job output for more information.

Step 4. Reconfigure Security

For information about configuring server security, see [Configure Security](#).

To reconfigure server security to OPSYS provider only:

1. Log on to TSO.
2. The libraries allocated to STEPLIB in IRUNJCL must be APF-authorized. All adapter/external load libraries should be allocated to the TASKLIB DDNAME.
3. Test server security by repeating the process described in [Step 3. Test the Installation](#)

Preventing Unsecured Starts After Upgrades

If the security provider is set to OPSYS in the configuration file and, additionally, the explicit environment variable EDAEXTSEC is set to OPSYS (or ON), and the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the edaprint log.

This feature prevents an unsecured server start after a software upgrade if any of the required post-upgrade reauthorization steps are missed on a UNIX, IBM i, or z/OS USS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server edaenv.cfg configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
I Configured primary security is 'OPSYS' as set in configuration file
```

```
E Server security explicitly set to OPSYS, but lacks authority!
```

```
Workspace initialization aborted.
```

```
(EDA13171) UNABLE TO START SERVER
```

Step 5. Reconfigure Adapters

While most adapters do not require additional steps after updating binary files, the following table notes the adapters that do require some consideration.

Adapter	Steps After Updating Binaries
Adabas	<ul style="list-style-type: none"> • Change the value for EDALOAD in member EDAENV of your current server configuration library (qualif.PDS.WFS.DATA) to point to the new P.HOME.LOAD. • Re-enable the module containing SVC using the WebFOCUS Reporting Server browser interface adapter configuration page. • Test the adapter from the adapter page before running your applications.
Db2 CAF	<ul style="list-style-type: none"> • Rerun the IDB2BIND JCL found in your current server configuration library WFS.PDS.WFS.DATA. This needs to be done for each subsystem that is used. • Test the adapter from the adapter page before running your applications.

Accounting for PDS - SMF Records

The server provides an optional facility to use for accounting purposes that enables you to log resource utilization on a per-user basis. This facility enables the server to generate SMF records for query-level and user-level accounting.

Server accounting requires that the server STEPLIB data sets be APF-authorized. When SMF records are generated, they contain:

- The logon ID and security ID of the user.
- The CPU time and EXCPs consumed.
- Data based on the type of record written.

You can process the SMF records using the accounting programs that exist at your site. Examples of SMF records are provided in [SMF Record Format for RECTYPES 1 and 4](#).

In order to write SMF records, the server must be running APF authorized.

Two sample Master Files (SMFVSAM and SMFFIX) are provided for accessing accounting statistics. They reside in *qualif.P.HOME.MAS*.

Their difference is that SMFVSAM can be used to report directly from the system-live SYS1.MANx records, while SMFFIX can be used to report from a sequential file produced from running the SMFDUMP utility. These Master Files enable you to interpret the SMF records generated by the accounting facility using reporting requests or store procedures. Both Master Files are for logoff records only, as indicated by ALIAS=2 on the RECTYPE field entry.

A sample procedure report to query the SMF data is also provided in *qualif.P.HOME.FEX* (SMFMAN1).

Enable Accounting

To enable accounting, insert the following statement into the server configuration file (edaserve.cfg):

```
smf_recno=smfnumber
```

where:

smfnumber

Is an integer in a range from 128 to 255, inclusive. This number represents the SMF number used by the accounting facility when it sends records to the SMF system.

By default, both RECTYPE pairs will be created when accounting is enabled. You can override the default by coding the following parameter on edaserve.cfg:

```
smf_subtype = {all|logon|query}
```

where:

all

Cuts all records. This is the default.

logon

Cuts logon records only (RECTYPE pair 1 and 2).

query

Cuts query records only (RECTYPE pair 4 and 5).

Set the Accounting Field

Up to 40 characters can be supplied that appear in the SMF records field SMFOFA40. The SET BILLCODE command can be used in any support server profile to provide the account field information. The syntax is

```
SET BILLCODE=value
```

where:

value

Is the 1–40 characters to be used on each SMF record produced.

This information can also be set dynamically from a client application by coding an RPC with the SET command and executing it with the value as a parameter. WebFOCUS users can send the SET command to the server.

Report From SMF Data

To report from SMF data, execute the sample procedure **smfman1.fex**, provided under home/catalog (DDNAME EDAHFEX for a PDS Deployment server).

You will be prompted for the DSN of the SMF VSAM data set from which you want to report, and the **smf_recno** value used to produce the SMF records.

The following is a listing of smfman1.fex:

```

DYNAM ALLOC FI SMFVSAM DSN &SMFDSN.Please provide SMF VSAM DSN. SHR REU

DEFINE FILE SMFVSAM

CPU/D8.2 = SMFOFCPU / 100 ;

USER/A20 = SMFOFUID ;

EXCPS/I6 = SMFOFEXC ;

TIME/D9.2 = SMFOFLTM / 100 ;

HR/I2 = SMFOFTME / 360000 ;

MIN/I2 = (SMFOFTME - (HR*360000)) / 6000 ;

TOD/A5 = EDIT(HR) | ':' | EDIT(MIN) ;

END

TABLE FILE SMFVSAM

PRINT USER CPU EXCPS TIME TOD

WHERE SMFOFRTY EQ &SMFNUM.Please provide SMF number(type) for report.

END

```

SMF RECTYPES

There are four RECTYPE values defined to produce SMF records:

RECTYPE	Description
1	Indicates a start of task record. When included in a report, these statistics tell when a task initiation occurred, and are of no particular use in chargeback. By pairing start and end of task records for all tasks within a time period, statistics, such as average active time, peak task count, and average task count, can be determined. These values can be used for future capacity

RECTYPE	Description
	planning activities for the server.
2	Indicates the start of a task record. When included in a report, these statistics tell when a task termination occurred. These records are cut for both publicly and privately deployed services and contain statistics for the subtask as a whole. For privately deployed services, RECTYPE (2) records contain statistics associated with a single user connection.
4	Begin the query. Record layout is the same as RECTYPE (1).
5	End the query. Record layout is the same as RECTYPE (2).

SMF Record Format for RECTYPES 1 and 4

The record format for RECTYPES 1 and 4 of the SMF records written by the server is defined below. The format is provided in the System 390 assembler DSECT form.

```

SMFON      DSECT

          SPACE

*-----*

*  USAGE ACCOUNTING SMF RECORD LAYOUT FOR LOGON RECORDS.          *

*                                                                    *

*  THIS IS THE DSECT DESCRIBING THE SMF RECORD WHICH IS PASSED TO  *

*  YOUR EXIT ON AT USER LOGON TIME.  IT IS COMPLETELY READY TO BE  *

*  WRITTEN WHEN YOUR EXIT RECEIVES CONTROL.                        *

*-----*

          SPACE

```

* THE FIRST TWENTY FOUR BYTES OF THE RECORD ARE THE SMF HEADER. *

* THESE FIELDS ARE REQUIRED IN ALL SMF RECORDS (18 BYTES FOR RECORDS *

* WITHOUT SUBTYPES; WE USE SUBTYPES, THE HEADER IS 24 BYTES). *

SPACE

SMFONLEN DS	H'116'	RECORD LENGTH
SMFONSEG DS	XL2'0000'	SEGMENT DESCRIPTOR (0 UNLESS SPANNED)
SMFONFLG DS	XL1	SYSTEM INDICATOR
SMFONRTY DS	XL1	RECORD TYPE
SMFONTME DS	XL4	TIME, IN HUNDREDTHS OF A SECOND
SMFONDTE DS	PL4	DATE, 00CYDDDF, WHERE F IS THE SIGN
SMFONSID DS	CL4	SYSTEM IDENTIFICATION
SMFONSBS DS	CL4	SUBSYSTEM IDENTIFICATION
SMFONSBT DS	XL2'0001'	SUBTYPE OF RECORD - X'0001' INDICATES X
		THIS IS A LOGON RECORD

SPACE

* THE NEXT FIELDS ARE THOSE PRESENT IN THE LOGON *

* RECORD FOR THE START OF A USER SESSION. *

SPACE

SMFONMSO DS	CL8	JOBNAME
SMFONJID DS	CL8	JOBID (FROM SSIBJBID)

SMFONASI DS	Y	ASID	
SMFONRV1 DS	XL2	RESERVED	
SMFONUID DS	CL20	SECURITY USERID	
SMFONLID DS	CL20	USERID PRESENTED AT LOGON (SAME AS	X
		SMFONSID UNLESS CHANGED VIA MSIDTR	X
		SECURITY EXIT)	
SMFONRSV DS	XL8	RESERVED FOR FUTURE EXPANSION	
SMFONCTI DS	XL4	RESERVED FOR FUTURE EXPANSION	
SMFONSRV DS	CL8	SERVICE NAME FROM SERVICE BLOCK	
SMFONRS0 DS	XL4	RESERVED FOR FUTURE EXPANSION	
SMFONCNT DS	XL1	CONNECTION TYPE	
SPACE			
SMFONTSO EQU	1	CONNECTION VIA TSO	
SMFONCIC EQU	2	CONNECTION VIA CICS	
SMFONVTM EQU	4	CONNECTION VIA VTAM	
SMFONPSR EQU	8		
SPACE			
SMFONRS1 DS	XL3	RESERVED	
SMFONID1 DS	F	SYSPLEX ID 1	
SMFONID2 DS	F	SYSPLEX ID 2	
SMFOFPID DS	XL20	POOLED USER ID	
SMFONRS2 DS	XL12	RESERVED	

SMFONL	EQU	*-SMFON	LENGTH OF THE SMF LOGON RECORD
--------	-----	---------	--------------------------------

SMF Record Format for RECTYPES 2 and 5

The record format for RECTYPES 2 and 5 of the SMF records written by the server is defined below. The format is provided in the system 390 assembler DSECT form.

```

SMFOF    DSECT
        SPACE

*-----*

*  USAGE ACCOUNTING SMF RECORD LAYOUT FOR LOGOFF RECORDS.          *
*                                                                    *
*  THIS IS THE DSECT DESCRIBING THE SMF RECORD WHICH IS PASSED TO  *
*  YOUR EXIT ON AT USER LOGOFF TIME.  IT IS COMPLETELY READY TO BE *
*  WRITTEN WHEN YOUR EXIT RECEIVES CONTROL.                        *
*-----*

        SPACE

```

```

*-----*

*  THE FIRST TWENTY FOUR BYTES OF THE RECORD ARE THE SMF HEADER.    *
*  THESE FIELDS ARE REQUIRED IN ALL SMF RECORDS (18 BYTES FOR RECORDS *
*  WITHOUT SUBTYPES; WE USE SUBTYPES, THE HEADER IS 24 BYTES).      *
*-----*

```

SPACE

SMFOFLEN DS	H'168'	RECORD LENGTH
SMFOFSEG DS	XL2'0000'	SEGMENT DESCRIPTOR (0 UNLESS SPANNED)

SMFOFFLG DS	XL1	SYSTEM INDICATOR
SMFOFRTY DS	XL1	RECORD TYPE
SMFOFTME DS	XL4	TIME, IN HUNDREDTHS OF A SECOND
SMFOFDTE DS	PL4	DATE, 00CYDDDF, WHERE F IS THE SIGN
SMFOFSID DS	CL4	SYSTEM IDENTIFICATION
SMFOFSBS DS	CL4	SUBSYSTEM IDENTIFICATION
SMFOFSBT DS	XL2'0002'	SUBTYPE OF RECORD - X'0002' INDICATES X THIS IS A LOGOFF RECORD

SPACE

* THE NEXT FIELDS ARE THOSE PRESENT IN THE LOGOFF *

* RECORD FOR THE END OF A USER SESSION. *

SPACE

SMFOFMS0 DS	CL8	JOBNAME
SMFOFJID DS	CL8	JOBID (FROM SSIBJBID)
SMFOFASI DS	Y	ASID
SMFOFRV1 DS	XL2	RESERVED
SMFOFUID DS	CL20	SECURITY USERID
SMFOFLID DS	CL20	USERID PRESENTED AT LOGON (SAME AS X SMFOFSID UNLESS CHANGED VIA MSIDTR X SECURITY EXIT)

SMFMEMA	DS	XL4	MEMORY ABOVE THE LINE (IN KILOBYTES)	
SMFMEMB	DS	XL4	MEMORY BELOW THE LINE (IN KILOBYTES)	
SMFZIIP	DS	XL4	ZIIP CPU NORMALIZED (HUNDREDTHS OF A SEC)	
SMFOFSRV	DS	CL8	SERVICE NAME FROM THE SERVICE BLOCK	
SMFZPOCP	DS	XL4	ZIIP ON CP (HUNDREDTHS OF A SEC)	
SMFOFCNT	DS	XL1	CONNECTION TYPE	
SPACE				
SMFOFTSO	EQU	1	CONNECTION VIA TSO	
SMFOFCIC	EQU	2	CONNECTION VIA CICS	
SMFOFVTM	EQU	4	CONNECTION VIA VTAM	
SMFOFPSR	EQU	8		
SMFOFCC	DS	XL3	COMPLETION CODE FOR THE TASK	
SMFOFACT	DS	CL8	USER ACCOUNTING INFORMATION; THIS FIELD CURRENTLY PASSED AS LOW VALUE	X
SMFOFCPU	DS	XL4	CPU TIME IN HUNDREDTHS OF A SECOND	
SMFOFEXC	DS	XL4	COUNT OF EXCP'S	
SMFOFLTM	DS	FL4	LOGON DURATION IN HUNDREDTHS OF A SECOND	X
SMFPRTY	DS	XL1	PRIORITY	
SMFCOMPL	DS	XL1	COMPLETION TYPE	
	DS	XL2	RESERVED	
SMFOFID1	DS	F	SYSPLEX ID 1	

SMFOFID2	DS	F	SYSPLEX ID 2
SMFOPID	DS	XL20	POOLED USERID
SMFOFA40	DS	CL40	FULL 40-BYTE ACCOUNTING FIELD
		SPACE	
SMFOFL	EQU	*-SMFOF	LENGTH OF THE SMF LOGOFF RECORD

Accounting for Db2 in an ibi WebFOCUS Reporting Server Task

When using a server to access Db2 data, certain processing takes place within the Db2 address space and is governed by the Db2 chargeback system. If a user requests data from Db2, the server passes the request to the Db2 subsystem. The Db2 subsystem then processes the request, performing such tasks as retrieving rows and aggregating the data. It generates the answer set, and passes the output back to the server. The server then performs any joins and formatting which have not been performed by Db2 to satisfy the original request.

Charges incurred while the request was being processed by the Db2 subsystem are added to the charges accumulated in the server task that originated the request for processing. If the server accounting is enabled, these charges are associated with the user logon and security IDs in the SMF records described earlier.

Enabling Use of the zIIP Specialty Engine

If your site has a zIIP (System **z**Integrated Information **P**rocessor) specialty engine from IBM, you can offload specific categories of workload from the Central Processors to the zIIP.

The zIIP engine is a restricted version of a Central Processor (CP), also referred to as a General Processor (GP). The capacity of the zIIP engine does not count toward the overall MIPS rating of the mainframe image, so the CPU usage incurred on the zIIP is effectively free. Central Processors are often configured to run at speeds below their maximum rating for cost saving and capacity planning purposes. For Central Processors, *100% capacity* typically refers to the maximum MIPS that the processor is allowed to generate at that

installation, in accordance with your contract with IBM. In contrast, the zIIP engine always runs at true 100 percent of capacity.

As much as 80 percent of server processing is enabled to run on the zIIP engine. Typical workloads are expected to offload 30 to 80 percent of CPU processing to the zIIP engine.

To make use of the zIIP enablement feature, the server must run in an authorized state.

What Is a zIIP Specialty Engine?

Though physically identical to a central processor, the zIIP engine is microcoded at installation time to run specific types of workloads. The central processor continues to handle the operating system, I/O interrupts and timer interrupts, job initiations, and user interactions with the operating system. The zIIP concentrates on CPU intensive workloads, leaving the central processor more time to absorb otherwise queued workloads, thereby achieving some overall performance improvement across all mainframe activity.

Steps to zIIP Enablement

This section describes steps and requirements for the server use of the zIIP processor.

The steps to server zIIP enablement are:

1. Obtain APF authorization for the server load library.
2. Activate the zIIP feature using the SET ZIIP=ON or SET ZIIP=ON/SIMMAXZIIP command. For instructions, see [Activating a zIIP Environment or Projecting zIIP Usage](#).

Usage Notes for Use of the zIIP Processor

- Maximize the block sizes of data sources that are read or written by the server to reduce the number of I/Os required to access the file. This will reduce the number of switches to non-zIIP mode that the server agents have to make, thus permitting a greater percentage of zIIP contribution to the request.
- Move or rewrite functions developed at your site since the server must switch to non-zIIP mode for each call to such routines. You may be able to use one of the following possible solutions:
 - Move the routines from DEFINES to COMPUTEs to reduce the number of times

they are referenced. This tactic must be applied carefully, and only when report results would not change.

- Rewrite the routines using DEFINE FUNCTION, which executes on the zIIP processor.
- Confine the routine to a pre-step run with ZIIP=OFF which collects its calculated results, then use those calculations in the next step with ZIIP=ON.

Activating a zIIP Environment or Projecting zIIP Usage

The last step in zIIP enablement is to activate the use of the zIIP processor in the server. zIIP enablement is activated by the SET ZIIP command.

The SET ZIIP command has three options:

- **OFF.** This setting prevents the server from offloading its processing to a zIIP.
- **ON.** This setting causes the server to offload processing to a zIIP engine if you have a zIIP processor and the environment is properly APF-authorized.
- **ON/SIMMAXZIIP.** This setting enables you to project zIIP processing in two different environments:
 - **You do not have a zIIP processor.** Using this setting along with the PROJECTCPU parameter, you can project how much server workload would have been offloaded to a zIIP.
 - **You do have a zIIP processor.** Using this setting you can project how much advantage you would achieve by offloading 100% of eligible server processing to the zIIP.

Activate the zIIP Enablement Feature

You can issue the SET ZIIP command in a server profile or in a particular FOCEXEC.

```
SET ZIIP={ON[/SIMMAXZIIP] | OFF}
```

where:

ON

Configures the server to offload processing to the zIIP engine.

This setting:

- Determines if the zIIP processor is accessible to the LPAR in which a job is running.
- Determines if the server environment has been properly authorized to run a zIIP workload.

i Note: If the server determines that the zIIP processor is not accessible or that the environment has not been authorized correctly, it issues a message describing the reason and continues in ZIIP=OFF mode, which forwards all subsequent work to the Central Processor.

ON/SIMMAXZIIP

Configures the server to either:

- Project what the zIIP usage would be if the server could offload processing to a zIIP, when the server is operating in an LPAR without a zIIP. This requires that the PROJECTCPU parameter be set to YES.

The SYS1.PARMLIB member IEAOPTxx contains the PROJECTCPU statement. Activating the PROJECTCPU parameter projects zIIP consumption when a zIIP processor is not yet defined to the LPAR. SMF type 30 records will show the potential calculated zIIP time, so that you can accurately project zIIP usage. This enables you to evaluate the effect of configuring a zIIP processor to be available for server usage. The Systems Programmer for your site will have access to this data. Use this option for simulation purposes only.

Since the zIIP engine is not actually present, all zIIP-eligible workload will be diverted to the Central Processor. Thus, all of that CPU utilization will be recorded in a server variable called &FOCZIIPONCP. This is the amount of workload that would have run on the zIIP engine, and would have appeared in &FOCZIIPCPU, had the zIIP been present and accessible to server work. This information is also recorded in the server job statistics as well as in IBM SMF type 30 records.

To use this option, insert the following parameter in SYS1.PARMLIB for your LPAR, and also issue the SET ZIIP=ON/SIMMAXZIIP command:

```
PROJECTCPU=YES
```

This setting:

- Determines if the PROJECTCPU=YES command has been set in the LPAR.
- Determines if the server environment has been properly authorized to run a zIIP workload.
- Projects zIIP utilization if 100% of eligible server processing could be offloaded to the zIIP, when the server is running in an LPAR with a zIIP. This lets you determine what you would gain by configuring Workload Manager to give the server a bigger share of zIIP processing.

IBM Workload Manager (WLM) prioritizes workloads among the Central Processors and zIIP processors at your site based on a complex set of goals and rules established by the system administrator. These rules apply to all workloads from all sources, not just the server. These goals combine to influence the decision to direct server requests to the zIIP engine at any particular moment.

Utilizing this setting with a zIIP present can help you determine how much advantage you would get if the server had more of a share of the zIIP processor. To see the difference in actual and projected zIIP usage, run the same job with SET ZIIP=ON and then with SET ZIIP=ON/SIMMAXZIIP and compare the results. For more information about evaluating zIIP usage, see [Evaluating zIIP Usage](#).

This setting:

- Determines if the zIIP processor is accessible to the LPAR in which a job is running.
- Determines if the server environment has been properly authorized to run a zIIP workload.

i Note: If the server determines that the environment has not been authorized correctly, it issues a message describing the reason and continues in ZIIP=OFF mode, which forwards all subsequent work to the Central Processor.

OFF

Configures the server not to offload processing to the zIIP engine. OFF is the default value.

i Note: Turn off zIIP enablement only when you know for sure that a job will not gain any advantage from using the zIIP processor or if the system operator or administrator requires that you turn it off.

Setting the PROJECTCPU Parameter in SYS1.PARMLIB Member IEAOPTxx

Use the following sample as a guide for setting the PROJECTCPU parameter in SYS1.PARMLIB(IEAOPTxx):

```
/* ***** */
/*          SYS1.PARMLIB(IEAOPTxx)          */
/* ***** */

PROJECTCPU=YES
```

How the ibi WebFOCUS Reporting Server Takes Advantage of the zIIP Processor

The server diverts eligible workload to the zIIP engine by switching from TCB (Task Control Block) mode for workloads that can run only on a central processor to SRB (Service Request Block) mode for execution of enabled workloads on the zIIP engine.

Types of server processing that are offloaded to the zIIP engine include:

- Computations
- Aggregation
- Screening
- Sorting
- Report formatting and styling
- Transaction Processing

The server zIIP Monitor detects situations in which the overhead cost of zIIP usage is exceeding the CPU benefits gained. When this threshold is reached, the server may decide to suspend use of the zIIP for the duration of a logical phase of the server request. When it does so, it places a message to that effect in the JES log. It then resets to make the zIIP processor accessible to the next logical phase of the server request.

TABLE, MATCH, MODIFY, and MORE requests may suspend and resume more than once as they progress through the logical phases of execution.

In every case, the server attempts to optimize the use of the zIIP and minimize chargeable CPU costs.

Applications that perform significant database I/O, high-volume sorting, or the use of third-party tools or user functions during processing require switching out of SRB (zIIP) mode into TCB (non-zIIP) mode to communicate, and then back again to continue processing. Although each switch is minuscule, the cumulative effect can absorb measurable amounts of CPU time on both the zIIP engine and the central processor.

In order to diminish this effect, the server buffers the collection of records passed to the system sort utility and some adapters rather than passing one record at a time, thus reducing the number of switches between TCB and SRB modes.

These third-party products may themselves be zIIP enabled and may offload some or all of their processing to the zIIP engine independent of the server. The server always calls these products from the central processor because it cannot know whether they will perform any processing that is prohibited on the zIIP.

Even though zIIP usage occurs more frequently on non-optimized requests to a relational data source, optimized requests are still inherently more efficient and, therefore, may incur less CPU time. Being zIIP enabled, Db2 may also take advantage of the zIIP processor for server requests based on the local configuration of Db2 relative to the server.

Requests against some types of data sources whose I/O can be buffered gain a lot of advantages from zIIP enablement. Data sources that gain the most benefit from zIIP processing due to buffered I/O include:

- Blocked flat files
- FOCUS
- XFOCUS
- VSAM
- Db2

Evaluating zIIP Usage

In order to evaluate server zIIP processing in a session, you can query three Dialogue Manager variables that accumulate statistics about CPU processing:

- &FOCCPU accumulates the time spent on a central processor. This is an existing

variable that precedes zIIP enablement.

- **&FOCZIIPCPU** accumulates the time actually spent on the zIIP processor (in SRB mode). This is the normalized CPU value using the same scale as **&FOCCPU**.
- **&FOCZIIPONCP** accumulates the time that processing could have been offloaded to the zIIP processor but was diverted to the central processor by the system.

Note:

- **&FOCCPU** includes the value of **&FOCZIIPONCP**.
- The sum of **&FOCZIIPCPU** and **&FOCCPU** represents the total CPU utilized by the server agent.
- If you set **ZIIP=OFF**, the zIIP variables do not accumulate further but are not reset to zero. If you later set **ZIIP=ON**, they resume accumulating statistics.

The RM (Resource Manager) that monitors server usage also captures zIIP statistics.

Performance Considerations for PDS

There are several ways in which you can improve the server performance:

- **Server initialization commands.** You can specify DYNAM commands in member **SRVINIT** of the data set referenced by **//EDACCFG DD** in **IRUNJCL**. For more information, see [Server Initialization Commands Configured in SRVINIT Member](#).
- **Non-swappable address space.** We recommend that you run the server in a non-swappable address space. For more information, see [Running the ibi WebFOCUS Reporting Server in a Non-Swappable Address Space](#).
- **Workload Manager (WLM).** You can balance server workload by using Workload Manager. For more information, see [Workload Manager](#).

Server Initialization Commands Configured in SRVINIT Member

It is possible to specify DYNAM commands in member **SRVINIT** of the data set referenced by **//EDACCFG DD** in **IRUNJCL**. These commands will be executed during server startup and will be in effect until the server is shut down. You can execute the following DYNAM commands from **SRVINIT**:

- `DYNAM SET APP FOR filetype [SKIP|CREATE] [POSTFIX a.b] [parms]`

Specify the types of component files that are skipped or created for the application when an APP CREATE command is issued. By default, all component file types are generated.

where:

filetype

Are the component types that may be affected by this command: ACCESS, DTD, ETG, FOCCOMP, FOCEXEC, FOCSTYLE, GIF, HTML, MAINTAIN, MASTER, SQL, WINFORMS, XML, XSD. You must issue a separate command for each component type you wish to affect.

SKIP

Indicates that the designated file type should not be created when the APP CREATE command is issued.

CREATE

Creates the designated file type when the APP CREATE command is issued. This is the default setting.

POSTFIX

Specifies the lower-level qualifier of the DSN (data set name) for the component type. The APPROOT value is used to complete the full DSN, which is expressed as

```
aprootvalue.appname.component_type
```

The default value for component_type is

```
filetype.DATA
```

parms

Are the allocation parameters you can set. The default parameter values are:

Filetype	Parms
ACCESS	RECFM FB TRKS LRECL 80 BLKSIZE 22000 SPACE 50 50 DIR 50
DTD	RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50
ETG	RECFM FB TRKS LRECL 80 BLKSIZE 22000 SPACE 50 50 DIR 50
FOCCOMP	RECFM VB TRKS LRECL 32756 BLKSIZE 32760 SPACE 50 50 DIR 50
FOCEXEC	RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50
FOCSTYLE	RECFM FB TRKS LRECL 1024 BLKSIZE 27648 SPACE 50 50 DIR 50
GIF	RECFM VB TRKS LRECL 1028 BLKSIZE 27998 SPACE 50 50 DIR 50 GIF type creates libraries for GIF and JPG files.
HTML	RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50

Filetype	Parms
	50 DIR 50
MAINTAIN	RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50
MASTER	RECFM FB TRKS LRECL 80 BLKSIZE 22000 SPACE 50 50 DIR 50
SQL	RECFM VB TRKS LRECL 32756 BLKSIZE 32760 SPACE 50 50 DIR 50
WINFORM	RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50
XML	RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50
XSD	RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50

- DYNAM APP app1 [app2 ...]

Enable application libraries to be allocated during the server startup, improving performance. This command is not applicable to sequential data sets in the application (for example, FOCUS, FTM) which will only be allocated when they are referenced. For example:

DYNAM APP IBISAMP BASEAPP (default command at installation time)

- DYNAM ALLOC commands

For sequential data sets in the application (for example, FOCUS, FTM) to be allocated at server startup (equivalent to adding a JCL allocation for these files in IRUNJCL).

Running the ibi WebFOCUS Reporting Server in a Non-Swappable Address Space

We recommend that you run the server in a non-swappable address space. In order to make the server address space permanently non-swappable, add the following entry to SYS1.PARMLIB(SCHEDxx):

PPT PGMNAME(TSCOM300)	/* PROGRAM NAME */
NOSWAP	/* NON-SWAPPABLE */
CANCEL	/* CAN BE CANCELLED */

Do not use the KEY 0 parameter, or any other parameter (such as NOPASS), unless the system programmer completely understands the consequences of adding the parameter.

All local spawn transactions will perform in the mode of the server. For example, if the server address space is non-swappable, all local spawn transactions execute as non-swappable.

The server executes limited non-local spawn, such as when the user executes a UNIX system command. Non-local spawn execute as swappable.

The server never executes a fork subroutine. (A fork subroutine creates a new process. The new process called the child process, is an almost exact copy of the calling process, which is called the parent process.)

Workload Manager

Although the server may run in a specific performance group, transactions submitted by server agents may perform differently than the server by adding the following keyword to edaserve.cfg:

```
wlm_enclave_trname = WLM_transaction_name
```

where:

WLM_transaction_name

Can be up to 8 characters.

This is a service-level keyword.

Using this setting, the task will join a Workload Manager (WLM) enclave when a request starts, and leave the enclave when the request finishes. This gives WLM control of the dispatching priority of the task. The transaction rules defined on WLM will determine the default service class assigned to this transaction, and that service class will determine how the request runs.

This feature helps to balance a workload so that a long request will not affect a short request. This can be achieved through WLM rules designed to lower the priority of a long request after a certain period of time. Without this feature, all requests share the region priority.

The transaction name passed in this keyword must match one defined in the WLM Classification Rules for the Job Entry Subsystem (JES). A corresponding WLM Service Class pointed to by this rule will then be associated with this service.

The classification rules for JES must be used even if the server is started as a started task. The subtasks are always run under JES.

For example, you would include the following in edaserve.cfg:

```
SERVICE = DEFAULT

BEGIN

wlm_enclave_trname = IWAYFAST

.

.

.

END
```

The WLM definition is:

```
Subsystem Type JES - Batch Jobs
```

Classification:

Default service class is PRDBATLO

There is no default report class.

	Qualifier	Qualifier	Starting	Service	Report
#	type	name	position	Class	Class

1	TN	IWAYFAST		EDAQRYHI	

WLM sub-rules (levels 2 and above) are supported. For a server request to join an enclave in a particular service class, the names of all rule qualifiers below our transaction name are checked. For example, consider the following WLM definition:

Subsystem Type JES - Batch Jobs

Classification:

Default service class is PRDBATLO

There is no default report class.

	Qualifier	Qualifier	Starting	Service	Report
#	type	name	position	Class	Class

1	SSC	PRDMVS		PRDDFLT	
2	TN	IWAYFAST		EDAQRYHI	

In this particular case, the qualifier 1 type is SSC (Subsystem Collection), and a server request will only join the enclave IWAYFAST if it is running on a particular LPAR in the SYSPLEX. This qualifier (PRDMVS) must match the XCF group definition: issue \$DMASDEF (for JES2) and check the value of XCFGRPNM field.

You can handle WLM scheduling environments by defining them to WLM and then adding the JOB statement parameter SCHENV=xxxxx to the ISTART JCL.

General Information for a z/OS PDS Installation

This section covers general information for a z/OS installation.

Sample Metadata, Data, and Other Tutorial Samples

The WebFOCUS Reporting Server browser interface has a feature on the ribbon and on the application tree (under *new*), **Tutorials** (the Create Tutorial Framework page), which has a pull-down select list for various samples. The ibi Data Migrator desktop interface also has this feature on the application tree.

There are currently about 10 different tutorial/sample selections available on the pull-down select list to match various customer needs. The bulk of the prior IBISAMP sample objects can be generated by selecting the **Create Legacy Sample Tables and Files** tutorial. Other prior IBISAMP ibi Data Migrator sample objects (usually starting with the characters dm*) are now loaded by choosing their respective ibi Data Migrator tutorials. Under the new method, the tutorials/samples may be loaded to any application, not just IBISAMP.

If you are doing just a software refresh, the prior IBISAMP objects remain unchanged (because a refresh does not touch app directories).

Frequently Asked Questions for PDS

Q: Why might someone want to use the PDS deployment?

A: PDS deployment provides the same rich level of features as the USS-deployed server, including the WebFOCUS Reporting Server browser interface, but removes the requirement for interaction with UNIX System Services at installation and run time. It deploys the server

software in partitioned data sets. Configuration and user-created source files, such as procedures and metadata, are also stored in PDS libraries.

Administration of the server, from a systems perspective, has been streamlined to match that of the classic MVS version of the server (also known as the SSCTL server). There are fewer user ID requirements for installing and operating the PDS-deployed server than the USS-deployed version, and security management has been simplified.

Q: Does this replace the older MVS server (also known as SSCTL)?

A: The z/OS server with PDS deployment is a migration path from the older MVS server.

Q: Can one refresh a server's installation software that had been deployed one way with software using other type of deployment?

A: No. Each deployment type is independent of the other with regard to installation.

Q: Can both deployments of the server coexist on one z/OS system?

A: Yes.

Q: Can one configure two server instances of the same server, one instance a USS deployment, and the other a PDS deployment?

A: No. Although the media and installation are unified, once the base server software is installed, the two deployment types run separately.

As with the USS deployment, the PDS deployment can have many instances running from the same EDAHOME set of libraries.

Q: Can I monitor server startup by checking the MVS SYSLOG?

A: Yes.

The following messages are written to the SYSLOG when

- The Server starts successfully:

```
(EDA13023) ALL INITIAL SERVERS STARTED
```

- The Server does not start:

```
(EDA13171) UNABLE TO START IWAY SERVER
```

Q: What, if anything, does the PDS deployment not support? In what installation implementation?

A: The PDS deployment of the server currently does not support the following functions:

- The WebFOCUS Reporting Server browser interface Run Stress option.
- Displaying server logs and traces in the WebFOCUS Reporting Server browser interface.
- Formats XLSX and PPTX.



Note: As a workaround, you can issue the SET EXCELSERVURL command to point to ibi™ WebFOCUS® Client ibi_apps context root.

To set this parameter, you can issue the following in a procedure:

```
SET EXCELSERVURL = http[s]://servername:port/ibi_apps
```

Alternatively, you can issue the following in the WebFOCUS Administration Console:

```
IBIF_excelservurl = http[s]://servername:port/ibi_apps
```

where:

servername

Is the name of the machine where the Application Server is running.

port

Is the port used by WebFOCUS to communicate with the Application Server. The default port is 8080. It should also be noted that the protocol may be http or https based on the customer configuration.

- Adobe Flex.
- RACF TEMPDSN class—Supported except for FOCCACHE application datasets.

Third-Party Software and Licenses

All license information is available on the WebFOCUS Reporting Server browser interface by clicking the Help (?) menu, and then selecting **Licenses**, which displays the EULA End-User Agreement and third-party licenses.

Common Windows-Based Java Implementations

For more information about the common Windows-based Java implementations, see [Common Windows-Based Java Implementations](#).

Troubleshooting for PDS

If you have a problem and cannot resolve it yourself, contact Customer Support. In addition, supply the following information to Customer Support:

- Server trace (see [Generate a Trace](#)).
- JCL for IRUNJCL.
- Job output.
- System dump, if needed (see [Generate a System Dump](#)).
- Any additional information regarding how the problem occurred.

Problem: The ibi WebFOCUS Reporting Server Abends With a U4039 Code

Problem: The server abends with a U4039 code.

Cause: This is a generic abend.

Solution: Find out what caused the abend by checking the edaprint.log file, SYSOUT *ddname*, and the MVS system log.

Generate a Trace

To generate a server trace:

Procedure

1. Turn tracing on by doing one of the following:
 - Going to the WebFOCUS Reporting Server browser interface menu bar, selecting **Workspace**, and then **Enable Traces**.
 - Starting the server by running the ITRCON JCL member.
 - On the MVS Console or SDSF, issue the following operator MODIFY command
F jobname, -traceon
where *jobname* is the job under which the server is running.
2. Reproduce the problem.
3. Submit the ISAVEDIA member to produce additional diagnostic information.
4. Send the server JES log, and the ISAVEDIA JES log, to Customer Support.

Generate a System Dump

To generate a system dump:

Procedure

1. Allocate DDNAME SYSMDUMP pointing to the data set with the following DCB parameters:

```
RECFM=FB,LRECL=4160,BLKSIZE=4160.
```

2. To get the first dump, add the parameter FREE=CLOSE to your DD statement. The DD statement should appear as follows:

```
//SYSMDUMP DD DISP=SHR,DSN=MYID.EDAPTH.SYSMDUMP,FREE=CLOSE
```

3. To get the last dump, the statement should appear as follows:

```
//SYSMDUMP DD DISP=SHR,DSN=MYID.EDAPTH.SYSMDUMP
```

Only two IDs must have privileges to write into this data set: ISERVER and IADMIN. General server users DO NOT need read or write access to the SYSMDUMP data set.

4. To prevent the Abend-AID from intercepting the dump, add:

```
//ABNLIGNR DD DUMMY
```

5. To prevent the Language Environment from intercepting the dump, specify:

```
EDADUMPOPT=UAIMM in EDAENV DD
```

This enables you to get more accurate information reflecting the moment the abend actually occurs.

6. Save the entire job output for the server (including JES logs), and send it to Customer Support.

Result

Instead of using JCL allocations to add SYSMDUMP, the procedure described below can be used alternatively.

Add JCL Allocations to a Running ibi WebFOCUS Reporting Server

A z/OS operator can issue modify commands from the z/OS system console to allocate DDNAMES to the server without restarting it. This procedure is useful if you need to re-allocate a file that was freed to allow a batch overnight utility to run, or perhaps to add SYSMDUMP allocation to a running server.

Allocate a Data set From the z/OS System Console

```
F <iway_server_jobname/started task>,DYNAM ALLOC FI <ddname> DA <dsname>  
  
<optional dynam parameters>
```

Allocating a VSAM Data set

```
F IWAY2,DYNAM ALLOC F VSAMFILE DA VSAM.FILEA.CLUSTER SHR
```

Allocating a SYSMDUMP Data set With FREE=CLOSE Option

```
F IWAY2,DYNAM ALLOC FILE SYSMDUMP DA PROD2.SYSMDUMP.DATA SHR CLOSE
```



Note: The examples above assume IWAY2 is the jobname/started task ID for the server.

All valid DYNAM ALLOC syntaxes are supported. For more information on the DYNAM command, refer to the *ibi™ WebFOCUS® Stored Procedure and Subroutine Reference for 3GL Languages* guide.

The following message will be issued in the server JESMSG LG indicating if the command was processed successfully or not.

Success:

```
+DYNAM COMMAND SUCCESSFULLY PROCESSED Rc=0
```

Failure:

```
+DYNAM ERROR: IKJ56225I DATA SET IWAY.TEST ALREADY IN USE, TRY LATER
```

Free Data sets Allocated to the ibi WebFOCUS Reporting Server

A z/OS operator can issue modify commands from the z/OS system console to free DDNAMEs or DSNAMES allocated to the server. Both global allocations (made at the server ISTART JCL) and local ones (DYNAM ALLOC commands issued by user tasks) can be freed. This procedure is useful if you need to free an allocation to run a batch utility overnight, without restarting the server.

Free a Data set From the MVS System Console

To free a single DDNAME:

```
F <iway_server_jobname/started task>,DYNAM FREE FI <ddname>
```

To free a single DSNNAME (all occurrences in the server):

```
F <iway_server_jobname/started task>,DYNAM FREE DS <dsname>
```

To free multiple DDNAMEs, passing a pattern (free all DDNAMEs starting with AB):

```
F <iway_server_jobname/started task>,DYNAM FREE FI AB*
```

To free multiple DSNAMES (all occurrences in the server), passing a pattern (free all allocations of data sets starting with IWAY.VSAM):

```
F <iway_server_jobname/started task>,DYNAM FREE DA IWAY.VSAM*
```

A message is issued in the iway_server JESMSGLOG indicating if the command was processed successfully or not, as follows.

Success:

```
+DYNAM COMMAND SUCCESSFULLY PROCESSED Rc=0
```

Failure:

```
+DYNAM ERROR: IKJ56225I DATA SET IWAY.TEST ALREADY IN USE, TRY LATER
```

Freeing an Allocated Data Set

Suppose ISTART JCL (jobname IWAY2) has the following allocation:

```
//VSAMFILE DD DISP=SHR,DSN=VSAM.FILEA.CLUSTER
```

The operator can free this file using the command (from the MVS console):

```
F IWAY2,DYNAM FREE FI VSAMFILE
```

Initialize the RDAAPP Application

RDAAPP is an interactive client test application that facilitates the execution of SQL statements and stored procedures on the unified server. During the installation process, JCL and REXX routines are created in the installation data set as members IRDAAPPJ and IRDAAPPC respectively.

The following installation data set is used for USS deployment.

```
qualif.WFS.DATA
```

The following installation data set is used for PDS deployment.

```
qualif.PDS.WFS.DATA
```



Note: The RDAAPP application is not intended for use as a production tool.

Procedure

1. To use the IRDAAPPJ JCL, you must first edit the member IRDAAPPJ and add your request details.
 - a. To edit the member IRDAAPPJ, change the following field,

```
//SYSIN DD *  
  
Put your request here  
  
//
```

to

```
//SYSIN DD *
```

```

1
<userid>
<password>

S SELECT COUNTRY    FROM CAR

S SELECT CAR,SEATS  FROM CAR

Q

//

```

b. Complete the panel as follows.

Field	Instructions
<enter userid>	Enter a valid user ID or blank line if the userid of the user who submitted the job is to be used for a trusted connection.
<enter password>	Enter the password for the above userid or a blank line if the userid/password of the user who submitted the job is to be used for a trusted connection.
1	Match a node name in the EDACS3 allocation in the IRDAAPPJ JCL. Default (1) means LOOPBACK.

Field	Instructions	
<enter request>	Enter one of the following values:	
	S	To enter an SQL SELECT statement. Type the statement after you enter the value S (see the following example).
	Q	To quit.
	?	For this list of commands.
Q	Quit RDAAPP (It is needed twice).	

- c. After you have made the above edits, submit the JCL for execution.
2. Type the following command at the TSO ready prompt to use the IRDAAPPC REXX routine:

```
EX 'qualif.WFS.DATA(IRDAAPPC)'
```

or

```
EX 'qualif.PDS.WFS.DATA(IRDAAPPC)'
```

3. After the prompts, enter the same information as specified in the above table.

IRDAAPPC REXX Execution

The following is the screen output from a sample execution of the IRDAAPPC REXX routine:

```
*****
**                                RDAAPP Client test tool                                **
```

```
*****
```

```
Allocating environment handle...
```

```
List of available servers:
```

```
1 - LOOPBACK
```

```
Enter corresponding server entry number or name (default=1):
```

```
1
```

```
Enter User Name:
```

```
Enter Password:
```

```
Allocating connection handle...
```

```
Attempting connect to the datasource: LOOPBACK ...
```

```
Connect status = 0
```

```
New ODBC Connector Test.
```

```
Enter Command:
```

```
S SELECT COUNTRY FROM CAR
```

```
Alloc stmt ...
```

```
Return code from alloc stmt is 0
```

```
Issuing SQLPrepare call for SELECT COUNTRY FROM CAR
```

```
Return code from SQLPrepare call is 0
```

```
Executing SELECT COUNTRY FROM CAR stmt...
```

```
Issuing SQLNumResultCols call for SELECT COUNTRY FROM CAR
```

```
Number of resultset columns is 1
```


Printing select item descriptions:

```
Issuing SQLDescribeCol call for colNum=1  
item #1  
colname = COUNTRY  
coltype = 1  
precision = 10  
scale = 0  
nullable = 0
```

```
Binding columns...  
Fetching report data...  
ENGLAND  
FRANCE  
ITALY  
JAPAN  
W GERMANY  
  
<<< 5 record(s) processed. >>>
```

```
New ODBC Connector Test.  
Enter Command:  
S SELECT CAR,SEATS FROM CAR  
Alloc stmt ...  
Return code from alloc stmt is 0
```

```
Issuing SQLPrepare call for  SELECT CAR,SEATS FROM CAR  
Return code from SQLPrepare call is 0  
Executing  SELECT CAR,SEATS FROM CAR stmt...  
Issuing SQLNumResultCols call for  SELECT CAR,SEATS FROM CAR  
Number of resultset columns is 2  
Printing select item descriptions:
```

```
Issuing SQLDescribeCol call for colNum=1  
  
item #1  
  
colname = CAR  
  
coltype = 1  
  
precision = 16  
  
scale = 0  
  
nullable = 0  
  
    Issuing SQLDescribeCol call for colNum=2  
  
item #2  
  
colname = SEATS  
  
coltype = 4  
  
precision = 22  
  
scale = 0  
  
nullable = 0
```

```
Binding columns...  
  
Fetching report data...  
  
JAGUAR
```

2

JAGUAR

5

JENSEN

4

TRIUMPH

2

PEUGEOT

5

ALFA ROMEO

2

ALFA ROMEO

2

ALFA ROMEO

4

MASERATI

2

DATSUN

4

TOYOTA

4

AUDI

```
5
BMW
5
BMW
4
BMW
5
BMW
5
BMW
5
BMW
5
<<< 18 record(s) processed. >>>
```

New ODBC Connector Test.

Enter Command:

Q

Committing...

Return code from commit is 0

Disconnecting DBC ...

Freeing DBC handle...

Freeing ENV handle...

```
<<< RDAAPP : Exiting... >>>
```

Security Providers

The default security provider for a new installation is the internal security provider, PTH. The PTH provider implements security using user IDs, passwords, and group memberships stored in the admin.cfg configuration file. After the initial installation, the Server Administrator that was configured during the installation can start the server and use the Reporting Server browser interface to further customize security settings, for example, to configure alternate or additional security providers, create additional PTH IDs, and register groups and users in a security role. For more information about security providers, see the *Server Security* chapter in the *ibi™ WebFOCUS® Reporting Server Administration* manual.

Using Applications

The Open Data Hub for Mainframe ODBC Connector is compliant with the ODBC 3.5 specification.

Using the Open Data Hub for Mainframe ODBC Connector

The following procedures describe how to use the Open Data Hub for Mainframe ODBC Connector from Microsoft Excel, Microsoft Power BI, and Tableau.

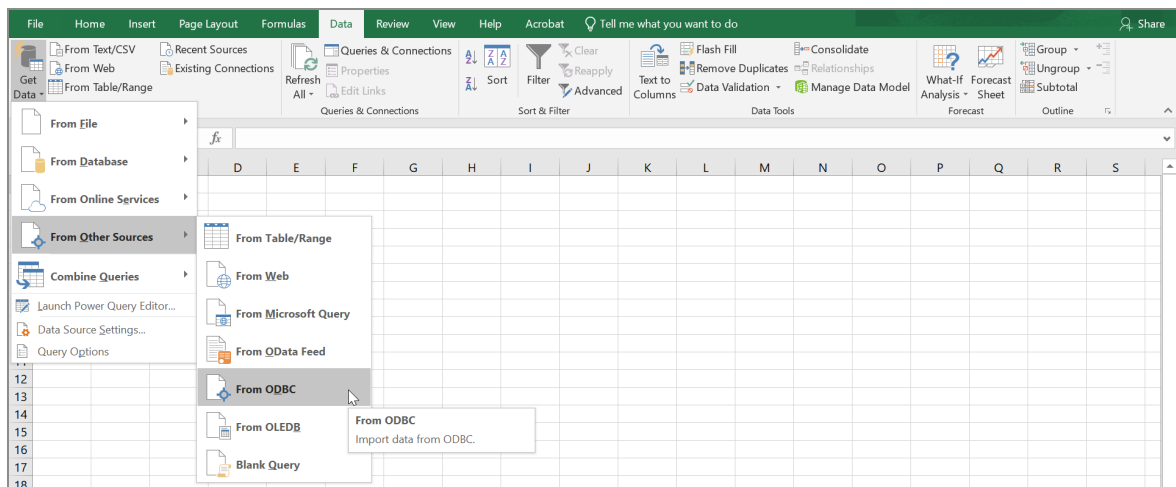
Open Data Hub for Mainframe ODBC Connector from Microsoft Excel

The following procedure describes how to use the Open Data Hub for Mainframe ODBC Connector from Microsoft Excel and create a visualization.

Use the ODBC Connector from Microsoft Excel

Procedure

1. From Microsoft Office, open Microsoft Excel.
2. From the Data tab, select **Get Data**.
3. From the Get Data drop-down list, select **From Other Sources**, and then select **From ODBC**, as shown in the following image.



The From ODBC dialog box opens.

4. Select the Data Source Name, for example, DATA, as shown in the following image.



5. Click **OK**.

The Application Directory Navigator dialog box opens.

Note: To see all the application directory folders on the Application Directory Navigator dialog box, select **Folders** from the Schemas drop-down list on the ODBC Driver Configuration dialog box, as shown in the following image.

ibi™ ODBC Driver Configuration

ODBC Connector

Connection Parameters

Data Source Name: DATA

Description: ibi ODBC Driver

TCP/IP Server: MVS123 Port: 8120

Security: Explicit Test

User: srvadmin

Password: ••••••••

Data source

Service:

Schemas: Folders

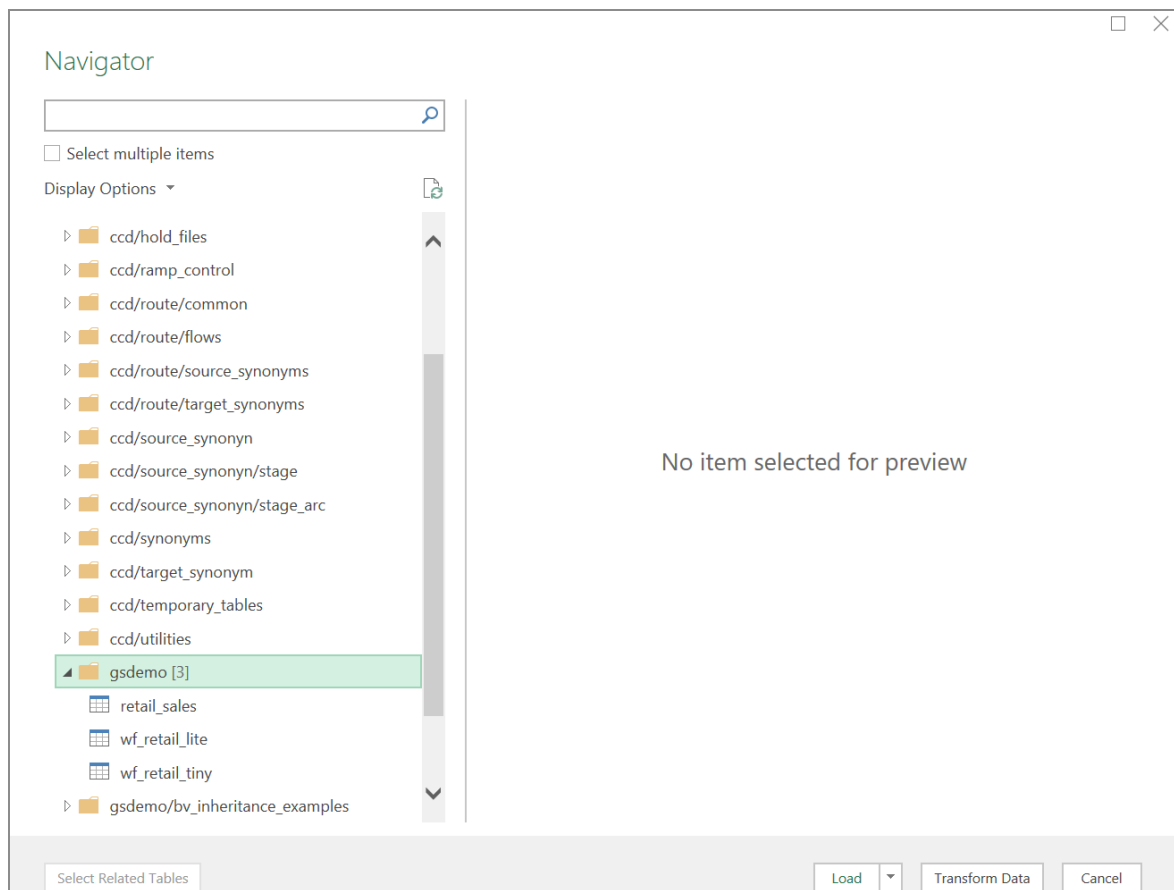
Cluster connection ☐ Cluster Name (optional):

Global

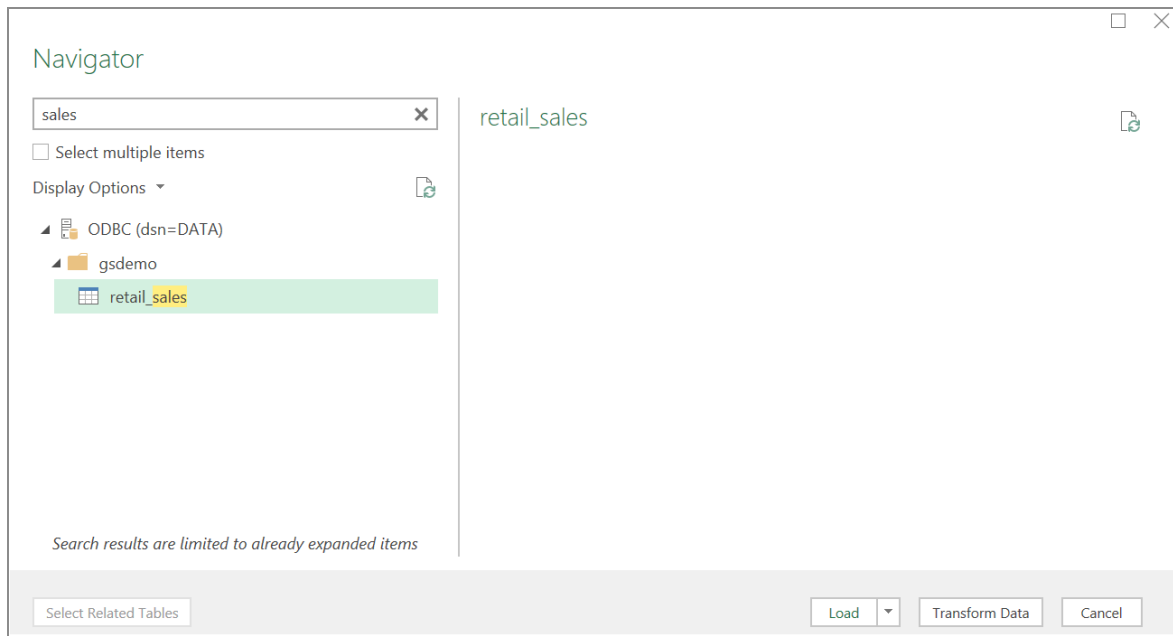
Enable tracing ☒

Advanced << OK Cancel

6. Select the application directory name, as shown in the following image.

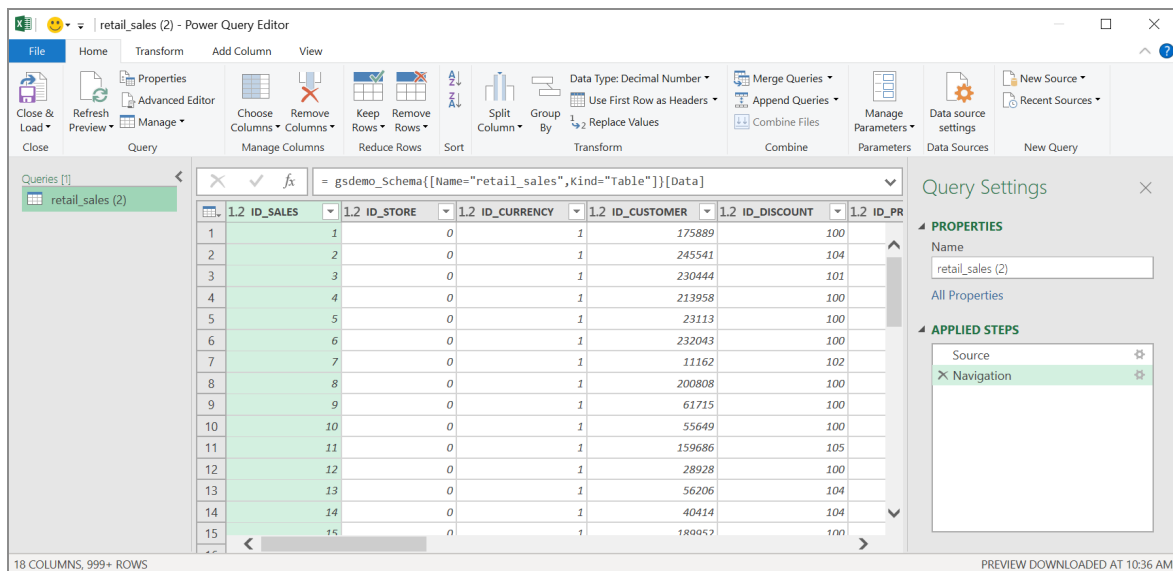


You can also search for a data source name, as shown in the following image.



7. Double-click the data source to load the data or click **Transform Data** to edit the data before loading.

If you click **Transform Data**, the Power Query Editor opens, as shown in the following image.



8. Using the Excel Queries and Connections option, you can create a query against the data.

Open Data Hub for Mainframe ODBC Connector from Microsoft Power BI

The following procedures describe how to use the Open Data Hub for Mainframe ODBC Connector from Microsoft Power BI and create a visualization.

Microsoft Power BI supports two methods of data access:

- Import of data from underlying data sources into a cache.

With the import method, data is never current and must be re-retrieved prior to use. For ODBC data sources, this cache can become large as all data is brought down to the cache. Once cached, performance can be good as this data is not re-retrieved for the session.

For information on using the ODBC Connector from Microsoft Power BI Import to create a visualization, see [Use the ODBC Connector from Microsoft Power BI Import](#).

- Direct Query, which queries the underlying data source each time a dashboard or report is loaded or changes definitions in the tool.

With the Direct Query method, data is much more current, but performance may be an issue if the underlying data source does not perform.

For information on using the ODBC Connector from Microsoft Power BI Direct Query to create a visualization, see [Use the ODBC Connector from Microsoft Power BI Direct Query](#).

Use the ODBC Connector from Microsoft Power BI Import

The following procedure describes how to use the ODBC Connector from Microsoft Power BI Import and create a visualization.

Note: The following instructions are included as a guideline. Your system and the necessary steps might vary. Refer to your development tool documentation and perform thorough testing of your system after establishing the connection between the ODBC Connector and Power BI Import.

Procedure

1. Open Microsoft Power BI.

2. Select **Get data**.

The Get Data dialog box opens.

3. Select **Other** and then select **ODBC**.

4. Click **Connect**.

The ODBC driver dialog box opens.

5. Type your user name and password and click **Connect**.

The Application Directory Navigator dialog box opens.

Note: Power BI caches your user ID and password. After the first time you enter your credentials, you will not be prompted again.

6. Select the application directory name and table or tables.

7. Click **Load**.

8. Create a visualization with Power BI.

Use the ODBC Connector from Microsoft Power BI Direct Query

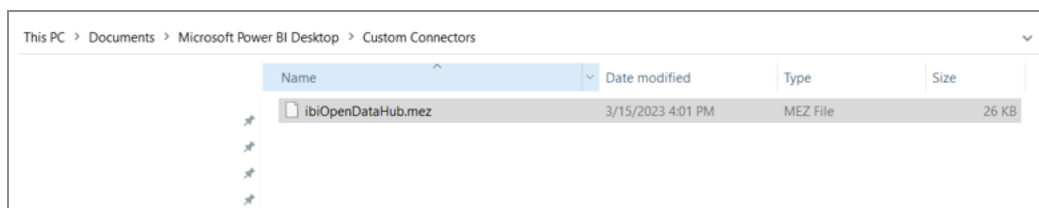
Open Data Hub for Mainframe contains a plugin to allow Power BI to retrieve data using the Direct Query method against mainframe data sources. This capability is available by creating a custom connector .mez for the Open Data Hub for Mainframe.

Note: The following instructions are included as a guideline. Your system and the necessary steps might vary. Refer to your development tool documentation and perform thorough testing of your system after establishing the connection between the ODBC Connector and Power BI Direct Query.

Procedure

1. Copy the .mez file to the following location, where Power BI Desktop is installed:
Documents\Microsoft Power BI Desktop\Custom Connectors

For example:



Note: If this directory does not exist, you can manually create it and restart Power BI. You will then be ready to use Open Data Hub for Mainframe in Direct Query Mode.

2. Make sure you have added the Open Data Hub for Mainframe connection to the ODBC settings on your desktop.
3. To access mainframe data using Open Data Hub in Direct Query Mode, open Power BI Desktop.
4. Click **Get data**.
5. From the list of Data Sources, select **Databasee**.
6. Select **ibi Open Data Hub (Beta)** and click **Connect**.

7. On the Welcome screen, supply the name of the ODBC-defined Open Data Hub for Mainframe connection (for example, DATA) and select the **DirectQuery** radio button.
8. Click **OK**.
9. From the Navigator Panel, you will see the listing of APP directories from the ibi mainframe WebFOCUS Reporting Server. Select the data source you wish to use in Direct Query Mode.
10. Select the check box next to the file and click **Load**.

Upon load, no data is imported into the Power BI store. Instead, when you build a visualization, Power BI Desktop sends queries to the underlying data source to retrieve the necessary data. The time it takes to refresh the visual depends on the performance of the underlying data source.

Open Data Hub for Mainframe ODBC Connector from Tableau

The following procedure describes how to use the ODBC Connector from Tableau and create a visualization.

Note: The following instructions are included as a guideline. Your system and the necessary steps might vary. Refer to your development tool documentation and perform thorough testing of your system after establishing the connection between the ODBC Connector and Tableau.

Use the ODBC Connector from Tableau

Procedure

1. Start **Tableau Desktop**.
2. Under **Connect To a Server**, select **More**, and then select **Other Databases (ODBC)**.
3. Select the Data Source Name and click **Sign In**.
The iWay ODBC dialog box opens.
4. Type your User ID and password, and click **OK**.
5. On the Connections screen, select **EDADB** for Database (it is your only choice).
6. Type a schema name or % to see all the schemas.
7. Type a full table name, or a partial table name.
8. Select a table from the list and drag it to the work area to start.
9. Create a visualization using Tableau Desktop.

Using ODBC Escape Clauses

Use the ODBC Escape Clause to run remote procedures. ODBC uses similar escape clauses to define various extensions to ANSI standard SQL.

Using ODBC Escape Clauses to Run Remote Procedures

```
--(*vendor(Microsoft),product(ODBC) call proc_name[(parm1,parm2...)]*)--
```

where:

proc_name

Specifies the name of the procedure stored on the server.

parm1,parm2...

Specifies the name of one or more optional parameters.

Invoking Remote Procedures Using Shorthand Syntax

```
{call proc_name[(parm1,parm2...)]}
```

The Connector driver supports the shorthand syntax.

Note: Some ODBC applications use their own syntax for calling remote procedures. These applications also convert the syntax into the ODBC Escape Clause syntax internally.

Using ODBC Escape Clauses for Dates, Times, and Timestamps

```
{d 'date_value'}  
{t 'time_value'}  
{ts 'timestamp_value'}
```

The Connector modifies the ODBC syntax to match the appropriate ANSI SQL form. For example, the Connector changes the ODBC escape clause {d 'date_value'} to the ANSI SQL equivalent 'date_value'. The date value is not modified and must be entered in the appropriate form from the ODBC application.

Issuing Your Own SQL Statement

You can issue your own SQL statement if the Advanced Options feature is available in the third-party product you are using. You can click *Advanced Options* and then use the data source in an SQL statement.

For example, in Excel, click **Advanced Options**, as shown in the following image.



Type the SQL statement in the SQL statement input box.

×

From ODBC

Data source name (DSN)

DATA ▾

▲Advanced options

Connection string (non-credential properties) (optional) ⓘ

Example: Driv...

SQL statement (optional)

Supported row reduction clauses (optional)

(None) ▾

Detect

OK

Cancel

Open Data Hub for Mainframe JDBC Connector

The Open Data Hub for Mainframe JDBC Connector provides access to a server. It receives incoming JDBC calls (requests) from a JDBC application and converts the calls into the appropriate API commands. The SQL statement is sent to the server in the form passed from the application.

Using the Open Data Hub for Mainframe JDBC Connector

The Open Data Hub for Mainframe JDBC Connector consists of a single self-contained .jar file named *jlink_standalone.jar*.

When the setup_odbc_client.exe file is executed, by default, the *jlink_standalone.jar* file is included in the C:\ibi\odh_client9x\home\etc\java\svr folder.

Use the Open Data Hub for Mainframe JDBC Connector With sqlline

You can test the Open Data Hub for Mainframe JDBC Connector using the open source program sqlline.

Procedure

1. Download the sqlline-1.12.0-jar-with-dependencies.jar file from the following website:
<https://search.maven.org/search?q=sqlline>
2. Extract the two .jar files to the same directory.
 - jlink-standalone.jar
 - sqlline-1.12.0-jar-with-dependencies.jar
3. For Windows, create a batch file called **sqlline**, with the following code:

```
java -cp "%~dp0\*" sqlline.SqlLine %* --color=true
```

Connect to a Server Using a URL

The Connector uses a standard JDBC URL to locate a server. You can include all the necessary information to connect to a server in a URL, using the following syntax:

```
sqlline> ! connect  
jdbc:jlink://host:port;keyword1=value1;keyword2=value2
```

For example:

```
sqlline> ! connect jdbc:jlink://MVS123:8120;user=sysadmin;pswd=sysadmin
```

where:

jdbc:jlink

Identifies the interface you are using. This indicates that the Connector should be loaded.

host

Is the IP address or Domain Name Service (DNS) of the server.

port

Is the TCP/IP port number on which the server listens.

keywords

You can pass all the required communications properties in the URL. Properties are specified as *keyword=value* pairs and must be separated by a semicolon (;). Possible values are:

user or userid

Is the user identification for access to the server.

password or pswd

Is the user password for access to the server.

trace

Identifies the active trace level. A trace setting can be any combination of the numbers 1, 2, 3, and 4. You can use one or more of the trace levels for tracing and debugging applications. The following table provides detailed information about each trace level. The numbers for each trace level represent the numbers as they appear on the trace.

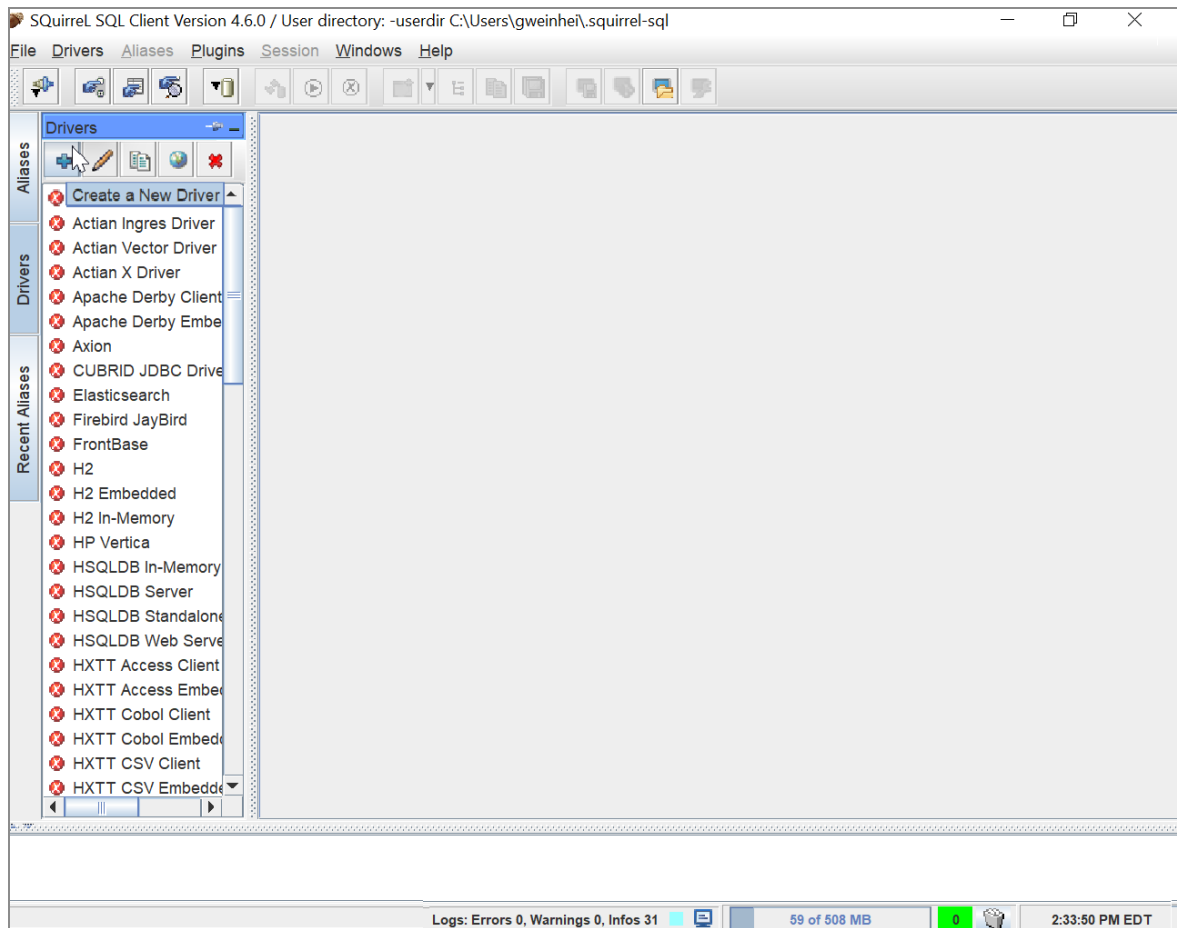
Level	Description
1	Displays each entry and exit to and from a Connector function, along with the parameter values processed.
2	Displays data transmission and internal logic. Key decisions made in JLINK are traced.
3	Displays internal logic. Input and output are traced.
4	Displays internal debugging information.

Use the Open Data Hub for Mainframe JDBC Connector With Squirrel SQL

You can use the Open Data Hub for Mainframe JDBC Connector with the Squirrel SQL Client open source program on Windows and other platforms.

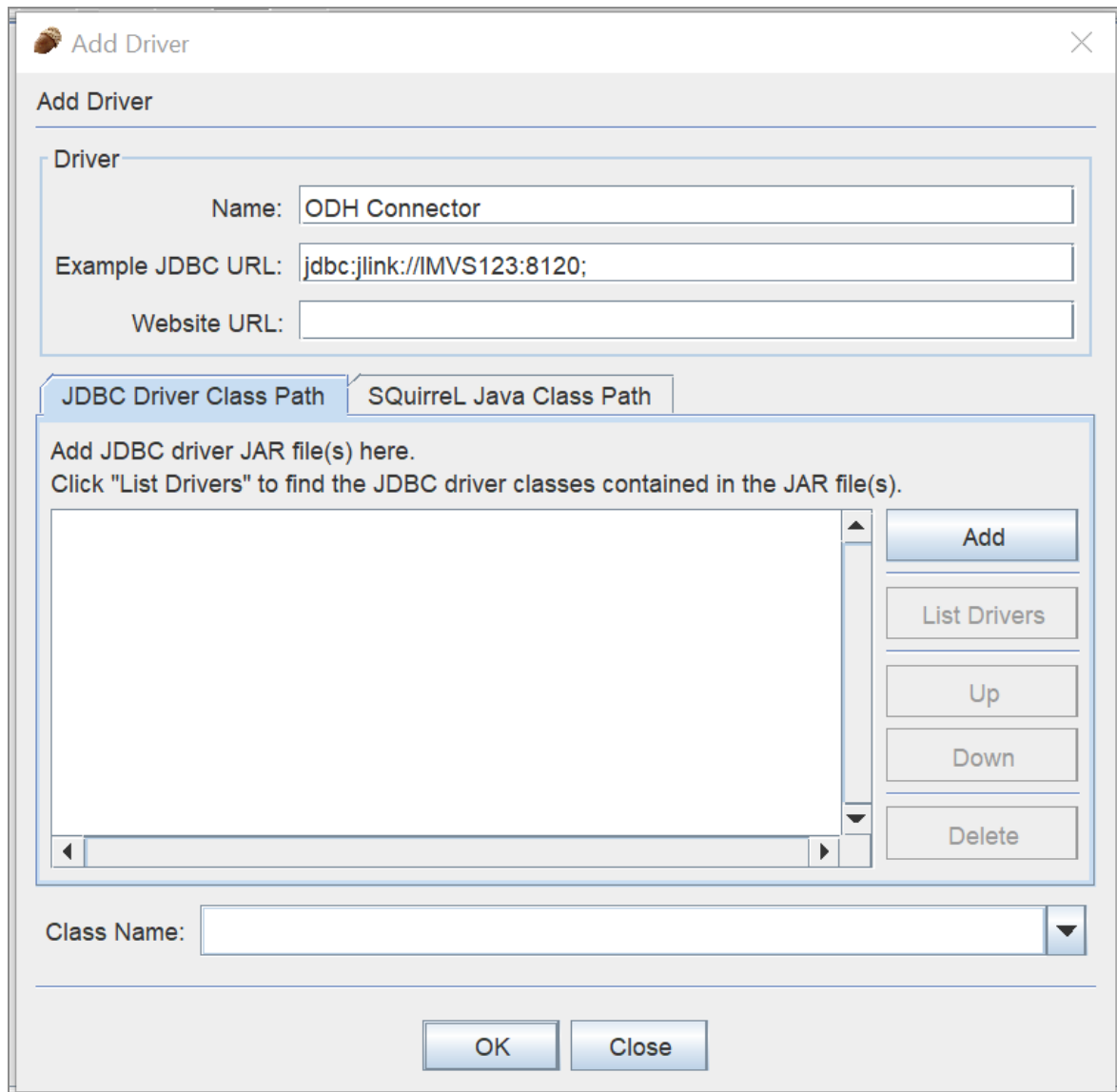
Procedure

1. Download the Squirrel SQL Client from the following website and follow the installation instructions:
<http://www.squirrelsql.org/#installation>
2. Open the Squirrel SQL Client.
3. Click the **Drivers** tab, and then click the plus (+) button to add a new driver, as shown in the following image.

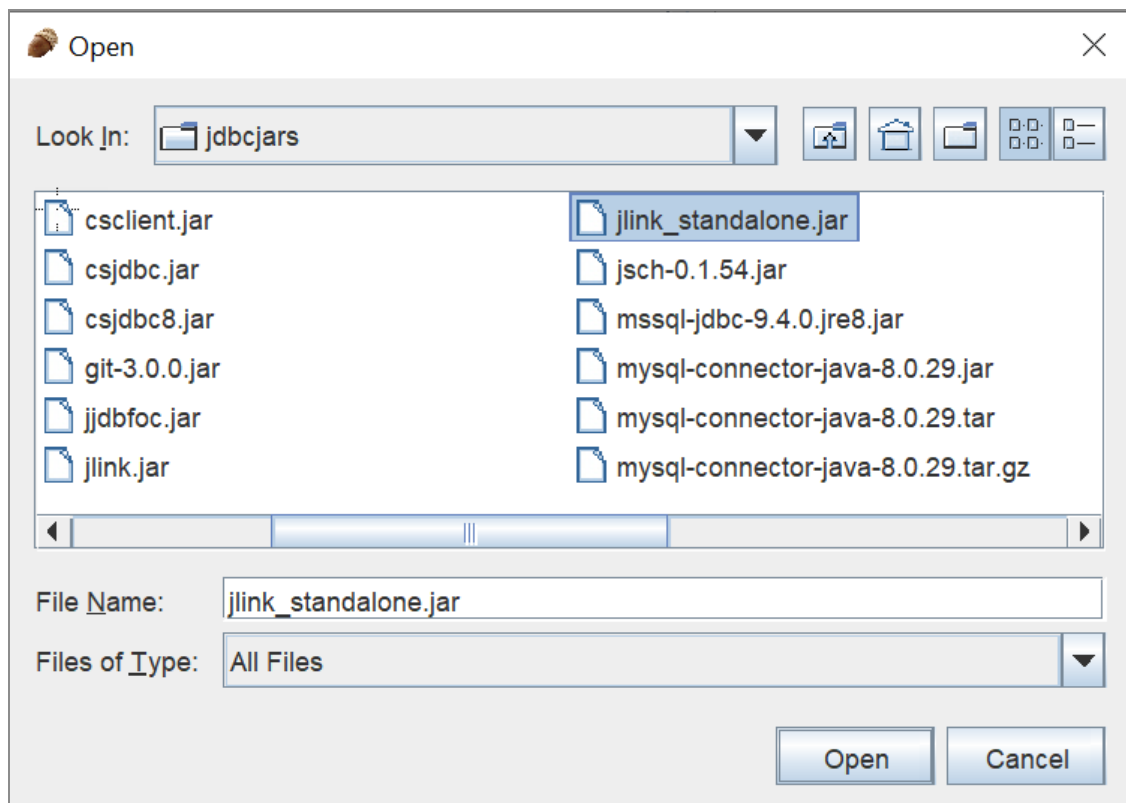


The Add Driver dialog box opens.

4. In the Name field, type a name for the driver, for example, *ODH Connector*, and in the Example JDBC URL field, type the URL for your server, for example, *jdbc:link://MVS123:8120;*, as shown in the following image.

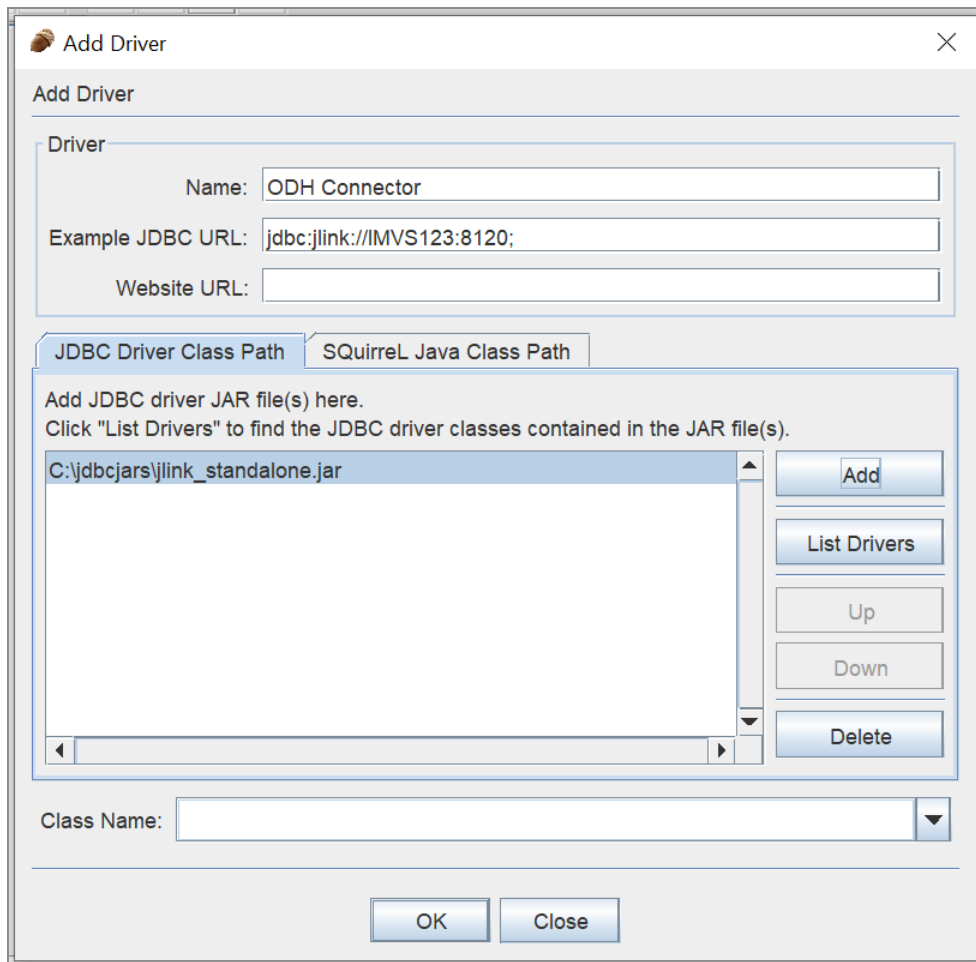


5. Click the *Squirrel Java Class Path* tab and then click *Add*.
6. Select the `jlink_standalone.jar` file that you downloaded, as shown in the following image.



7. Click **Open**.

The jlink_standalone.jar file is successfully added, as shown in the following image.



8. Click **List Drivers**.

The `ibi.jdbc.EdaDriver` class name will be populated in the Class Name field.

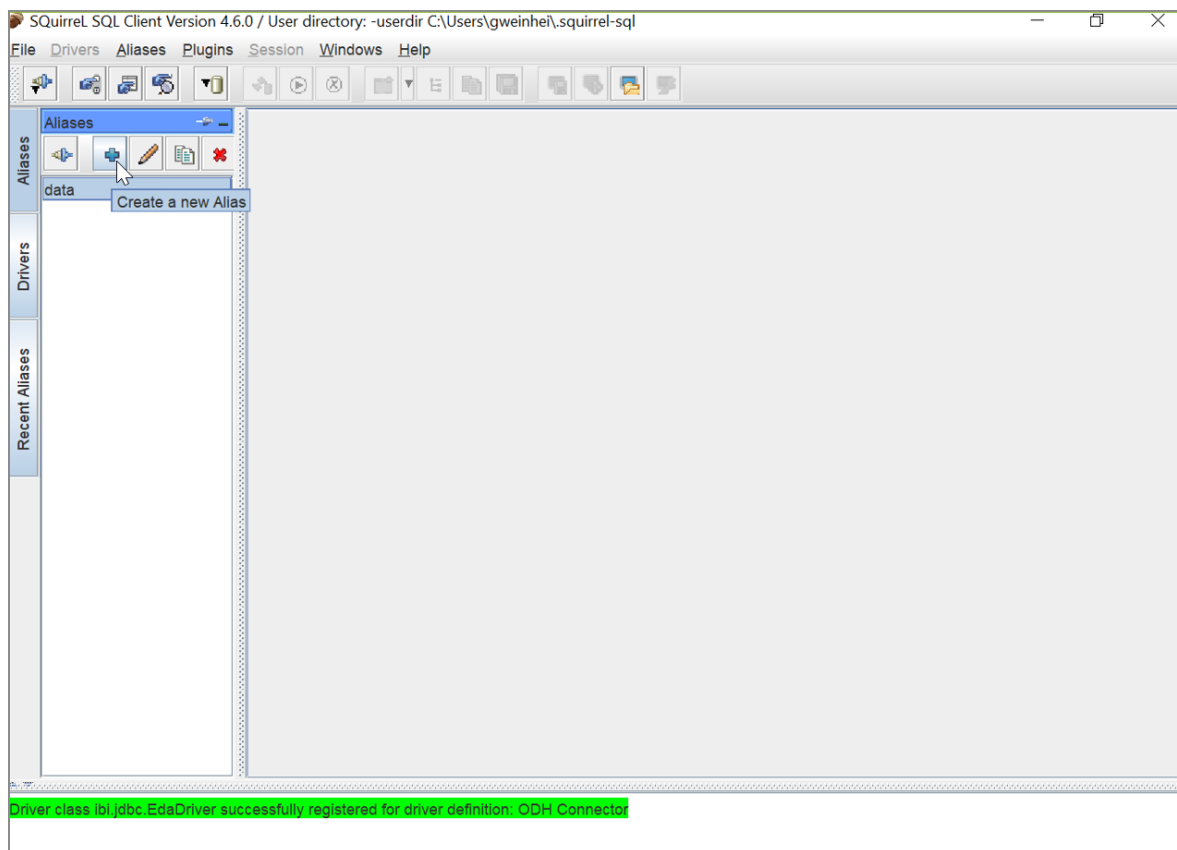
9. Click **OK**.

Create an Alias

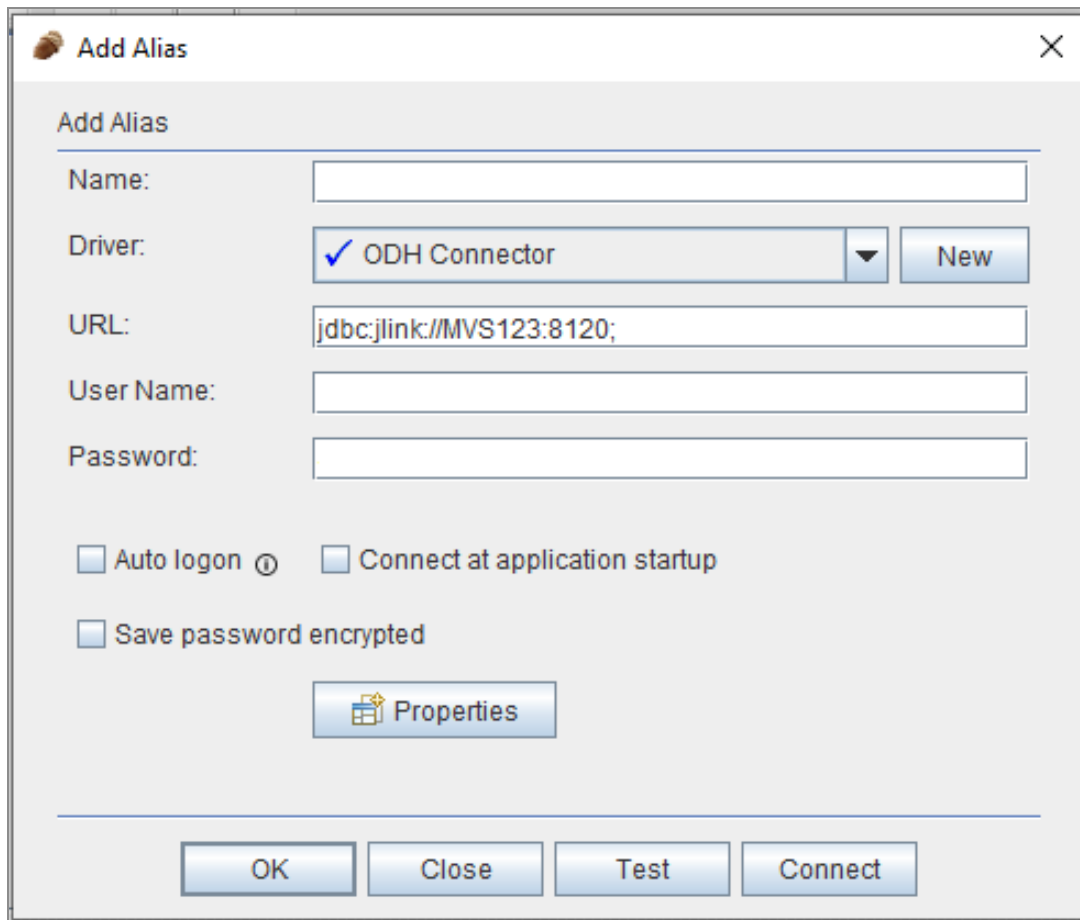
Procedure

1. Click the **Aliases** tab, and then click the plus (+) button to add a new alias, as shown in the following image.

Note: An Alias is what Squirrel calls a connection to a server.



The Add Alias dialog box opens, as shown in the following image.



The image shows a Windows-style dialog box titled "Add Alias". It contains several input fields and checkboxes. The "Name:" field is empty. The "Driver:" dropdown menu is set to "ODH Connector" with a checkmark, and there is a "New" button next to it. The "URL:" field contains the text "jdbc:jlink://MVS123:8120;". The "User Name:" and "Password:" fields are empty. There are three checkboxes: "Auto login" (with a help icon), "Connect at application startup", and "Save password encrypted", all of which are currently unchecked. Below the checkboxes is a "Properties" button with a small icon. At the bottom of the dialog are four buttons: "OK", "Close", "Test", and "Connect".

Add Alias

Name:

Driver: ✓ ODH Connector New

URL:

User Name:

Password:

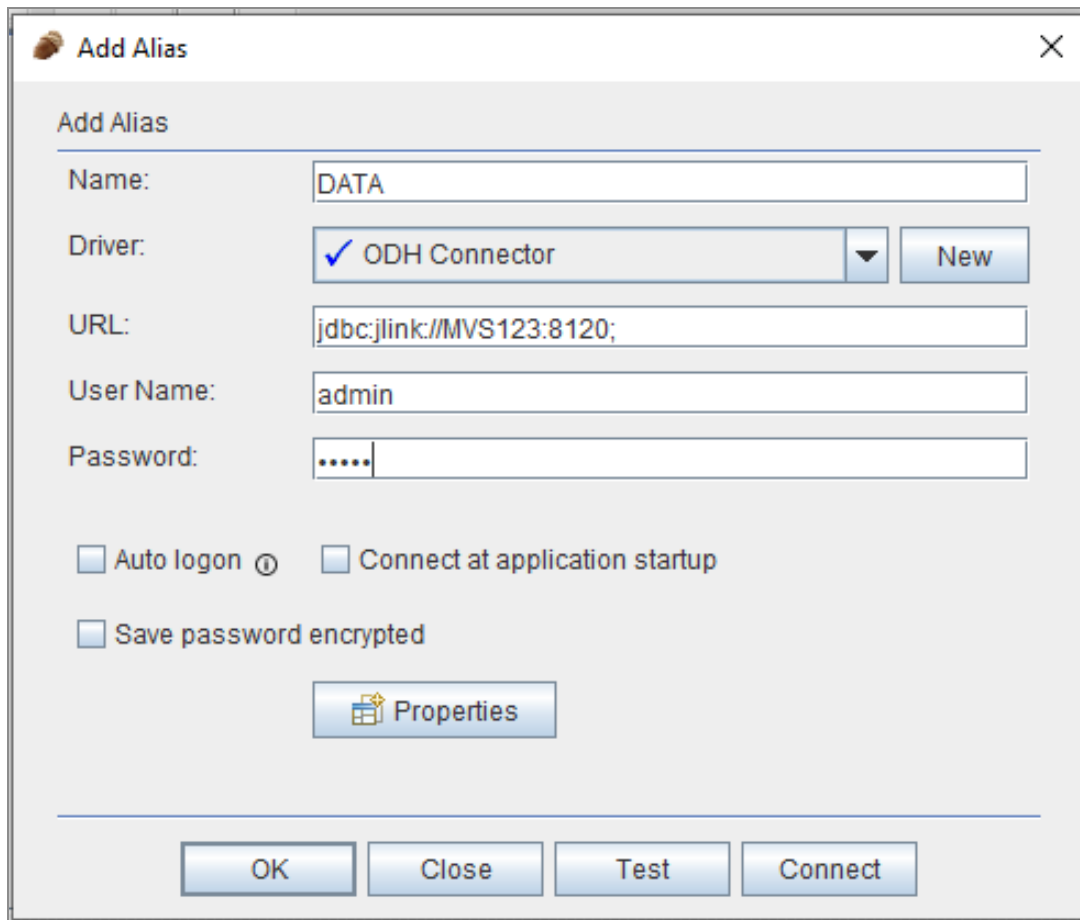
☐ Auto login ⓘ ☐ Connect at application startup

☐ Save password encrypted

Properties

OK Close Test Connect

2. In the Name field, type a name for the alias, for Driver, select **ODH Connector**, and for URL, type the connection information for your server, as shown in the following image.



The image shows a Windows-style dialog box titled "Add Alias". It contains several input fields and checkboxes. The "Name" field is filled with "DATA". The "Driver" dropdown menu is set to "ODH Connector" with a checkmark, and there is a "New" button next to it. The "URL" field contains "jdbc:jlink://MVS123:8120;". The "User Name" field contains "admin". The "Password" field has five dots. Below these fields are three checkboxes: "Auto login" (with a help icon), "Connect at application startup", and "Save password encrypted". A "Properties" button with a gear icon is located below the checkboxes. At the bottom of the dialog are four buttons: "OK", "Close", "Test", and "Connect".

Add Alias

Name: DATA

Driver: ✓ ODH Connector New

URL: jdbc:jlink://MVS123:8120;

User Name: admin

Password:

☐ Auto login ⓘ ☐ Connect at application startup

☐ Save password encrypted

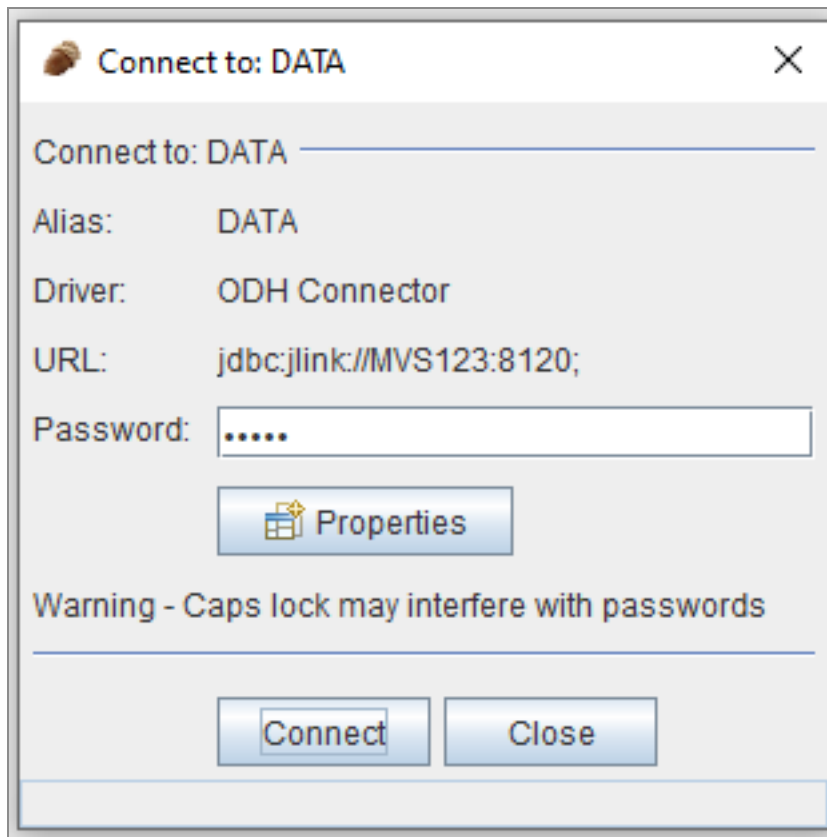
Properties

OK Close Test Connect

3. Click **Test**.

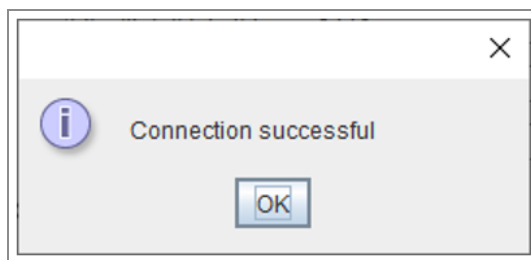
The Connect to data dialog box opens, as shown in the following image.

Note: If you did not enter a password on the previous Add Alias dialog box, type a password on the Connect to data dialog box, as shown in the following image.

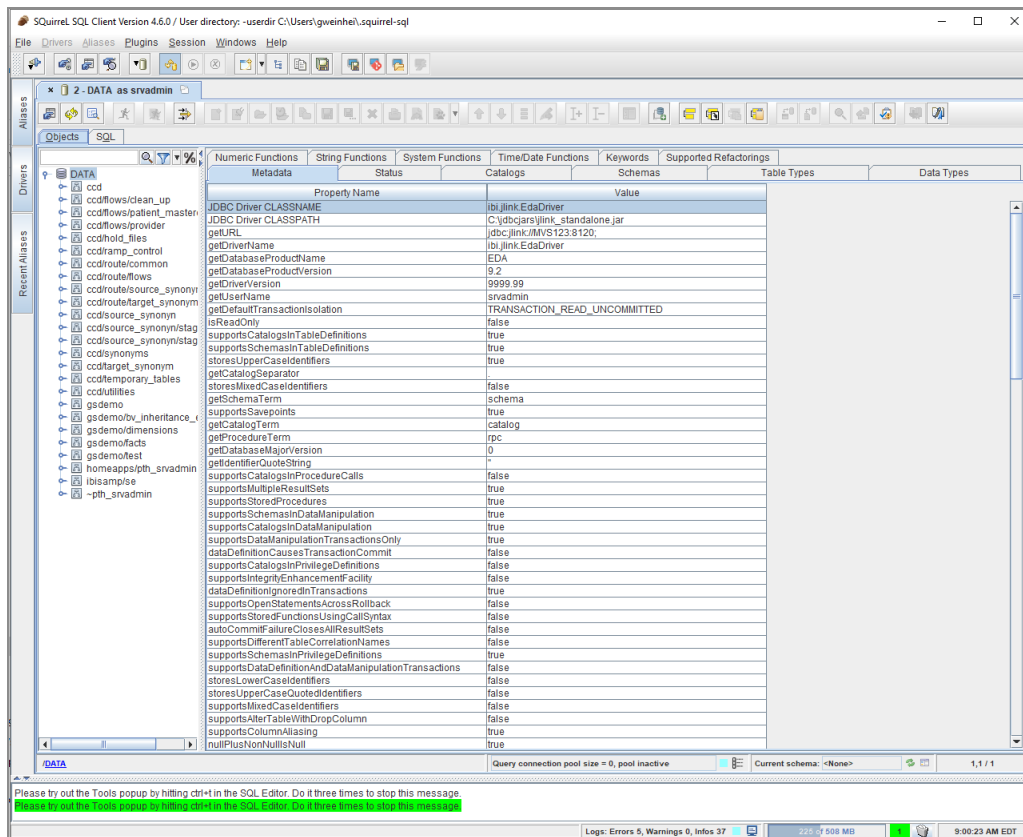


4. Click **Connect**.

You should see a Connection successful message, as shown in the following image.



5. Click **OK** and then click **Close**.
6. You can now click **Connect** to connect to your configured server. The first screen shows the properties of the JDBC Connection, as shown in the following image.



7. Click the **SQL** tab.

You can now type a select statement for a table on your server. Click the running man to run the select statement and view the results, as shown in the following image.

The screenshot shows the Squirrel SQL Client Version 4.6.0. The main window displays a query result for the query: `select FULLNAME, sum(REVENUE_US), sum(COGS_US) as cost from retail_sale group by FULLNAME order by FULLNAME`. The result is limited to 100 rows. The table has three columns: FULLNAME, REVENUE_US, and COST. The data is as follows:

FULLNAME	REVENUE_US	COST
A'dab Totah	438.44	296.0
A'idah Touma	3984.6400000000003	2924.0
A'ishah Assaf	1439.44	1015.0
A'ishah Touma	6657.749999999999	5102.0
aAl Truong	13893.779999999999	9762.0
Aaliyah Adams	4739.799999999999	3727.0
Aaliyah Alhtar	13097.519999999993	9140.0
Aaliyah Bird	6085.99	4306.0
Aaliyah Brookes	6992.339999999997	4931.0
Aaliyah Butcher	10410.759999999998	7781.0
Aaliyah Coles	3079.01	1923.0
Aaliyah Connor	2428.45	1561.0
Aaliyah Dennis	9609.449999999997	6576.0
Aaliyah Dunn	789.97	513.0

The status bar at the bottom indicates: Query 1 of 1. Rows read: 100. Elapsed time (seconds): Total: 4.431. SQL query: 0.901. Reading results: 4.431.

ibi Documentation and Support Services

For information about this product, you can read the documentation, contact Support, and join Community.

How to Access ibi Documentation

Documentation for ibi products is available on the [Product Documentation website](#), mainly in HTML and PDF formats.

The [Product Documentation website](#) is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

The documentation for this product is available on the [ibi™ Open Data Hub for Mainframe Connectors Documentation](#) page.

How to Contact Support for ibi Products

You can contact the Support team in the following ways:

- To access the Support Knowledge Base and getting personalized content about products you are interested in, visit our [product Support website](#).
- To create a Support case, you must have a valid maintenance or support contract with a Cloud Software Group entity. You also need a username and password to log in to the [product Support website](#). If you do not have a username, you can request one by clicking **Register** on the website.

How to Join ibi Community

ibi Community is the official channel for ibi customers, partners, and employee subject matter experts to share and access their collective experience. ibi Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from ibi products. For a free registration, go to [ibi Community](#).

Legal and Third-Party Notices

SOME CLOUD SOFTWARE GROUP, INC. (“CLOUD SG”) SOFTWARE AND CLOUD SERVICES EMBED, BUNDLE, OR OTHERWISE INCLUDE OTHER SOFTWARE, INCLUDING OTHER CLOUD SG SOFTWARE (COLLECTIVELY, “INCLUDED SOFTWARE”). USE OF INCLUDED SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED CLOUD SG SOFTWARE AND/OR CLOUD SERVICES. THE INCLUDED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER CLOUD SG SOFTWARE AND/OR CLOUD SERVICES OR FOR ANY OTHER PURPOSE.

USE OF CLOUD SG SOFTWARE AND CLOUD SERVICES IS SUBJECT TO THE TERMS AND CONDITIONS OF AN AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER AGREEMENT WHICH IS DISPLAYED WHEN ACCESSING, DOWNLOADING, OR INSTALLING THE SOFTWARE OR CLOUD SERVICES (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH LICENSE AGREEMENT OR CLICKWRAP END USER AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE SAME TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc.

ibi, the ibi logo, iWay, Omni-Gen, FOCUS, and TIBCO are either registered trademarks or trademarks of Cloud Software Group, Inc. in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only. You acknowledge that all rights to these third party marks are the exclusive property of their respective owners. Please refer to Cloud SG’s Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

Cloud SG software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the “readme” file for the availability of a specific version of Cloud SG software on a specific operating system platform.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. CLOUD SG MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S), THE PROGRAM(S), AND/OR THE SERVICES DESCRIBED IN THIS DOCUMENT AT ANY TIME WITHOUT NOTICE.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "README" FILES.

This and other products of Cloud SG may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>.

Copyright © 2021-2024. Cloud Software Group, Inc. All Rights Reserved.