WebFOCUS
Server Administration
DataMigrator Server Release 7 Version 7.06
WebFOCUS Reporting Server Release 8.1M
Contents

Preface .................................................................................................................................11
  Documentation Conventions..........................................................................................12
  Related Publications.......................................................................................................13
  Customer Support..........................................................................................................13
  Information You Should Have.......................................................................................14
  User Feedback................................................................................................................15
  iWay Software Training and Professional Services......................................................15

1. Server Introduction .................................................................................................17
  Using the Web Console....................................................................................................18
    Web Console Ribbon......................................................................................................20
  Console Options...............................................................................................................20
    My Console Options.....................................................................................................26
  Other Icon Options.........................................................................................................28
  Configuration Overview..................................................................................................29
  Running and Configuring the FOCUS Database and FOCUS Database Server...........30
  Server Profiles...............................................................................................................33
    Profile Level................................................................................................................33
    Profile Commands......................................................................................................37
    Profile Command Formats..........................................................................................38

2. Server Security ........................................................................................................41
  Server Security Overview...............................................................................................41
    Authentication...............................................................................................................42
    Security Providers.......................................................................................................43
    Privileges and Other Authorizations.........................................................................45
    Encryption....................................................................................................................48
  Configuring Authentication............................................................................................49
    Configuring a New Security Provider.........................................................................50
    Configuring OPSYS Authentication..........................................................................53
Configuring PTH Authentication..................................................................................59
Configuring DBMS Authentication...........................................................................66
Configuring LDAP Authentication..............................................................................70
Configuring Custom Authentication..........................................................................81
Authenticating Users Across Multiple Security Providers.........................................89
Enabling Trusted Connections....................................................................................90
Identifying a Default Provider for Trusted Groups....................................................91
Setting an Anonymous User ID................................................................................92
Configuring User Password Settings.........................................................................92
Configuring Privileges and Other Authorizations.......................................................95
Configuring DBMS Authorization.............................................................................97
Configuring Server DBA Security.............................................................................97
Calculating Privileges for Any Registered or Unregistered User or Group................97
Permissions for Server Application Files and Directories Using a Non-OPSYS Security Provider...........................................................................................................99
File Permissions for an OPSYS Security Provider....................................................108
Configuring General Server and Web Console Actions............................................110
Configuring Groups..................................................................................................121
Configuring Roles....................................................................................................123
Registering Users and Groups in a Role.....................................................................128
Configuring Server Encryption................................................................................139
Encrypting Passwords Stored in Configuration Files................................................139
User-Defined Password Encryption and Decryption...............................................140
Encrypting Data at Rest...........................................................................................141
Configuring Secure Socket Layer (SSL) Encryption for the TCP/HTTP Listener........143
Configuring Data Encryption for a Remote Server....................................................144
Encoding HTML Tags in Data..................................................................................146
Access to Connection Information in WebFOCUS Procedures....................................146
Configuring the Server for Multi-Tenant Deployment..............................................147
Configuring Multi-Tenant Application Folders.........................................................147
Configuring Multi-Tenant Groups and Users............................................................148
Configuring Multi-Tenant DBMS Connections..........................................................148
Configuring Security Providers for Multi-Tenant Deployment...................................148
Naming Conventions for Multi-Tenant Deployment...................................................148
3. Managing Applications

What Is an Application?

Generating Samples and Tutorials

Procedures and Metadata on the Application Tree

Managing Applications and Paths

Creating and Mapping Applications

Using an SQL Database to Store Application Contents

Nested Application Directories

Home Application Directories for Users

Configuring the Application Path

Filtering the Application Tree

Searching for Files

Sorting the Application Tree

Managing Application Files

Application Commands Overview

Search Path Management Commands

APP PATH

APP PREPENDPATH

APP APPENDPATH

APP MAP

APP SET METALOCATIONSAME

APP ? METALOCATIONSAME

APP SHOWPATH

Application and File Management Commands

APP CREATE

APP COPY

APP COPYFILE

APP MOVE

APP MOVEFILE
APP DELETE ..........................................................................................................236
APP DELETF[ILE] ..................................................................................................237
APP PROPERTY CODEPAGE ..................................................................................238
APP RENAME .........................................................................................................238
APP RENAMEF[ILE] .................................................................................................239

Designating File Types for APP Commands ..............................................................240

Output Redirection Commands .............................................................................244
APP HOLD .............................................................................................................246
APP HOLDDATA .....................................................................................................247
APP HOLDMETA .....................................................................................................247
APP FI[LEDEF] ........................................................................................................248

Application Metadata Commands and Catalog Metadata ...........................................248
Retrieving Basic Information ................................................................................249
Retrieving Extended Catalog Information ..................................................................254

Help Information: APP HELP ................................................................................257

Restricting the Use of APP Commands ....................................................................258

Accessing Metadata and Procedures .....................................................................260
Search Rules ........................................................................................................260
Creation Rules for Procedure Files ........................................................................261
Locating Master Files and Procedures ....................................................................261
Accessing Existing Data Files ................................................................................262
Creation Rules for Data Files ................................................................................262

Data Set Names .....................................................................................................264
Allocating Temporary Files ....................................................................................265
Temporary Space Usage and Location .....................................................................268
Temporary Disk Space Usage for Non-PDS Deployment ..........................................268

Application Tools ..................................................................................................271

EX Procedure and Amper Variables........................................................................271

4. Data Adapters .....................................................................................................277
Changing Common Adapter Settings ......................................................................278
Configuring an Adapter ..........................................................................................278
Changing the Adapter Configuration ......................................................................280
Configuring a Remote Server ................................................................................282
5. Metadata ........................................................................................................... 289
   Creating Synonyms .................................................................................................. 290
   Testing Synonyms .................................................................................................... 291
   Managing Synonyms ................................................................................................ 293
   Using the Wizards ..................................................................................................... 295
     SQL Wizard ........................................................................................................... 295
     Upload Wizard ...................................................................................................... 309

6. Stored Procedures ................................................................................................. 321
   Working With Stored Procedures ............................................................................ 322
   Creating a Stored Procedure ................................................................................... 322
   Sending Stored Procedure Report Output to Server-Side Printers ......................... 325
   Editing a Stored Procedure ..................................................................................... 325
   Running a Stored Procedure .................................................................................. 326
     Running a Stored Procedure ................................................................................ 326
     Running a Procedure With Different Variables .................................................. 327
     Prompting for Amper Variables in Procedures ..................................................... 328
   Scheduling a Procedure ........................................................................................... 329
   Sending an E-mail Notification for a Procedure ..................................................... 340
   Procedure Run-Time Processing Essentials ........................................................... 342
     Commands in a Stored Procedure ....................................................................... 342
     Dialogue Manager Commands and Processing .................................................. 343
     Using Variables ..................................................................................................... 348
     Supplying Values for Variables ............................................................................ 356
     Branching .............................................................................................................. 361
     Calling Another Procedure ................................................................................... 365
     Creating Expressions ............................................................................................ 366
     ON TABLE HOLD ............................................................................................... 373
     ON TABLE PCHOLD ............................................................................................ 374
### Contents

Platform-Specific Commands and Features.................................................................375
  DYNAM Command (z/OS PDS and HFS Deployments)........................................376
  Comparison of TSO Commands, JCL, and DYNAM............................................397
  FILEDEF Command Under UNIX, Windows, IBM i, z/OS, and OpenVMS............399
  Server Side OFFLINE Printing...........................................................................402
Stress Testing a Procedure.....................................................................................406
  Recording User Actions Into a Script Using Run Stress......................................407
  Running Impact Analysis Reports........................................................................411

#### 7. Server Workspace Manager........................................................................417
  Configuring Workspace Manager.......................................................................418
    Workspace Manager Configuration Privileges.................................................418
    Quiesce Server...............................................................................................419
    Configuring an Agent Service.........................................................................421
    Configuring Deployment Modes......................................................................426
    Multiple Cluster Manager Configurations......................................................428
  Workspace Configuration Settings.....................................................................428
    E-mail SMTP Server Settings.........................................................................429
    Event Routing.................................................................................................431
    National Language Support Settings..............................................................438
    Login Message................................................................................................449
    Web Console Appearance................................................................................453
    Profile Settings..............................................................................................454
    Core Engine Settings......................................................................................456
    Core System Variables....................................................................................458
    Core Engine Global Variables.........................................................................460
    Application Settings.......................................................................................462
    Miscellaneous Settings...................................................................................465
    License Settings.............................................................................................470
    Migrate Settings.............................................................................................472
  Editing Configuration Files................................................................................473
  Configuring Java Services..................................................................................474
  Fine-Tuning the Server.....................................................................................476
  Cluster Manager...............................................................................................479
Server Processes..........................................................................................................614
Server Work Space Manager Daemon.........................................................................614
Deferred Requests Special Services Daemon.............................................................614
Server Log Daemon....................................................................................................615
Server Check Up Daemon..........................................................................................615
HTTP Listener Daemon............................................................................................615
TCP Listener Daemon...............................................................................................615
FDS Special Services Daemon..................................................................................615
Java Services Daemon...............................................................................................615
Agent Daemons..........................................................................................................615
Gathering Diagnostic Information for Customer Support Services..........................616

A. Unicode Support....................................................................................................625
Unicode and the WebFOCUS Reporting Server..........................................................626
Accessing Unicode Data..............................................................................................628
Selecting, Reformatting, and Manipulating Characters..................................................635
Sort Order Under Unicode............................................................................................637
Added Unicode Support for Master Files, Data Files, and Application Directory Names.....638
Unicode PDF Output....................................................................................................638

B. Platform-Specific Methods for Specifying EDAEXTSEC......................................639
Platform-Specific Methods for Setting EDAEXTSEC..................................................640

Reader Comments......................................................................................................657
Preface

This documentation describes how to use the Web Console to configure, operate, monitor, tune, and troubleshoot the Server. It is intended for server administrators, database administrators, and application developers.

How This Manual Is Organized

This manual includes the following chapters:

<table>
<thead>
<tr>
<th>Chapter/Appendix</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Server Introduction</td>
<td>Describes how to use the console and provides an overview of server configuration.</td>
</tr>
<tr>
<td>2 Server Security</td>
<td>Describes security modes and their authentication process.</td>
</tr>
<tr>
<td>3 Managing Applications</td>
<td>Describes how to work with Application Files, how to control the APP environment, and how to use APP methods to simplify the process of moving a user application from one platform to another.</td>
</tr>
<tr>
<td>4 Data Adapters</td>
<td>Provides general information on configuring adapters and outlines configuration options.</td>
</tr>
<tr>
<td>5 Metadata</td>
<td>Discusses how to create a synonym using the Web Console.</td>
</tr>
<tr>
<td>6 Stored Procedures</td>
<td>Explains how using procedures enables application logic to be written once and executed many times, and how the Procedures page enables the creation and testing of stored procedures.</td>
</tr>
<tr>
<td>7 Server Workspace Manager</td>
<td>Describes how to run, monitor, and tune your server.</td>
</tr>
</tbody>
</table>
### Documentation Conventions

The following table describes the documentation conventions that are used in this manual:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>THIS TYPEFACE</strong></td>
<td>Denotes syntax that you must enter exactly as shown.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td><strong>this typeface</strong></td>
<td>Represents a placeholder (or variable) in syntax for a value that you or the system must supply.</td>
</tr>
<tr>
<td><strong>underscore</strong></td>
<td>Indicates a default setting.</td>
</tr>
<tr>
<td><strong>this typeface</strong></td>
<td>Represents a placeholder (or variable), a cross-reference, or an important term. It may also indicate a button, menu item, or dialog box option that you can click or select.</td>
</tr>
<tr>
<td>Key + Key</td>
<td>Indicates keys that you must press simultaneously.</td>
</tr>
<tr>
<td>{  }</td>
<td>Indicates two or three choices. Type one of them, not the braces.</td>
</tr>
<tr>
<td>[  ]</td>
<td>Indicates a group of optional parameters. None are required, but you may select one of them. Type only the parameter in the brackets, not the brackets.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>...</td>
<td>Indicates that you can enter a parameter multiple times. Type only the parameter, not the ellipsis (...).</td>
</tr>
<tr>
<td>.</td>
<td>Indicates that there are (or could be) intervening or additional commands.</td>
</tr>
</tbody>
</table>

### Related Publications

Visit our Technical Content Library at [http://documentation.informationbuilders.com](http://documentation.informationbuilders.com). You can also contact the Publications Order Department at (800) 969-4636.

### Customer Support

Do you have any questions about this product?

Join the Focal Point community. Focal Point is our online developer center and more than a message board. It is an interactive network of more than 3,000 developers from almost every profession and industry, collaborating on solutions and sharing tips and techniques. Access Focal Point at [http://forums.informationbuilders.com/eve/forums](http://forums.informationbuilders.com/eve/forums).

You can also access support services electronically, 24 hours a day, with InfoResponse Online. InfoResponse Online is accessible through our website, [http://www.informationbuilders.com](http://www.informationbuilders.com). It connects you to the tracking system and known-problem database at the Information Builders support center. Registered users can open, update, and view the status of cases in the tracking system and read descriptions of reported software issues. New users can register immediately for this service. The technical support section of [www.informationbuilders.com](http://www.informationbuilders.com) also provides usage techniques, diagnostic tips, and answers to frequently asked questions.

Call Information Builders Customer Support Services (CSS) at (800) 736-6130 or (212) 736-6130. Customer Support Consultants are available Monday through Friday between 8:00 a.m. and 8:00 p.m. EST to address all your questions. Information Builders consultants can also give you general guidance regarding product capabilities. Please be ready to provide your six-digit site code number (xxxx.xx) when you call.

To learn about the full range of available support services, ask your Information Builders representative about InfoResponse Online, or call (800) 969-INFO.
Information You Should Have

To help our consultants answer your questions most effectively, be ready to provide the following information when you call:

- Your six-digit site code (xxxx.xx).
- Your configuration:
  - The software version and release. You can find your server version and release using the Version option in the Web Console.
    
    **Note:** The MVS and VM servers do not use the Web Console.
  - The communications protocol (for example, TCP/IP or LU6.2), including vendor and release.
  - The stored procedure (preferably with line numbers) or SQL statements being used in server access.
  - The database server release level.
  - The database name and release level.
  - The Master File and Access File.
- The exact nature of the problem:
  - Are the results or the format incorrect? Are the text or calculations missing or misplaced?
  - Provide the error message and return code, if applicable.
  - Is this related to any other problem?
  - Has the procedure or query ever worked in its present form? Has it been changed recently? How often does the problem occur?
  - What release of the operating system are you using? Has it, your security system, communications protocol, or front-end software changed?
  - Is this problem reproducible? If so, how?
  - Have you tried to reproduce your problem in the simplest form possible? For example, if you are having problems joining two data sources, have you tried executing a query containing just the code to access the data source?
  - Do you have a trace file?
  - How is the problem affecting your business? Is it halting development or production? Do you just have questions about functionality or documentation?
User Feedback

In an effort to produce effective documentation, the Technical Content Management staff welcomes your opinions regarding this document. Please use the Reader Comments form at the end of this document to communicate your feedback to us or to suggest changes that will support improvements to our documentation. You can also contact us through our website, http://documentation.informationbuilders.com/connections.asp.

Thank you, in advance, for your comments.

iWay Software Training and Professional Services

Interested in training? Our Education Department offers a wide variety of training courses for iWay Software and other Information Builders products.

For information on course descriptions, locations, and dates, or to register for classes, visit our website (http://education.informationbuilders.com) or call (800) 969-INFO to speak to an Education Representative.

Interested in technical assistance for your implementation? Our Professional Services department provides expert design, systems architecture, implementation, and project management services for all your business integration projects. For information, visit our website (http://www.informationbuilders.com/support).
The Web Console enables you to configure, operate, monitor, tune, and troubleshoot the server environment from a single, easy-to-use interface.
Using the Web Console

The Web Console enables you to remotely view and manage the server environment. From a single, easy-to-use interface, you can:

- Select, add, and configure data adapters.
- Create and manage adapter metadata.
- Control data access and security.
- Configure remote servers.
- Configure, edit, and run applications and deferred query processing.
- Configure communications and special services.
- Operate, monitor, tune, and troubleshoot your server.
- Edit configuration files.
- Migrate from a previous server release.
- Control aspects of your own environment.

Procedure: How to Open the Web Console

To open the Web Console:

1. If the server is not running, start it using the instructions for your platform in the installation guide.

2. Type the following URL in the address space of the Web browser

   http://ip_address:http_service

   where:

   ip_address

   Is the IP address of the machine on which the server is running.
**http_service**

Is the value for HTTP Service entered during the server configuration procedure.

- If you have trouble contacting the server, see *Troubleshooting the Console* on page 613.

- If you are running your server with security, see *Security Providers* on page 43 for information on the requirements and options associated with the security mode you are using.

The Web Console home page opens, as shown in the following image. The menu bar provides access to the different features of the Web Console.

![Web Console Home Page](image)

3. Select an option from the menu bar to access the corresponding console page and ribbon. For tasks that display information or require no additional navigation, the console displays corresponding information in the right pane. For tasks that require additional task-centered navigation, the console opens a new ribbon or window. Use the navigation pane of the new window on the left to access the corresponding information in the right pane.

On Web Console navigation panes:

- Right-click behavior opens pop-up menus by default.

- Double-click behavior executes the first option on a pop-up menu.

The console offers online help with two kinds of links to appropriate sections of this documentation:

- Click *Help* on the menu bar and choose *Contents and Search* to display the full Web Console help system.

- Click the ? icon, when available, to display contextual help specific to the item.
Web Console Ribbon

Web Console functionality is available through a ribbon or through the menu at the top of the interface. The ribbon is the default, and it can be toggled on and off using the Show Ribbon and Hide Ribbon icons above the navigation pane.

The ribbon available from the Applications page is shown in the following image.

The interface includes the following areas:

- The Quick Access Toolbar, as shown in the following image.

- The Main Menu bar, as shown in the following image.

- The ribbon.

The ribbon provides the same options that are available from the right-click menus of the top nodes in the navigation pane.

Console Options

In this section:

My Console Options

If you click the Console icon, as shown in the following image, the following options are available:
**Login Info**

Displays user login status and browser-related information. Login status information includes user name, group, and role, location of all profiles (user, group, and role) if they exist, and type of authentication (explicit or cookie). HTTP information reflects the properties of the current browser session, for example, the cookie.

**Stop**

Stops the server.

**Restart**

Restarts the server.
**Quiesce**

Quiesces or stops the server from accepting new connections. A custom message can be displayed for new connections when the server is quiesced. For more information, see *How to Quiesce the Server and Set a Custom Message* on page 420.

**Enable Traces**

Enables traces to provide diagnostics assistance. For more information, see *Tracing Server Activity* on page 584.

**Savediag - Report a Bug**

Provides an option to gather, package, and ship trace files and other diagnostic information for Customer Support Services. For more information, see *Gathering Diagnostic Information for Customer Support Services* on page 616.

**Scalability**

Provides the ability to run stress tests on the server. For more information, see *Recording and Reproducing User Actions* on page 601.

**My Console**

Provides options to show your privileges, change your password, manage agents, save your last report, and edit your profile. For more information, see *My Console Options* on page 26.

**Preferences**

Enables you to indicate preferences for Run Options, Column Management, Synonym Editor, Dimension View Display, Web Console Appearance, and Reporting Options.
Run Options are **Default Data Service**, as shown in the following image. The choices are DEFAULT, WF_DEFAULT, SCHED_DEFAULT, and DFM_DEFAULT.

The Column Management section is shown in the following image.

The Column Management options are:

- **Column name display strategy**. The choices are Name, Title, Description, and Alias.

- **Use segment to qualify field reference**. The choices are For duplicate fields and always.
The Synonym Editor section is shown in the following image.

The Synonym Editor options are:

- **Use application directory name with synonym.**
- **Undo/Redo Limit.** The default is 50.
- **Support extended options.**
- **Default Join Type.** The choices are One-to-One and One-to-Many,

The Dimension View Display section is shown in the following image.

The Dimension View Display option is Show Easy View.

The Web Console Appearance section is shown in the following image.
The Web Console Appearance options are:

- **Show Web Console reports in the following location.** The choices are Right Frame, Same detached window, and Different detached window.

- **Appearance.** The choices are Adhere to server appearance default, RIA-CarbonRounded, RIA-Default, and RIA-OceanRounded.

- **Default page on User Login.** The choices are Applications, Adapters, Resource Management, Workspace, Access Control, and Scalability.

- **Menu or Ribbon.** The choices are Menu, Ribbon, and Adhere to server appearance default.

- **WebFocus 80 compatibility.** The choices are Yes, No, and Adhere to server appearance default.

The Browser Support section shows the appearance modes supported for each browser version.

The Reporting Options section is shown in the following image.

![Reporting Options](image)

The Reporting Options are:

- **Show Web Console reports in the following format.** The choices are HTML, Absolute Positioned HTML, Active Report, PDF, Excel, and Powerpoint.

- **Maximum number of rows for test reports.** The default is 50.

- **Maximum number of columns for test reports.** The default is 999,999.

  Indicate your preferences, and click **Update**.

The main menu bar also includes **Sign In As Different User.** When you click this console option, the dialog box shown in the following image is displayed. Supply the requested information, and click **Sign in**.
My Console Options

The My Console options are available from the Console icon. They provide users with functionality that supports the tasks they are authorized to perform. The options that a user has under My Console depend on the user role and general privileges assigned to the user.

In the descriptions that follow, each option applies to the user who is connected to the current Web Console session.

**Show My General Privileges.** Shows the privileges set by the Server Administrator for the user who is logged in to the current Web Console session. Privileges can be customized for each role, group, or user. See *General Privileges* on page 111, for details on the information supplied on the General Privileges pane.
**Change My Password.** Enables you to specify a new password to replace your current password. When you click this console option, the dialog box shown in the following image is displayed. Supply the requested information, and click *Update*.

![User Information](image)

**Note:** The LDAP security mode also allows you to change your password in the LDAP directory.

![User Information](image)
**Manage My Agents.** Enables you to monitor and manage Data Service Agents, based on your role and privileges. For example, if you are a Basic user, by default you can monitor and manage your own agents (that is, the agents that match your user ID). If granted the applicable privileges, you can also monitor, or monitor and manage, the agents of the other users in your group (that is, users with the same group ID).

When you click *Manage My Agents*, a Performance Report for Data Service Agents is displayed, showing statistics for the agents that you are authorized to see. You can customize and filter the report to display only those statistics that you are interested in.

To determine your privileges, click *Show General Privileges* from the Web Console menu bar. See *General Privileges* on page 111 for details on the information supplied on the General Privileges pane.

**Save My Last Report.** Saves the last report (procedure) that you ran with the values that you chose for the amper variables. The report is saved as a new, separate procedure. You can run the saved report without having to manually supply the values for the amper variables as you did before.

When you click this console option, you can select for the application directory in which to save the report and enter a file name for the report.

**Edit My Profile.** Enables you to make changes to your current user profile settings.

---

**Other Icon Options**

The other icons at the top-left of the console provide the following options:

**Stop My Requests**

Stops your current Web Session requests.

**Hide/Show Tree**

Toggles the display of the navigation pane.

**Show/Hide Session Log Window**

Toggles the display of the session log window.

**Show/Hide Ribbon**

Toggles the display of the ribbon, as shown in the following image.
Wizards

Launches the Wizard page where you can generate, run, email, and schedule reports using the SQL Wizard, Upload Wizard, or Quick Copy Wizard.

Configuration Overview

The characteristics of an individual server are determined by a set of configuration files. These configuration files define the protocols, services, and data sources supported by the server. In the UNIX, z/OS HFS Deployment (USS), Windows, OpenVMS, and IBM i (formerly known as i5/OS) environments, these files are maintained in directories designated by the environment variable EDACONF.

The initial installation procedure creates an installation instance, represented in manuals as the logical name EDAHOME, and one default configuration instance, known as EDACONF. After you successfully install the server, you can configure a default configuration instance to create an operational instance, or create an additional one at your site. An operational instance of the server is one that is configured to support specific protocols, services, and access to data sources.

You must run the Installation/Configuration Utility for each new instance of the server that you want to configure, and then use the Web Console to configure all necessary functionality.

To configure a server instance, use the Web Console to:

1. Select and configure data adapters.
2. Optionally, configure remote servers.
3. Configure communications nodes and protocols.
4. Optionally, set parameters for deferred query processing.

If necessary, you may edit configuration files. Some configuration errors can make the server start in a limited mode called safe mode, in which the Web Console is still operational, to enable you to correct the errors.
Running and Configuring the FOCUS Database and FOCUS Database Server

Example:

Using the Integrated FOCUS Database Server From a Global Server Profile (suprof.prf or edasprof.prf)

Using the Integrated FOCUS Database Server With a JCL Statement (z/OS Only)

Using the Integrated FOCUS Database Server From Other Profiles or in a Procedure (FOCEXEC)

Using the Legacy FOCUS Database Server (Separated Batch Job, z/OS Only)

The server supports its own internal database known as a FOCUS Database, and includes its own FOCUS Database Server, also called a Sink Machine, for multi-user use. Sites running z/OS have the option of using the integrated FOCUS Database Server or keeping their FOCUS files on a legacy FOCUS Database Server, which runs as a separate batch job.

In many simple cases, syntax, such as ON TABLE HOLD AS MYAPP/MYDATA FORMAT FOCUS, will generate all that is needed for proper initial creation internally. However, more precise creations require a USE statement. On z/OS, a DYNAM or a JCL DD is also required, and the USE syntax will vary if a legacy database server is in use.

The general syntax of the USE statement is:

```
USE
XXX [NEW]
ZZZ [ON server]
XXX01 AS XXX [ON server] READ
XXX02 AS XXX [ON server] READ
{path}AAA.foc AS AAA [ON server]
{path}BBB.foc AS BBB NEW
{app}/CCC AS CCC [ON server]
{app}/AAA AS AAA NEW
END
```

The AS phrase effectively allows you to access a file under an alternate name, with a different Master File or synonym, but it also allows you to concatenate the access of data partitioned as separate files. The AS phrase is also required syntax for path and app use. Syntax using full-path, native file names is only applicable to non-z/OS platforms (z/OS uses DYNAMs or DD names to point at specific datasets).

The NEW parameter indicates that the file is being specified for creation purposes (CREATE FILE). Creates may not be done on a database server. They must be done independent of the server and then placed under server access.
The ON phrase indicates the use of a database server. On z/OS, the choices for server names are FOCSU01 (server integrated) or FOCSBS (FOCUS legacy). All other platforms use the server name FOCSU01. The FOCSU01 node is a pre-configured and reserved name for the integrated FOCUS Database Server and may not be used for any other purposes. The server communication file (ODIN), can be configured to support additional FOCUS Database Server nodes and/or have additional nodes that point to the nodes of FOCUS Database servers configured under other servers.

When using an AS phrase in conjunction with an ON phrase for files where the physical name (not including path or extension) and the AS name do not match, the READ parameter is required to prevent an unintended opening for write.

**Important:** On z/OS, a single file cannot be accessed by both a legacy and an integrated FOCUS Database Server. You must select one or the other to manage access or you will encounter queue conflicts.

**Example:** Using the Integrated FOCUS Database Server From a Global Server Profile (suprof.prf or edasprof.prf)

Using the Web Console, edit either suprof.prf (preferred) or edasprof.prf (alternative). On z/OS, add DYNAM ALLOC allocations and USE statements. On other platforms, only add USE statements.

For example, use the following syntax to enable the FOCUS Database Server to control access to the CAR data source.

**On z/OS:**

```
DYNAM ALLOC FI CAR DA dsname SHR REU
USE
CAR ON FOCSU01
END
```

**On other platforms:**

```
USE
CAR ON FOCSU01
END
```

**Example:** Using the Integrated FOCUS Database Server With a JCL Statement (z/OS Only)

IRUNJCL JCL allocation

Add JCL statements for the FOCUS files to be managed, for example:

```
//CAR DD DISP=SHR, DSN=dsname
```
The following sample USE command enables the FOCUS Database Server to control access to the CAR data source:

```
USE
CAR ON FOCSU01
END
```

**Example:** Using the Integrated FOCUS Database Server From Other Profiles or in a Procedure (FOCEXEC)

The syntax is similar when used in a profile, but on z/OS, the DYNAM uses the PERM option and is equivalent to a JCL allocation using IRUNJCL JCL.

For example, use the following syntax to enable the FOCUS Database Server to control access to the CAR data source:

**On z/OS:**

```
DYNAM ALLOC FI CAR DA dsname SHR PERM
USE
CAR ON FOCSU01
END
```

**On other platforms:**

```
USE
CAR ON FOCSU01
END
```

**Example:** Using the Legacy FOCUS Database Server (Separated Batch Job, z/OS Only)

The following sample code identifies a legacy FOCUS Database Server using the odin.cfg node block FOCSBS:

```
USE
CAR ON FOCSBS
END
```

This sample node block resides in odin.cfg and can be constructed using the Web Console:

```
NODE=FOCSBS <==== USS server (odin.cfg file)
BEGIN
    SUBSYS = xyzw <==== optional parameter to specify IBI subsystem name
    (not needed if you are using the name IBIS)
    PROTOCOL=SBS
    CLASS=SUCLIENT
    PORT=X.Y.Z <====== communications dataset
END
```
Server Profiles

In this section:
Profile Level

A server or global profile, edasprof.prf, is created during installation. You can customize this profile which is applied to all users. Optionally, you can create separate profiles to customize the server environment for a role, a group of users or an individual user. You can also create service profiles, which specify settings for the server environment. For information, see Profile Settings on page 454. Profiles are executed in the following sequence: server, service, role, group, and user.

A profile can include almost any command that a client application can send to the server, however, profiles are used most frequently for application set up commands, such as SETs, search path set up, and DBMS connection information, which may vary by adapter.

- For information about the syntax for commands typically used in profiles, see Profile Settings on page 454.

- For a description of the profile commands that are available for a particular adapter, go to the Adapter Administration manual. In the adapter chapter, look for topics on customization and optimization.

- For information about the relationship between profiles and security modes, see Security Providers on page 43.

Two key aspects of profile customization are level and associated search order. The server processes all profiles found in the search order. If it finds duplicate settings or commands, the last setting or command processed will be active for the connection.

When you create a profile, take into account that the more processing performed by the profile, the more time it takes for an application to connect to the server. An exception is pooled deployment, where only one profile is processed when the server agent initially starts or is refreshed.

Profile Level

How to:
Create a User Profile

The server supports various levels of profiles to provide flexibility for designing and running production applications. The order in which the following profiles are listed correlates with the search order in which they are processed by the server when multiple profiles exist.
Global profile. The first level of profile, the global profile, is a startup file that is automatically created during installation and configuration of the server. It contains default environment settings required for the correct operation of the server.

The global profile remains in effect throughout a user session. You can modify the global profile default settings. You can also add any commands or code that all connected users require before application processing begins.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>edasprof.prf</td>
</tr>
<tr>
<td>Location</td>
<td>UNIX: $EDACONF/etc directory</td>
</tr>
<tr>
<td></td>
<td>Windows: $EDACONF\etc directory</td>
</tr>
<tr>
<td></td>
<td>IBM i: IFS $EDACONF/etc directory</td>
</tr>
<tr>
<td></td>
<td>OpenVMS: EDACONF [.ETC] directory</td>
</tr>
<tr>
<td>Override</td>
<td>Set the environment variable EDASPROF to point to an alternate location of edasprof.prf (you cannot rename edasprof.prf).</td>
</tr>
<tr>
<td>Sequence in search order</td>
<td>First</td>
</tr>
<tr>
<td>Scope</td>
<td>Applies to all connected users.</td>
</tr>
</tbody>
</table>

Service profile. A service profile specifies settings for the server environment, but the settings in this level of profile apply only to users associated with a specific service. When a user connects to the server, the service profile settings are applied and remain in effect throughout the user session.

A service profile may contain settings that are the same as those in a global profile. You can specify a service profile in the Web Console by selecting Workspace from the menu bar. In the navigation pane, right-click the Workspace folder, and select Settings, and then Profile Settings.

You can create a service profile from the Workspace folder. Expand the Configuration Files folder in the navigation pane. Right-click Server Profiles and select Edit. You can also use any standard system editor. If you use an editor, create the service profile in the correct location.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>name.fex</td>
</tr>
<tr>
<td>Characteristic</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location</td>
<td>Follows the normal search path for procedures (focexecs).</td>
</tr>
<tr>
<td>Override</td>
<td>None</td>
</tr>
<tr>
<td>Sequence in search order</td>
<td>Second</td>
</tr>
<tr>
<td>Scope</td>
<td>Applies to all users of the same service.</td>
</tr>
</tbody>
</table>

- **Role profile.** A role profile specifies settings for the server environment, but the settings in this level of profile apply only to users assigned to a specific role. When a user connects to the server, the role profile settings are applied and remain in effect throughout the user session.

- **Group profile.** A group profile specifies settings for the server environment, but the settings in this level of profile apply only to users associated with a specific security group. When a user connects to the server, the group profile settings are applied and remain in effect throughout the user session.

  A group profile may contain settings that are the same as those in a global profile.

  Server Administrators need to register group profiles and users to give them privileges that are different from those they inherit from their default role. Group profiles are used to set DBMS connections, variables, and other settings that should be executed for group users when they connect.

  If you use an editor, create the group profile in the correct location.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td><code>group_name.prf</code></td>
</tr>
<tr>
<td>Location</td>
<td>UNIX: <code>base_directory_name/ibi/profiles</code></td>
</tr>
<tr>
<td></td>
<td>Windows: <code>base_directory_name\ibi\profiles</code></td>
</tr>
<tr>
<td></td>
<td>IBM i: IFS <code>base_directory_name/ibi/profiles directory</code></td>
</tr>
<tr>
<td></td>
<td>OpenVMS: <code>base_directory_name [.IBI.PROFILES] directory</code></td>
</tr>
<tr>
<td>Override</td>
<td>Set the edaserve.cfg keyword edaprfu to point to an alternate location of <code>group_name.prf</code>.</td>
</tr>
<tr>
<td>Sequence in search order</td>
<td>Third</td>
</tr>
<tr>
<td><strong>Characteristic</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Scope</td>
<td>Applies to all users of the same security group.</td>
</tr>
</tbody>
</table>

**User profile.** A user profile specifies settings for the server environment, but the settings in this level of profile apply only to a specific user ID. When a user connects to the server, the user profile settings are applied and remain in effect throughout the user session. A user profile may contain settings that are the same as those in a global profile.

**Procedure: How to Create a User Profile**

You can create a user profile at any time as by:

1. From the menu bar, select *Workspace*.
2. Expand the *Configuration Files* folder in the navigation pane.
3. Right-click the *User/Group Profiles* folder, and select *New Profile*. The Edit New Profile page opens.
4. Enter the profile parameters and click the Save As button.

![Edit New Profile](image)

The Create new user profile page opens.
5. Enter a profile name and click Save.

You can also use any standard system editor. If you use an editor, create the user profile in the correct location.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>user_id.prf</td>
</tr>
<tr>
<td>Location</td>
<td>UNIX: base_directory_name/ibi/profiles</td>
</tr>
<tr>
<td></td>
<td>Windows: base_directory_name\ibi\profiles</td>
</tr>
<tr>
<td></td>
<td>IBM i: IFS base_directory_name/ibi/profiles directory</td>
</tr>
<tr>
<td></td>
<td>OpenVMS: base_directory_name [,IBI.PROFILES] directory</td>
</tr>
<tr>
<td>Override</td>
<td>Set the edaserve.cfg keyword edaprfu to point to an alternate location of user_id.prf.</td>
</tr>
<tr>
<td>Sequence in search order</td>
<td>Fourth</td>
</tr>
<tr>
<td>Scope</td>
<td>Applies to a specific user.</td>
</tr>
</tbody>
</table>

Profile Commands

In this section:

Profile Command Formats

The following topics describe commands that you can include in any of the supported server profiles. These commands affect the behavior of the server for the duration of the connected session. You can code additional commands, such as data access commands, in any of the supported server profiles. For more information, see specific adapter topics in the online help.

For more information on the server profile commands, launch the online help using the adjacent question mark (?) icons in the Web Console.
Profile Command Formats

**How to:**
Use a Direct SET Command
Use an SQL Engine SET Command
Use an SQL Translator Command

**Example:**
Using a Direct SET Command
Using an SQL Engine SET Command
Using an SQL Translator Command

Each server command takes one of three possible formats. The syntax and an example of these formats follow. Ensure that you use the correct format for any server command you use.

**Syntax:**  How to Use a Direct SET Command
To use a direct SET command

```
SET command=value
```

where:

```
command
```

Is the server command.

```
value
```

Is the value selected from the available choices.

**Example:**  Using a Direct SET Command

```
SET SQLENGINE=DB2
```

**Syntax:**  How to Use an SQL Engine SET Command
To use the SQL Engine SET command

```
ENGINE sqlengine SET command value
```

where:

\textit{sqlengine}

Is the target DBMS. You can omit this parameter value if you previously issued the SET SQLENGINE command.

\textit{command}

Is the server command.

\textit{value}

Is the value selected from the available choices.

**Example: Using an SQL Engine SET Command**

\begin{verbatim}
ENGINE SQLORA SET OWNERID EDAUSER
\end{verbatim}

**Syntax: How to Use an SQL Translator Command**

To use an SQL Translator command

\begin{verbatim}
SQL SET command=value END
\end{verbatim}

where:

\textit{command}

Is the SQL Translator command.

\textit{value}

Is the value selected from the available choices.

**Example: Using an SQL Translator Command**

\begin{verbatim}
SQL SET APT=OFF END
\end{verbatim}
Profile Commands
This chapter describes the security providers that can be configured on a server. It also describes how an administrator enables a particular security provider and assigns privileges to users and groups.

Topics:
- Server Security Overview
- Configuring Authentication
- Configuring Privileges and Other Authorizations
- Configuring Server Encryption
- Access to Connection Information in WebFOCUS Procedures
- Configuring the Server for Multi-Tenant Deployment
Server Security Overview

In this section:
- Authentication
- Security Providers
- Privileges and Other Authorizations
- Encryption

Server security is based on a three step process: authenticating the connecting user, establishing his/her group and role, and then assigning privileges and other authorizations based on the user, group, and role.

**Note:** NLS characters are supported for user ID, group name, password, and domain name on the Web Console Access Control configuration pages.

The Access Control page on the Web Console provides a server administrator with the tools needed to manage server security. Using ribbon buttons and right-click options, the server administrator can perform the following security operations:

- Manage security providers.
- Edit Access Control and Encryption settings.
- Filter the Access Control tree display.
- Register users, groups, and roles.
- Show privileges for specific users, groups, and roles.
- Generate a report listing System and Security functions with their parameters and descriptions.

**Authentication**

Authentication can be performed based on the following types of credentials:

- **Explicit.** User ID and password are supplied when signing in to the server.

- **SSO (Single sign on).** The user is authenticated by a single sign on product prior to signing in to the server, and a token is passed to the server. Single sign on products include Kerberos, NTLM tickets or browser cookies such as passed by MYSAPSSO2.

- **Trusted.** The user ID is submitted without the password from the application server or mid-tier, which has the user already authenticated.
Security Providers

A security provider is used to authenticate the incoming connection. When a security provider is configured, it is added to edaserve.cfg as a security provider block. Multiple active security providers can be configured, in which case the security_provider attribute will consist of a comma-separated list of security providers. The first one on the list is the primary provider.

The security provider can be of several types:

- **OPSYS.** Users are authenticated against the native OS security repository, such as the windows domain controller, z/OS RACF/ACF2, UNIX password files or other operating system security products using the native OS API.

- **LDAP.** Users are authenticated against an LDAP server or active directory using the LDAP API.

- **DBMS.** Users are authenticated by connecting to a DBMS such as Oracle, SAP, or DB2.

- **PTH.** Users are authenticated against a list of users kept internally by the server in the admin.cfg configuration file.

- **CUSTOM.** Users are authenticated using a custom procedure.

After the server is installed, the default security provider configured by the installation process is the PTH (server internal) provider. This provider keeps a list of groups and group membership in the admin.cfg file. During installation of the server, a server administrator user ID is created in admin.cfg. The installer can accept the default user ID (srvadmin) or change it, but the installer must provide a password for this ID. The user ID will be created as a two-part name in the form `security_provider\user_ID`, for example, `PTH\srvadmin`.

When the server starts with security PTH, the PTH\srvadmin user ID (or the one configured during installation) is the server administrator user that is used to connect to the Server Web Console, and that user can make additional security changes to the server, such as adding and changing active security providers and changing access control privileges for users, groups, and roles. We recommend that you keep the PTH provider as an active security provider, so user PTH\srvadmin can be used as a backup Server Administrator.

All new security subjects for all security providers will be registered with a two-part name, `provider\userid` or `provider\groupid`. For example, the following group named grp1 is registered under the LDAP1 security provider:

```
LDAP1\grp1
```

The following user, whose ID is user1, is registered under OPSYS security in the IBI domain:

```
OPSYS\IBI\user1
```

If one-part name registrations exist from a prior release, they are respected and are assumed to be primary provider registrations.
Note: If the silent installation is used, the server administrator user ID with its associated password needs to be provided. If none is provided, the default user ID PTH\srvadmin with the password srvadmin will be configured.

OPSYS security has specific operating requirements in order to be activated. For details, see Configuring OPSYS Authentication on page 53.

If you want to use an OPSYS, LDAP, DBMS, or CUSTOM security provider, you must configure it on the Web Console Access Control page. When you configure one of these security providers, the server edits the edaserve.cfg file to add a block for the new security provider. You can then use the Web Console to change to this provider. In response, the server sets the security_provider attribute in edaserve.cfg to this provider name, after which this provider is considered the primary provider and defines the security used by the server.

You can configure multiple security providers, and the server will add multiple provider blocks in edaserve.cfg. When multiple providers are chosen to be active, the security_provider attribute in edaserve.cfg is set to the list of active providers. In this case, the first provider on the list is considered to be the primary provider and defines the security used by the server.

Note: In order for a signed-in user to start or manage a server using the edastart command script, the signed-in user ID has to be registered as a server administrator in admin.cfg, even if OPSYS is not an active security provider. This is required in order to protect the server from unauthorized actions by users who can sign in to the system where the server resides.

EDAEXTSEC can be set to OFF in order to override the security provider set in the security_provider keyword of edaserve.cfg and start the server with security OFF. For information on setting EDAEXTSEC in different operating environments, see Platform-Specific Methods for Specifying EDAEXTSEC on page 639.

An example of configuring multiple providers is having two distinct LDAP providers configured against two separate LDAP servers that can contain different users and different groups.

One provider is considered the primary provider. For all providers, the user name is a two-part name prefixed with the provider name, for example LDAP1\usera. Note that users (or groups) from two providers that have identical names (such as LDAP1\usera and LDAP2\usera) are considered different security subjects and can be given different privileges and profiles.

At sign-in time, a user needs to select the security provider name in addition to user ID and password. If a user signs in to the server using the primary provider, the server will automatically prepend the user ID with the provider name, if the user does not supply a two-part name.

OPSYS providers can be configured with other security providers. On Windows, multiple Windows domains act as different security providers and users. For example, domain1\usera and domain2\usera are not identical.
Privileges and Other Authorizations

In this section:
- DBMS
- Server DBA
- Data and Application Folder Access
- General Server and Web Console Actions
- Groups
- Roles
- Registering Users and Groups Under Roles

The server supports a large number of objects, and access to them should normally be restricted.

**DBMS**

With DBMS authorization, the main object to be protected is the DBMS-resident data that the server reads and writes. Access control is implemented using ENGINE CONNECTION_ATTRIBUTES statements that define the security attributes that are used by the server agent for connecting to the DBMS. The connection security type depends on the DBMS and can be one of three subtypes:

- **Explicit.** The userid/password is stored in a profile (encrypted).
- **Password pass-through.** The userid/password combination or cookie, such as MYSSAPSSO2, that were provided during the connection to the server is passed to the DBMS connection.
- **Trusted.** This type of connection applies to security provider OPSYS where the operating system process of the agent impersonates the user, and the DBMS connection is derived from that process.

The CONNECTION_ATTRIBUTES statement itself can be defined in the user, group, role or server profile, and they override each other in this order.

It is common initially to create connections in the edasprof server profile. They will then be inherited by all users. Subsequent configuration steps may define connections on other levels, such as the group or user level.

The CONNECTION_ATTRIBUTES statement in effect passes the credentials to the DBMS, and the DBMS server ensures the correct access control: read and read/write rules on the DBMS tables, views, columns, and rows.
**Server DBA**

The server engine can add an additional level of access control by defining DBA rules in synonyms to restrict access to columns and certain data values. This applies only to data access using the WebFOCUS language, and not to Direct SQL Passthru requests. For more information about Server DBA, see the *Describing Data With WebFOCUS Language* manual.

**Data and Application Folder Access**

The server reads operating system files using standard I/O calls.

With the OPSYS security provider, the proper OS read/write privileges should be given using native OS tools such as RACF rules or Windows/UNIX permissions. Run-time access control is achieved by the operating system validating the data agent access to any given file based on the agent process impersonation of the connecting user.

To protect files in other modes (LDAP, PTH, DBMS), the server access control feature should be used to assign read/write privileges to OS files and folders. The privileges are managed from the Web Console Access Control page and stored in the server admin.cfg file. They can be assigned at the role, group, and user levels and be allotted on the folder and file levels. Normal inheritance rules apply. A subfolder inherits from its parent folder, a file inherits from its parent folder, a user inherits from the group, and so on.

Note that this protection applies to WebFOCUS metadata objects in application folders such as synonyms, FOCEXECs, HTML files, style files, and to data files such FOCUS data sources and sequential files.

Application folders and files can have four types of privileges, read, write, execute, and list. For data files such as FTM files, only two privileges are used: read and write.

You can disable operating system shell commands using the SET OPSYSCMD or the NOSYS general privilege. You may want to consider disabling these commands as they are not subject to access control.

**General Server and Web Console Actions**

The Web Console provides various actions, such as adapter configuration, server configuration and monitoring, Resource Analyzer configuration, metadata creation, and other actions, such as the ability to issue Direct SQL Passthru requests. To manage access to these actions, the server administrator uses the server access control feature to assign *general* privileges to users, groups, and roles.
Groups

Groups are collections of users typically defined by the security provider for the purpose of giving common authorization to multiple instead of individual users. Groups are defined either on an external repository such as RACF, LDAP, or internal PTH. The DBMS security provider does not support groups. Except for PTH, user provisioning and all associated administration tasks (such as password reset, invalidating users, volume user creation) are accomplished using the respective security provider software and are outside of the reporting server software.

Roles

Roles are a collections of privileges defined on the server for the purpose of registering groups and users to the collection (as opposed to assigning privileges to individual users). Five predefined user roles (Server Administrator, Application Administrator, Operator, Basic, and None) are created at server installation time. For example, the Server Administrator role has all privileges, and the Application Administrator role has privileges related to the creation of applications, such as creating synonyms and related tasks.

New roles can be added and existing roles can be modified to include and exclude individual privileges.

At server installation time, file access privileges are created with full access rights (read/write/execute/list) for all roles, in order to maintain compatibility with previous releases.

Registering Users and Groups Under Roles

When the server is installed, the user ID specified as the server administrator is automatically registered as Server Administrator. All other users and groups are defaulted to the server default role—Basic.

Note that no group, user, or role profile exists initially after the installation. It is typical at the initial stage to have the DBMS connections defined in the server profile, edasprof. Privileges are derived from the Basic role and are in effect for all users except the Server Administrator.

Recommended steps for securing the server:

- Review default privileges for role Basic and change them if necessary. You can change the default role to another role.
- Review and change the file privileges for the default role at the file root level.
Customize groups:

- Register groups to roles. For example, register LDAP group GRP1 to the Application Administrator role.
- Create group profiles with DBMS connections and APP PATH. For example, for group GPR1, create grp1.prf (through the Web Console Adapter page or the application path configuration).
- Customize application level file privileges for groups. For example, group GRP1 can have read but not write access to baseapp.

Optional steps:

- Create new roles or customize the role privilege list. This should be done only if existing roles are not satisfactory. It allows registering groups to these roles.
- Register users. This should be done only if groups are not created adequately, and for special users such as managers.
- Register file privileges on the file level. This should be avoided in favor of folder level privileges, as they are inherited by files and are easier to manage.

Encryption

Using the Web Console, you can encrypt passwords in configuration files, enable Secure Socket Layer (SSL) encryption for the TCP/HTTP listener, and encrypt data passed between the server and a remote server. For more information about encrypting communication between the server and the WebFOCUS Client, see the WebFOCUS Security and Administration Manual.
Configuring Authentication

Authentication is the process of validating user credentials. Individuals who use WebFOCUS may have user IDs and passwords managed by other systems. WebFOCUS Managed Reporting and the Reporting Server can each be configured to authenticate users to an external security system, or to trust that authentication has already taken place. Users benefit because they do not have to sign in multiple times or manage separate user ID/password combinations. If a user signs in to WebFOCUS with credentials from an outside security package, the package provides some type of authentication confirmation to the WebFOCUS Client or the Reporting Server. This information may be in the form of a browser cookie or a logon ticket and may be needed by the Reporting Server in order for it to access and retrieve the data required by the WebFOCUS application.

Depending on your operating environment, user credentials can be validated by:

- The operating system on which the server is running (OPSYS security).
- A list of users stored in the server file named admin.cfg (PTH security).
- An LDAP or Active Directory repository (LDAP security).
- A DBMS (DBMS security).
- A custom user-supplied procedure (CUSTOM security).

Multiple security providers can be configured. You can configure additional providers using the Web Console Access Control page.
Configuring a New Security Provider

Example:
Security Provider Blocks in edaserve.cfg

Security providers must be configured from the Web Console Access Control page.

To switch to security provider LDAP, DBMS, or CUSTOM, you first need to add a new provider under the appropriate security provider on the Access Control tree. When you add a new provider, the server updates configuration file edaserve.cfg with provider blocks named LDAP_PROVIDER, DBMS_PROVIDER, or CUSTOM_PROVIDER. These blocks are inserted with all attributes that apply to the provider type between BEGIN and END dividers.

Security provider PTH is configured during installation of the server. The OPSYS security provider is always on the list of providers. In order to make it an active provider, the server must be authorized (privileged) to start with security OPSYS. There is no need for the additional step of creating a new provider as is needed for LDAP, DBMS, and CUSTOM providers. By default, the effective server administrator ID shown on the Manage Providers page is the server administrator ID. You can change this using the Access Control Settings page. Once the server is installed, you can start adding new PTH users and PTH groups, and you can assign PTH users to PTH groups.

Security provider CUSTOM supports using non-standard security storage. You can create DBMS tables to store users, groups, and passwords. You must then write procedures to read these tables and perform the basic security tasks. This security mechanism has to be created prior to configuring the CUSTOM security provider and must be available when the CUSTOM provider is added to the server provider configuration. It must perform the following standard security tasks:

- Retrieve the user ID and its password to authenticate the user on connecting to the server.
- Retrieve the list of users and groups on user and group registration.
- Retrieve the list of users in each group.
- Retrieve user membership in all available groups.

Once the provider is added, you can change security providers from the Access Control page. Right-click the Security Providers folder and select Manage Providers to switch to a newly added provider. At this point, edaserve.cfg is updated with the security_provider attribute that specifies the provider name.
Multiple security providers can be configured. When you configure OPSYS as one of multiple security providers:

- The server has to be authorized to run security OPSYS, and it needs to have a valid OS user ID and password for starting an agent.
- No provider name can be the same as any domain name.

The Access Control Settings page lets you enter valid OS credentials.

When you configure multiple providers, you choose one to be primary on the Access Control Manage Providers page. Drop-down lists are available for assigning the other providers as secondary providers or inactive. The primary provider defines the security under which the server is running:

Manage Providers

<table>
<thead>
<tr>
<th>Security Provider</th>
<th>Status</th>
<th>Accepts Trusted</th>
<th>Server Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTH</td>
<td>Primary</td>
<td>✓</td>
<td>user2, ad03703, pgmsa1, B1\ad03703, pmsaa, PTH\syadmin, dzy</td>
</tr>
<tr>
<td>OPSYS</td>
<td>Secondary</td>
<td>✓</td>
<td>OPSYS\B1\ad03703</td>
</tr>
<tr>
<td>CUSTOM - cut01</td>
<td>Inactive</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

During connection to the server, all provider users are connected with a two-part user ID consisting of the provider name and the user ID, for example, MyLDAP\User1 or MyDBMS\User2, where MyLDAP or MyDBMS is the name of a configured secondary provider.

This naming convention is also used when users and groups are registered to server roles. Users and groups are registered with a two-part name. If the PTH provider is a secondary provider, PTH users and groups are registered (and used on connection) as PTH\userid and PTH\groupid.
Example:  **Security Provider Blocks in edaserve.cfg**

The following is an example of a security_provider attribute and security provider block for starting the server with security LDAP (provider name MyLDAP):

```plaintext
security_provider = MyLDAP
LDAP_PROVIDER = MyLDAP
BEGIN
  ldap_host = ldaphost
  ldap_port = post
  ldap_secure_connection = n
  ldap_user_base = dc=ibi,dc=com
  ldap_user_scope = subtree
  ldap_user_class = person
  ldap_user_attribute = uid
  ...
  ...
END
```

The following is an example of a security_provider attribute and security provider block for starting the server with security DBMS (provider name MyDBMS):

```plaintext
security_provider = MyDBMS
DBMS_PROVIDER = MyDBMS
BEGIN
  security_dbms = MSSQL
  security_connection = CON01
END
```
Configuring OPSYS Authentication

In this section:
- Preventing Unsecured Server Starts After Upgrades
- Using Password Phrases for Authentication on z/OS
- Configuring Linux and AIX Pluggable Authentication Modules (PAMs)

How to:
- Change the Impersonation User ID
- Enable Primary Group Support for Windows Active Directory
- Configure an OPSYS Security Provider

When security provider OPSYS is configured, the user credentials from the client connection are authenticated by the native security system of the operating system. The server then allocates a data access agent that impersonates the user so that access to files or other objects is controlled by the native system.

Profiles for operating-system users are supported on all platforms. On Windows, Active Directory groups are supported based on the win_primgroup_adsi setting.

Details about OPSYS security requirements are provided in the Server Installation manual, where specific sections are provided for each platform. Refer to this manual for installation instructions and platform-specific setup steps. The following is a summary of the OPSYS requirements:

- **On UNIX**, the startup tscom300 executable must have root setuid authority.

- **On Windows**, the server must be started as a service under SYSTEM account (Administrators Group authority) or as a user ID with Windows Administrator authority.

  On Windows, the Server Administrator password is required for this security provider. If the password is not provided in the configuration, the server starts in safe mode and displays a message to that effect. Multiple administrators are allowed. For more information on creating server administrators and other roles, see Registering Users and Groups in a Role on page 128.

- **On z/OS**, the MVS load library must be APF-authorized, and for HFS deployment, certain HFS executables must be given +a authorization.

- **On IBM i** (formerly known as i5/OS), the ownership of certain library files must be changed to have QSECOFR ownership and, therefore, authority.

- **On OpenVMS**, the account starting the server must have a specific set of privileges to have proper authorities.
Note that some system specific settings in the edaserve.cfg file are provided to allow further adjustments of the authentication mechanism. Those relevant for some UNIX systems are:

- require_logon_privilege (AIX only. Allows no sign-in IDs to access the server.)
- update_security_db (AIX and HP-UX only. Registers failed sign-in attempts.)

For Windows systems, the logon_method setting (for interactive, network, or batch) is relevant to explicit connections.

**Note:** For more information on limiting user access to the Web Console, see *Configuring General Server and Web Console Actions* on page 110.

**Procedure: How to Change the Impersonation User ID**

When you first add an OPSYS security provider, the impersonation ID is created by copying the effective server administrator ID.

If you need to change the impersonation ID for an OPSYS security provider, do the following.

1. Sign in to the server with Server Administrator privileges.
2. Go to the Access Control page.
3. Right-click the Access Control tree and select Settings from the context menu, or click **Settings** on the ribbon.

The Access Control Settings page opens.

1. Enter the user ID and password for the impersonation ID in the appropriate fields.
2. Click **Apply and Restart Server**.
**Procedure: How to Enable Primary Group Support for Windows Active Directory**

When the Reporting Server runs on the Windows platform configured for an OPSYS security provider against an Active Directory, you can set the `win_primgroup_adsi` keyword to support Active Directory primary group notation. When you set the parameter to `y`, the server uses the primary group of the user as the name for the group profile and for some access controls under the Web Console. (Note that you can only set the primary group from Windows Active Directory interface to Users management.) In order to take advantage of this setting, you must ensure that the Windows machine that hosts the server resides in the same domain as the Active Directory.

1. Access the Web Console with a server administrator user ID.
2. Click **Access Control**.
   The Access Control page opens.
3. Open the **Security Providers** folder in the navigation pane.
4. Right-click **OPSYS** and select **Properties**.
   The OPSYS Security Configuration page opens.

5. Select `y` from the `win_primgroup_adsi` drop-down menu.
6. Click **Save**.

**Procedure: How to Configure an OPSYS Security Provider**

This procedure assumes that the server is already running configured for a non-OPSYS security provider.

1. Access the Web Console with a server administrator user ID.
2. Click **Access Control**.
The Access Control page opens.
The server security provider is displayed on the Access Control page.

3. Right-click the Access Control folder in the navigation pane, and select Manage Providers.
The Manage Providers page opens.

Manage Providers

Effective Server Administrator: User2

<table>
<thead>
<tr>
<th>Security Provider</th>
<th>Status</th>
<th>Accepts Trusted</th>
<th>Server Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTH</td>
<td>Primary</td>
<td></td>
<td>user2, se02703, pgmtst1, IFI\se02703, pmssae, PTH\srvadmin, dev</td>
</tr>
<tr>
<td>OPSYS</td>
<td>Secondary</td>
<td></td>
<td>OPSYS\s02703</td>
</tr>
</tbody>
</table>

Note: For more information about changing security providers, see Considerations for Changing the List of Security Providers From the Web Console on page 90.

4. Click Save Provider’s Status.

Note: If you change the privileges of tscom300, the server will start with security OPSYS by default. For more information, see the Server Installation manual.

5. **For z/OS Unified Server only.** Starting with z/OS 1.7, the z/OS security package provides extended password support. If this option is enabled, you must add mixed_case_password=on to the edaserve configuration file before starting the server in configured for an OPSYS security provider. For HFS deployment, this file is in $EDACONF/etc and for PDS deployment it is in qualif.servertype.CONF.CFG, where servertype is determined by your license key.

6. If the server is not running, start it using the instructions for your platform in the installation guide.
The server will start configured for an OPSYS security provider.

7. Examine the edaprint.log file. If it indicates errors, stop the server, correct the errors, then start it with security OPSYS.
8. Restart your browser and connect to the Web Console. When prompted, enter a valid operating system user ID and password.

If you wish to register other users in a role or group or create new roles, first connect as a Server Administrator. Then, follow the instructions in Registering Users and Groups in a Role on page 128.

**Preventing Unsecured Server Starts After Upgrades**

If the environment variable EDAEXTSEC is explicitly set to OPSYS, and the server fails to start because it lacks system privileges to start configured for an OPSYS security provider, the server start aborts and error messages are written to the edaprint log file.

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 HFS 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:

- Configured security is 'ON' as set by EDAEXTSEC variable.
- Server has no root privilege. (UNIX)
- Server is not APF-authorized. (z/OS HFS)
- TSCOM300.PGM has no QSECOFR authority. (IBM i)
- Workspace initialization aborted.
- (EDA13171) UNABLE TO START SERVER

**Using Password Phrases for Authentication on z/OS**

### How to:

Change Passwords on the Web Console Logon Screen

Starting with z/OS 1.8, IBM introduced password phrases which can be used for authentication, and starting with z/OS 1.10 password phrases can be used for TSO Logon as well. Password phrases can be from 14 to 100 characters long.

z/OS IDs can have both a password (1 to 8 bytes) and a passphrase (from 14 to 100 bytes). The two forms of credentials are independent. Changing one does not change the other. The server recognizes the type of credential being presented by its size (sizes between 9 and 13 are invalid on z/OS).

No special configuration is needed to enable password phrases.
When a users log into the Web Console, there are two possible ways they can change their passwords or passphrases:

- On the initial Web Console Logon page. This option is disabled by default. For more information on enabling this option, see [How to Change Passwords on the Web Console Logon Screen](#) on page 58.

- After the initial logon, by choosing Change Password on the My Console menu. A new screen opens with three separated fields (old password, new password, and confirm new password).

**Procedure: How to Change Passwords on the Web Console Logon Screen**

By default, passwords cannot be changed on the Web Console Logon page because the following parameter is in effect:

```
password_change_wclogin = n
```

To enable the option to change passwords when logging into the Web Console:

1. Select Access Control from the Web Console menu bar.
2. Right-click Access Control on the tree and select Settings from the context menu.
3. Change the value of the password_change_wclogin parameter to y.

On the same configuration page, you can change the delimiter used to separate the user ID from the password or passphrase to any valid character accepted by the operating system. By default, the delimiter is a comma:

```
password_change_delimiter= ,
```

Once the option to change passwords on the Web Console Logon page is enabled, users can change their passwords or passphrases by entering the following in the password field of the Web Console Logon page (if the password delimiter has been changed, use that character between the old and new passwords instead of the comma):

```
old_password,new_password
```

When `password_change_wclogin = y`, passwords and passphrases cannot contain the password delimiter character.

When `password_change_wclogin = n` (the default), the setting for `password_change_delimiter` is ignored, and passwords can contain all valid characters allowed by the operating system.
Configuring Linux and AIX Pluggable Authentication Modules (PAMs)

**How to:**
Configure PAM Security on Linux and AIX

In a Linux or AIX environment, OPSYS security can be configured to use Pluggable Authentication Modules.

**Procedure:** How to Configure PAM Security on Linux and AIX

   The Access Control Page opens.
2. Right-click the OPSYS security provider and select Properties from the context menu.
3. Select y from the security_pam drop-down list.
   This parameter is only applicable for the Linux and AIX operating systems. The parameter defines if the server uses the Pluggable Authentication Modules mechanism to implement security. If y, the server uses PAM calls, if n the server uses native UNIX security calls.
4. Click Save and Restart Server.

Configuring PTH Authentication

**In this section:**
- Configuring Password Properties for a PTH Security Provider
- Disabling a PTH Security Provider Account

**How to:**
Configure a PTH Security Provider

By default, the server installation process establishes PTH security with a PTH server administrator user ID and password. If you deleted the PTH server administrator ID, you can reconfigure PTH security.
The PTH security provider only controls access to the Web Console. When the server is configured for this security provider, there is no impersonation by data agents or authentication of a non-Web Console connected user. From the operating system point of view, all server processes run as a single user ID, and access to the Web Console is controlled by authenticating names against those defined in the admin.cfg file unless authenticate_all_pthuser is set to y. The setting is available on the PTH Security Configuration page, which can be accessed by right-clicking PTH in the Security Providers folder on the Access Control navigation pane.

You must configure the Server Administrator password before starting a server configured for a PTH security provider, either by providing it at installation time or by configuring it in the Web Console. For details, see Registering Users and Groups in a Role on page 128.

The PTH security provider supports profiles for users and groups on all platforms.

**Note:** For more information on limiting user access to the Web Console, see Configuring General Server and Web Console Actions on page 110.

### Procedure: How to Configure a PTH Security Provider

2. Right-click the Access Control folder, and select Manage Providers.
   
The Manage Providers page opens.
3. Select the PTH drop-down list, and select Primary or Secondary. from the list of providers in the last Security Provider drop-down box and enter a Server Administrator ID and Password.
4. Click Save Provider’s Status.
   
Once the server has restarted, the PTH security provider has icons for adding and viewing its users and groups.
5. If the server is not running, start it using the instructions for your platform.
   
The server will start configured for a PTH security provider.
6. Examine the edaprint.log file. If it indicates errors, stop the server, then start it with security OFF to correct the errors.
7. Restart your browser and connect to the Web Console. When prompted, enter a valid PTH user ID and password.

If you wish to add other PTH users, first connect as a PTH user defined as server administrator. Then, follow the instructions in How to Manage Users and Groups With PTH Security on page 134.
Note: A common problem when switching from OPSYS to PTH is the existence of files in EDATTEMP that cannot be removed due to insufficient privileges. To handle this problem, use edastart -cleardir (or member ICLRDIR on the z/OS platform) using an OPSYS security provider to clear the directory before switching.

Configuring Password Properties for a PTH Security Provider

How to: Configure Password Properties for a PTH Security Provider

When the Server Administrator creates or updates a user under a PTH security provider, by default the password never expires, can be any length, and are not case-sensitive.

The Server Administrator can configure a new or existing user password to expire after a specified number of days, can set a minimum length for passwords, and can enable case-sensitive passwords.

Procedure: How to Configure Password Properties for a PTH Security Provider

To assign an expiring password:

1. Select Access Control.

2. Right-click PTH and select Manage Users/Groups.
   The PTH Users and Groups Management page opens.

3. If the user does not yet exist, create the user. Then, select the user on the list and click Properties.
   By default, the Password never expires box is checked.
4. Uncheck the *Password never expires* box.

5. Click **OK**.

The current date is saved in admin.cfg as *admin_passdate* for this user. This is the last password change date.

6. Click **Save**.

7. Configure the number of days before passwords expire and whether they are case sensitive:
   a. Right-click the PTH Security Provider and select *Properties*.
   b. Set *pthpass_lifetime* to the number of days after which the password should expire.
c. To make the passwords case-sensitive, select y from the pthpass_casesensitive drop-down list.

d. To set a minimum length for passwords, enter a number of characters in the pthpass_length entry field.

e. Click Save and Restart Server.

When the password expires, the user gets a password expired message on the logon screen and is provided with a New Password field in order to enter a new password.

At this time, the new password and new password change date are recorded in admin.cfg.
Note that changing the password by selecting Change Password from the My Console menu also resets the password change date.

8. Optionally, configure a warning message to begin displaying a specified number of days before the password expires.

**Disabling a PTH Security Provider Account**

You can disable an account that is registered in admin.cfg under the PTH security provider in order to prevent a user from signing in to the server with that account.

To disable a PTH account:

1. Right-click PTH under the Security Providers folder, and select Manage Users/Groups from the context menu.
   
The PTH Users and Groups Management page opens, listing all registered users on the left, and all registered groups on the right.

2. Select a user and click Properties.
   
The PTH User properties dialog box opens.

3. Click Account disabled as shown in the following image:
4. Click OK.

A red x is displayed in the Disabled column for that user on the PTH Users and Groups Management page.

5. Click Save.
Configuring DBMS Authentication

With a DBMS security provider, there is no impersonation by data agents, but connection credentials are authenticated against a configured DBMS. This technique is called password passthru, as user IDs and passwords supplied by the client are passed to the DBMS for authentication.

A DBMS security provider supports profiles for users on all platforms. Profiles for groups are not supported.

**Note:** For more information on limiting user access to the Web Console, see Configuring General Server and Web Console Actions on page 110.

**Procedure:** **How to Configure DBMS Authentication**

This procedure assumes that the server is already running.

1. Access the Web Console with a server administrator user ID.
2. From the Adapter pane, configure a DBMS adapter and connection.
3. Select the *Password Passthru* security option on the Adapter configuration pane.

![Add Connection for MS SQL Server](image)

Note that the *Test* button, which appears next to the *Configure* button, will not work until you configure the DBMS security provider. Do not restart the server at this point.


   The server security provider is displayed on the Access Control page.

5. To add the DBMS provider, expand the Security Provider folder, right click *DBMS*, and choose *New*.

6. Enter a name for the DBMS provider.

7. Select a *security_dbms* from the drop-down list.

   This option identifies the database engine used to authenticate incoming requests.

8. Select a *security_connection* from the drop-down list. This list shows all DBMS connections that are configured with Password Passthru.

   This option identifies the database connection used to authenticate incoming requests.

9. At this point, it is a good idea to click the *Test* button to make sure the DBMS connection is working. You will be prompted for a password for the selected user ID. Click *Continue*. The DBMS will authenticate this ID. If it is a valid DBMS ID, a message will be returned indicating that authentication was successful. If the ID is not a valid DBMS ID, the DBMS will return messages indicating that authentication was not successful.
10. Right-click the Access Control folder in the navigation pane, and select Manage Providers. The Manage Providers page opens.

11. Select the DBMS drop-down list, and select Primary or Secondary.

12. Supply the Server Administrator user ID. Alternatively, you can enter a new user ID that will be added to the admin.cfg file as a Server Administrator.

13. Click Save Provider’s Status.
   
   **Note:** For more information about changing security providers, see Considerations for Changing the List of Security Providers From the Web Console on page 90.

14. If the server is not running, start it using the instructions for your platform.
   
   The server will start configured for a DBMS security provider.

15. Examine the edaprint.log file. If it indicates that there were any errors, stop the server and then start it with security OFF to correct the errors.

16. Restart your browser and connect to the Web Console. When prompted, enter a valid DBMS user ID and password.

   If you wish to add other DBMS users, first connect as a DBMS user defined as server administrator. Then, follow the instructions in Registering Users and Groups in a Role on page 128.

   **Note:** A common problem when switching from OPSYS to a DBMS provider is the existence of files in EDATEMP that cannot be removed due to insufficient privileges. To handle this problem, use edastart -cleardir (or member ICLRDIR on the z/OS platform) with EDAEXTSEC=OPSYS to clear the directory before switching.

**Reference:** Usage Notes for DBMS Security

- If an error is detected in the security_dbsms definition, the DBMS is down, or your DBMS user ID is invalid, you will not be able to access the Web Console or connect to the server. In these situations, you must bring the server down using the line console and correct the problem.

- The server may have other DBMS connections defined, but only one DBMS connection can be used for user authentication.

**Reference:** Password Pass-through and Security DBMS

Security DBMS (using password pass-through) is supported for the following engines:

- DB2
- Informix
Single sign-on (SSO) enables users to login to the SAP portal with their credentials and then access WebFOCUS components, such as the Reporting Server with the SAP R/3 and SAP BW adapters, the Web Console, and the WebFOCUS client (Managed Reporting) without a secondary logon. This is achieved in the following manner:

- The user logs on to the SAP portal with a user ID and password. The portal authenticates the user and places a MYSAPSSO2 cookie in the browser.
- When the user accesses the Web Console or the WebFOCUS servlet, the servlet will not do the authentication, but will, instead, trust the user ID and use it in the Managed Reporting environment and in the Web Console security scheme. For example, a user may be given server_admin or application_admin level privileges on the Reporting Server (using the admin.cfg file).
- When the user runs a backend SAP report, the cookie is processed and passed to the SAP RFC connection that provides access to the SAP data.

**Procedure: How to Ensure Compliance With SSO Prerequisites for SAP BW and SAP R/3**

Complete the following steps to ensure that prerequisites have been met:

1. Export the public key certificate from the SAP portal into $EDACONF/etc.
2. Set Server security to DBMS.
3. Configure the SAP/BW or SAP R/3-ECC connection for Password-Passthru.
4. Ensure that Security DBMS with Password-passthru to SAP/BW or SAP R/3-ECC is working.
5. Ensure that SAP RFCSDK 6.40, SAP SSOEXT, and SAP SECULIB 5.4 are in the path. (Check your Operating System or consult a system administrator for details.)

Once prerequisites have been satisfied, complete the SSO verification procedure.

**Procedure: How to Complete SSO Verification**

1. From the SAP portal (http://sapportal.mydomain.com:50000), execute a command that requires authentication (using a logon screen from the Portal).
   
   This generates an SSO cookie.

2. Overwrite the SAP portal url with the one for the WebFOCUS Reporting Server, using the same domain (for example, http://iwayserv.mydomain.com:8101).
   
   At this point, no logon screen should pop up since the user is logged in and SSO login has been successfully verified.

**Configuring LDAP Authentication**

**How to:**

Configure an LDAP Security Provider

Remove an LDAP Security Provider From the Web Console

**Example:**

Making Sun LDAP Library Files Available

**Reference:**

LDAP Vendor Library Prerequisites

With an LDAP (Lightweight Directory Access Protocol) security provider, there is no impersonation by data agents, but connection credentials are authenticated against the established directory services. From the operating system point of view, all server processes run as a single user ID.

An LDAP security provider is presently supported on Windows, UNIX, IBM i, and the Unified Server (HFS and PDS deployments).

An LDAP security provider supports profiles for LDAP users and LDAP groups.
Note: For more information on limiting user access to the Web Console, see Configuring General Server and Web Console Actions on page 110.

Procedure: How to Configure an LDAP Security Provider

1. Sign in to the Reporting Server Web Console as a server administrator.
2. Open the Access Control page.
3. If this is the first LDAP security provider being configured:
   a. Right-click the LDAP folder under Security Providers, and select Properties from the context menu.
   b. Select the LDAP vendor from the drop-down list and click Continue.

   If you choose OpenLDAP on LINUX, you will see two additional fields, ldap_libldap and ldap_liblber. These parameters specify the names of the OpenLDAP libraries that the server module loads at run time. The path to the libraries should be available to the server at run time. You are prompted to specify the library name at run time. If you do not supply a different name a default library name is used.

4. Under the Security Providers folder, right-click LDAP and select New.
   The LDAP Security Provider Configuration page opens.
5. Enter or select values for the following Connection Properties.

   **LDAP_PROVIDER**
   Specifies a name for this provider.

   **ldap_host**
   Is a host identifier consisting of a host name or an IPv4 dotted string representing the IP address of a host running the LDAP server to connect to.
   Alternatively, it may contain a list of space-delimited host identifiers. Each host identifier may include a trailing colon and port number. In the case where more than one host identifier is specified, each host identifier in turn will be contacted until a connection can be established. For example:
   ```
   directory.example.com
   192.0.2.0
   directory.example.com:1050 people.catalog.com 192.0.2.0
   ```

   **ldap_port**
   Is a positive integer that defines the TCP port number used to connect to the LDAP server. Note that ldap_port is ignored for any host identifier which includes a colon and port number. The server default port is 389 or 636 (for SSL connection).
ldap_secure_connection

Specifies whether the server uses a Secure Socket Layer (SSL) session with the LDAP server. Select No or Yes. The server default is No.

An LDAP (Lightweight Directory Access Protocol) security provider supports Secure Sockets Layer (SSL) API calls to establish an SSL/TLS connection. Using server authentication only, the Reporting Server initiates API calls to verify that the LDAP server being connected to is the same server that provided certification.

You can set the LDAP secure connection from the Web Console:

- Select No, the default value, if you do not wish to enable SSL.
- Select Yes to enable an encrypted Secure Sockets Layer (SSL) session with the LDAP server.

If you have selected IBM, Sun, or Novell as the your ldap_lib_vendor, when you select Yes in the ldap_secure_conection field, additional options are added to the Connection tab:

- For Sun and IBM, ldap_ssl_certificate is added.
- For Novell, ldap_ssl_certificate and ldap_ssl_certification_encoding are added.

ldap_ssl_certificate. Enter the name of the LDAP attribute used by the API to establish the SSL/TLS connection. The server employs server authentication only, checking through API calls that the LDAP server you are connecting to is the one that provided the certificate. Values depend on the LDAP vendor, as follows:

- **Novell API** specifies the file name, including path, of the Trusted Root Certificate that the LDAP server provided for authentication.
- **Sun/Netscape API** specifies the path to cert7.db, Netscape certificate database, excluding the file name, that the LDAP server provided for authentication.
- **IBM API** specifies the file name, including the path, for ldapkey.kdb (IBM key database file that the LDAP server provided for authentication). The ldapkey.sth password stash file should be in the same directory. Note that in addition to IBM LDAP client libraries, Global Security Kit libraries are needed to make SSL work. On Windows machines, GSK must be installed.
- **Microsoft API** ignores the ldap_ssl_certificate configuration parameter since it is not used in an Active Directory. The server certificate should be installed in a certificate store.

ldap_ssl_certificate_encoding. For Novell, select the standard used to encode the certificate from the drop-down list. Encryption and file format depend on API vendor specifications. The options are B64 and DER.
security

Determines the type of bind used. Can be one of the following.

Anonymous

The bind is performed using no credentials. This is the internal default value.

Windows security (NEGOTIATE)

The reporting server authentication is performed against Active Directory utilizing a Windows-specific API.

The bind is done under the Windows account that started the server.

The windows machine that hosts the reporting server should be in the same domain as Active Directory.

Explicit

The bind is performed under the account that is defined by configuration parameters `ldap_principal` and `ldap_credentials`.

Note: When connecting to Active Directory using Explicit or NEGOTIATE, `ldap_user_attribute` should have the value `sAMAccountName` or `userPrincipalName`.

ldap_search_timeout

Specifies the timeout in seconds for ldap_search. The server default value is 60 seconds.

ldap_principal

Specifies the DN of a service account with sufficient access rights to locate user entries in the directory. Consists of attribute=value pairs, separated by commas. This parameter is required when the LDAP provider is configured with a security setting that requires credentials in order to initiate a search for a user, group, or related information.

ldap_credentials

Contains the password of the service account defined in ldap_principal.

6. Click Next.

The server will try to connect and get User and Group properties. If it is not successful, you must manually edit User and group properties.

7. If the server could not connect with just the Connection Properties, enter values for the User and Group properties.

Note: If the properties for a specific category are not visible, click the down arrow on the separator bar for that category to display them.
**User properties**

ldap_user_base

Specifies the DN of the entry that serves as the starting point for the search. Consists of attribute=value pairs, separated by commas.

ldap_user_scope

Specifies the scope with which the LDAP realm should search for users. Select *Subtree, Onelevel, or Base*:

*Subtree* scope indicates that the LDAP realm should search everything under the base DN.

*Onelevel* scope tells the LDAP server to only search entries one level down from the base DN.

*Base* indicates that the search should be done at the search base only.

The server default is *Subtree*.

ldap_user_class

Specifies the object class used when searching for user entries. The server default is *person*.

ldap_user_attribute

Specifies the LDAP attribute used when searching for user entries. *uid* is the default value for LDAP and *sAMAccountName* is the suggested value for Active Directory. One possible reason to change the default value would be to allow users to logon with an email address instead of a user ID. In this case, you might change the value to *mail* or *userPrincipalName* (if this corresponds with the name of the appropriate attribute in your directory).

ldap_user_group_attribute

Specifies the LDAP attribute used to identify a group in a user object.

The Active Directory standard is *Memberof*.

ldap_user_description

Specifies the name of the attribute whose value contains description of an object (user, group). The server default is *description*.

ldap_user_email

Specifies the name of the attribute whose value contains the user email address. The server default is *mail*.

**Note:** ldap_user_class, ldap_user_attribute, ldap_group_class, ldap_group_attribute are parameters that form a search filter.
The search filter standard syntax conforms to the following structure:

\[(\text{Property}\_\text{Name}=\text{Property}\_\text{Value})(\text{Property}\_\text{Name}=\text{Property}\_\text{Value})\]

If you change value of the ldap_user_class and ldap_group_class parameters to an asterisk (*), the search filter syntax can be reduced to the following simplified form (although group support will not work properly):

\[(\text{Property}\_\text{Name}=\text{Property}\_\text{Value})\]

By specifying an asterisk for these parameters, you achieve simplified search filter syntax, but in effect, disable group support.

**Group properties**

*ldap_group_base*

Specifies the DN of the entry that serves as the starting point for the search. The server default is the *ldap_user_base* value.

*ldap_group_scope*

Specifies the scope with which the LDAP realm should search for groups. Select *Subtree*, *Onelevel*, or *Base*:

- **Subtree** scope indicates that the LDAP realm should search everything under the base DN.
- **Onelevel** scope tells the LDAP server to only search entries one level down from the base DN.
- **Base** indicates that the search should be done at the search base only.

The server default is *Subtree*.

*ldap_group_class*

Specifies the object class used when searching for group entries. The server default is *groupofuniquenames*. The Active Directory standard is *group*.

*ldap_group_attribute*

Specifies the LDAP attribute used to identify the name of the group. The server default is *cn*.

*ldap_member_attribute*

Specifies the LDAP attribute used to identify users in a group. The server default is *uniqueMember*. The Active Directory standard is *Member*.

*ldap_nested_groups*

Disables or enables LDAP nested groups support. Select *No* or *Yes*. The server default is *No*, which disables nested group support.
8. To test the connection, click *Test*.

   A Test LDAP Connection logon window opens.

   a. Enter a valid user ID and password for this LDAP security provider.
   b. Click *Continue*.

   If your configuration and credentials are valid, a window opens telling you that you were successfully authenticated.

   If they are not valid, you will get a corresponding message.

9. To save this configuration, click *Save*.

   The Change Effective Security Provider(s) page opens.

   a. Select a Security Provider name from the drop-down list.

      **Note:** Each time you select an LDAP Security Provider, another Security Provider drop-down box is generated.

   b. Enter or select the user ID of the Server Administrator. The user must be a valid server administrator in the LDAP database.

   c. If the server was not started configured for an LDAP security provider, the button at the bottom of the page says *Apply and Stop Server*. Click the button and manually start the server configured for an LDAP security provider.

      If the server is already running configured for an LDAP security provider, the button at the bottom of the page says *Apply and Restart Server*. Click the button and wait for the server to restart.

10. If the server was started configured for an OPSYS security provider, click the *Apply and Stop* button. Otherwise, click the *Apply and Restart* button.

    - If you click *Apply and Stop*, the server stops; proceed with Step 9.
    - If you click *Apply and Restart* button, the server restarts configured for an LDAP security provider.

    **Note:** For more information about changing security providers, see *Considerations for Changing the List of Security Providers From the Web Console* on page 90.

11. If the server is not running, start it using the instructions for your platform.

    The server will start configured to use an LDAP security provider.

12. Examine the edaprint.log file. If it indicates errors, stop the server, then start it with security OFF to correct the errors.
13. Restart your browser and connect to the Web Console. When prompted, enter a valid LDAP user ID and password.

14. When you start the server using an LDAP security provider, you can select an LDAP Provider from the Security Provider drop-down list. By default, the primary (first) LDAP security provider is selected.

**Note:** A common problem when switching from OPSYS to LDAP is the existence of files in EDATEMP that cannot be removed due to insufficient privileges. To handle this problem, use edastart -cleardir (or member ICLRDIR on the z/OS platform) with EDAEXTSEC=OPSYS to clear the directory before switching.

**Procedure:** How to Remove an LDAP Security Provider From the Web Console

1. Logon to the server with Server Administrator credentials.

2. Select Access Control.

   The Access Control page opens.

3. Right-click the security provider that you want to remove in the Security Providers folder and select Remove from the context menu.

   A dialog box opens asking you to confirm that you want to remove the provider.

4. Click OK.

**Reference:** LDAP Vendor Library Prerequisites

**Important:** Although the Server supports a number of vendor libraries for each platform, as described in the following chart, Information Builders recommends that, whenever possible, you use the native libraries for your Operating System.

**System Requirements.** An LDAP Security provider requires the appropriate LDAP vendor library files to be available to the server at run time:

1. If the LDAP vendor library files are not currently available on the server platform, download them from the appropriate vendor Web site, unzip them if necessary, and transfer them to the server platform.

2. Edit the library path or (on Windows) the system path to include the location of the library files.

**Windows:** The LDAP vendor library files for Windows systems are:
**IBM z/OS and IBM i:** The LDAP vendor library files for IBM z/OS and IBM i systems are:

<table>
<thead>
<tr>
<th>OS</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS</td>
<td>statically linked</td>
</tr>
<tr>
<td>IBM i</td>
<td>statically linked</td>
</tr>
</tbody>
</table>

**UNIX:** The LDAP vendor library files for UNIX systems are:

<table>
<thead>
<tr>
<th>OS</th>
<th>Vendor</th>
<th>IBM</th>
<th>Novell</th>
<th>OpenLDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>libldap50.so libnsspr4.so libnss3.so libplc4.so libplds4.so libprldap50.so libssasl.so libssl3.so libssldap50.so (64 bit NA)</td>
<td>statically linked</td>
<td>libldapsdk.so (64 bit NA)</td>
<td>N/A</td>
</tr>
<tr>
<td>OS</td>
<td>Vendor</td>
<td>IBM</td>
<td>Novell</td>
<td>OpenLDAP</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-----------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td><strong>Sun</strong></td>
<td>(Sun ONE Directory Server Resource Kit 5.2.1, except as noted)</td>
<td>statically linked</td>
<td>libldapsdk.sl</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>libldap50.sl</td>
<td>(64 bit NA)</td>
<td>libldapssl.sl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>libnspr4.sl</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libnss3.sl</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libplc4.sl</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libplds4.sl</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libprlldap50.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libasasl.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libssl3.sl</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libsslldap50.sl</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(see notes following chart)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Linux</strong></td>
<td>libldap50.so</td>
<td>libibmldap.so</td>
<td>libldapsdk.so</td>
<td>libldap_r.so</td>
</tr>
<tr>
<td></td>
<td>libnspr4.so</td>
<td>(64 bit NA)</td>
<td>libldapssl.so</td>
<td>libiblber.so</td>
</tr>
<tr>
<td></td>
<td>libnss3.so</td>
<td></td>
<td>(64 bit NA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>libplc4.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libplds4.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libprlldap50.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libasasl.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libssl3.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libsslldap50.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(64 bit NA)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SunOS 5.8</strong></td>
<td>libldap50.so</td>
<td>libibmldap.so</td>
<td>libldapsdk.so</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>libnspr4.so</td>
<td>(64 bit NA)</td>
<td>libldapssl.so</td>
<td></td>
</tr>
<tr>
<td></td>
<td>libnss3.so</td>
<td></td>
<td>(64 bit NA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>libplc4.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libplds4.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libprlldap50.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libasasl.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libssl3.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>libsslldap50.so</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(64 bit NA)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SunOS 5.9 and 5.10</strong></td>
<td>libldap.so</td>
<td>libibmldap.so</td>
<td>libldapsdk.so</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>(Native SunOS library)</td>
<td>(64 bit NA)</td>
<td>libldapssl.so</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(64 bit NA)</td>
<td></td>
</tr>
</tbody>
</table>

2. Server Security
Note:

- NA = Not Available from vendor.
- LDAP SSL for Novell is not supported on the AIX platform.
- Statically linked builds do not require external libraries.
- When using third-party libraries, complete products should be installed and the associated libraries must be on the library path of the server before start up. The library path is driven by different variables depending on platform (Windows: PATH, HP-UX: SHLIB_PATH, AIX: LIBPATH, USS: LIBPATH, IBM i: Library Path, Other UNIX's: LD_LIBRARY_PATH).
- Libraries shown in this table are the main libraries our module is linked with; they may, in turn, load a chain of system libraries, which also need to be present.
- Not all vendors provide 64 bit versions, but, when available, they are configurable.
- Before starting the configuration steps, independently verify your LDAP connection and any configuration ids being used. Testing may be done by downloading and installing an LDAP connection test tool such as Softerra LDAP Browser, at http://www.ldapbrowser.com/.

Example: Making Sun LDAP Library Files Available

To make Sun LDAP library files available to the server at run time:

   (Note that this URL is correct as of the date these Release Notes were published. Third-party URLs are subject to change.)

2. Click the Download link at the bottom right of the Web page. (Do not click the Downloads menu option at the top of the page.)
   The login page opens. You will be prompted for a registered user login or to register.

3. Enter your Sun username and password. If you do not have an account, click Register Now and follow the prompts to create an account and then log in. This is free.

4. Accept the license agreement.

5. Download the appropriate platform package. Select the optimized package, not the debug version.

6. Once downloaded, unzip the file, and then unzip the second zip file contained within the first.
7. Navigate to the directory in which you unzipped the downloaded file, and then cd to the lib subdirectory.

8. FTP the files you need (as indicated in *LDAP Vendor Library Prerequisites* on page 77), in binary format, to their own directory on the server platform.

9. Edit the library path to include the location of the library files you just FTPed.

**Configuring Custom Authentication**

**How to:**
Configure a Custom Security Provider

**Reference:**
Creating an Authentication Procedure for a Custom Provider
Creating a Procedure That Returns Users
Creating a Procedure That Returns Groups

CUSTOM security providers are used when the installation maintains non-standard repositories for users and groups, that is, when the standard methods like OPSYS and LDAP do not apply. An example of such a setup can be having RDBMS tables containing valid user IDs and their encrypted passwords, and also containing the mapping of users to groups. The customer may chose to access these tables using SQL SELECT statements, SQL Stored procedures, or Web Services. Typically these methods already exists and are used by other non-Information Builders components.

To enable the custom server security provider, the administrator needs to provide code that allows the server security module to perform these tasks:

- Authenticate the user based on user ID and password.
- Obtain all groups for a user (used at run time).
- Obtain all groups in the system (used for administrative actions).
- Obtain all users for a group and all users in the system (used for administrative actions).

The code for performing these tasks is written in the WebFOCUS language as TABLE FILE or SQL SELECT commands against the synonyms representing the SQL table, SQL Stored Procedure, or Web Service. The code can be debugged by running the server with security OFF and running the glue code from application folders. Once debugged, the code is deployed in EDACONF/catalog/xxx, and the CUSTOM provider made active.
A tutorial sample called WebFOCUS - Custom SQL Security Provider is available that creates examples of user and group storage and custom procedures that can be used as prototypes. To generate a tutorial, right-click an application on the Application page and select New then Tutorials from the context menu.

**Procedure: How to Configure a Custom Security Provider**


2. Enter values for the following parameters:

   **CUSTOM_PROVIDER**
   
   Is a name to assign to the security provider.

   **cust_authenticateuser**
   
   Is the name of the procedure that authenticates users. For information about creating an authentication procedure, see Creating an Authentication Procedure for a Custom Provider on page 84.

   If you do not specify an authentication procedure, you must have a default server administrator user ID and password to use when connecting to the server. A default server administrator user ID was configured during server installation.

   **cust_usersbygroup**
   
   Is the name of the procedure that returns the list of all users or, if the group name is passed to the procedure, the list of all users in the group. For information about creating a procedure that returns users, see Creating a Procedure That Returns Users on page 86.
cust_groupsbyuser

Is the name of the procedure that returns the list of all groups or, if a user ID is passed to the procedure, the list of all groups for the user ID. For information about creating a procedure that returns groups, see Creating a Procedure That Returns Groups on page 87.

cust_service

Defines the data service to execute stored procedures specified in the custom security provider.

trust_ext

Specifies whether the server should accept trusted client connections using this provider.

The procedures can be located under the server configuration directory (EDACONF/catalog), the installation directory (EDAHOME/catalog), or in an application that is on the application path of every user.

We suggest that the synonyms used by custom provider procedures be copied to the directory EDACONF/catalog/custom. This will cause the server to protect adapter connections used by custom procedures. This means that only the Server Administrators and users with privilege WSCFG will have access to security data in those synonyms. All other users attempting to use this adapter connection will get an unauthorized message.

3. To test your configuration, click Test.

4. When you are satisfied with the test results, click Save.

Your custom security provider is listed under the CUSTOM item on the Access Control tree.

5. Select the appropriate primary security provider from the drop-down list and click Next.
If you are changing primary providers, you may be asked to select or enter a Server Administrator user ID.

6. Click Save and Restart Server.

**Reference: Creating an Authentication Procedure for a Custom Provider**

The authentication FOCEXEC for a custom provider must check the user ID and password passed to the Reporting Server against the custom provider data source and return a code that defines to the Reporting Server the status of those credentials.

The server calls your authentication FOCEXEC using the following syntax:

```
EX ptauth ID=user1, PASSWD=pass1
```

where:

**ptauth**

Is the authentication procedure entered in the cust_authenticateuser field of the CUSTOM provider configuration page.

A simple example of an authentication procedure, ptauth.fex, is provided in the home/catalog directory.

**user1**

Is the user ID to be authenticated. It is stored in a variable named &USERID.

**pass1**

Is the corresponding password to be authenticated. It is stored in a variable named &PASSWD.

The authentication procedure must authenticate this user ID and password combination against the data source that contains the user credentials.

If the password is stored in encrypted form in the data source, the authentication procedure must encrypt the password using the same encryption process prior to authenticating it.

The authentication procedure must return a code to the Reporting Server based on the result of the authentication process. The syntax is:

```
-SET &a = SETAUTH(error_code, 'primary_group');
```

where:

**a**

Can be any valid variable name, for example &A.
error_code

Must be one of the following integers:

0
Indicates that the user ID and password are valid.

1
Indicates that the user ID is invalid.

2
Indicates that the password is invalid.

3
Indicates that the user ID has expired.

4
Indicates that the password has expired.

5
Indicates that another error occurred.

primary_group

Returns the primary group for the user. Enter the group ID enclosed in single quotation marks. If there is no primary group, enter two consecutive single quotation marks. For example:

-SET &A = SETAUTH(2, '');

You can provide messages in the authentication procedure using the -TYPE command. For example:

-INVALIDPASS
- TYPE invalid password
-SET &A = SETAUTH(2, '');

The message will display when you click the Test button on the CUSTOM Security Configuration page.

When a user actually attempts to sign in to the server, the server will:

- Sign the user in, if the credentials are valid.

- Prevent the user from signing in, if the credentials are not valid. In this case, the server will display a standard message on the sign-in page identifying the nature of the error.
Creating a Procedure That Returns Users

The procedure entered in the cust_usersbygroup field on the CUSTOM Provider Configuration page has to return either all users or, if passed a group ID, all users for that group.

The procedure should retrieve the following fields (some are mandatory, some are optional) from the data source that stores all user IDs and their properties:

**User ID**
- Mandatory
- Contains alphanumeric user IDs with a maximum length of 99 (A99).

**User Description**
- Optional
- Contains alphanumeric descriptive information with a maximum length of 97 (A79).

**User Email Address**
- Optional
- Contains an alphanumeric email address with a maximum length of 127 (A127).

**Group ID**
- Mandatory
- Contains alphanumeric group IDs with a maximum length of 99 (A99).

After retrieving the fields, you must issue the PCHOLD FORMAT COMT FORMATTED command to place them in a comma-delimited file with each field value enclosed in double quotation marks. For example:

```plaintext
ON TABLE PCHOLD FORMAT COMT FORMATTED
ON TABLE SET PAGE-NUM OFF
ON TABLE SET HOLDATTR OFF
```

The procedure should be able to retrieve the list of all users and the user list for one group.
The following procedure sets the variables &ID, &NAMEFILTER, and &DESCFILTER to _FOC_NULL by default.

It tests these variables to see if a specific group ID, a filter for the user ID, or a filter for the user description was passed to the FOCEXEC:

```
-DEFAULT &ID='FOC_NULL',&NAMEFILTER='FOC_NULL',&DESCFILTER='FOC_NULL';
TABLE FILE USERINFO
PRINT DST.USERID DST.USERDESC DST.UEMAIL
IF GROUPID EQ &ID
IF USERID CONTAINS &NAMEFILTER
IF USERDESC CONTAINS &DESCFILTER
ON TABLE PCHOLD FORMAT COMT FORMATTED
ON TABLE SET PAGE-NUM OFF
ON TABLE SET HOLDATTR OFF
END
```

This procedure can be run as follows:

- To list all users:
  ```
  EX ptusers
  ```
- To list users who are members of group group1:
  ```
  EX ptusers ID=group1
  ```
- To list users where the user description contains the characters One:
  ```
  EX ptusers DESCFILTER='One'
  ```

A simple example of a users procedure, ptusers.fex, is provided in the home/catalog directory.

**Reference:** Creating a Procedure That Returns Groups

The procedure entered in the cust_groupsbyuser field on the CUSTOM Provider Configuration page has to return either all groups or, if passed a user ID, all groups for that user.

The procedure should retrieve the following fields (some are mandatory, some are optional) from the data source that stores all user IDs and their properties:

**Group ID**

- Mandatory
- Contains alphanumeric group IDs with a maximum length of 99 (A99).

**Group Description**

- Optional
- Contains alphanumeric descriptive information with a maximum length of 97 (A79).
User ID

Mandatory

Contains alphanumeric user IDs with a maximum length of 99 (A99).

After retrieving the fields, you must issue the PCHOLD FORMAT COMT FORMATTED command to place them in a comma-delimited file with each field value enclosed in double quotation marks. For example:

```
ON TABLE PCHOLD FORMAT COMT FORMATTED
ON TABLE SET PAGE-NUM OFF
ON TABLE SET HOLDATTR OFF
```

The procedure should be able to retrieve the list of all groups and group list for one user. The following procedure sets the variables &ID, &NAMEFILTER, and &DESCFILTER to _FOC_NULL by default.

It tests these variables to see if a specific user ID, a filter for the group ID, or a filter for the group description was passed to the FOCEXEC:

```
-DEFAULT &ID=_FOC_NULL',&NAMEFILTER=_FOC_NULL',&DESCFILTER=_FOC_NULL'
TABLE FILE USERINFO
PRINT GROUPID GROUPDESC
IF USERID EQ '&ID'
IF GROUPID CONTAINS &NAMEFILTER
IF GROUPDESC CONTAINS &DESCFILTER
BY GROUPID NOPRINT
ON TABLE SET PAGE-NUM OFF
ON TABLE SET HOLDATTR OFF
ON TABLE PCHOLD FORMAT COMT FORMATTED
END
```

This procedure can be run as follows:

- To list all groups:

  ```
  EX ptgroups
  ```

- To list groups that have user *user1* as a member:

  ```
  EX ptgroups ID=user1
  ```

- To list groups where the group name contains the characters *yyy* and the group description contains the characters *xxx*:

  ```
  EX ptgroups NAMEFILTER='yyy' DESCFILTER='xxx'
  ```

A simple example of a groups procedure, ptgroups.fex, is provided in the home/catalog directory.
Authenticating Users Across Multiple Security Providers

How to:
Change the Security Provider List

Reference:
Considerations for Changing the List of Security Providers From the Web Console

The Reporting Server can search across multiple LDAP sources, DBMS providers, an OPSYS provider, and a PTH server when authenticating users.

When authenticating or assigning privileges for a provider that is not the primary provider, the user ID is a two-part name consisting of the provider name and the user ID:

\textit{provider.userid}

The authentication is done based on a two-part name.

The Server Administrator can add and remove security providers from the list at any time.

For instructions on configuring PTH and LDAP security providers, see \textit{Configuring PTH Authentication} on page 59 or \textit{Configuring LDAP Authentication} on page 70.

Procedure: How to Change the Security Provider List

If you want to change the list of security providers:

1. Logon to the server with Server Administrator credentials.

2. Click Access Control, and the Manage Providers page appears in the right pane. You can also right-click the Access Control folder and select Manage Providers from the context menu.

   The Manage Providers page opens.

3. You change the status of a provider by selecting a value from its drop-down list. If you make a provider Primary, the provider that previously had that status changes to Secondary.

Note:

- You can change the effective administrator ID by going to the Access Control page, right-clicking Access Control at the top of the Access Control tree, and selecting Settings from the context menu.

- When registering and assigning privileges for a user or group, the server uses a two-part name consisting of the provider name and the user or group name (for example, ldap2/user1 or ldap2/group3).
Considerations for Changing the List of Security Providers From the Web Console

You can configure multiple security providers using the Web Console. A security provider can have the status Primary, Secondary, or Inactive. It is important that there be a valid server administrator ID for one of the active (Primary or Secondary) security providers so that you can use it to connect to the Web Console or Data Management Console as a Server Administrator after changing the active security providers list.

When you switch between security providers from the Web Console, you will be prompted to restart the server.

Environment variable EDAEXTSEC is only used to disable server security.

Enabling Trusted Connections

You can enable trusted connections separately for each security provider.

You can configure a security provider to accept trusted connections by setting its trust_ext value to y.

1. Right-click a security provider on the Access Control tree and select Properties on the context menu. This example shows a PTH security provider, but the same setting is available for all security providers.

   The Configuration page for that security provider opens.

2. From the trust_ext drop-down list, select y.

   This setting is available for all types of security providers.
3. Click Save and Restart Server.

**Identifying a Default Provider for Trusted Groups**

When multiple security providers are configured, one must be identified as the default provider for trusted connections when WebFOCUS or other client software sends a trusted group ID without a security provider to the server.

To set the default provider for trusted groups:

1. On the Access Control page, click Settings on the ribbon, or right-click the Access Control folder and select Settings from the context menu.

The Access Control Settings page opens, as shown in the following image.

**Access Control Settings**

![Image of Access Control Settings](image.png)

2. You can select a security provider that accepts trusted connections from the trusted_group_default_provider drop-down list. You can also enter IP addresses to be mapped to a specific provider, if no provider name is supplied by the client.
Setting an Anonymous User ID

How to:
Set an Anonymous User ID

An authorized server administrator can set an anonymous user ID that can access the Web Console when the user ID/password fields on the Web Console login screen are blank and the user clicks Log in.

This anonymous user ID provides the ID and, in turn, the user rights for the Web Console and the server. Further configuration for the anonymous user can be achieved by creating a user profile for the anonymous user ID. If an anonymous ID matches a user in the admin.cfg list, the applicable role and privileges are applied.

Note: On Windows, for security provider OPSYS only, you must turn IWA security off to use this feature. From the Workspace folder in the navigation pane, open the Special Services and Listeners folder, right-click TCP/HTTP, and select Properties. Click the Security IWA check box to deselect it.

Procedure: How to Set an Anonymous User ID

1. Log on to the Web Console using a user ID that has server administration rights.
2. Select Access Control from the Web Console menu bar.
3. Right-click Access Control in the navigation pane, and select Settings.
   The Access Control Settings pane opens.
4. Enter a user ID in the anonymous_id field.
5. Enter a password in the anonymous_pass field and repeat it in the Confirm Password field.
6. Click Apply and Restart Server.

Configuring User Password Settings

In this section:
Viewing or Changing the Password Separator Character
Enabling Password Changes From the Web Console Sign-in Page
Sign-in Password Expiration Warning

You can configure the following password settings for any security provider:
View or change the password separator character.

Enable users to change passwords from the Web Console login page.

Control the start time of warning messages on operating systems that support password expiration.

### Viewing or Changing the Password Separator Character

**How to:**

View or Change the Password Separator Character

When an application has the option to change a user password, the old and new passwords are sent to the server using a separator character (by default, a comma). For example:

```
old_password, new_password
```

The separator character is defined by the `password_change_delimiter` field. The separator needs to be reset if the current separator character is contained in the password itself or if it is allowed by the server.

This feature is not supported when Security is OFF.

**Procedure:** **How to View or Change the Password Separator Character**

1. From the Web Console menu bar, select **Access Control**.
2. Right-click **Access Control** in the navigation pane, and select **Settings**.

   The Access Control Settings page opens.

3. In the `password_change_delimiter` field, enter a single character to use as the delimiter between an old and new password. (The default character is a comma.)

   Note that you cannot use the designated `password_change_delimiter` character in a password.

4. Click **Apply and Restart Server**.
Enabling Password Changes From the Web Console Sign-in Page

**How to:**
Enable Password Changes From the Web Console Sign-in Page

A Server Administrator can allow users to change their password from the Web Console sign-in page. By default, users cannot change their passwords from the Web Console sign-in page.

**Procedure:** How to Enable Password Changes From the Web Console Sign-in Page

1. Sign in to the Web Console with Server Administrator privileges.
2. From the Web Console menu bar, choose Access Control.
3. Right-click Access Control in the navigation pane, and select Settings, or click Settings on the ribbon.
   The Access Control Settings page opens.
4. Enter y in the password_change_wclogin field. The default is n.
5. Click the Apply and Restart Server button.

Sign-in Password Expiration Warning

**How to:**
Initiate Notification of an Imminent Password Expiration

On Operating Systems that support password expiration, you can specify that a warning message be displayed a specified number of days prior to the expiration date. The message will appear after the initial login screen. You must then click the Continue button to open the Web Console. Users can employ standard tools to change their passwords before expiration occurs.

**Note:** The password expiration warning is supported only on operating systems where IDs are configured to expire and this extended security feature is active for the user ID. However, expiration warning is not currently supported on the Windows platforms.

**Procedure:** How to Initiate Notification of an Imminent Password Expiration

1. From the menu bar, select Workspace.
2. In the navigation pane, expand the Special Services and Listeners folder, then click TCP/HTTP and select Properties from the context menu. The Listener Configuration pane opens.

3. Expand the Advanced group.

4. In the PASS_EXPIRE_NOTIFICATION field, enter the number of days prior to expiration that you want the warning to begin to appear when a user whose password is about to expire logs in.

5. Click the Save and Restart Server button.

**Configuring Privileges and Other Authorizations**

*In this section:*
- Configuring DBMS Authorization
- Configuring Server DBA Security
- Calculating Privileges for Any Registered or Unregistered User or Group
- Permissions for Server Application Files and Directories Using a Non-OPSYS Security Provider
- File Permissions for an OPSYS Security Provider
- Configuring General Server and Web Console Actions
- Configuring Groups
- Configuring Roles
- Registering Users and Groups in a Role

WebFOCUS users are authenticated against one of the supported authentication sources (OPSYS, LDAP, DBMS, PTH internal, or CUSTOM). The underlying security system may divide users into groups. For example, for OPSYS security the groups are defined in the operating system, and in LDAP they are defined in the LDAP database. With a PTH security provider, the server file named admin.cfg defines groups. A CUSTOM provider executes custom requests against user-defined security storage, for example an SQL database.

To assign privileges to server application and data files, you must register groups of users to a server role and customize the privileges. In exceptional cases, you may register individual users to a server role and customize its privileges. The authorizations then depend on the privileges assigned to the role.
With any type of security, access to the following categories of resources must be controlled:

- **DBMS data.** Access is controlled by the CONNECTION attributes in effect at the time the data is accessed. The connections are stored in user or group profiles or in the server edasprof profiles.

- **Access to Web Console system functions.** This category includes functions such as change of server profiles, creation of metadata, or starting the servers. Access to these functions is defined by the role assigned to the user or group and is stored in the admin.cfg file.

- **WebFOCUS repository files that constitute the application.** These files include FOCEXECs, Master and Access Files, HTMLFORMs, and application files that are stored in the application directories.

The Server provides an Access Control function that enables the Server Administrator to create and edit permissions for different categories of users and groups. These permissions define whether specific users and groups can read, write, and/or execute WebFOCUS repository files and perform various Web Console system functions. To open the Access Control page, select Access Control on the Web Console menu bar.

In addition to users and groups, the server supports security subjects called roles. The server comes with a set of standard roles, and these roles come with a fixed set of general privileges. For more information about these standard roles, see Configuring Roles on page 123.

The Server Administrator can register roles, groups, and users. When registered, they are assigned a set of general privileges and file access privileges. By default, groups inherit privileges from the roles they are assigned, and users inherit their privileges from the groups or roles to which they are assigned. The Server Administrator can create new roles and customize privileges for any role, group, or user. The Server Administrator always has full privileges, and those privileges are not adjustable.

It is considered good practice for a large user community to define access rules on the group level and not on the individual user level. This technique allows volume user provisioning to be handled outside of WebFOCUS Server software (for example in the LDAP server). The WebFOCUS Server in general registers group access rights, plus some individual users as an exception, such as managers or special project people.

The following defines the order of precedence for access rights:

- User access overrides group access, and group access overrides role access.

- If the user belongs to multiple groups, the server group_profile setting determines whether only the primary group is in effect or whether the user can select a group at logon.
Configuring DBMS Authorization

With DBMS authorization, the main object to be protected is the DBMS resident data that the server reads and writes. Access control is implemented using ENGINE CONNECTION_ATTRIBUTES statements that define the security attributes that are used by the server agent for connecting to the DBMS. The connection security type depends on the DBMS and can be one of three subtypes:

- **Explicit.** The userid/password is stored in a profile (encrypted).
- **Password passthru.** The userid/password combination or cookie, such as MYSAPSSO2, that were provided during the connection to the server is passed to the DBMS connection.
- **Trusted.** This type of connection applies to security provider OPSYS where the agent operating system process impersonates the user, and the DBMS connection is derived from that process.

The CONNECTION_ATTRIBUTES statement itself can be defined in the user, group, role or server profile, and they override each other in this order.

It is common initially to create connections in the edasprof server profile. They will then be inherited by all users. Subsequent configuration steps may define connections on other levels, such as the group or user level.

The CONNECTION_ATTRIBUTES statement in effect passes the credentials to the DBMS, and the DBMS server ensures the correct access control: read and read/write rules on the DBMS tables, views, columns, and rows.

For more information about the CONNECTION_ATTRIBUTES command, see the Adapter Administration manual.

Configuring Server DBA Security

The server engine can add an additional level of access control by defining DBA rules in synonyms to restrict access to columns and certain data values. This applies only to data access using the WebFOCUS language, and not to Direct SQL Passthru requests. For more information about Server DBA, see the Describing Data With WebFOCUS Language manual.

Calculating Privileges for Any Registered or Unregistered User or Group

The server administrator can calculate the privileges of any registered or un-registered user or group on the server by right-clicking the Access Control tree and selecting Show Privileges from the context menu.
The Show Privileges page opens.

### Show Privileges

- **Type**: User
- **Security Provider**: OPSYS
- **User ID**: 

When you click Next, the server calculates the appropriate privileges and returns a page of Properties for registered users and groups with tabs for General Privileges and File/directory Privileges. This page also indicates whether the security subject you chose is registered and, if not, which privileges it inherits. If your server is configured with profile_setting=all, and you select a user who belongs to multiple registered groups, the privileges of all will be combined in the display.
Permissions for Server Application Files and Directories Using a Non-OPSYS Security Provider

Example:

Search for Privileges for Users Who Are Not Registered
Search for Privileges for Registered Users
Useful Combinations of Permissions
Sample Permissions

Reference:

Understanding Access Control Permissions
Access Control vs. APP PATH
Permissions for FOCCACHE and EDATEMP
Access Control Implications For Scheduling

The Server Administrator can specify read/write, execute, and list privileges for files in application directories and for the directories themselves. This control is in addition to operating system file access control which follows the current umask setting.

The Server Administrator can view or edit File and Directory privileges by clicking the Directory/File Privileges tab on the Access Control page for a role, group, or user. The Server Administrator can view and edit General privileges for other users, groups, and roles.

Non-Server Administrator users can right-click any object on the left panel and select Properties to see their privileges for that file or directory object. The Server Administrator has the option to manage privileges by right-clicking an object.

By default, for compatibility with previous releases, file access control allows complete access to all files and directories. However, the Server Administrator can reset this default by right-clicking a row in the table and choosing Edit Privileges. For information, see How to Configure General Privileges on page 110.

After initial server installation, the Server Administrator should review individual privileges for each role and customize them if needed. For example, the write privileges for basic users to applications on the APPPATH can be removed.
File privileges can be defined on the lowest level, such as a specific file and specific user, but the recommended policy is to define them on the application folder level and on the role and group levels to reduce administrative overhead. Privileges defined on the application level will apply to (be inherited by) all files in this application and by all nested (lower level) application directories, unless overridden on a lower level. The same applies to roles, groups, and users. Privileges defined on the group level will be inherited by the users in the group, unless overridden by explicit user registration.

The following schematic shows the flow of privilege assignments and inheritance.
In effect, when the system opens a file such as app1/app2/car.mas for user user1 in group1 belonging to role1, the server uses a specific search path until the privileges are found. The server administrator can also see the directory and file privileges from the Application Directories page by right-clicking an application and selecting the Privileges option. Users without administrator rights can see the privileges from the file or directory Properties option.

**Example: Search for Privileges for Users Who Are Not Registered**

The following describes the search path if user1 is not registered or has not been assigned a role in admin.cfg. Assume the user is in group1 and group1 is registered under role1:

1. App1/app2/car.mas for group1.
2. App1/app2 for group1.
3. App1 for group1.
4. * for group1
5. App1/app2/car.mas for role1.
6. App1/app2 for role1.
7. App1 for role1.
8. * for role1.

If group1 were not registered, the user would be assigned the default role.

**Example: Search for Privileges for Registered Users**

If user1 is registered in admin.cfg, the server uses the following search path. The lines ending with an asterisk (*) denote a recommended practice:

1. App1/app2/car.mas for user1.
2. App1/app2 for user1.
3. App1 for user1.
5. App1/app2 for role1.
6. App1 for role1.
7. * for role1.

If the user is registered under a role, the server does not consider group privileges when access to the file or directory is calculated.
Understanding Access Control Permissions

When file and directory access control privileges are being set, the registration of physical file locations is not saved using a full path reference in all cases. When a location is in a folder under one of the server internal locations EDACONF, EDAHOME, APPROOT, or EDAPRFU, it is registered as a reference that is relative to that server location. The physical paths to EDACONF, EDAHOME, EDAPRFU and APPROOT are defined when the server is installed.

For example, if the privilege is for the directory D:\ibi\srv77\wfsV8\etc, and if the EDAHOME location has been established as D:\ibi\srv77\wfsV8, any privilege registered for that location will be registered using a relative reference based on EDAHOME:

```plaintext
admin_privilege = (EDAHOME)\etc;PRRUN
```

Then, if a new server release is installed in a different file system, the privilege will be applied to the correct directory in the new file system because the EDAHOME location will contain the correct directory reference for that system.

Registration of files and directories located outside of EDACONF, EDAHOME, APPROOT and EDAPRFU locations are registered as full physical paths.

Access Control parameters are saved in the server admin.cfg file.

```plaintext
{admin_id|admin_group} = name
admin_privilege = object; privilege_name, privilege_name[, ...]
```

where:

- **name**
  - Is a user (admin_id) or group (admin_group) name.

- **object**
  - Defines the directory or file path.
  - Can be one of the following:
    - Physical path to the file or directory.
      - For example
        ```plaintext
c:\myapp\appl c:\myapp\myfile.foc
```
      - where * is a token that designates all physical files on the system.
    - A path relative to one of the server internal locations EDACONF, EDAHOME, APPROOT, or EDAPRFU.
      - For example:
        ```plaintext
        (APPROOT)\appl (APPROOT)\ibisamp\car.foc
        ```
**privilege_name**

Defines the type of access. Can be one of the following:

- **ARREAD** reads and displays the content of a file to the user. For example, the user can see (but not change) procedures and synonyms. The user needs read permission to open data files.

- **ARWRT** Write allows the user to read, edit, and write procedures and metadata.

- **PRRUN** Execute. This privilege is typically given to end users who need to execute FOCEXECs and use Master Files and relevant utility procedures. However, the data file used by a FOCEXC and Master File only requires read permission.

- **ALIST** allows the user to list and view files and folders on the application tree or the output of a deferred execution run.

- **ANONE** revokes all permissions.

Note that definitions in the admin_privilege strings can contain relative path references for application directories under APPROOT and other internal locations. However, fully-qualified physical paths are also respected.

**Example: Useful Combinations of Permissions**

1. **Full Access** - read, write, execute, list

   This setting is typically used by developers on applications that they develop and create directly.

   This is the default for all files not explicitly customized, unless the default is reset. To explicitly specify full access, issue the following setting in admin.cfg:

   ```
   admin_privilege = directory/file_path; ARWRT, AREAD, PRRUN, ALIST
   ```

2. **Read, execute, and list.**

   This permission can be used by developers for other utility application directories that they invoke while developing their own.

   For example, a developer can keep common synonyms and utility FOCEXECs in such a directory. Of course, the person that creates such a directory needs full access to it, but all others only need read and execute. Read is needed to open data files.

   ```
   admin_privilege = directory/file_path; AREAD, PRRUN, ALIST
   ```

3. **Execute.**

   This permission is typically given to end users who need to execute FOCEXECs and use Master Files and relevant utility procedures.

   ```
   admin_privilege = directory/file_path; PRRUN, ALIST
   ```
4. Execute and hidden.

This is the same as Execute except that it is not shown on the Web Console.

```
admin_privilege = directory/file_path; PRRUN
```

5. List and View.

This allows the user to view reports from deferred jobs. This privilege is lower than execute.

```
admin_privilege = directory/file_path; ALIST
```

6. No Permissions.

This revokes all permissions from the directory or file.

```
admin_privilege = directory/file_path; ANONE
```

**Example: Sample Permissions**

The privileges for locations relative to EDACONF, EDAHOME, APPROOT, and EDAPRFU are set using the following syntax

```
admin_privilege=(APPROOT)/baseapp;ARREAD, ARWRT, PRRUN, ALIST
```

However, existing privileges set using the full physical name are respected.

These examples use the following directories and files:

```
/u1/pgmabb/myapp
/u1/pgmabb/myapp/data1.dat
```
The following shows a sample permission distribution list:

```plaintext
admin_id = chief_developer
BEGIN
admin_level = APP
admin_privilege = *; ARWRT,AREAD,PRRUN,ALIST
admin_privilege = (APPROOT)/work_app; AREAD,PRRUN,ALIST
END
admin_group = team_developer
BEGIN
admin_level = APP
admin_privilege = (APPROOT)/main_app; AREAD,PRRUN,ALIST
admin_privilege = (APPROOT)/synonym_app ; AREAD,PRRUN,ALIST
admin_privilege = (APPROOT)/work_app; ARWRT,AREAD,PRRUN,ALIST
admin_privilege = /u1/admin/server/prod_data ; AREAD,ALIST
END
admin_group = end_user
BEGIN
admin_level = USR
admin_privilege = (APPROOT)/main_app; PRRUN,ALIST
admin_privilege = (APPROOT)/synonym_app ; PRRUN
END

These security declarations define the following roles and permissions:

- A user with the ID chief_developer has full access to all applications, including main_app and synonym_app, but he has no write access to work_app for the team_developer group.

- A user that belongs to the group team_developer develops applications in his own directory but needs Read and Execute access to main applications to see what was done before. A user with this role has read-only access to production data in /u1/admin/server/prod_data. When the developer user is finished, the chief_developer copies his procedures to the main_app.

- The end_user group contains end users who need to execute the procedures from the main_app, but do not need to see synonym_app on the Web Console.

**Reference:** Access Control vs. APP PATH

APP PATH defines two main aspects of the system:

- Search path for applications at run time for one part file reference such as TABLE FILE CAR.

- List of applications shown on the Web Console and Data Management Console (DMC) application tree for the Application page.

The privileges are on the physical directories, not the application, so if the application is mapped to a different directory, the privileges from the new directory will be in effect.
Note that with Access Control, all such access is subject to Access Control rules which take precedence over APP PATH:

- A one-part file reference that searches APP PATH and finds a file in a directory without access will skip it and search further in APP PATH.

- A two-part file reference or FILEDEF attempting to access a file or directory without permission will produce an error.

- The Web Console and DMC will gray out actions such as saving a procedure or synonym where they are prohibited.

For example, user u1 has the following in his profile where both app1 and app2 contain file xxx.mas, and f1.fex:

APP PATH app1 app2 app3,

In admin.cfg for user u1, access to these applications defined as:

admin_privilege = /u1/app1; AREAD, PRRUN
admin_privilege = /u1/app2; PRRUN
admin_privilege = /u1/app3; ARWRT, AREAD, PRRUN

When user u1 tries to execute the FOCEXEC f1 (EX f1), the one from app1 will be executed. When user u1 tries to issue TABLE FILE xxx, the app1/xxx.mas will be opened, since it only needs Execute privileges.

When user u1 issues the following command, the app1/xxx.mas will be opened, since it requires Read privileges:

EDAGET MASTER, xxx, T, ANY

When user u1 tries to issue the following command ENCRYPT FILE XXX, the app1/xxx.mas will be read, and an attempt to rewrite it in place will be made. Since user u1 does not have sufficient privileges, an error will occur and an error message will be issued.

Protection against hacking

- The admin.cfg file itself cannot be accessed with a WebFOCUS command. This rule is enforced in the code.

- All files that are not covered by explicitly registered privileges are covered by the system wide default.

**Reference:** Permissions for FOCCACHE and EDATEMP

EDATEMP is a location where the server creates temporary files during agent connection. All of these files are deleted on disconnect to provide a clean environment for the next connection.
FOCCACHE stores temporary files during execution of one Web session. These temporary files can be stored in FOCCACHE for multiple agent connections, and data can be accessed through the Web Console and WebFOCUS Server. FOCCACHE is an internally mapped application directory to a unique physical location for each Web session.

Both of these locations have a full set of permissions for a connected user unless the default location has been overridden by HOLDDATA, HOLDMETA, and remapping of FOCCACHE from its default location using APP commands. In this case, the access controlled permissions are applied based on the admin role, group, or user.

**Reference: Access Control Implications For Scheduling**

The DataMigrator scheduler initiates requests based on procedures (flows) with scheduling headers that it finds in the application path. The procedures are submitted for execution using the user ID and related profiles that depend on the value of the sched_run_id keyword. If the option is set to the following value, the effective server administrator ID is used:

```
sched_run_id = server_admin_id
```

If the option is set to the following value, the user ID found in the flow is used:

```
sched_run_id = user
```

The encrypted password is taken from the admin.cfg file. If the user is registered without a password, trusted connection is used for the LDAP and OPSYS security modes on all operating systems except Windows.

If the installation has a large number of users, it is good practice to protect which procedures the users are allowed to schedule. The method to accomplish this is to define a special application directory, for example `schedule_app_1`, that contains process flows with scheduling headers only. The actual procedures can be in any other application directory including a home directory, for example `app2`. The process flows will contain references to the actual procedures, for example:

```
EX app2/myrpoc
```

A special scheduling directory such as `schedule_app_1` can be protected with file access privileges so that only a designated user ID, for example `user1` can write to it and create and modify schedules in it. The `user1.prf` profile should have `app1` in its application path.

The scheduler is configured to scan this application directory by setting the following keyword:

```
sched_scan_id=user1
```

This ensures that only the schedules located in `schedule_app_1` are in effect and that `user1` is the only user controlling the scope of scheduling.
File Permissions for an OPSYS Security Provider

Impersonation is when the server executes code in the context of an authenticated and authorized user. Access to files is controlled by the operating system security features in the native file systems. Files are protected according to the permissions set for the impersonated user.

Users who have server privileges to make configuration changes (update configuration files such as edaserve.cfg, admin.cfg, odin.cfg, or edasprof.prf) must also have operating system privileges to update those files.

The main file areas within a configuration are organized into four locations:

- **EDAHOME** (the software installation structure).
- **EDACONF** (the specific software configuration structure).
- **APPROOT** (the file structure for holding application-related programming files).
- **EDATEMP** (the runtime user area for server processes, which is normally located under the EDACONF area).

Permissions for new files depend on how the server is installed and started.

- **On UNIX, z/OS (HFS deployment), and IBM i**, the permission mask setting of the process (umask) that started the server is inherited down to the creation of each subdirectory or file with a few exceptions, and thus defines the permissions used for object creation.

- **On z/OS (PDS deployment)**, the rules (permissions) are set but the security package (RACF, ACF/2, or Top Secret).

- **On OpenVMS**, the permission mask of the process (SET PROTECTION= /DEFAULT) that started the server is inherited down to the creation of each subdirectory or file, and thus defines the permissions used for object creation.

- **On Windows**, the permissions are inherited down from directory to subdirectory, and the permissions for any object created are taken from its parent directory. So unless specific permissions are applied at any level, default permissions will depend on where the server was installed.
**Reference:** Consequences for Files Under the EDAHOME/EDACONF Hierarchy

All users who are expected to use the server must have Read/Execute access to files under the hierarchies. Server administrators that share common resources (such as admin.cfg), should be members of a group that provides writable access to those resources. Non-shared resources should provide each user or group with the specific permissions required.

**Reference:** Consequences for Files Under the APPROOT Hierarchy

Care must be taken when defining default permissions under APPROOT directories for application administrators who will create files that need to be accessed by regular users. When application files are written under any application, they are created according to the rules of ownership and default permissions applicable to the user who signed in to the Reporting Server. Thus, application developers must share a common default group if they are to work on a shared project.

**Reference:** Consequences for Files Under the EDATEMP Hierarchy

In a server that runs with security OPSYS, special conditions apply to the edatemp subdirectory and its contents. The basic principle is that agent subdirectories under edatemp are owned at any given moment by the user that the agent is impersonating.

With an OPSYS provider, this means that once a user connects to an agent, he is explicitly given ownership of his agent subdirectory, regardless of which user the agent impersonated during previous connections. This ownership and the inherited permissions defines how other users can access the connected user temporary files, if at all.

**On UNIX, z/OS (HFS deployment), and IBM i,** the edatemp subdirectory itself is an exception because it is set up similarly to the /tmp directory. While it allows any user to add files and directories underneath, only the creator of a file can later rename or delete it. Files directly under edatemp (for example, traces) and listener subdirectories are owned by the super user (root, QSECOFR). If edatemp is pre-created or adjusted to an alternate permission, then that permission will be respected. However, be aware that edastart -cleardir will remove the edatemp directory, and therefore necessitate the repeated recreation to the desired permission.

**On z/OS (PDF deployment),** all temporary files created by a user are based on the rules in the Security package.

**On Windows,** the permissions of the parent directory of edatemp (usually EDACONF), which were applied when the server was installed, are inherited when edatemp and then the agent subdirectories are created, defining the kind of access other users have to an agent subdirectory and its contents.
Configuring General Server and Web Console Actions

In this section:
Transferring File Permissions With the GRANT Privilege

How to:
Configure General Privileges
Control Access to the Web Console and DMC
Minimize User Access to the Server Through the Web Console
Set the Default Administration Role

Reference:
General Privileges

An authenticated user interacts with the server using the Web Console or Data Management Console (DMC). The Server Administrator controls access to the Web Console actions permitted by assigning general privileges to roles and registering users and groups into roles.

Procedure: How to Configure General Privileges

General privileges define access to the Web Console and DMC control pages such as the Adapter and DBMS Connections configuration pages, the Metadata creation pages, the Procedure editor and Procedures and Flows Run Options page, and the Server Configuration pages.

These privileges can be reviewed or customized from the Web Console by choosing Access Control on the Web Console menu bar. General privileges can be set on the role, group and user levels. Groups and users registered under any role inherit the general privileges of that role unless they are customized on the group or user level.
Users other than the Server Administrator can see their own general privileges by choosing *Show Privileges* on the My Console menu. Server Administrators do not have this option because they have full privileges to all pages of the Web Console and Data Management Console.

WebFOCUS procedures can use the CHECKPRIVS() function that, when given a privilege code (for example, NODPT), returns the value Y (yes) or N (no) depending on whether the connected user is has that privilege. For more information, see the *Using Functions* manual.

**Reference:** General Privileges

The following image shows a sample General Privileges pane for a Basic user, with default values.
The following table describes the general privileges.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adapters</strong></td>
<td></td>
</tr>
<tr>
<td>ADPTP</td>
<td>You can configure adapters and add DBMS connection attributes.</td>
</tr>
<tr>
<td>NODPT</td>
<td>You can disable Direct Passthru.</td>
</tr>
<tr>
<td>NOSYS</td>
<td>You can disable the ability to execute certain operating system commands.</td>
</tr>
<tr>
<td><strong>Metadata</strong></td>
<td></td>
</tr>
<tr>
<td>METAP</td>
<td>You can launch tools to create and edit metadata.</td>
</tr>
<tr>
<td>DATMG</td>
<td>Data Management (allows users to create DBMS tables for the synonym, run Quick Copy, upload to Relational Database, and re-load data).</td>
</tr>
<tr>
<td><strong>Procedures</strong></td>
<td></td>
</tr>
<tr>
<td>PRSAV</td>
<td>You can launch tools to edit procedures, upload procedures.</td>
</tr>
<tr>
<td>PRSTR</td>
<td>You can use the stress tool.</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>PRDFR</td>
<td>You can Schedule/Email/Submit.</td>
</tr>
<tr>
<td>PRRPT</td>
<td>You can view output, DM log and statistics, impact analysis, scheduler and flow reports.</td>
</tr>
<tr>
<td>PROUT</td>
<td>You can view log and output of submitted requests.</td>
</tr>
</tbody>
</table>

**Workspace**

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSCFG</td>
<td>You can perform server administrative functions, such as access control, server configuration and migration, scalability control, and application path control.</td>
</tr>
<tr>
<td>GRANT</td>
<td>You can grant file privileges that you have to other users.</td>
</tr>
<tr>
<td>MONIT</td>
<td>You can monitor agents, sessions, connections, and services for all users.</td>
</tr>
<tr>
<td>KILAL</td>
<td>You can kill and stop agents, sessions, connections, and services for all users.</td>
</tr>
<tr>
<td>SRVLG</td>
<td>You can view server logs and traces, and you can create Savediag.</td>
</tr>
<tr>
<td>STPSV</td>
<td>You can stop and restart the server.</td>
</tr>
<tr>
<td>RARGP</td>
<td>You can use Resource Analyzer and Resource Governor.</td>
</tr>
</tbody>
</table>

**My Console**

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHGPW</td>
<td>You can change your password.</td>
</tr>
<tr>
<td>MONUS</td>
<td>You can monitor Data Service Agents that match your user ID.</td>
</tr>
<tr>
<td>MONGR</td>
<td>You can monitor Data Service Agents that match your group ID.</td>
</tr>
<tr>
<td>KILT3</td>
<td>You can kill Data Service Agents that match your user ID.</td>
</tr>
<tr>
<td>KILGR</td>
<td>You can kill Data Service Agents that match your group ID.</td>
</tr>
<tr>
<td>APATH</td>
<td>You can change your application path (no applock).</td>
</tr>
<tr>
<td>UPROF</td>
<td>You can edit your user profile.</td>
</tr>
<tr>
<td>DBMSC</td>
<td>You can manage your own DBMS connections.</td>
</tr>
</tbody>
</table>
### Privileges and Other Authorizations

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPROF</td>
<td>You can edit your own user profile.</td>
</tr>
<tr>
<td>APROF</td>
<td>You can list application profiles.</td>
</tr>
<tr>
<td>UIINFO</td>
<td>You can disable display of My Console, detailed error messages, sign-in information, list of privileges for the user, server version, console log, help, and the Privileges section of the Properties page for a file or directory.</td>
</tr>
</tbody>
</table>

**Procedure:** How to Control Access to the Web Console and DMC

Authenticated users are permitted to perform certain control operations on the Web Console, depending on their definitions in admin.cfg as Server Administrator, Application Administrator, Server Operator, Basic User, or other custom role defined on the server. Within a given role, additional administration privileges may be applied. As a result, available Web Console features may vary from site to site or between server configurations at a site.

The Web Console or DMC functions available to the user are determined by his role. If a user is not assigned a role, does not belong to a group, or the group is not registered, his access to Web Console functions is based on the `default_admin_role` setting.

Access to the Web Console is also affected by the security provider in effect:

- **Security OPSYS.** Access to the Web Console is protected by user authentication at the operating system level.
- **Security PTH.** Access to the Web Console is protected by user authentication against the admin.cfg file.
- **Security DBMS.** Access to the Web Console is protected by user authentication against the selected DBMS.
- **Security LDAP.** Access to the Web Console is protected by user authentication against the LDAP (or AD) server.
- **Security OFF.** With security OFF, anyone can access the Web Console, with full, unrestricted use of its features.

Alternatively, if a server administrator has established an Anonymous ID, it can be used to access the Web Console, without an explicitly entered user ID. For details, see [Setting an Anonymous User ID](#) on page 92.

Access to the Web Console and DMC can be restricted for individual users or for a group of users.

1. Access the Web Console with a server administrator user ID.
2. From the Web Console menu bar, select `Access Control`.  

---

**Configuring Privileges and Other Authorizations**
The Access Control page opens.

3. Expand a Roles folder.

4. Right-click a user or group and select Properties.
   The General Properties page opens.

5. Select a role from the Inherit Privileges from drop-down menu.
   The options are:
   - Server Administrator
   - Application Administrator
   - Server Operator
   - Basic User
   - None. (No access allowed.)

   Select the value you want to apply. If only users defined in the admin.cfg are to be allowed access, select None.

   **Note:** If the Server Administrator has created custom roles, they will available in the drop-down menu.

6. Click Update.

   **Note:** If a server administrator has established an Anonymous ID, it can be used to access the Web Console without an explicitly entered ID. For more details, see *Setting an Anonymous User ID* on page 92.
**Procedure:** How to Minimize User Access to the Server Through the Web Console

Users need some access to the Web Console in order to execute procedures and upload files. However, you can minimize their access to the server when they are signed in to the Web Console by implementing the following steps:

1. Remove all general privileges. Set all `disable privileges`: NODPT, NOSYS, UINFO.
2. Set all file privileges for * to Execute and List.
3. Adjust privileges to applications so they only allow necessary actions.

When a user tries to perform an action that you have not permitted, a message similar to the following displays:

![Message Display](image)

**Procedure:** How to Set the Default Administration Role

A default administration role provides access to Web Console or DMC functions and to the server for users who are not assigned a role, do not belong to a group, or whose group is not registered. It is based on a selected role.

1. Access the Web Console with a server administrator user ID.
2. From the Web Console menu bar, select Access Control.
   
   The Access Control page opens.
3. Right-click Access Control and select Settings from the context menu, or click Settings on the ribbon.
   
   The Settings page opens.
4. Select a role from the `default_admin_role` drop-down menu in the General section.
5. Click Apply and Restart Server.
Transferring File Permissions With the GRANT Privilege

**Example:**

Granting Permissions to Another User

The server administrator normally provides access control permissions for application folders to groups and users. If the server administrator issues the GRANT privilege to another security subject (role, group, or user), that security subject can then grant its own file permissions to any other security subject,

For example if user A has Read but not Write permission on folder X, he can transfer Read permission to user B. He cannot grant Write permissions to anyone.

Note that if user A loses the permission later on, user B will retain his transferred permission.

**Example:**  Granting Permissions to Another User

In the following configuration, user pgmtst2 is an Application Administrator with the GRANT privilege:
User pgmtst2 has Read, Execute, and List privileges on application app06, while user pgmtst3 has no privileges on this application:
Since user pgmtst2 has the GRANT privilege for this application, user pgmtst2 can edit the privileges for user pgmtst3:
However, the privileges pgmtst2 can edit are only those that pgmtst2 has for this application. Therefore, the ARWRT privilege is not available for editing:

![File/Directory Privileges](image)

When user pgmtst2 clicks Apply, user pgmtst3 will be assigned Read and List privileges to app06.
Configuring Groups

**Reference:**

Customizing Group Privileges

The Server Administrator registers a group or user within a role that has a set of privileges. Users and groups can be registered for special privileges, both general privileges and file privileges. It is a good practice to assign users to groups and to control groups rather than individual users. The installation has a choice of grouping users in LDAP or using the operating system security mechanism. This grouping is external to the WebFOCUS or server software and must be accomplished by the administrators for those external products. The groups are then registered in the server, and a role is chosen for them. By default, the privileges are inherited from the role in which the group is registered.

At sign-in time, the user group is determined and the proper privileges are assigned. If the user does not belong to any registered group or role, the privileges are taken from the default role. At installation time, the default role is set to Basic User, but the server administrator can change this designation. The default role can be reset on the Access Control General Privileges pages using the default_admin_role keyword.
A group can be assigned a profile stored as `groupname.prf`. Group profiles support the same syntax as role profiles, which are described in Configuring Roles on page 123.

The Access Control page for a user or group has tabs that enable the Server Administrator to view or edit the Application Path, General Privileges, Directory/File Privileges, Administration File, for a user, the list of group memberships, and, for a group, the list of members.

**Note:** Profile settings affect how groups connect to the server.

To open the Access Control page for a group or user, right-click the group or user and select Properties.

Note that for LDAP security, if the LDAP database contains the email address, it is automatically populated on this page. This requires the ldap_user_email attribute to be set in the LDAP provider configuration.

If a user belongs to multiple groups, the server either uses the primary group privileges, allows the user to select the effective group at sign-in time, or merges the privileges from all groups. How the server handles privileges for users in multiple groups is determined by the group_profile setting in the edaserve.cfg file. You can access this setting from the Access Control page by right-clicking the top level of the Access Control tree and selecting Settings.

The default value for group_profile setting is to use the primary group. If the security provider is OPSYS, the operating system determines the primary group. For LDAP, the primary group is the first group alphabetically for the user.

GRPLIST is a function that returns a group name or a list of group names (separated by colons) for the connected user. This function is supported for LDAP security with all types of connections. If the group list is empty or there is an error in the function parameters, the function returns blanks.

There are also three &vars (&FOCSECUSER, &FOCSECGROUP, and &FOCSECGROUPS) that store the connected user and its primary group or the list of all groups (if the server is configured with profile_setting=all). These variables are populated by the server and cannot be changed by the application.
Reference: Customizing Group Privileges

Although the recommended policy is to control groups, there may be a need to create different sets of privileges for some individual users. If a user cannot be assigned to a group or to a custom role, the user can be registered with any role, and the Server Administrator can customize the privileges as needed. The customization can include general and file privileges, application path, and DBMS connections. Such users should be kept to a minimum.

Configuring Roles

How to:

Create a Custom Role
Set Customized Privileges for Roles

The server is shipped with five predefined roles that allow basic operational control. Roles are listed under Access Control on the Web Console menu bar:

The roles come with a fixed set of general privileges as follows:

- **Server Administrator.** Groups and users assigned to this role have full control of the workspace, adapters, synonyms, and procedures.
- **Application Administrator.** Groups and users assigned to this role have privileges to create synonyms and procedures and to run them.
- **Server Operator.** Groups and users assigned this role have privileges to start and stop the server and monitor and kill agents.
- **Basic User.** Groups and users assigned to this role can execute procedures.
- **None.** Users assigned to this role have no privileges on the Web Console and Data Management Console (DMC).

The default file and directory privileges allow full access.

The Server Administrator can customize the default privileges and can create custom roles and assign them general and file privileges. The only roles that cannot be changed are the Server Administrator role, which always has full privileges, and the NONE role, which has no privileges. If the Server Administrator customizes a role, it displays with the text (Customized) next to its name on the Access Control tree.

Roles can be assigned profiles that are stored in the location identified by the $EDAPRFU variable. The profile for each role is stored as the file named rolename.prf. The following items can be controlled by a profile:

- DBMS connections that are configured on the Adapter page.
Application path that controls the search for unqualified file names (for example, TABLE FILE CAR). The application path is configured from the Access Control page.

Other WebFOCUS commands.

Predefined roles are assigned predefined names:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV</td>
<td>Server Administrator</td>
</tr>
<tr>
<td>APP</td>
<td>Application Administrator</td>
</tr>
<tr>
<td>OPR</td>
<td>Server Operator</td>
</tr>
<tr>
<td>USR</td>
<td>Basic User</td>
</tr>
</tbody>
</table>

Note: When a user connects to the server, the role profile is executed after the server profile.

Procedure: How to Create a Custom Role

1. From the Access Control page, either click the Register button at the top of the page or right-click the Roles folder, and select Register Role from the context menu.

   The Register Custom Role page opens.

2. Enter a name for the role, and click Apply.

   A dialog box opens informing you that a new role will be registered.

3. Click OK.

   A page opens on which you assign privileges to this new role.
The page opens to the General Privileges tab, but you can click the Directory/File Privileges tab to assign file and directory privileges.

4. You can assign privileges by:
   - Checking each privilege you want to assign to this role and then clicking Apply.
   - Clicking Reset to Default Privileges to assign the privileges from the default role to this new role. Then you can edit the privileges as needed.
   - Clicking Copy Privileges from Other Subjects to assign privileges based on other users, groups, or roles.
The **Select Copy Source** page opens.

![Select Copy Source](image_url)

5. To copy the privileges from one of the listed subjects, right-click the icon on the left of the subject and click **Copy**.

   A dialog box opens informing you of the source and destination subjects.

6. Click **OK** to copy the privileges.

**Note:**

- Once the custom role has been created, the Server Administrator can register users and groups to the role.

- The Server Administrator can create a role profile that will be executed when a user registered to this role connects to the server.

- The Server Administrator can set the custom role as `default_admin_role` on the Access Control/General Settings page.
Procedure: How to Set Customized Privileges for Roles

A server administrator can set selected privileges for basic users, application administrators, and server operators. Configurable options are tailored to each user group.

1. On the Web Console menu bar, select Access Control.
2. Right-click a role in the navigation pane.

![Access Control Menu]

The General Privilege page opens.

3. Select the check boxes for the functions you want the role to be able to perform. Configurable options vary by user group.
4. Click Apply to confirm these settings.
5. Click Reset to Default Privileges if you wish to revert to the standard privileges assigned to that user group.
Registering Users and Groups in a Role

How to:

- Perform Single User Registration
- Perform Multiple User Registration
- Perform Single Group Registration
- Perform Multiple Group Registration
- Manage Users and Groups With PTH Security
- View or Change Existing User or Group Registrations
- Unregister a User or Group

A server administrator can assign specific users the following roles: Server Administrator, Application Administrator, Server Operator, Basic User, or All Users. A server administrator can also create additional roles and select or deselect certain privileges for these users or groups.

The user and group roles are stored in a release independent file called admin.cfg, which is located, by default, in .../ibi/profiles. This location is defined with the server configuration parameter EDAPRFU, which is stored in the edaserve.cfg file. The admin.cfg file should not be shared between servers that run with different security providers.

When registering users and groups under an LDAP or OPSYS security provider, you can retrieve a list of groups and users from the operating system. The list can be filtered to minimize the number of candidates retrieved. The User and Group Description is retrieved when available. This feature is available on Windows, UNIX, iSeries, and zOS/USS.

Procedure:  How to Perform Single User Registration

This procedure assumes that the user is signed in to the Web Console as a server administrator.

Note that for the PTH security provider, the user first has to be created using the PTH Users and Groups Management page.

1. From the Web Console menu bar, select Access Control.
   The Access Control page opens.

2. Right-click a role and select Register User from the context menu.
The Register Multiple Users page opens. For information about registering multiple users, see *How to Perform Multiple User Registration* on page 130.

3. Click *Single User Registration*.

The Register User page displays for providers for which the server does not have support for retrieving user and group lists from the security provider. For example, single registration is used for a DBMS provider or an OPSYS provider on z/OS PDS deployment, as shown in the following image.

![Register User page](image)

4. Enter a user ID in the *User* field.

5. If you use domain names with the user IDs (Windows only), enter the domain name in the *Domain* field or select one from the drop-down menu (OPSYS only).

6. Optionally, in the *Password* and *Confirm Password* fields, enter the password for the user ID. A password is only required for scheduled runs.

7. Enter an email address for the user.

8. Select an administrator level from the *Inherit Privileges from* drop-down menu. The options are: Server Administrator, Application Administrator, Server Operator, Basic, or None.

9. Click *Register*. 
**Procedure: How to Perform Multiple User Registration**

User registration can be done for providers that are active.

You can register a single user ID by clicking *Single User Registration*, which navigates to the Single User Registration page described in *How to Perform Single User Registration* on page 128.

1. On the Access Control menu, right-click a role and select *Register User*.

   The Multiple Users Registration page opens, as shown in the following image.

   ![Multiple Users Registration](image)

   For multiple users, you can filter the users retrieved by specifying a pattern in one more of the filter entry fields (UserID, Description, Email, and others). The list of filter fields can vary depending on a security provider.

2. To retrieve all users for the security provider, click *Next*.

3. To limit the list retrieved, check the Filter User box. This enables you to enter search criteria.

   a. Enter a User ID search string, for example *abc*, in the User ID field. Depending on the operating system, the User ID search may be case-sensitive.

   b. Optionally, select a domain or enter a search string in the Domain drop-down list.

   c. Optionally, enter a search string in the Description field. The Description search is not case-sensitive.

   d. Click *Next*.

   The list of users is returned, as shown in the following image, and the role you first selected appears in the *Inherit Privileges from* drop-down list.
e. Optionally, select a different role from the Inherit Privileges from drop-down list.

f. If you want to override the existing registration for the users, check the override the existing registration box.

g. Either check the boxes for the users you want to register, or click Select All to select all the users on the list.

h. Click Register.

**Procedure: How to Perform Single Group Registration**

For security PTH, the group first has to be created using the PTH Users and Groups Management page.

This procedure assumes that the user is signed in to the Web Console as a server administrator.

For the OPSYS, LDAP, Custom, or PTH security providers, a server administrator can assign a role to groups of users by following these steps:

1. From the Web Console menu bar, select Access Control.

   The Access Control page opens.

2. Right-click a Role from the Roles folder and select Register Group.
The Multiple Groups Registration page opens. For information about registering multiple groups, see *How to Perform Multiple Group Registration* on page 132.

3. Click Single Group Registration.

The Register User page opens, as shown in the following image.

**Single Group Registration**

- **Security Provider**: PTH<internal>
- **Group**: [entry field]
- **Description**: [entry field]
- **Inherit Privileges from**: Server Administrator

4. Select the security provider from the Security Provider drop-down list.
5. Enter a name for the group in the Group entry field.
6. Optionally, enter a description in the Description entry field.
7. To establish the privileges for this group, select a role from the Inherit Privileges from drop-down list.
8. Click Register.

**Procedure: How to Perform Multiple Group Registration**

Before you can retrieve a list of groups from the operating system, LDAP or OPSYS must be the active security provider.

You can register a single group by clicking Single Group Registration, which navigates to the Single Group Registration page, as described in *How to Perform Single Group Registration* on page 131.

1. On the Access Control menu, right-click a role and select Register Group.
The Multiple Groups Registration page opens, as shown in the following image.

![Multiple Groups Registration](image)

2. To retrieve all groups for all domains, click Next.

3. To limit the list retrieved, check the Filter Group box. This enables you to enter search criteria.

   a. Enter a Group ID search string, for example *abc*, in the Group ID field. Depending on the operating system, the Group ID search may be case-sensitive.

   b. Optionally, select a domain or enter a search string in the Domain drop-down list.

   c. Optionally, enter a search string in the Description field. The Description search is not case-sensitive.

   d. Click Next.

   The list of groups is returned, as shown in the following image, and the role you first selected appears in the Inherit Privileges from drop-down list.
Optionally, select a different role from the *Inherit Privileges from* drop-down list.

If you want to override the existing registration for the groups, check the *override the existing registration* box.

Either check the boxes for the groups you want to register, or click *Select All* to select all the groups on the list.

Click *Register*.

**Procedure: How to Manage Users and Groups With PTH Security**

This procedure assumes that the user is signed in to the Web Console as a server administrator.

1. From the Web Console menu bar, select *Access Control*.
   
The Access Control page opens.

2. Expand the *Security Providers* folder.

3. Right-click the PTH folder and select *Manage Users/Groups*.
   
The *PTH Users and Groups Management* page opens, as shown in the following image.
4. You can drag users (listed on the left) to groups (listed on the right) or drag groups to users. In addition, you can select a user or group and use the arrows between the two panes to move them.

   **Note:** You must click Save in order to make these changes permanent.

5. To add a user or group, click New on the appropriate pane.
For a new user, the New PTH User dialog box opens, as shown in the following image:

- a. Enter a user ID.
- b. Optionally, enter a description in the Description field.
- c. In the Password and Confirm Password fields, enter a password for the user ID.
- d. Enter an email address for the user.
- e. By default, the password never expires. If you want to set an expiration date, uncheck Password never expires.
- f. If you want to temporarily disable the account, check Account disabled.
- g. Click OK.
  The user is added to the list.
- h. Click Save.
  **Note:** If you do not click Save, the user will not be saved on the list.
For a new group, the New PTH Group dialog box opens, as shown in the following image:

![New PTH Group dialog box](image)

- Enter a group ID.
- Optionally, enter a group description.
- Click Next. The group is added to the list.
- Click OK.
  
  **Note:** If you do not click Save, the group will not be saved on the list.

6. To delete a user or group, select the ID and click *Delete*.

A confirmation dialog box opens.

- Click OK.
- Click Save.
  
  **Note:** If you do not click Save, the user or group will not be deleted.

7. To view or change the properties of a user or group, select an ID and click *Properties*.
For more information, see *How to View or Change Existing User or Group Registrations* on page 138.

**Procedure: How to View or Change Existing User or Group Registrations**

1. From the Web Console menu bar, select *Access Control*.
   
   **Note:** You can also view and change the properties on the *PTH Users and Groups Management* page.
   
The Access Control page opens.

2. Expand a Role from the *Roles* folder.

3. Right-click the user or group whose properties you want to view or change, and select *Properties*.
   
The General Properties page opens, as shown in the following image.

4. You can change the user role by select a different role from the *Inherit privileges from* drop-down menu. For more information, see *How to Configure General Privileges* on page 110.
   
   **Note:** If only one user is defined as a Server Administrator, you cannot change that user role.

5. Click *Update*.
   
The user or group is moved to the new role.

**Procedure: How to Unregister a User or Group**

1. From the Web Console menu bar, select *Access Control*.
   
The Access Control page opens.
2. Expand a Role from the Roles folder.

3. Right-click the user or group and select Unregister.
   You are prompted to confirm that you want to unregister the user or group.

4. Click OK.
   The user or group is unregistered.

Configuring Server Encryption

The server supports encryption of passwords in configuration files, as well as SSL encryption for the TCP/HTTP Listener and encryption of data passed between a hub server and a remote server or cluster server.

Encrypting Passwords Stored in Configuration Files

How to:

Encrypt Passwords Stored in Configuration Files

You can select an encryption algorithm for passwords stored in configuration files.

Procedure: How to Encrypt Passwords Stored in Configuration Files

1. From the Web Console menu bar, choose Access Control.

2. Click Settings on the menu bar, or right-click the Access Control tree and select Settings. Then select Encryption Settings.
   The Encryption and Decryption page opens.

3. To define the cipher used to encrypt passwords in configuration files, click the drop-down list for cfgfile_cipher and select:
User-Defined Password Encryption and Decryption

**Procedure: How to Set Up User-Defined Password Encryption and Decryption**

1. Select **Access Control** from the Web Console menu bar.

2. Right-click the Access Control navigation tree and select **Settings**, or click **Settings** on the ribbon.

   The Access Control Settings page opens.
3. Select *user defined program* from the *cfgfile_cipher* drop-down menu. Two additional parameters are displayed.

4. Enter the full paths to the encryption and decryption programs in the *cfgfile_cipher_encrypt* and *cfgfile_cipher_decrypt* fields respectively, as shown in the following image.

```
<table>
<thead>
<tr>
<th>Password and Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cfgfile_cipher</strong></td>
</tr>
<tr>
<td><strong>cfgfile_cipher_encrypt</strong></td>
</tr>
<tr>
<td><strong>cfgfile_cipher_decrypt</strong></td>
</tr>
<tr>
<td><strong>password_change_delimiter</strong></td>
</tr>
<tr>
<td><strong>password_change_wdirect</strong></td>
</tr>
</tbody>
</table>
```

5. Click *Apply and Restart Server*.

**Encrypting Data at Rest**

When the server *io_encryption* setting is ON, binary, alpha, and delimited HOLD files in edatemp and foccache are encrypted. Data agent trace files (tsxxx.trc) and agent output files (tsxxx.tro) are also encrypted as a result of this setting. After encryption, the extensions for these files are .trce and troe, respectively. This prevents the user from opening these files in editors outside of the Web Console or Data Management Console. Trace files and agent output files can be viewed from the Web Console *Workspace* page under *Traces And Logs*.

To turn on the *io_encryption* setting, do the following:

1. On the Access Control page, either click the *Settings* button on the ribbon, or right-click the *Access Control* folder and select *Encryption Settings* from the context menu.
The Encryption and Decryption page opens.

2. Select y from the io_encryption drop-down list, as shown in the following image.

The default encryption algorithm is DES. You can change the type of encryption using the \textit{cfgfile_cipher} setting available on the same page.

3. Click \textit{Apply and Restart Server}.

This setting will be added in the edaserve.cfg configuration file.
Configuring Secure Socket Layer (SSL) Encryption for the TCP/HTTP Listener

**How to:**
Enable SSL

You can enable SSL for the TCP/HTTP Listener to encrypt all traffic between the server and any client application, such as the WebFOCUS Client, a remote server, or a cluster server.

**Procedure: How to Enable SSL**

1. From the menu bar, select **Workspace**.
2. Open the **Special Services and Listeners** folder, right-click **TCP/HTTP**, and select **Properties of HTTP**.
   
The Listener Configuration page opens.

3. In the **Security** section, select **Yes (OpenSSL)** or **Yes (Microsoft)** from the **Enable HTTPS** drop-down list.
   
   Additional fields needed for SSL configuration appear.
Note that OpenSSL libraries libeay32.dll and ssleay32.dll must be in the path to enable SSL.

4. Enter the following values:

   **SSL_CERTIFICATE**
   
   Contains the certificate chain in order, starting with the certificate for the listener and ending with the root CA certificate. Each of these entries must be in PEM format.
   
   Note that the administrator at the installation site must acquire valid security certificates (self signed or commercial).

   **SSL_PRIVATE_KEY**
   
   Defines the file that contains the private key of the listener. It must correspond to the public key embedded within in the certificate and must be in PEM format.

   **SSL_PASSPHRASE_E**
   
   If the file defined in SSL_PRIVATE_KEY is encrypted, a passphrase must be provided here to decrypt the private key.

   **SSL_CA_CERTIFICATE**
   
   Defines the name of a file containing a trusted CA certificate in PEM format. It is used to verify the client certificate. If the client fails to send a certificate or verification fails, connections are rejected. More than one CA certificate may be present in the file.

5. Click the **Save and Restart Server** button.

### Configuring Data Encryption for a Remote Server

**How to:**

Configure Data Encryption for a Remote Server

You can enable encryption of data passed between the server and a remote server or cluster server.

**Procedure:** How to Configure Data Encryption for a Remote Server

1. You can access the Remote Server Configuration page by selecting **Adapters** on the Web Console menu bar. Remote Servers is an item in the Available folder.

2. Right-click Remote Servers on the Adapter page and select **Configure**.
The Remote Server Configuration page opens.

3. Click the **ENCRYPTION** drop-down list for and select:

- **0** for no encryption.

- **DES** for 56-bit fixed-key Data Encryption Standard in Electronic Code Book (ECB) mode. The same key is used in all connections with no key exchange between client and server.

- **ADVANCED** to select an encryption cipher (3DES, AES128, AES192 or AES256), encryption mode (ECB or CBC), and RSA key length (512 or 1024 bits). In advanced mode, the client randomly generates a new RSA key pair (public and private keys of the specified length) and sends the public key to the server. Upon receipt of the public key, the server generates a random secret key. The length of the secret key depends on the chosen cipher strength. The secret key is encrypted with the public RSA key and sent back to the client, which decrypts it with its private RSA key. After the exchange, the client and the server both share the same secret key, and use it to encrypt and decrypt all communications between them.

The following encryption ciphers are available:

- **3DES** for triple Data Encryption Standard.
- **AES128** for Advanced Encryption Standard (key size 128 bits).
- **AES192** for Advanced Encryption Standard (key size 192 bits).
- **AES 256 bits** for Advanced Encryption Standard (key size 256 bits).

The following encryption modes are available:

- **ECB** for Electronic Code Book mode. This is the default mode.
- **CBC** for Cipher Block Chaining mode.

The following RSA key lengths are available:

- **512 bits.**
- **1024 bits.**

- **IBCCRYPT** for a user-defined algorithm. The key is 512-bit RSA-encrypted.

4. Click the Save button.

**Encoding HTML Tags in Data**

You can set the HTMLENCODE parameter to control whether HTML tags in data are encoded as plain text or HTML tags. The value **ON** encodes the tags as plain text so that the browser does not consider them to contain executable code. This prevents an attack on the server by inserting executable code into data. You can set the value of HTMLENCODE to **ON** on the server Miscellaneous Settings page, available from the Workspace tab of the Web Console. Doing so places this setting in edasprof and enforces it server wide.

**Access to Connection Information in WebFOCUS Procedures**

The WebFOCUS Client can pass a browser cookie or HTTP header to the Reporting Server for use in WebFOCUS procedures.

The following server built-in functions can be used to retrieve this information and use it in a procedure.

- The GETCOOKI function can be used to retrieve the browser cookie value.
- The GETHEADR function can be used to retrieve variable values from the HTTP header.

For more information about WebFOCUS functions, see the *Using Functions* manual.

In addition, three Dialogue Manager system variables contain connection information.

- **&FOCSECUSER** returns the user ID of the connected user,
- **&FOCSECGROUP** returns the primary group ID for the connected user, if there is one.
&FOCSECGROUPS returns the list of group IDs for the connected user (required the server to be configured with profile_setting=all).

## Configuring the Server for Multi-Tenant Deployment

**In this section:**

- Configuring Multi-Tenant Application Folders
- Configuring Multi-Tenant Groups and Users
- Configuring Multi-Tenant DBMS Connections
- Configuring Security Providers for Multi-Tenant Deployment
- Naming Conventions for Multi-Tenant Deployment
- Configuring Application File Privileges for Multi-Tenant Deployment
- Effect of Multi-Tenant Deployment on File Upload and HOLD Files
- Shared Metadata Under Multi-Tenant Deployment
- Configuring Security Templates for Multi-Tenant Environments

In multi-tenant software architecture, each tenant (client) shares certain computing resources and application code with other tenants. In addition, each client has its own individual resources that are logically isolated from those belonging to other tenants. Metadata associates each resource with the correct tenant.

Within the server framework, in a typical setup each tenant has its own:

- Application folders.
- Groups and users.
- DBMS connections

### Configuring Multi-Tenant Application Folders

The main application folder for each tenant should contain its unique metadata (synonyms), uploaded data files and HOLD files, StyleSheet files, and server-based procedures. The tenant should have no access to other tenant folders. However, a tenant may have access to common installation-wide folders under approot, which is useful when metadata and utilities are shared between tenants. Nested folders under the main tenant application folder can be added as needed.
Configuring Multi-Tenant Groups and Users

Each tenant will have at least two groups. One group (registered to the application administrator role) has read/write access to the tenant folders and is able to create metadata and other files. The other group (registered to the basic role) can have only execute and list privileges on the tenant folder.

More groups can be added as needed.

It is recommended that groups and users be defined externally (in LDAP, for example) so that user provisioning, password expiration, and other administrative tasks can be done with the standard tools. However, the PTH security provider with server-maintained users and groups can be used as well.

Configuring Multi-Tenant DBMS Connections

DBMS connections can be defined for all tenants in edasprof or in the group profile for each tenant.

Configuring Security Providers for Multi-Tenant Deployment

The server administrator can give each tenant administrator the ability to add and remove users independently by configuring a separate security provider for each tenant. Appropriate LDAP server privileges can be given to selected users for each tenant. Alternatively, a single provider can be used. These setup choices are part of the LDAP configuration techniques for the site.

Naming Conventions for Multi-Tenant Deployment

A naming convention should be developed for creating application folders and groups that contain the tenant ID as a suffix or prefix. In the following example, the tenants have IDs 01 and 02, and folders and groups are named the following:

```
app01, app02, grp01_app, grp01_bas, grp02_app, grp02_bas
```

This will make administrative tasks more transparent and allow easier replication of the configuration when new tenants are created.

Configuring Application File Privileges for Multi-Tenant Deployment

It is recommended that an application named tenants be created under approot and that all application files be created under the tenants application.
Once the tenants application is created, the administrator should remove all privileges to it from the application administrator and basic roles. This will ensure that tenants do not have any access to the applications owned by other tenants:

![Manage Privileges for c:\lib\apps\tenants](image)

Next, give each tenant group access to its own application.
For example:
Grp01_app has all file privileges registered to tenants/app01.
Grp01_bas has only execute/list file privileges registered to tenants/app01.
Both tenant 01 groups have no access outside of their folder.

**Effect of Multi-Tenant Deployment on File Upload and HOLD Files**

Uploading can be done to a designated subfolder of the tenant application. Even basic role users need write access to the upload folder.

For example:
Grp002_bas has all file privileges registered to tenants/app01/upload

Alternatively each user can use his home folder and not share the files, even with users of the same tenant.

**Shared Metadata Under Multi-Tenant Deployment**

The administrator may choose to share all synonyms and procedures for all tenants. A common application folder outside of the tenant application should be created with only list/execute permissions for all tenant groups. This folder is updated centrally for the whole installation. In this case, the tenant folders can be used only for upload and HOLD files.
Configuring Security Templates for Multi-Tenant Environments

How to:
Configure Security Templates

Reference:
Configure Security Templates
Summary of Regular Expressions

Very often, multiple tenants in a multi-tenant environment have an identical security structure. Each tenant has an identical set of application folders and groups that conform to a standard naming convention that includes the tenant ID in the name of each subgroup and application folder. The folder and group setup is repeated from one tenant to the others. In most cases, tenants have no access rights outside of their main application folder.

In this type of configuration, you can establish file privileges for a model tenant and its associated groups, and dynamically apply them to other tenant groups by creating a template based on the model tenant. The template defines regular expressions that identify which actual group names should be assigned file privileges based on that template. Each group ID should match only one template.

Procedure: How to Configure Security Templates

The following steps outline the tenant management process in the Reporting Server.

1. Identify the tenant root application folder.

   The tenant root application folder can be under approot or can be a mapped application or SQL mapped folder. The application must be in the APP PATH. For example, c:\ibi\apps\tenants.

2. Set the permission for this folder to no access for all non-server administrator roles. in order to prevent tenants from accessing folders assigned to other tenants.

3. Using the established naming convention, create the model tenant folder under the tenant root. Give the model tenant groups explicit access permissions to the model folder and its subfolders.

   The model tenant groups must follow the tenant group structure and naming conventions established in the security software for the installation. The model group must be registered in the admin.cfg file. If the security provider is PTH, the tenant groups must also be registered in the admin.cfg file.
For example, using the departments application as the tenant root, create the sales application under the tenant root. The server administrator creates the groups sales, sales/dev, sales/basic, and any other groups needed.

In the following image, the tenant root folder is called *departments*, and the sales application is the model application. The sales application is not only a model, it is an existing group or tenant that must be registered, with privileges to the application departments/sales. Once you create one registration you can assume it as the model and create a template based on it:

The server administrator defines the file and directory privileges for the sales, sales/dev and sales/basic groups on the sales folder and its children. These privileges will be replicated in groups for other tenants when their group ID matches one of the established template group IDs.

The following image shows that the sales group, whose role is Basic User, has been given Read, Execute, and List privileges on the sales folder:
4. Establish a template that specifies how the model access rules are replicated to other tenants.

   a. On the Access Control page, right-click the Templates folder and select Register Group Template from the context menu:
The Group Template Registration page opens:

**b.** Enter the following values to establish the rules for deriving access control privileges for groups that match the template, and click *Register:*

**Template Group ID**

Is a regular expression that must contain a tagged expression. The tagged expression is used to identify a part of the model group ID that will be replaced by the corresponding characters in the actual group ID passed to the Reporting Server for the connected user.

For information about regular expressions, see *Summary of Regular Expressions* on page 157.

**Model Group**

Identifies the group that will be replicated.

**Exclude Group IDs**

Is a regular expression that identifies any group IDs that should be excluded in the template matching process.

**Replace Pattern**

Is used for admin_privilege strings to model file/directory privileges from the model group registration to a target group.
For example, the sales application has the sales/dev group that is registered with specific privileges on the sales folders. When the finance application is created, it will have a group named finance/dev that will be assigned the same privileges on the finance folders that the sales/dev group has on the sales folders. The finance groups will not be registered, but the template describes how to replace the word sales with the word finance when the group name ends with the characters /dev.

When you register the template, the following attributes are added to the admin.cfg file:

```
admin_group_template = (\w+)/dev
BEGIN
  model_group = sales/dev
  file_replace_pattern = departments\(sales
END
```

For example, the template group ID pattern (/\w+)/dev specifies that any word followed by the characters /dev matches the template pattern.

The replace pattern departments\(sales) indicates that the text sales will be replaced. If the group ID finance/dev is passed to the Reporting Server, the tagged expression in the Template Group ID will cause the characters finance to replace the characters sales in order to determine the file privileges for the connected user. Therefore, a user in the group finance/dev will inherit the privileges under the finance tenant application that the group sales/dev has under the model sales application.
To create a template that applies to the group sales, you need to make sure that you exclude other group names that start with the characters sales/ because without the exclusion, sales will match all of the templates, and it may be assigned the wrong one. The following image shows the template for the sales group:

The regular expression (/) in the Exclude Group IDs field specifies that group names that contain a slash do not match the template. For information about regular expressions, see Summary of Regular Expressions on page 157.

At this point, the system is ready to add new tenants.

To add a new tenant (for example, finance), the server administrator must create the finance application under the tenants root application. The installation must provision groups and users (that conform to the established naming conventions) in the relevant security provider, for example LDAP, OPSYS, or Custom. This is done outside of Information Builders software. The new tenant is now ready to be used. No access control for it needs to be established by the server administrator. The server will dynamically assign the access control privileges based on the model and the template.

For example, the user fbas1 (which is part of the finance group) logs on. The properties for this user show that the user has Read, Execute, and List privileges on the finance folder because the sales model group was given those privileges on the sales folder:
Note that the sales tenant is not visible to this user,

**Reference: Summary of Regular Expressions**

A regular expression is a string containing a tagged expression. A tagged expression is a portion of the string that will be replaced with actual characters passed to the Reporting Server in the group ID for a user.

Tagged expressions must be enclosed in parentheses. The backslash character (\) is a special character in tagged expressions. If a group ID actually contains a backslash character, you indicate that you want the backslash character to be treated as a normal character by entering two successive backslash characters (\\).

The following can be used to create the tagged expression:

```
abc
```

    Matches *abc* anywhere within the string.

```
(abc)
```

    Matches *abc* anywhere within the string, but the parentheses act as a tag.
[]

Defines a character class (or set) that matches any one of the characters in the class. For example, [abc] matches the character a or b or c. The expression [x-y] matches any character from x to y.

.

Matches any single character except newline.

\w

Matches any word character string (alphanumeric plus ".").

\W

Matches any non-word character.

\s

Matches any whitespace character.

\S

Matches any non-whitespace character.

\d

Matches any digit.

\D

Matches any non-digit character.

\t

Matches a tab character.

\r

Matches a return character.

\f

Matches a formfeed character.

\e

Matches an escape character.

\b

Matches a word boundary or a backspace. For example, test\b matches test, but not testing. However, \b matches a backspace character when specified inside a class (that is, [\b]).
\B
Requires that there is no word boundary. hello\B matches hello, but not hello there.

^ Matches characters only at the beginning of the string. For example, ^abc matches abc at the beginning of the string.

$ Matches characters only at the end of the string. For example, abc$ matches abc at the end of the string.

| Specifies alternative matching characters. For example, a|b matches either a or b. This metacharacter can also be used with words, for example, abc|def.

[^abc] Matches a character that is not in the set. [^abc ]+ will match such strings as hello, test, and perl.

\ Is the escape character. For example, \* matches the * character. Use the backslash (\) character to escape (remove the special meaning of) characters that have significance in a regular expression.

(?i) Ignores case. For example, (a(?i)b|c) matches aB, c, and C.

You can follow any character, wildcard, or series of characters and/or wildcards with a repetition indicator:

* Matches 0 or more occurrences of the character sequence.

+ Matches 1 or 0 occurrences of the character sequence.

? Matches 0 or more occurrences of the character sequence or the shortest match.

{} Is the repetition modifier.

{n} Matches exactly n occurrences of the character sequence.
(n,)
Matches at least \( n \) occurrences of the character sequence.

\((n,m)\)
Matches at least \( n \) but not more than \( m \) occurrences of the character sequence.
Managing Applications

An application is a platform-independent repository for a group of related components, such as procedures, Master and Access Files, data files, HTML files, PDF files, and image files.

You can use a variety of application (APP) commands to control the application environment, including the application itself, its component files, and its search paths.

**Topics:**

- What Is an Application?
- Procedures and Metadata on the Application Tree
- Managing Applications and Paths
- Application Commands Overview
- Search Path Management Commands
- Application and File Management Commands
- Output Redirection Commands
- Application Metadata Commands and Catalog Metadata
- Help Information: APP HELP
- Restricting the Use of APP Commands
- Accessing Metadata and Procedures
- Allocating Temporary Files
- Temporary Space Usage and Location
- Temporary Disk Space Usage for Non-PDS Deployment
- Application Tools
What Is an Application?

An application is a platform-independent repository for a group of related components, such as procedures, Master and Access Files, data files, HTML files, PDF files, and image files. It provides an area on the server that both confers a unique identity on the application components and facilitates the sharing of components across applications in an organized manner. This construct also simplifies the process of moving a user application from one platform to another and of deploying PC-developed applications.

These components are physically grouped together on an application-by-application basis for run-time execution. This physical grouping can be within an application under a common root or a mapping to an application anywhere in the file system. The physical application or mapped name is referred to as the application name in this document. A comprehensive set of application (APP) commands are provided to control/manipulate the application components, as well as to facilitate applications that can be written and deployed to any platform.

The physical location of an application and its components is determined by a configuration parameter called approot. This parameter is set at installation time and stored in the server configuration file edaserve.cfg. The default value is dependent on the platform, relative to the install ID home directory, where applicable, as indicated in the following chart.

Application directories can be nested, except on z/OS under PDS deployment. A nested application directory is an application created within a higher-level application. For more information, see Nested Application Directories on page 192.

You can also create a home application directory for each user. Providing a user home application gives each user a place where he has full control to create, change, and run his applications. For more information, see Home Application Directories for Users on page 195.

Note: Where directories are referenced in the chart, lowercase application directories are created below the approot value. The application names must be lowercase and must not contain spaces. For a PDS deployment on the Unified Server, data sets are created for each component type using the approot value as the high-level qualifier.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Default Value for approot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Server HFS Deployment</td>
<td>../ibi/apps</td>
</tr>
<tr>
<td>z/OS PDS Deployment</td>
<td>approotvalue.appname.component_type</td>
</tr>
<tr>
<td>UNIX</td>
<td>../ibi/apps</td>
</tr>
</tbody>
</table>
Default Value for approot

<table>
<thead>
<tr>
<th>Platform</th>
<th>Default Value for approot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>../ibi/apps</td>
</tr>
<tr>
<td>Windows</td>
<td>../ibi\apps</td>
</tr>
<tr>
<td>IBM i (formerly known as i5/OS)</td>
<td>../ibi/apps</td>
</tr>
<tr>
<td>OpenVMS</td>
<td>[.IBI.APPS]</td>
</tr>
</tbody>
</table>

Two applications are provided during installation, a default application called baseapp and an application in which you can generate legacy sample files called ibisamp.

In addition, when you connect to the server, a temporary directory called foccache is added as the first directory in the search path. When you want to be able to reuse data within the same browser session, you can store the data in the form of a HOLD, SAVE, or SAVB file in the foccache directory. As long as the browser session remains active, the files stored in the foccache directory can be referenced in requests.

Access to a particular application component can be explicit or implicit. Implicit access is dependent upon the search path in effect at the time of execution. The search path always includes the default application, baseapp. There is no need to explicitly declare this application.

You can change the search path from the Web Console, from the Data Management Console, or from within your application code. You can also change the search path temporarily to add application names to the beginning or end of an existing search path. APP commands are described briefly in Application Commands Overview on page 219 and in detail later in this chapter.

In addition to explicit APP names under APPROOT or an APP MAP command, which might look like myapp/myproc, there are also special reference names for internal locations that may be useful. They are:

<table>
<thead>
<tr>
<th>Reference Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_edatemp</td>
<td>Current directory location. For server use this is the EDACONFIG edatemp agent directory (that is, ts000001, where 000001 is tscomid of the agent). For PDS Deployment, this is a temporary HFS location. For edastart -t, -x and -f uses, this is the current user directory.</td>
</tr>
<tr>
<td>_edahome</td>
<td>EDAHOME installation location.</td>
</tr>
</tbody>
</table>
What Is an Application?

<table>
<thead>
<tr>
<th>Reference Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_edaconf</td>
<td>EDACONF configuration location.</td>
</tr>
</tbody>
</table>

While the EDAHOME and EDACONF catalog locations are internally already on a server search path, special handles such as these allow you to explicitly reference names of the form _edahome/catalog/sysapps, which is one of a number of internal catalog tables.

**Note:** For platforms that support the Universal Naming Convention (UNC), you can specify a network drive for approot. The UNC must be:

- Minimally one folder below the initial shared location.
- Not contain spaces. For example:
  
  `\\mynode\myshare\accting`

### Generating Samples and Tutorials

You can generate several types of sample files and save them in an application in order to run sample procedures and test features and configurations.

The Web Console Applications page has a button named *Tutorials*, which you can click to open the *Create Tutorial Framework* page. You can also right-click an application folder and select *New*, then *Tutorials*, from the context menu.

Following is the list of available tutorials.

- WebFOCUS - Retail Demo
- WebFOCUS - Express Demo
- WebFOCUS - State Population Demo
- WebFOCUS - Star Schema with Variable Data
- WebFOCUS - Custom SQL Security Provider DataMigrator - General
- DataMigrator - Iterator
- DataMigrator - File Listener
- DataMigrator - Star Schema
- Create Legacy Sample Tables and Files

In the past, a static application directory named IBISAMP was created and populated with a number of files. Additionally, there were Web Console and Data Management Console (DMC) folder options for selecting and creating items to be used with those products.
The IBISAMP folder is still created as part of the installation process, but it is not populated. You can create those legacy sample files by choosing Create Legacy Sample Tables and Files from the Tutorial drop-down list.

Because the change is implemented at the folder level, you can choose to continue using IBISAMP as the location for creating the legacy files, or you can select any other folder. The drop-down option for Legacy samples creates most, but not all, of the sample files that used to be in IBISAMP. Some of the prior files were actually DataMigrator-related, and those have been moved to their own tutorials.

Under z/OS PDS Deployment there are some additional restrictions. The z/OS PDS JSCOM Listener option must have been selected at installation time. The PDS JSCOM option also co-installs some HFS source files that are used by the various create options. If the HFS files for a z/OS PDS Deployment are not present, request to create a tutorial will produce a specific HFS files not found message. Note that not all tutorials are implemented for z/OS, and those will produce a not implemented message, if selected.

### Procedures and Metadata on the Application Tree

**Reference:**

- Application Tree Icons
- Context Menu Options for the Application Directories Tree
- Context Menu Options for an Application Directory
- Context Menu Options for All Files in an Application Directory
- Context Menu Options for Stored Procedures
- Context Menu Options for DataMigrator and Direct Load Flows
- Context Menu Options for Quick Queries
- Context Menu Options for User Functions
- Context Menu Options for HTML Files
- Context Menu Options for Custom Pages
- Context Menu Options for Synonyms

The Applications menu groups all application files, including procedures, synonyms, HTML files, data flows, user functions, and other files on a single application tree. By default, files in an application are listed in order of file type. The file type is indicated by a unique icon for each type that displays to the left of the file name in the tree. However, you can sort or filter the list to generate custom views of each application.
The following image shows an Application tree with some typical file icons.

Right-clicking an item brings up a context menu. The items you see on the context menu depend on your role and the type of file. Some items are only available to administrators or other users with administrator privileges. Some of the items on the context menu provide shortcuts to items on the Workspace or My Console menu.
**Reference: Application Tree Icons**

The following table lists the icons displayed for each type of file on the application tree.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Type of File</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Closed application directory</td>
</tr>
<tr>
<td></td>
<td>Opened application directory</td>
</tr>
<tr>
<td>![Icon]</td>
<td><strong>Metadata</strong></td>
</tr>
<tr>
<td>![Icon]</td>
<td>Synonym (.mas)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Cluster synonym (.mas)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Business View synonym (.mas)</td>
</tr>
<tr>
<td>![Icon]</td>
<td><strong>Procedures</strong></td>
</tr>
<tr>
<td>![Icon]</td>
<td>Stored Procedure (.fex)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>DataMigrator Flow (.fex)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>DataMigrator Flow with IUD (.fex)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>DBMS SQL Flow (.fex)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Direct Load Flow (.fex)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Direct Load Flow with IUD (.fex)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>User Function (.fex)</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Scheduled Only (.fex)</td>
</tr>
<tr>
<td>Icon</td>
<td>Type of File</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Documents</td>
</tr>
<tr>
<td><img src="image" alt="HTML" /></td>
<td>HTML file (.htm, .html, .shtml, .htt, .mht, .mhtml, .cfm, .tpl, .hta, .htb)</td>
</tr>
<tr>
<td><img src="image" alt="Excel" /></td>
<td>Microsoft Excel® Document (.xls, .xlsx, .xlsb, .xht, .xltx, .xlsm, .xltm)</td>
</tr>
<tr>
<td><img src="image" alt="PDF" /></td>
<td>Adobe Acrobat Document (.pdf, .ai)</td>
</tr>
<tr>
<td><img src="image" alt="XML" /></td>
<td>XML Document (.xml, .wsd, .xsd, .wsdl, .mxml, .gcl, .xul, .dtd, .xsl, .xslt, .axl)</td>
</tr>
<tr>
<td><img src="image" alt="JSON" /></td>
<td>JavaScript Object Notation (.json)</td>
</tr>
<tr>
<td><img src="image" alt="PowerPoint" /></td>
<td>Microsoft PowerPoint® Document (.ppt, .pptx, .pptm)</td>
</tr>
<tr>
<td><img src="image" alt="Word" /></td>
<td>Microsoft Word® Document (.doc, .docx, .docm, .dot, .dotx, .dotm)</td>
</tr>
</tbody>
</table>
### Reference: Context Menu Options for the Application Directories Tree

The following options are available when you right-click the top level of the Application Directories tree:

- **New.** Enables you to create new application files. The available context menu options are:
  - **Procedure.** Opens a text box in which you can create a new FOCEXEC as text.
  - **Synonym (Create or Update).** Opens a window that enables you to configure an adapter or create a synonym.
  - **Custom Page.** Enables you to create pages that monitor the various services available from the Workspace folder, as well as run procedures.
Procedures and Metadata on the Application Tree

- **File.** Opens a text box in which you can create a new file as text.
- **Application Directory.** Enables you to create a new application directory folder.
- **Upload file.** Enables you to upload a file to an application directory folder.
- **Filter.** Enables you to customize the items that display on the application tree. Selecting any item on the context menu opens the Filter Applications Tree screen. For more information, see *Filtering the Application Tree* on page 205.
- **Search File.** Enables you to find files bases on a range of search criteria. For more information, see *Searching for Files* on page 212.
- **Sort by.** Enables you to sort application files by Name, Size, Type (the default), or date Modified. For more information, see *Sorting the Application Tree* on page 214.
  
  If you select Sort by Size, the size in bytes of each file is indicated next to its name on the Application tree.
  
  If you select Sort by Modified, the date each file was last modified is indicated next to its name on the Application tree.

- **Application Preferences.** Enables you to customize the tree display. The available options are:
  
  - **Show sub-directories last.** Shows subdirectories at the bottom of the tree.
  
  - **Show Applications not in Path.** Adds an Inactive Directories tree listing all of the applications not in the path to the Application Tree. When the Inactive Directories tree is displayed, the context menu option changes to Hide Applications not in Path.
    
    Note that this option is only available for the server administrator and users with server administrator privileges. Users with these privileges can manage (add, delete, copy, move, or modify files) directories that are not in the Application Path.

  - **Show Statistics on Applications Tree.** Shows the number of files in the directory when the mouse hovers over an application directory.

  - **Show Descriptions on Applications Tree.** Shows the file description when the mouse hovers over a file.

  - **Show Application Profile.** Shows the current application profile.

  - **Show edahome, edaconf, edaprfu, scaroot, edatemp and foccache of all users.** Shows the foccache, edatemp, and other internal locations as folders of all users. This option is only available for the Server Administrator and users with administrator privileges.
Number of files per page on Application Tree. Enables you to separate the contents of a folder into pages, displaying a Next icon to page to additional files. The default is zero (0), which does not separate the contents into pages.

Application Settings. Opens the Application Settings pane.

Manage SQL Repository. Provides options to create and manage SQL repositories, allowing you to store the contents of an application folder in an SQL database.

Application Path. Opens the Application Path pane under the My Console menu while leaving the Application Directories tree open in the left pane.

Create My Home. Creates the home application directory of the user. (DataMigrator or Managed Reporting license required.)

Schedule and E-mail. Enable you to view or manage events while leaving the Application tree open in the left pane. You can select Scheduler Agents or Scheduled Events.

Log and Statistics. Enable you to view various logs and statistics while leaving the Application tree open in the left pane.

Impact Analysis. Reports on your use of synonyms, columns, and procedures. The choices are Synonyms by Procedure, Procedures by Synonym, Columns by Procedure, and Procedures by Column. In addition, you can select a Summary or Detailed flow report.

Tutorials. Opens the Create Tutorial Framework page where you can create samples tables and metadata.

Reference: Context Menu Options for an Application Directory

Like the top level of the Application Directories tree, application directory folders include New, Schedule and E-mail, and Impact Analysis options, as described in Context Menu Options for the Application Directories Tree on page 169.

Application directory folders also include the following right-click options:

Refresh. Refreshes the list of files in the application.

Show All Files. Overrides the Number of files per page on Application Tree setting for this application folder.

Quick ETL Copy. Enable you to copy data when you have configured SQL adapters.
Manage Files. Opens the Manage Files pane that lists all files and applications in the selected application with their sizes, date modified, adapter type for synonym files, description, and table name, if applicable:

![Manage Files Pane]

You can select one or more files and applications and click the following buttons:

- **Copy.** Copies the files to another application directory. Select the target application from the drop-down list.

- **Move.** Moves the files to another application directory. Select the target application from the drop-down list.

- **Refresh Synonym.** Updates synonyms.
- **Delete.** Deletes the files from the application directory.

- **Cancel.** Closes the Manage Files pane.

**Note:** If you want to overwrite existing files of the same name in the target application, check the *Overwrite existing file when Copy/Move* check box. Copy, move and delete also allow you to include the subfolders of an application. Subfolders are copied, moved, or deleted with all their files and subfolders.

- **Logs and Statistics.** Opens the Logs and Statistics page where you can view a range of log and statistics reports.

- **Copy.** Copies the application directory.

- **Privileges.** Opens the Manage Privileges pane for the selected application:

If you check the *Filter* check box, you can filter which users or groups show on the pane.
Each user is listed under the appropriate roles, and the privileges for the role and the individual users are indicated by check marks in the relevant columns.

Right-click a user name to choose *Edit Privileges*. The File/Directory Privileges pane opens.

![File/Directory Privileges](image)

Check or uncheck the box in the *Effective* column to add or remove the indicated privileges for this user, and click *Apply* to save the changes.

Click *Reset to Default Privileges* to reestablish the default privileges based on the role this user was assigned.

- **Delete**. Deletes the application directory and is only available for application directories that you created.

- **Cut**. Cuts the application directory and is only available for application directories you created.

- **Paste**. Pastes the application directory.

- **Properties**. Opens the Properties pane that shows the location of the application directory, number of files in the directory, the date the directory was last modified, and the description. You can also edit the description using the text box provided.
Reference: Context Menu Options for All Files in an Application Directory

All files include the standard right-click options of Cut, Copy, Paste, and Delete. They include the Privileges option, as described in Context Menu Options for an Application Directory on page 171.

Files also include the following right-click options:

- **Open.** Opens the file in the editor associated with that type of file (not available for Quick Query, HTML, and Synonym).

- **Properties.** Opens the Properties pane that shows the location of the file, the date it was last modified, the Job Type, the description, and the privileges associated with the file.

Reference: Context Menu Options for Stored Procedures

Stored procedures include the Schedule and E-mail, Impact Analysis, and Privileges options, as described in Context Menu Options for the Application Directories Tree on page 169.

Stored procedures also include the following right-click options:

- **Run.** Runs the file if it is an executable file.

- **Run Advanced.** Opens a menu containing the following options:
  
  - **Submit with E-Mail.** Enables you to set up email notification when the procedure starts and/or completes, and to change default values of amper variables.

  - **Run Stress.** Opens a pane that enables you to set the number of threads, the interval, and the time to keep alive the procedure when it runs. You can also choose to generate statistics and comparisons for this run.
- **Debug.** Enable you to run the procedure in debug mode, as shown in the following image. You can step through the code, viewing the result for each line.

![Debug Focexec: ibisamp / carinst](image)

- **Logs.** Provides the following options:
  - **Last Log.** Displays the log from the last time the procedure was run.
  - **Last Output.** Displays the output from the last time the procedure was run.
  - **Logs and Statistics.** Opens the Logs and Statistics page where you can view a range of log and statistics reports.
Dependencies Analysis. Displays the Dependencies Analysis page, as shown in the following image. It enables you to see the synonym(s) and other procedures that are used by the procedure.

![Dependencies Analysis](image)

Reference: Context Menu Options for DataMigrator and Direct Load Flows

DataMigrator and Direct Load Flows include the Schedule and E-mail and Impact Analysis options, as described in Context Menu Options for the Application Directories Tree on page 169. They include the Run, Run Advanced, Logs, and Dependencies Analysis options, as described in Context Menu Options for Stored Procedures on page 175.

DataMigrator and Direct Load Flows also include the following options:

- **Submit.** Submits the flow for processing.
- **Flow Report.** Displays details about the flow, including source and target information, load options, SQL select statements, transformations, execution properties, and record logging.

Reference: Context Menu Options for Quick Queries

Quick Queries include the Schedule and E-mail and Impact Analysis options, as described in Context Menu Options for the Application Directories Tree on page 169. They also include the Run, Run Advanced, Submit with Options, and Logs options, as described Context Menu Options for Stored Procedures on page 175.
**Reference:** **Context Menu Options for User Functions**

In addition to the standard file options (Cut, Copy, Paste, Delete, and Properties), User Functions include the Test right-click option, which tests the function.

**Reference:** **Context Menu Options for HTML Files**

In addition to the standard file options (Cut, Copy, Paste, Delete, and Properties), HTML files include the Run and Logs options, as described in [Context Menu Options for Stored Procedures](#) on page 175.

HTML files also include the following options:

- **Edit.** Enables you to edit the HTML code.
- **View.** Enables you to view how the file displays in a browser.

**Reference:** **Context Menu Options for Custom Pages**

Custom Pages include the standard file options (Open, Cut, Copy, Paste, Delete, Privileges, and Properties). Custom Pages also include an Edit option.

**Reference:** **Context Menu Options for Synonyms**

Synonyms include the Impact Analysis option, as described in [Context Menu Options for the Application Directories Tree](#) on page 169. They include the Quick ETL Copy option, as described in [Context Menu Options for an Application Directory](#) on page 171. They also include the Dependencies Analysis option, as described in [Context Menu Options for Stored Procedures](#) on page 175.

Synonyms also include the following options:

- **Edit as Text.** Opens a Master File in a text editor.
- **Edit Access File as Text.** Opens an Access File in a text editor.
- **Sample Data.** Runs a sample report against a synonym.
- **Data Profiling.** Runs a report against a synonym listing its segments, fields, and field information, with a drill-down report to field values.
- **Data Management.** Enables you to recreate a DBMS table, delete all data, or produce sample data from a synonym.
Managing Applications and Paths

In this section:

Creating and Mapping Applications
Using an SQL Database to Store Application Contents
Nested Application Directories
Home Application Directories for Users
Configuring the Application Path
Filtering the Application Tree
Searching for Files
Sorting the Application Tree
Managing Application Files

Path management tasks are available from the Applications page, which is accessed by clicking Applications on the Web Console menu bar. The Application Directories tree displays is on the navigation pane. The ribbon and the top of this pane include a set of icons that provide the quickest way to initiate path management tasks.

A single click on one of the following icons is enough to get you started.

- Hide and Show tree
  Toggles the navigation pane on and off, allowing one or both panes to occupy the screen.
  Note that these icons are displayed in any context in which you might wish to toggle the navigation pane on and off.

- Filter
  This icon opens the Filter Applications Tree page, where you can filter files on a range of criteria.

- Application Path
  This icon provides a quick way to manage the application path.
Opens the Application Path pane where you can create applications, add applications to the search path, map and reorder applications, and delete applications or mappings.

The Application Path pane provides additional icons designed to facilitate these tasks.

- Refresh

Depending upon the selected context in the navigation pane, this icon refreshes the synonyms or procedures and HTML files listed in the application tree.

Note that this icon is displayed in any context in which you might wish to refresh the display of objects on the navigation pane.

**Note:** You can also right-click the Application Directories folder in both the Web Console and the Data Management Console to access the *Application Path* option.

**Creating and Mapping Applications**

**How to:**
- Create an Application
- Map an Application to a Physical Directory
- Delete an Application or the Application Mapping

Applications are designed to group related components.

- When you create a new physical application, it becomes available for addition to the search path in a selected profile.

- When you map an application name to an existing physical location outside of approot, the mapped application becomes available for inclusion in the search path of a selected profile.

Applications can be created and mapped in either the Web Console or the Data Management Console.

Application directory names must comply with the following rules:

- The maximum length is 64 characters.

- For multi-part Application directories, the total length is limited to 512 characters.
Names can contain any valid alphanumeric character except the following:

- space character
- star character
- question mark
- less than sign
- greater than sign
- ampersand
- backslash
- comma
- dot
- colon
- double quotation mark
- single quotation mark
- tab
- null terminator character

**Procedure: How to Create an Application**

1. From the Web Console menu bar, click **Applications**, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Applications page opens.

2. Right-click the **Application Directories** folder, select **New**, and then **Application Directory**.
The Create New Application page opens.

3. Use the default Application Type, New Application under APPROOT.

4. Enter a name in the Application Name field.

5. Optionally, select the Recreate application if exists check box.
   **Warning:** Choosing this option will overwrite the existing application and any content in it.

6. Enter a description in the Description field.

7. The Add directory to APPPATH option is the default. Optionally, you can decide not to add the directory.

8. Select a position from the Position in APPPATH drop-down menu. The options are Last and First. The default is Last.

9. Select a profile from the Profile drop-down menu. For Server Administrators, the default is edasprof. For all other users, the default is the user profile.

10. Click OK.

   The application is added to the Application Directories folder.
Procedure: How to Map an Application to a Physical Directory

You can map an application name to a physical directory anywhere in the file system. This application name can be then used in APP commands.

Application mappings can be added and deleted based on profiles from either the Web Console or the DMC.

1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Applications page opens.

2. Right-click the Application Directories folder, select New, and then Application Directory.

   The Create New Application page opens.

3. Select Application Mapping to Disk or SQL Repository from the Application Type drop-down menu.

   ![Create New Application](image)

4. Enter a name in the Application Name field.

5. Accept the default Physical location, enter a different location, or click the selector button (...) and navigate to a directory on your file system.
For platforms other than z/OS HFS Deployment, in addition to using the selector button, you can enter the full path of the physical directory to be mapped, in the format required on your platform. (If there are spaces in the directory you are mapping, you must enclose the entire path in double quotation marks.)

For z/OS HFS and PDS servers, in addition to using the selector button, you can enter values using the following formats:

\[\text{ext} = \\DD:ddname[; \text{ext2} = \\DD:ddname2][...][; \text{extn} = \\DD:ddnamen]\]

where \text{extn} are file type extensions.

\text{/dir/subdir}

entered manually or using the selector button.

For z/OS PDS servers, you can also inform the high-level qualifiers of the data set collection that comprise this application. Here is an example of the format:

\text{iADMIN.SRV77.MAPAPP}

where the user has the following datasets (not in approot):

\text{IADMIN.SRV77.MAPAPP.FOCEXEC.DATA}
\text{IADMIN.SRV77.MAPAPP.MASTER.DATA}
\text{IADMIN.SRV77.MAPAPP.ACCESS.DATA}
6. Select *New application (directory will be created)* from the *Map to* drop-down menu, as shown in the following image.

![Create New Application](image)

7. Optionally, enter a description in the *Description* field.

8. *Add directory to APPPATH* is the default. Optionally, you can decide not to add the directory.

9. Select a position from the *Position in APPPATH* drop-down menu. The options are *Last* and *First*. The default is *Last*.

10. Select a profile from the *Profile* drop-down menu.

    For Server Administrators, the default is *edasprof*. For all other users, the default is the user profile.

11. Click *OK*.

    The mapping is added to the *Application Directories* folder.

**Procedure: How to Delete an Application or the Application Mapping**

Applications and application mappings can be deleted from either the Web Console or the DMC.
1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Applications page opens.

2. Right-click the application or application mappings and select Delete or Delete Mapping, respectively.

   A confirmation dialog box opens.

3. Click OK to delete the application or application mapping.

   **Note:** Deleting an application mapping will delete it from any APP PATH commands that reference it, if the APP PATH command is in the same profile as APP MAP.

**Using an SQL Database to Store Application Contents**

**How to:**

Create an SQL Repository to Store Applications

Create an Application With SQL Content

In addition to using a physical location, the contents of an application folder can also be stored in an SQL database. To use an SQL database, you must first create a new SQL Repository. After the repository is created, you can create applications mapped to the SQL Repository and store files there.

**Warning:** It is advisable to create a separate SQL Connection to use in creating an SQL Repository. If an existing SQL Connection is used, only Server Administrators or users with WSCFG privileges will be able to use the synonyms from this SQL connection in the application. This provides protection for the SQL Repository, preventing unauthorized users (without administrator privileges) from accessing the contents of the SQL Repository through a synonym.

**Procedure:** How to Create an SQL Repository to Store Applications

You must have an adapter connection configured to an SQL database.
1. From the ribbon, click the **Manage SQL Repository** icon and select **Create New**, or right-click the **Application Directories** folder in the navigation pane, select **Manage SQL Repository**, and then **Create New**, as shown in the following image.

![Manage SQL Repository](image1.png)

The Create New SQL Repository page opens, as shown in the following image.

![Create New SQL Repository](image2.png)

2. Select a configured adapter from the Adapter drop-down menu.
3. Select a connection from the Connection drop-down menu.

4. Enter a prefix in the Prefix field.

5. Optionally, select the Overwrite existing repository tables and their synonyms check box.

6. Click OK.
   
   A warning message is displayed, as shown in the following image.

   ![Select an Option](image)

7. Click OK.

   Two SQL Repository catalog tables are created with this connection, as shown in the following image.

   ![List and Delete SQL Repository](image)

   The tables are:

   - `prefixIOHFILETABLE`
   - `prefixIOHRECORDTABLE`

   Two synonyms describing the catalog tables are also created in EDACONF/catalog/IOH.

8. Optionally, click Create New Application.
The Create New Application page opens, as shown in the following image.

**Procedure:** How to Create an Application With SQL Content

You must have created an SQL Repository.
1. From the Applications page, right-click the Application Directories folder in the navigation pane, select New, then Application Directory, as shown in the following image.

The Create New Application page opens.
2. Select *New Application under repository - DBMS (Connection name)* from the Application Type drop-down menu, as shown in the following image.

![Create New Application](image)

**Note:** The choices will include the repository, adapter type, and connection name. In this example, they are the bks repository, Adapter for Microsoft SQL Server, and CON01 connection.

3. Enter a name in the *Application Name* field.

4. Optionally, select the *Recreate application if exists* check box.

   **Warning:** Choosing this option will overwrite the existing application and any content in it.

5. Optionally, enter a description in the corresponding field.

6. Optionally, deselect the *Add directory to APPPATH* check box. The application is added to the APPPATH by default.

7. Select a position for the application from the *Position in APPPATH* drop-down menu. The choices are *Last* or *First*. The default value is *Last*.

8. Select a profile from the *Profile* drop-down menu. For server administrators, the default value is *edaprof*. For non-administrators, their user profile is the default value.

9. Click *OK*.

The application is added to the navigation tree. You can now use this application to store procedures, synonyms, data files, and other content.
Nested Application Directories

How to:
Set the Level of Nested Application Directories
Create a Nested Application Directory

A nested application directory is one created within a higher-level application. The server allows five levels of nested application directories by default, except on z/OS under PDS deployment, where applications cannot be nested. The server must be configured for deeper or unlimited levels.

Nested application directories are implicitly added to the application path if the parent directory is on the application path.

For example, the following application tree has a directory named new1 that has a child directory named new2.

The APP PATH command explicitly places new1 on the application path:

```app
APP MAP new1 "C:\ibi\apps\new"
APP PATH baseapp ibisamp new1
```

However, you can test the path to see all of the implicitly added directories by right-clicking the top level of the Applications Directories tree and selecting Application Path. When the Application Path page opens, click Test:
The effective application path also includes new1/new2:

![Test Application Path](image)

**Procedure:** How to Set the Level of Nested Application Directories

1. From the menu bar, select Applications.

2. From the ribbon, click the Application Settings icon, or right-click the Applications folder, and select Application Settings.

   The Application Settings page opens.
3. Enter the level of nested applications in the `nested_app` field or select `y` from the drop-down menu. The default value is 5. Selecting `y` allows unlimited levels of nested applications.

![Application Settings](https://example.com/app_settings.png)

**Note:** For z/OS servers, this setting is only applicable to directory-style applications. It is not applicable to PDS-style applications or to applications mapped as a collection of ddnames.

4. Click the `Save and Restart Server` button.

After the server restarts, you can create a new application subdirectory by right-clicking an application folder and selecting `New` and then `Application Directory` from the context menu.

**Note:** Nested applications must be in effect in order to create user home application directories.

**Procedure:** **How to Create a Nested Application Directory**

1. From the Web Console menu bar, click `Applications`, or from the Data Management Console, expand the Server node folder.
   
   On the Web Console, the Applications page opens.

2. Right-click an application, select `New`, and then `Application Directory`. 


The Create New Application Directory page opens.

3. Enter a name in the Application Name field.

4. Optionally, enter a description in the Description field.

5. Click OK.

The nested application is added to the application tree under its parent application folder.

Home Application Directories for Users

You can configure the server to allow each user to have a home application directory. Providing a user home application directory gives each user a directory where he has full control to create, change, and run his applications.

The home application for any user who is not a server administrator appears in two places on the Web Console application tree. Both of these applications point to the same physical location, so that they can be referenced in two ways. The two applications are:

- Application myhome, which is prepended to APPPATH.
- Application homeapps, which is appended to APPPATH and can be expanded to see the user home application with the user ID name, such as pgmtst1.

Server administrator users have the myhome application prepended and the homeapps application appended to APPPATH, The homeapps folder can be expanded to show the home applications for all users.
The following image shows both the myhome application and the homeapps application for user *pgmtst1*:

The files created in home applications can be referenced in procedures as `myhome/procname.fex` and `homeapps/pgmtst1/procname.fex`.

The first type of reference can be ported easily to any user. It enables you to create a common application that utilizes data stored in the home applications of users as `myhome/data`, so that each user can run the same procedure but get a report based on the data stored in the home application of that user.

The second type of reference enables you to run applications specific to a user, referring to the data and procedure for each user as `homeapps/pgmtst1/proc1.fex` and `homeapps/pgmtst1/data`. This type of reference can be used for testing applications before moving them to common application folders.

Home application directories should be enabled only on secured servers. If the server runs with security OFF, all users have total control of files in all applications, and the home directories will not work as designed. Nested applications must be enabled in order to create user home application directories.

The Server Administrator can monitor and manage home application directories for all users and, therefore, all user home directories are visible and in the path on the Web Console application tree when the connected user has Server Administrator privileges.

When the server is enabled for home applications, user home application directories are not created automatically. Users can create them from the Web Console Application page, or ask their server admin to create them.
Home applications can also be stored in an SQL Repository. You must first create an SQL Repository and configure the application settings `homeapps` parameter to point to the SQL Repository, as described in *Using an SQL Database to Store Application Contents* on page 186.

After a home application directory is created for a user:

- The home application is added to the users application path by the server implicitly. A user cannot remove it from the path using APP commands.
- The home application directory is always first in the users active application path.
- Non-server administrator users will only see their own home application on the Application tree. The server admin or a user with server admin privileges will see all user home applications. The server admin has full privileges to manage user home applications.

**Note:** This feature is available only for customers that are licensed for Managed Reporting or DataMigrator.

**Procedure:**  **How to Manage Home Application Directories**

In order to set up home directories for individual users, nested applications must be enabled. They are enabled to five levels by default. The home directory under which user application directories will be created is set during installation. The default is `homeapps`. The `homeapps` directory can be changed to a different physical location on the Application Setting page. All user home directories will be nested under the home directory.

1. From the menu bar, select *Applications*.
2. From the ribbon, click the *Application Settings* icon, or right-click the *Applications* folder, and select *Application Settings*.

   The Application Settings page opens.

3. Check the location of the `homeapps` directory. You can set the `homeapps` parameter to point to a physical directory or to an existing SQL Repository.

4. Click the *Save and Restart Server* button to implement these changes.

   When the server restarts, go to the *Applications* menu. For a user with Server Administrator privileges, a *users home* folder will appear under the Application Directories tree and will have all of the user home directories.

   Users who do not have server administrator privileges can see their home directory under application *myhome*, which is prepended to APPPATH.

   Server administrator users have the myhome application prepended and the homeapps application appended to APPPATH. The homeapps folder can be expanded to show the home applications for all users.
The following image shows both the myhome application and the homeapps application for user `pgmtst1`:

The files created in home applications can be referenced in procedures as `myhome/procname.fex` and `homeapps/pgmtst1/procname.fex`.

The first type of reference can be ported easily to any user. It enables the server administrator to create a common application that utilizes data stored in the home applications of users as `myhome/data`, so that each user can run the same procedure but get a report based on the data stored in the home application of that user.

The second type of reference enables the server administrator to run applications specific to a user, referring to the data and procedure for each user as `homeapps/pgmtst1/proc1.fex` and `homeapps/pgmtst1/data`. This type of reference can be used for testing applications before moving them to common application folders.

**Procedure:** How to Store Home Applications in an SQL Repository

You must first create an SQL Repository. For information, see *How to Create an SQL Repository to Store Applications* on page 186.
1. From the ribbon, click the Application Settings icon, or right-click the Application Directories folder in the navigation pane, and select Application Settings, as shown in the following image.

The Application Settings page open, as shown in the following image.
2. Click the selector button (...) next to the homeapps field. The Select physical location dialog box opens.

3. Select SQL Repository, as shown in the following image.

![Select physical location dialog box]

4. Select a subfolder, and click OK.
   The subfolder is entered in the homeapps field, as shown in the following image.

![Homeapps field with SQL directory selected]

5. Click Save and restart Server.
   Home applications that are created will now be stored in the SQL database.
Configuring the Application Path

**How to:**
- Configure the Application Path
- Configure the Application Path in a User, Group, or Role Profile
- Edit a Profile

The applications available for inclusion in the search path are identified by name, type, and physical location. If the Add directory to APPPATH check box was selected when the application was created, it was automatically added to the search path. If not, you must explicitly add it to your search path.

**Note:** You can also create profiles from the Application Path page. Profiles are the locations in which the search path is saved.

**Procedure: How to Configure the Application Path**

You can configure the Application Path to add or remove applications or mappings from either the Web Console or the DMC.

1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.
   
   On the Web Console, the Applications page opens.

2. From the ribbon, click the Application Path icon, or right-click the Application Directories folder in the navigation pane, and select Application Path.
   
   The Application Path page opens.

3. Select a profile from the Profile drop-down menu. The default is edaprof.
4. Select the check box in the *In Path* column for the application or mapping.

5. Optionally, you can reorder applications in the APP PATH, using the *Up* and *Down* icons at the right. The top and bottom buttons move the application to the start or end of the APP Path. The center buttons move the application up or down one position.

6. To remove an application, deselect the check box in the *In Path* column.
7. Optionally, click Test to test modifications to the search path. A Test Application Path pane opens.

![Test Application Path](image)

The Test Application Path pane shows:

- **Executed profiles.** This depends on the level of the profile you selected.

- **Executed commands.** These are the APP commands executed for the profile you selected. The commands can include APP PATH, APP MAP, APP APPENDPATH, or APP PREPENDPATH.

- **Effective APP PATH.** This is the effective application tree that will result from all the executed profiles, including the selected profile level. The execution sequence is: server profile (edasprof.prf), service profile, role profile, group profile, and user profile.

8. Click Save.

The navigation pane is updated.

**Note:** You can also create a new profile from the Application Path page.

**Procedure:** How to Configure the Application Path in a User, Group, or Role Profile

The Application Path can be configured from either the Web Console or the DMC.
1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.

On the Web Console, the Applications page opens.

2. From the ribbon, click the Application Path icon, or right-click the Application Directories folder in the navigation pane, and select Application Path.

The Application Path page opens.

3. From the Profile drop-down menu, select New Profile.

4. Enter a name in the New Profile Name field.

5. Select an option from the Application Path drop-down menu.

The options are:
- Inherit from previously executed profiles
- Override previously executed profiles
- Prepend previously executed profiles
- Append to previously executed profiles
6. Optionally, click *Preview* to see the profile.

![Preview profile NewUSER-](image)

7. Click Save.

**Procedure: How to Edit a Profile**

1. From the menu bar, select *Workspace*.
2. On the navigation pane, open the *Configuration Files* and *User/Group Profiles* folders.
3. Right-click the profile and select *Edit*.

   The profile opens in a text editor with its current path displayed.

4. Edit the path information and click the *Save* icon.

**Tip:** You can also edit a profile search path by selecting and saving configuration options. Follow instructions for configuring the application path.

### Filtering the Application Tree

**How to:**

Filter Items on the Application Tree

Filtering enables you to customize the file listings on the Application tree, displaying only the files you choose. It can be based on file name, location, statistics, type, or any combination of items matching a number of criteria.
**Procedure:** How to Filter Items on the Application Tree

You can customize the items that display on the Application Tree by filtering. Your filtering selections apply to all applications displayed in the navigation pane.

1. From the Web Console menu bar, click **Applications**.

2. Click the **Filter** icon above the navigation pane, and select **Procedures**, **Synonyms**, or **Advanced**, as shown in the following image.

   ![Filter options](image)

   a. If you choose **Procedures**, you can display all procedures or only scheduled ones.

   b. If you choose **Synonyms**, you can display all synonyms or only cluster or business views.

   c. If you choose **Advanced**, The Filter Applications Tree page opens.
Using the File Name section, you can filter by name, extension, description and content, as shown in the following image. To filter the name, you can use the percent sign (%) as a wildcard character. Specifying e% displays all files whose name begins with the letter e.
3. Using the File Location section, you can filter by Application Directory, Application Path, Mapped Applications, and Applications under APPROOT, as shown in the following image.
4. Using the File Statistics section, you can filter by file size and modified date, as shown in the following image.
5. Using the File Type section, you can filter by type of file to be included.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata</td>
<td></td>
</tr>
<tr>
<td>Adapters</td>
<td></td>
</tr>
<tr>
<td>Cluster Only</td>
<td></td>
</tr>
<tr>
<td>Business View Only</td>
<td></td>
</tr>
<tr>
<td>Procedures</td>
<td></td>
</tr>
<tr>
<td>Flows</td>
<td></td>
</tr>
<tr>
<td>Regular Flows with IUD</td>
<td></td>
</tr>
<tr>
<td>DBMS SQL Flows</td>
<td></td>
</tr>
<tr>
<td>Direct Load Flows</td>
<td></td>
</tr>
<tr>
<td>Direct Load Flows with IUD</td>
<td></td>
</tr>
<tr>
<td>User Functions</td>
<td></td>
</tr>
<tr>
<td>Scheduled Only</td>
<td></td>
</tr>
<tr>
<td>Documents</td>
<td></td>
</tr>
<tr>
<td>HTML</td>
<td></td>
</tr>
<tr>
<td>MS Excel Documents</td>
<td></td>
</tr>
<tr>
<td>Adobe Acrobat Documents</td>
<td></td>
</tr>
<tr>
<td>XML Documents</td>
<td></td>
</tr>
<tr>
<td>JavaScript Object Notations</td>
<td></td>
</tr>
<tr>
<td>MS PowerPoint Documents</td>
<td></td>
</tr>
<tr>
<td>MS Word Documents</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
<tr>
<td>SQL Scripts</td>
<td></td>
</tr>
<tr>
<td>Data Files</td>
<td></td>
</tr>
<tr>
<td>Custom Monitor Pages</td>
<td></td>
</tr>
<tr>
<td>Graphical Files</td>
<td></td>
</tr>
<tr>
<td>Style Files</td>
<td></td>
</tr>
<tr>
<td>Cascading Style Sheets</td>
<td></td>
</tr>
<tr>
<td>Archive Files</td>
<td></td>
</tr>
<tr>
<td>Script Files</td>
<td></td>
</tr>
<tr>
<td>Log/Trace Files</td>
<td></td>
</tr>
<tr>
<td>Configuration Files</td>
<td></td>
</tr>
<tr>
<td>Other Documents</td>
<td></td>
</tr>
<tr>
<td>MAINtain Files</td>
<td></td>
</tr>
</tbody>
</table>
6. Optionally, select an adapter from the Adapters drop-down menu. Only synonyms created with that adapter that match the filtering criteria will appear in the tree.

7. Click Set Filter. The Filter Status page confirms that the filter was set.

When a filter is applied, the Application Directories tree label includes (Filtered), as shown in the following image.

![Filter Status for Applications Tree](image)

**Note:** You can remove the filter by clicking the Clear Filter button.

You can see the filter results by clicking Show Report, as shown in the following image.
Searching for Files

How to:

Search for Files

The Search Files tool provides a search function on the Application Tree. It can search for files using a variety of criteria, including file name, location, description, contents, statistics, and type, in an application directory or across the entire server.

To view the file search page, click the Search Files button on the Applications page ribbon, or right-click the Application Directories folder and select Search Files on the context menu.
The Search Files page opens, as shown in the following image.

**Search Files**

<table>
<thead>
<tr>
<th>Search</th>
<th>Cancel</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>File Name</th>
<th>Sample: .m%</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Extension</td>
<td>Sample: .txt</td>
</tr>
<tr>
<td>File Description</td>
<td>Sample: my desc</td>
</tr>
<tr>
<td>File Content</td>
<td>Sample: my text</td>
</tr>
</tbody>
</table>

Enter your search criteria, and click **Search**.

The report returned allows you to open procedures, Master Files, and displayable data in the editor.

**Procedure: How to Search for Files**

The Search Files page provides a wide range of search criteria.

1. From the Web Console menu bar, click **Applications**.
2. Click the **Search Files** icon.
   
The Search Files page opens.
3. Select the search criteria from the **File Name**, **File Location**, **File Statistics**, and **File Type** sections.
4. Click the **Search** button.

The Search Results are displayed, as shown in the following image.
Sorting the Application Tree

**How to:**
Sort the Application Tree

Sorting enables you to change the order in which items are listed on the application tree.

**Procedure:** How to Sort the Application Tree

1. From the Web Console menu bar, click Applications.
   
The Applications page opens.

2. From the ribbon, click the Sort by icon, and select a sort method, as shown in the following image.

   ![Sort by Icon](image)

   You can sort by Name, Size, Type, or Modified date. Type is the default.
Managing Application Files

How to:
Manage Application Files
Refresh Synonyms in an Application

You can copy and move files between applications, delete them from applications, and refresh synonyms in applications. You can also copy, move, or delete subfolders from one application to another. The subfolders will be copied, moved, or deleted with all of its files and all of its own subfolders.

Procedure: How to Manage Application Files

1. From the Web Console menu bar, click Applications.
2. Right-click an application folder and select *Manage Files*.
The Manage Files page opens.

3. Select the check box next to one or more files. To select all files, click Select All.

4. Enter an application folder in the Current Application field.
The selector (...) button opens the Select current application dialog box which allows you to navigate to the application, as shown in the following image.

5. Enter an application folder in the To Application field or click the selector button (...) and navigate to one.
6. Click Copy or Move.
   The file(s) are copied or moved to the selected application.
7. To delete files, select their check boxes and click Delete.

Procedure: How to Refresh Synonyms in an Application

1. From the Web Console menu bar, click Applications.
2. Right-click an application folder and select Manage Files.
   The Manage Files page opens.
3. Select the check box next to one or more synonyms.
   To refresh all listed synonyms in the selected application, click Select All.
4. Click Refresh Synonym.
Application Commands Overview

This topic lists the platform-independent application (APP) commands that enable you to control the application environment.

You can use the following wildcard characters in the file name and file type references for the APP commands COPYFILE, MOVEFILE, DELETEFILE, and RENAMEFILE.

- An asterisk (*) replaces any combination of characters of any length (including zero).

  Note that an asterisk can also be used to replace the entire filename or filetype parameter.

- A question mark (?) replaces zero or one character.

Reference: APP Commands Quick Reference

Click any command in the following charts to access detailed information, including the required syntax.

Search Path Management Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APP PATH</strong></td>
<td>Sets or resets the application search path.</td>
</tr>
<tr>
<td><strong>APP PREPENDPATH</strong></td>
<td>Temporarily adds application names to the beginning of an existing APP PATH search path.</td>
</tr>
<tr>
<td><strong>APP APPENDPATH</strong></td>
<td>Temporarily adds application names to the end of an existing APP PATH search path.</td>
</tr>
<tr>
<td><strong>APP MAP</strong></td>
<td>Defines a virtual application that points to a physical location outside of the approot structure. This command makes the virtual application available for addition to the search path. It does not automatically add it to the APP PATH.</td>
</tr>
<tr>
<td><strong>APP SET METALLOCATION_SAME</strong></td>
<td>Indicates whether corresponding Master and Access files must be in the same application directory.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>APP ? METALOCATION_SAME</td>
<td>Retrieves the value of APP SET METALOCATION_SAME.</td>
</tr>
<tr>
<td>APP SHOWPATH</td>
<td>Lists all the currently active applications in the search path.</td>
</tr>
</tbody>
</table>

**Application Management Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP COPY</td>
<td>Copies the contents of one application to a second application.</td>
</tr>
<tr>
<td>APP CREATE</td>
<td>Creates an application under the approot location.</td>
</tr>
<tr>
<td>APP DELETE</td>
<td>Deletes an application.</td>
</tr>
<tr>
<td>APP MOVE</td>
<td>Moves the contents of one application to a second application.</td>
</tr>
<tr>
<td>APP PROPERTY CODEPAGE</td>
<td>Specifies a code page for files in an application.</td>
</tr>
<tr>
<td>APP RENAME</td>
<td>Renames an application.</td>
</tr>
</tbody>
</table>

**File Management Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP COPYF[ILE]</td>
<td>*Copies a single component or component type from one application to another.</td>
</tr>
<tr>
<td>APP MOVEF[ILE]</td>
<td>*Moves a single component or component type from one application to another.</td>
</tr>
<tr>
<td>APP RENAMEF[ILE]</td>
<td>*Renames a single component or component type in an application.</td>
</tr>
<tr>
<td>APP DELETEF[ILE]</td>
<td>*Deletes a single component or component type from an application.</td>
</tr>
</tbody>
</table>

* The shortened form of the APP commands is used in the remainder of this document.
Output Redirection Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APP HOLD</strong></td>
<td>Controls where output files are created for any HOLD, SAVE, SAVB, CREATE SYNONYM, or APP QUERY HOLD process in the application, unless a FILEDEF command has been used to allocate data files.</td>
</tr>
<tr>
<td><strong>APP HOLDDATA</strong></td>
<td>Designates an application as the location for temporary data files created with the HOLD, SAVE, or SAVB command.</td>
</tr>
<tr>
<td><strong>APP HOLDMETA</strong></td>
<td>Designates an application as the location for temporary Master and Access Files created with the HOLD command.</td>
</tr>
<tr>
<td><strong>APP FILEDEF</strong></td>
<td>This command has been deprecated and aliased to FILEDEF.</td>
</tr>
</tbody>
</table>

Help Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Help Information: APP HELP</strong></td>
<td>Displays a list of APP commands with a brief description of each.</td>
</tr>
</tbody>
</table>

Reference: Application Metadata Commands and Metadata Tables

Click any command in the following chart to access detailed information, including the required syntax.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STATE app/file.extension</strong></td>
<td>Check file existence</td>
</tr>
<tr>
<td><strong>APP LIST app [HOLD]</strong></td>
<td>Lists the applications under approot. If the HOLD option is used, it lists the applications under approot and writes the output to a temporary file called focappl.ftm, which you can then use in a report request.</td>
</tr>
</tbody>
</table>
**Search Path Management Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APP QUERY app [HOLD]</strong></td>
<td>Lists all files in the application. If the HOLD option is used, it lists all files in the application and writes the output to a temporary file called focappq.ftm, which you can then use in a report request.</td>
</tr>
<tr>
<td><strong>catalog/sysfiles</strong></td>
<td>Table, list of accessible app name objects on path for a given type (default MASTER).</td>
</tr>
<tr>
<td><strong>catalog/sysdirs</strong></td>
<td>Table, recursive list of physical files under a physical directory.</td>
</tr>
<tr>
<td><strong>catalog/sysapps</strong></td>
<td>Table, metadata for physical objects on path.</td>
</tr>
<tr>
<td><strong>catalog/systables</strong></td>
<td>Table, app name of tables (and related metadata) on path.</td>
</tr>
</tbody>
</table>

The server has a default search path for application and system components. You can supplement this search path by using one or more of the following APP commands:

- APP PATH
- APP PREPENDPATH
- APP APPENDPATH
- APP MAP
- APP SET METALLOCATIONSAME
- APP ? METALLOCATIONSAME
- APP SHOWPATH
Generally, these commands add applications to the beginning of the default search path. The exception is temporary components that are created in the current session. These temporary components are searched first, before the user defined path.

You can issue the APP PATH command manually or set the application search path from the Web Console or the Data Management Console. When you configure the application path from the Web Console or the Data Management Console, the APP PATH command is stored in a selectable profile (global, group, or user). The global profile, edasprof, is the default.

**APP PATH**

**How to:**
Add an Application to the Search Path Manually

The APP PATH command sets the search path to a designated list of application names that refer to applications under the approot value. You can specify multiple application names to extend the search path.

**Syntax:**

**How to Add an Application to the Search Path Manually**

```
APP PATH app1[/] [app2[/] ...]
[appn[/]]
```

where:

`app1...appn`

Are application names. If you follow an application name with a slash (/), nested applications (the subtree of applications below the named application) will not be in the search path. If you do not follow the application name with a slash, the `nested_app` parameter in the edaserve.cfg file determines whether nested applications are searched for files referenced in a procedure, and to what level. If you need to specify more application names than can fit on one line, add the continuation character (\-) at the end of the first line, and code more application names on the next line.

**Note:**

- You can use the APP PATH command without an application name to reset the search path to the initial list.
- APP PATH does not validate the application list.
APP PREPENDPATH

How to:
Add Application Names to the Beginning of a Search Path

The APP PREPENDPATH command enables you to temporarily add application names to the
beginning of an existing APP PATH search path.

If you wish to use this command to alter the search path, you must code it manually in your
application.

Syntax: How to Add Application Names to the Beginning of a Search Path

APP PREPENDPATH app1[/] [app2[/]] ... [appn[/]]

where:

app1...appn

Are application names. If you follow an application name with a slash (/), nested
applications (the subtree of applications below the named application) will not be in the
search path. If you do not follow the application name with a slash, the nested_app
parameter determines whether nested applications are searched for files referenced in
a procedure, and to what level. If you need to specify more application names than can
fit on one line, add the continuation character (-) at the end of the first line, and code
more application names on the next line.

APP APPENDPATH

How to:
Add Application Names to the End of a Search Path

The APP APPENDPATH command enables you to temporarily add application names to the
end of an existing APP PATH search path.

If you wish to use this command to alter the search path, you must code it manually in your
application.
Syntax: How to Add Application Names to the End of a Search Path

APP APPENDPATH `app1[/] [app2[/]] ... [appn[/]]`

where:

`app1...appn`

Are application names. If you follow an application name with a slash (/), nested applications (the subtree of applications below the named application) will not be in the search path. If you do not follow the application name with a slash, the `nested_app` parameter determines whether nested applications are searched for files referenced in a procedure, and to what level. If you need to specify more application names than can fit on one line, add the continuation character (-) at the end of the first line, and code more application names on the next line.

APP MAP

How to:
Map a Physical File Location Outside of APPROOT Manually
Map DDNAME Allocations

Example:
Sample APP MAP Commands
Mapping DDNAME Allocations

Reference:
APP MAP With Universal Naming Convention (UNC)

The APP MAP command allows you to assign an application name to a non-approot application anywhere in the file system. This application name becomes a virtual application under approot, which can be referenced in an APP PATH command and any other APP command that takes an application name as a parameter.

Note that mapping does not automatically add a directory to the path, it simply makes it available for addition to the search path.
**Syntax:** How to Map a Physical File Location Outside of APPROOT Manually

APP MAP virtualname real_location

where:

*virtualname*

Is an application name of up to 64 characters that can later be used in an APP PATH command.

*real_location*

Is a real full path name or DDname in the native style of the given operating system.

Note that if the real location contains spaces, it must be surrounded by double quotation marks.

**Note:** On IBM i, the APP MAP command can only be used to map an IFS directory and not a QSYS library.

**Example:** Sample APP MAP Commands

Basic example for Windows:

APP MAP test c:\temptest\

Note that if a path name contains spaces, the name must be surrounded by double quotation marks. For example:

APP MAP test "c:\temp test"
**file_extension**

Is one of the following valid server file extensions:

- .mas
- .fex
- .acx
- .htm
- .sty
- .gif
- .psb

**ddname**

Is the ddname of the allocation you wish to map. The allocation can be performed using JCL code or a DYNAM command.

**Example:** **Mapping DDNAME Allocations**

DYNAM ALLOC FILE MYMAS DA EDAARH.MASTER.DATA SHR REU
APP MAP APP1 MAS=//DD:MYMAS;
APP APPENDPATH APP1

By default, the server has an APP MAP command in the edasprof.prf file to map the application MVSAPP to the allocations FOCEXEC, MASTER, ACCESS, HTML, FOCSTYLE, GIF, FOCPSB. While allocations of these ddnames are not required for the APP MAP command to be valid, once the ddnames are allocated by JCL or DYNAM commands, they become available for use.

**Reference:** **APP MAP With Universal Naming Convention (UNC)**

On platforms that support Universal Naming Convention (UNC), you must use the UNC to designate a network drive to access APP directories. The UNC must:

- Be minimally one folder below the initial shared location.
- Not contain spaces unless enclosed in single quotation marks. For example,

  ```
  \mynode\myshare\accting
  '\mynode\my share\accting'
  ```

**APP SET METALOCATIONSAME**

**How to:**

Control the Location of Synonym Files

The APP SET METALOCATIONSAME command identifies whether Master Files and their corresponding Access Files must be in the same location.
How to Control the Location of Synonym Files

Syntax:

APP SET METALLOCATION_SAME {ON | OFF}

where:

ON

Specifies that Master Files and their corresponding Access Files must reside in the same application directory. ON is the default value.

OFF

Specifies that once the Master File for a request is located, the server will use the active search path to find the corresponding Access File.

APP ? METALLOCATION_SAME

How to:

Query Whether Synonym Files Must Reside in the Same Location

The APP ? METALLOCATION_SAME command queries whether Master Files and their corresponding Access Files must be in the same location.

How to Query Whether Synonym Files Must Reside in the Same Location

Syntax:

APP ? METALLOCATION_SAME

If the result of this query command is ON, the server expects to find corresponding Master and Access Files in the same application directory. If the result is OFF, the server uses the active search path to find the Access File that corresponds to a given Master File.

APP SHOWPATH

How to:

List Active Applications

Example:

Listing Active Applications in the Search Path

The APP SHOWPATH command lists all the currently active applications in the search path, including baseapp, which is always last. This list mirrors the list of applications displayed in the applications tree on the navigation pane.
**Syntax:**  How to List Active Applications

APP SHOWPATH

**Example:**  Listing Active Applications in the Search Path

The server is generally installed with two default applications: ibisamp (contains sample files), and baseapp (which can contain any files you create).

The APP SHOWPATH command generates the following output is:

ibisamp
baseapp

**Application and File Management Commands**

In this section:

- APP CREATE
- APP COPY
- APP COPYF[ILE]
- APP MOVE
- APP MOVEF[ILE]
- APP DELETE
- APP DELETEF[ILE]
- APP PROPERTY CODEPAGE
- APP RENAME
- APP RENAMEF[ILE]

Designating File Types for APP Commands

The APP commands in this section provide management options for applications and their component files.
**APP CREATE**

**How to:**
Create an Application Manually
Change Default Characteristics of Component File Types (PDS Deployment Only)

**Example:**
Changing Default Characteristics of an Application (PDS Deployment)

In general, the APP CREATE command creates an application under the approot location.
The exception is a PDS deployment on a Unified Server, where an application is a physical entity and each of its component file types is stored in a separate PDS.
The APP CREATE command can create any number of applications with one command.

**Syntax:**

```
APP CREATE app1[/app1a...] [app2[/app2a...]] ...
   [appn[/appna...]] [DROP]
```

where:

- **app1...appn**
  - Are application names under approot. The application name can be up to 64 characters.

- **app1a...appna**
  - Are nested application directories, allowed when nested applications are configured. In order to create a nested application, the parent application must already exist.

- **DROP**
  - Deletes an application if one already exists with the same name as the one to be created, and then creates a new application with that name. Note that any files in the pre-existing application are deleted. Without the DROP option, a message will be generated, and the pre-existing application will not be deleted or changed.

The application name may not contain spaces. If the name contains spaces, each section is understood to be a separate application. If you require a name with spaces, you must create it using another mechanism, such as the Windows Explorer. You can then use the APP MAP command to add it to APPROOT.

If you need to specify more application names than can fit on one line, add the continuation character (-) at the end of the first line, and code more application names on the next line.

The word HOLD cannot be used as an application name.
How to Change Default Characteristics of Component File Types (PDS Deployment Only)

If you are working on a Unified Server in PDS deployment, you can change the default characteristics of individual component file types by issuing a DYNAM SET APP command. This command controls the types of component files that are generated for the application when an APP CREATE command is issued. By default, all component file types are generated.

The syntax is

\[
\text{DYNAM SET APP FOR} \quad \text{filetype} \quad \text{[SKIP|CREATE]} \quad \text{[POSTFIX aaa.bbb]} \quad \text{[parms]}
\]

where:

\textit{filetype}

Are the component types that may be affected by this command, in uppercase: FOCEXEC, MASTER, ACCESS, HTML, GIF, FOCSTYLE, MAINTAIN, WINFORMS, ETG. You must issue a separate command for each component type you wish to affect.

\textit{SKIP}

Indicates that the designated file type should not be created when the APP CREATE command is issued.

\textit{CREATE}

Creates the designated file type when the APP CREATE command is issued. This is the default setting.

\textit{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

\[
\text{approotvalue.appname.component_type}
\]

The default value for component_type is \textit{filetype.DATA}.

\textit{parms}

Are the allocation parameters you can set. The default parameter values are:

<table>
<thead>
<tr>
<th>File Type</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOCEXEC</td>
<td>RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50</td>
</tr>
<tr>
<td>MASTER</td>
<td>RECFM FB TRKS LRECL 80 BLKSIZE 22000 SPACE 50 50 DIR 50</td>
</tr>
<tr>
<td>ACCESS</td>
<td>RECFM FB TRKS LRECL 80 BLKSIZE 22000 SPACE 50 50 DIR 50</td>
</tr>
<tr>
<td>HTML</td>
<td>RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50</td>
</tr>
</tbody>
</table>
## Application and File Management Commands

### Example: Changing Default Characteristics of an Application (PDS Deployment)

The following command indicates that GIF files should not be created when the APP CREATE command is issued.

```plaintext
DYNAM SET APP FOR GIF SKIP
```

The following command indicates that Procedures (FOCEXECs) should be created when APP CREATE is issued.

```plaintext
DYNAM SET APP FOR FOCEXEC TRKS SP 10 20 DIR 30
```

### APP COPY

#### How to:

Copy an Application

The APP COPY command copies the entire contents of one application to another. The target application must already exist.

#### Syntax:

**How to Copy an Application**

```plaintext
APP COPY app1[/appla...] app2[/app2a...]
```

where:

```plaintext
app1[/appla...]
```

Is the application being copied. It can be a nested application name.
**app2[/app2a...]**

Is the application to which the contents of the first application are being copied. It can be a nested application name.

---

**APP COPYF[ILE]**

### How to:

Copy an Application Component Manually

The APP COPYF[ILE] command copies one or more components or component types from one application to another.

Note that if you copy a component manually, you can, optionally, rename it in the process.

If you copy a Master File, the corresponding Access File is also copied. However, copying an Access File (file type FOCSQL) does not automatically copy the corresponding Master File.

---

**Syntax:**

**How to Copy an Application Component Manually**

```plaintext
APP COPYF[ILE] app1[/appla...] {filename1|*} filetype1 app2 [/app2a...] {filename2|*} {filetype2|*} [IFEXIST] DROP
```

where:

**app1[/appla...]**

Is the application that contains the component to be copied. It can be a nested application name.

**filename1**

Are the components to be copied. Use an asterisk (*) to copy all components of file type `filetype1`.

You can use the following wildcard characters in the file name and file type references.

- An asterisk (*) replaces any combination of characters of any length (including zero). Note that an asterisk can also be used to replace the entire filename or filetype parameter.

- A question mark (?) replaces zero or one character.

**filetype1**

Is the file type, in uppercase, of the component to be copied.
Is the application to which the named component is being copied. It can be a nested application name.

Is the component name in the target application, after the copy process. Use an asterisk (*) to propagate the file names from the source application to the target application.

Is the component type, in uppercase, in the target application after the copy process. Use an asterisk (*) to propagate the file types from the source application to the target application.

IFEXIST

Ignores any component in the source application that does not exist.

DROP

Overwrites any component already in the target application with the same name and file type as a component being copied.

For a full list of the types of files you can copy with APP commands, see Designating File Types for APP Commands on page 240.

APP MOVE

How to:

Move an Application

The APP MOVE command moves the entire contents of one application to another. The target application must already exist.

Syntax:  

How to Move an Application

APP MOVE app1[/app1a...] app2[/app2a...]

where:

app1[/app1a...]

Is the application being moved. It can be a nested application name.

app2[/app2a...]

Is the application to which the contents of the first application are being moved. It can be a nested application name.
APP MOVEF[ILE]

How to:
Move an Application Component Manually

The APP MOVEF[ILE] command moves one or more components or component types from one application to another.

Note that if you move a component manually, you can, optionally, rename it in the process.

If you move a Master File, the corresponding Access File is also moved. However, moving an Access File (file type FOCSQL) does not automatically move the corresponding Master File.

Syntax: How to Move an Application Component Manually

APP MOVEF[ILE] app1[/app1a...]  
  {filename1|*} filetype1  app2 [/app2a...]  
  {filename2|*} {filetype2|*} [IFEXIST] [DROP]

where:

app1[/app1a...]
  Is the application that contains the component to be moved. It can be a nested application name.

filename1
  Is the name of the component to be moved. Use an asterisk (*) to move all components of file type filetype1.

You can use the following wildcard characters in the file name and file type references.

- An asterisk (*) replaces any combination of characters of any length (including zero).
  Note that an asterisk can also be used to replace the entire filename or filetype parameter.

- A question mark (?) replaces zero or one character.

filetype1
  Is the file type, in uppercase, of the component to be moved.

app2[/app2a...]
  Is the application to which the named component is being moved. It can be a nested application name.
filename2

Is the component name in the target application, after the move process. Use an asterisk (*) to propagate the file names from the source application to the target application.

filetype2

Is the component type, in uppercase, in the target application after the move process. Use an asterisk (*) to propagate the file types from the source application to the target application.

IFEXIST

Ignores any component in the source application that does not exist.

DROP

Overwrites any component already in the target application with the same name and file type as a component being moved.

For a full list of the types of files you can move with APP commands, see Designating File Types for APP Commands on page 240.

**APP DELETE**

**How to:**

Delete an Application Manually

The APP DELETE command deletes applications under approot.

**Syntax:**

**How to Delete an Application Manually**

APP DELETE app1[/app1a...] [app2[/app2a...] ... [appn[/appna...]]

where:

app1[/app1a...]... [appn[/appna...]]

Are application names. Nested application names are supported. If you need to specify more application names than can fit on one line, add the continuation character (-) at the end of the first line, and enter additional application names on the next line.
APP DELETEF[ILE]

**How to:**
Delete an Application Component Manually

The APP DELETEF[ILE] command deletes one or more components or component types from an application.

If you delete a Master File, the corresponding Access File is also deleted. However, deleting an Access File (file type FOCSQL) does not automatically delete the corresponding Master File.

**Syntax:**
How to Delete an Application Component Manually

APP DELETEF[ILE] app[/appna...] {filename|*} filetype

where:

appn[/appa...]

Is the application from which the component or component type is being deleted. Nested application names are supported.

filename

Is the name of the component to be deleted. Use an asterisk (*) to delete all files of type filetype.

You can use the following wildcard characters in the file name and file type references.

- An asterisk (*) replaces any combination of characters of any length (including zero).
  - Note that an asterisk can also be used to replace the entire filename or filetype parameter.

- A question mark (?) replaces zero or one character.

filetype

Is the component type, in uppercase, of the component to be deleted.

For a full list of the types of files you can use with APP commands, see Designating File Types for APP Commands on page 240.
APP PROPERTY CODEPAGE

How to: Specify a Code Page for an Application

The APP PROPERTY appname CODEPAGE command identifies the codepage to be used for non-data files in the application directory.

Syntax: How to Specify a Code Page for an Application

APP PROPERTY app[/appa...] CODEPAGE number

where:

app[/appa...]
Is an application name. Nested application names are supported.

number
Is the code page number for non-data files in the application.

APP RENAME

How to: Rename an Application

Example: Renaming an Application

The APP RENAME command renames an existing application.

Note: You cannot rename an application if it is active in the search path.

Syntax: How to Rename an Application

APP RENAME app1[/app1a...] app2[/app2a...]

where:

app1[/app1a...]
Is the application name to be renamed. It can be a nested application name.

app2[/app2a...]
Is the new application name of up to 64 characters. It can be a nested application name.
**Example:** Renaming an Application

The following shows app1 being renamed to app2.

```
APP RENAME app1 app2
```

**APP RENAMEF[ILE]**

**How to:**

Rename an Application Component

The APP RENAMEF[ILE] command renames one or more components in an application.

If you rename a Master File, the corresponding Access File is also renamed. However, renaming an Access File (file type FOCSQL) does not automatically rename the corresponding Master File.

**Syntax:**

How to Rename an Application Component

```
APP RENAMEF[ILE] app[/appa... ] filename1 filename2 filetype [DROP]
```

where:

- `app[/appa...]`
  - Is the name of the application that contains the component being renamed. It can be a nested application name

- `filename1`
  - Is the file name of the component to be renamed.
  
  You can use the following wildcard characters in the file name and file type references.
  
  - An asterisk (*) replaces any combination of characters of any length (including zero).
    
    Note that an asterisk can also be used to replace the entire filename or filetype parameter.
  
  - A question mark (?) replaces zero or one character.

- `filename2`
  - Is the new name for the component. The component name may be up to 64 characters.

- `filetype`
  - Is the file type, in uppercase, of the component to be renamed.
DROP

Overwrites an existing component with the same file name and file type.

For a full list of the types of files you can use with APP commands, see Designating File Types for APP Commands on page 240.

Designating File Types for APP Commands

Reference: APP Commands and File Types

The APP COPYF, APP MOVEF, APP DELETEF, and APP RENAMEF commands enable you to perform their actions on a wide variety of file types.

Reference: APP Commands and File Types

The following is a comprehensive list of the file types you can use with APP commands and the file extensions associated with the on-disk names for hierarchical file systems.

Note that the file types must be coded in uppercase in any APP command that requires it.

Note: This list reflects file types supported across all Information Builders products and release levels. Particular file types may not be supported in particular releases or with every product.

<table>
<thead>
<tr>
<th>File Type</th>
<th>File Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACX</td>
<td>.acx</td>
</tr>
<tr>
<td>ADR</td>
<td>.adr</td>
</tr>
<tr>
<td>AFM</td>
<td>.afm</td>
</tr>
<tr>
<td>BMP</td>
<td>.bmp</td>
</tr>
<tr>
<td>BST</td>
<td>.bst</td>
</tr>
<tr>
<td>Cascading Stylesheet</td>
<td>.css</td>
</tr>
<tr>
<td>CONTROL</td>
<td>.ctl</td>
</tr>
<tr>
<td>DATA</td>
<td>.dat</td>
</tr>
<tr>
<td>DDS</td>
<td>.DDS</td>
</tr>
</tbody>
</table>
The APP filename value is used to derive the physical extension for the APP command, so that unknown user-defined extensions may be supported in an APP command (for example, APP COPYFILE BASEAPP MYFILE.FOO DEFAULT BASEAPP MYFILE FOCEXEC).

<table>
<thead>
<tr>
<th>File Type</th>
<th>File Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>.dtd</td>
</tr>
<tr>
<td>DTD</td>
<td></td>
</tr>
<tr>
<td>EDANLS</td>
<td>.nls</td>
</tr>
<tr>
<td>EDAPRFU</td>
<td>.prf</td>
</tr>
<tr>
<td>EDAPROF</td>
<td>.prf</td>
</tr>
<tr>
<td>EDAPSB</td>
<td>.psb</td>
</tr>
<tr>
<td>EPS</td>
<td>.eps</td>
</tr>
<tr>
<td>ERRORS</td>
<td>.err</td>
</tr>
<tr>
<td>ETG</td>
<td>.etg</td>
</tr>
<tr>
<td>ETL</td>
<td>.etl</td>
</tr>
<tr>
<td>EXCEL</td>
<td>.xls</td>
</tr>
<tr>
<td>FMU</td>
<td>.fmu</td>
</tr>
<tr>
<td>FOCCOMP</td>
<td>.fcm</td>
</tr>
<tr>
<td>FOCDEF</td>
<td>.def</td>
</tr>
<tr>
<td>FOCEXEC OR FEX</td>
<td>.fex</td>
</tr>
<tr>
<td>FOCTFTMAP</td>
<td>.fmp</td>
</tr>
<tr>
<td>FOCPSB</td>
<td>.psb</td>
</tr>
<tr>
<td>FOCSQL</td>
<td>.acx</td>
</tr>
<tr>
<td>FOCSTYLE</td>
<td>.sty</td>
</tr>
</tbody>
</table>
### File Type

<table>
<thead>
<tr>
<th>File Type</th>
<th>File Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOCTEMP</td>
<td>.ftm</td>
</tr>
<tr>
<td>FOCUS</td>
<td>.foc</td>
</tr>
<tr>
<td>GIF</td>
<td>.gif</td>
</tr>
<tr>
<td>HLI</td>
<td>.hli</td>
</tr>
<tr>
<td>HTML</td>
<td>.htm</td>
</tr>
<tr>
<td>IBICPG</td>
<td>.sl</td>
</tr>
<tr>
<td>JPG</td>
<td>.jpg</td>
</tr>
<tr>
<td>JS</td>
<td>.js</td>
</tr>
<tr>
<td>LSN</td>
<td>.lsn</td>
</tr>
<tr>
<td>MAINTAIN</td>
<td>.mnt</td>
</tr>
<tr>
<td>MASTER OR MAS</td>
<td>.mas</td>
</tr>
<tr>
<td>MHT</td>
<td>.mht</td>
</tr>
<tr>
<td>Microsoft Access database</td>
<td>.mdb</td>
</tr>
<tr>
<td>MNTPAINT</td>
<td>.mpt</td>
</tr>
<tr>
<td>OMI</td>
<td>.omi</td>
</tr>
<tr>
<td>PDF</td>
<td>.pdf</td>
</tr>
<tr>
<td>PFA</td>
<td>.pfa</td>
</tr>
<tr>
<td>PFB</td>
<td>.pfb</td>
</tr>
</tbody>
</table>

**MASTER has a special behavior that any matching Access File (.acx) is also operated upon by the APP command. This is so metadata is operated upon as a matched pair. Use MAS if it is strictly desired to only operate on the Master File and not the Access File.**
<table>
<thead>
<tr>
<th>File Type</th>
<th>File Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>PNG</td>
<td>.png</td>
</tr>
<tr>
<td>PS</td>
<td>.ps</td>
</tr>
<tr>
<td>SMARTLIB</td>
<td>.knb</td>
</tr>
<tr>
<td>SQL</td>
<td>.sql</td>
</tr>
<tr>
<td>SVG</td>
<td>.svg</td>
</tr>
<tr>
<td>TABS</td>
<td>.txt</td>
</tr>
<tr>
<td>TDL</td>
<td>.tdl</td>
</tr>
<tr>
<td>TRF</td>
<td>.trf</td>
</tr>
<tr>
<td>TTEDIT</td>
<td>.tte</td>
</tr>
<tr>
<td>TXT</td>
<td>.txt</td>
</tr>
<tr>
<td>WINFORMS</td>
<td>.wfm</td>
</tr>
<tr>
<td>WSDL</td>
<td>.wsd</td>
</tr>
<tr>
<td>XHT</td>
<td>.xht</td>
</tr>
<tr>
<td>XLSM</td>
<td>.xlsm</td>
</tr>
<tr>
<td>XLSX</td>
<td>.xlsx</td>
</tr>
<tr>
<td>XLTM</td>
<td>.xltm</td>
</tr>
<tr>
<td>XLTX</td>
<td>.xltx</td>
</tr>
<tr>
<td>XML</td>
<td>.xml</td>
</tr>
<tr>
<td>XSD</td>
<td>.xsd</td>
</tr>
<tr>
<td>XSL</td>
<td>.xsl</td>
</tr>
</tbody>
</table>
Output Redirection Commands

In this section:
- APP HOLD
- APP HOLDDATA
- APP HOLDMETA
- APP FI[LEDEF]

Reference:
- Interactions Among Output Redirection Commands

Three APP commands (APP HOLD, APP HOLDDATA, and APP HOLDMETA) along with the FILEDEF and DYNAM commands comprise a class of commands that control where output is stored. In order to redirect output as you wish, it is important to understand the interactions among these commands.

Note: When the same behavior applies for APP HOLD, APP HOLDDATA, and APP HOLDMETA, these commands are referred to collectively as APP HOLD*. Note also that although DYNAM (USS only) and FILEDEF are not members of the APP family of commands, these file allocation commands interact with the APP HOLD* commands. Therefore, where appropriate, these commands are also included in this discussion. APP FI[LEDEF] has been deprecated and aliased to FILEDEF.

The most straightforward of these commands is APP HOLD, which allows you to relocate all output to a particular application. You can use this command with operations that produce output files, such as HOLD, SAVE and SAVB, as well as with CREATE SYNONYM and APP QUERY HOLD. (For details about HOLD, SAVE, and SAVB commands, see the Creating Reports With WebFOCUS Language manual.)

The APP HOLD* commands are particularly helpful when you are creating permanent files for other applications to use. However, if a command is used at an inappropriate point in the application or if it remains in effect when further steps are performed within the application, the target application may be flooded with intermediate and unintended files. Understanding the behavior of each command and the interactions among them will help you avoid this situation.
**Reference: Interactions Among Output Redirection Commands**

This chart describes the behavior associated with each redirection command and the interactions among them if multiple commands are used.

<table>
<thead>
<tr>
<th>Command</th>
<th>Stand Alone</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>APP HOLD</td>
<td>Redirects all Agent output from HOLD, SAVE, SAVB, CREATE SYNONYM, and APP QUERY HOLD commands to the designated application.</td>
<td>When issued without a specific <code>appname</code>, APP HOLD has the effect of turning off the command.</td>
</tr>
<tr>
<td>APP HOLDDATA</td>
<td>Redirects the <em>data</em> from HOLD, SAVE, and SAVB operations to the designated application, but does not redirect the associated <em>metadata</em> (see Note 1 after chart).</td>
<td>Overrides APP HOLD.</td>
</tr>
<tr>
<td>APP HOLDMETA</td>
<td>Redirects the <em>metadata</em> from HOLD, SAVE, and SAVB operations to the designated application, but does not redirect the associated <em>data</em> (see Note 1 after chart).</td>
<td>Overrides APP HOLD.</td>
</tr>
<tr>
<td>FILEDEF <code>ddname</code></td>
<td>Redirects the <em>data</em> from specific HOLD, SAVE, and SAVB operations to the designated target, but does not redirect the associated <em>metadata</em> (see Note 1 after chart).</td>
<td>Overrides APP HOLD and APP HOLDDATA.</td>
</tr>
</tbody>
</table>

The AS phrase must match the `ddname`. When there is no AS phrase, the `ddname` must match a predefined default name: HOLD for HOLD output files; SAVE for SAVE output files; and SAVB for SAVB output files.
Notes

Stand Alone

Command | Stand Alone | Notes |
---|---|---|
DYNAM ALLOC HOLDMAST | Redirects the *metadata* from HOLD, SAVE, and SAVB operations to the designated target (using the HOLDMAST *ddname*), but does not redirect the associated *data* (see Note 1 after chart). The recommended practice is to use this command on a request-by-request basis to avoid overriding previous output. If used as a global setting, previously held output will be overwritten with the same name. | Overrides APP HOLD and APP HOLDMETA. |

Note:

- Not all formats have associated metadata. For example, the HOLD FORMAT PDF command does not produce metadata, therefore, there is no metadata to redirect.

- The use of the APP HOLD command to redirect CREATE SYNONYM output is neither necessary nor desirable since the CREATE SYNONYM command directly supports application names using the syntax:

  ```markdown
  CREATE SYNONYM appname/synonym ...
  ```

APP HOLD

How to:

Designate a Storage Location for Temporary Files

The APP HOLD command defines an application in which to hold output data files (and associated Master and Access Files, if applicable) created by a HOLD, SAVE, or SAVB process in the application.

APP HOLD is intended to be used to refresh files that are common for all users of the application. It should not be used for private files since it points to an application area that is used by multiple users. If the same hold name (HOLD or AS *name*, for example) is used, conflicts between users could result.

For related information, see *Interactions Among Output Redirection Commands* on page 245.
Syntax: How to Designate a Storage Location for Temporary Files

APP HOLD appname[/appnamea...]  
where:

appname[/appnamea...]  
Is the application in which you wish to store output files. It can be a nested application name.

Note: Issuing APP HOLD without an appname turns off the effects of the command.

APP HOLDDATA

How to: Designate a Storage Location for Data Files

The APP HOLDDATA command designates an application as the location for storing data files created with the HOLD command. For related information, see Interactions Among Output Redirection Commands on page 245.

Syntax: How to Designate a Storage Location for Data Files

APP HOLDDATA appname[/appnamea...]  
where:

appname[/appnamea...]  
Is the name of the location for the data files created by any write process in the application. It can be a nested application name.

APP HOLDMETA

How to: Designate a Storage Location for Master and Access Files

The APP HOLDMETA command designates an application directory as the location for storing Master and Access Files created in the application. For related information, see Interactions Among Output Redirection Commands on page 245.

Syntax: How to Designate a Storage Location for Master and Access Files

APP HOLDMETA appname[/appnamea...]
where:

\texttt{appname[/appname...]}  
Is the name of the location for the Master and Access Files created in the application.  
It can be a nested application name.

\textbf{APP FI[LEDEF]}  
The \texttt{APP FI[LEDEF]} command has been deprecated and aliased to \texttt{FILEDEF}. For information, see the \textit{Stored Procedure Reference} manual.

\textbf{Application Metadata Commands and Catalog Metadata}

\begin{center}
\textbf{In this section:}
\end{center}

- Retrieving Basic Information
- Retrieving Extended Catalog Information

Developers may want to write applications that check application metadata and decide a course of action. For example, they may want to check the existence of a file or a file date, and decide on the need for another step, such as recreation of the file. There are multiple ways to accomplish a simple check for file existence or some other attribute, that have evolved over the release history of the product. However, some of these methods have limitations. A good example of this is the \texttt{STATE} command, which uses a native path name for UNIX. This type of path name would not match a Windows or OpenVMS file path and, therefore, would require \texttt{IF THEN ELSE} or \texttt{GOTO} logic to issue the correct version of the command for the operating environment, that might be quite cumbersome, depending on how often it is needed.

To solve part of this problem, commands such as \texttt{STATE}, \texttt{FILEDEF}, and \texttt{DYNAM} have been extended to support APP names (that is, issue \texttt{APP MAP} then use \texttt{STATE mymap/myproc.fex}). To deal with more complex issues, such as retrieving a list of available applications (APP names) and files within a particular application, a series of APP commands were developed (\texttt{APP LIST} and \texttt{APP QUERY}). However, as features such as nested applications (sub-directories) were implemented, it became apparent that a much more extended ecosystem for accessing application metadata was needed.
To satisfy this need for extended information, various internal tables were extended or created. Today the catalog/sysapps table is the primary method for accessing application metadata using standard TABLE or SELECT syntax. This is what is used in most internal applications. That is not to say that the prior methods are no longer supported. At times they can provide quick and simple coding for a specific need, but they have limitations (as noted). More complex situations require the use of the newer methods to access information. Additionally, tables such as catalog/systables and catalog/syscolum can provide additional information that is table specific, such as what DBMS a table is using and the data specification of particular columns, but they are beyond the scope of this section. It should also be noted that the newer methods occasionally overlap on how to accomplish a task. For example, a number of the catalog/sys* tables can be used to answer the question of whether a file exists. However, the tables differ from each other in the more detailed information, such as physical or application locations and attributes.

Retrieving Basic Information

**In this section:**

- STATE
- APP LIST
- APP QUERY

The following commands return basic information about files and applications.

**STATE**

**How to:**

Check File Existence

**Example:**

Checking the Existence of a File With the STATE Command

The STATE command lets you check for the existence of a file. The file reference you supply can be the full path native operating system file name, or a file name prefaced with an APP name. This section only described the use of APP name prefaced files. When an APP name is used, it does not matter if the name was natively created under the APPROOT location of the server or as an APP MAP name.

If the file does not exist, the STATE command displays a message to that effect. After issuing the STATE command, the &RETCODE system variable contains the value zero (0) if the file exists, or a non-zero value if the file does not exist.
How to Check File Existence

Syntax:

\[ \text{STATE appname/filename.filetype -TYPE RETCODE &RETCODE} \]

where:

- **appname**
  - Is the application under which the file is stored.

- **filename**
  - Is the name of the file.

- **filetype**
  - Is the file type or extension of the file.

If the file exists, the &RETCODE value will be 0 (zero). Otherwise, it will be non-zero and can be used to further direct the logic of the application, typically in a -SET or a -IF command. The STATE command will also output a *not found* message. To suppress this message, use the SET TRMOUT={OFF|ON} command.

For example, the following STATE command checks the existence of the file *myproc.fex* in the *baseapp* application. The STATE command displays a message if the file does not exist. The -TYPE command displays the value zero (0) if the file exists or the value -1 if the file does not exist.

\[ \text{STATE baseapp/mypoc.fex -TYPE RETCODE &RETCODE} \]

Example: Checking the Existence of a File With the STATE Command

The following partial example suppresses the message returned by the STATE command, issues the STATE command to check if the file *myproc.fex* exists in the baseapp application, checks the return code, and creates the file if it does not exist, before continuing with the next step in the application. If the file does exist, the code immediately transfers to the next step in the application, (-RESUME label):

\[ \text{SET TRMOUT=OFF} \]
\[ \text{STATE baseapp/mypoc.fex} \]
\[ \text{SET TRMOUT=ON} \]
\[ \text{-IF &RETCODE EQ 0 THEN GOTO RESUME;} \]
\[ \text{...} \]
\[ \text{* Some code to create the file goes here} \]
\[ \text{...} \]
\[ \text{-RESUME} \]
APP LIST

How to:
List the Applications in APPROOT

Example:
Using APP LIST to List and Work with Applications

The APP LIST command alphabetically lists the applications available under the application root, APPROOT, or under an APP MAPped location. It does not care if the APP is on the current application map or not, as it is a raw list of available applications.

Syntax: How to List the Applications in APPROOT

APP LIST [HOLD]

If the HOLD option is used, the output is written to a temporary file called focappl.ftm, (FOCAPPL on PDS Deployment), which can, in turn, be used in a request to drive a report or take an action using the catalog/focappl Master File.

Limitations:

- APP LIST does not display nested application names.
- On operating systems that use case sensitive file names (such as UNIX), uppercase physical directory names are not valid (so are not returned by APP LIST). APP names are case insensitive, but they are created on disk as lowercase, which may in turn be upper-cased by the native operating system (that is, OpenVMS ODS/2 disks and PDS uppercase file names). However, APP LIST returns them in lowercase, to be homogenous across operating systems.

Example: Using APP LIST to List and Work with Applications

The following request lists applications

APP LIST

The APP LIST output is:

BEGIN-APP-LIST
15/02/2000  13.36.38   baseapp
15/02/2000  13.36.38   ggdemo
15/02/2000  13.36.38   ncp
15/02/2000  13.36.38   template
END-APP-LIST
The following request lists applications that have been stored using the HOLD option

```
APP LIST HOLD
SQL SELECT DATE, TIME, APPNAME FROM FOCAPPL;
END
```

The APP LIST output is:

<table>
<thead>
<tr>
<th>DATE</th>
<th>TIME</th>
<th>APPNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>15/02/2000</td>
<td>13.36.38</td>
<td>baseapp</td>
</tr>
<tr>
<td>15/02/2000</td>
<td>13.36.38</td>
<td>ggdemo</td>
</tr>
<tr>
<td>15/02/2000</td>
<td>13.36.38</td>
<td>ncp</td>
</tr>
<tr>
<td>15/02/2000</td>
<td>13.36.38</td>
<td>template</td>
</tr>
</tbody>
</table>

The following practical example of using the APP LIST HOLD command issues a TABLE request against the HOLD file to check if any files exist in the application `myapp`. If no lines are returned, the application does not exist, so it is created, and the application continues. Otherwise, the application continues without creating the application.

```
APP LIST HOLD
TABLE FILE FOCAPPL
PRINT * ON TABLE HOLD WHERE APPNAME = 'myapp'
END
-IF &LINES GT 0 THEN GOTO RESUME
APP CREATE myapp
-RESUME
```

**APP QUERY**

**How to:**

List Components

**Example:**

Listing Application Files

The APP QUERY command lists files within a given application. Applications and specific nested applications can be queried.
Syntax:  

How to List Components

APP QUERY app1[/app1a...] [app2[/app2a]...] ...
[appn[/appna]] [HOLD]

where:

app1[/app1a...appn[/appna]

Are application names. They can be nested application names. If you need to specify
more application names than can fit on one line, add the continuation character (-) at
the end of the first line, and continue more application names on the next line.

If the HOLD option is used, the output is written to a temporary file called focappq.ftm
(FOCAPPQ on PDS Deployment), which can, in turn, be used in a request to drive a report
or take an action using the catalog/focappq Master File.

Limitations: All files within an APP are listed. On systems like UNIX, this may include files
of any case, so files such as MYPROC.FEX and myproc.fex may appear in a listing, but only
the lowercase version would be accessed in a request.

Example:  

Listing Application Files

The following request lists application files.

APP QUERY abc

The APP QUERY output is:

BEGIN-APP-QUERY: abc
24/10/2014 21.38.28        4 F myproc1.fex
24/10/2014 21.38.35        4 F myproc1.fex
24/10/2014 21.37.49        0 D myapp1
24/10/2014 21.32.36        0 D myapp2
END-APP-QUERY

The following request lists files that have been stored using the HOLD option.

APP QUERY ABC HOLD
SQL SELECT DATE, TIME, GMTTIME, SIZE, OTYPE, FILENAME, APPNAME FROM FOCAPPQ
;
END
The APP QUERY output is:

<table>
<thead>
<tr>
<th>DATE</th>
<th>TIME</th>
<th>GMTTIME</th>
<th>SIZE</th>
<th>OTYPE</th>
<th>FILENAME</th>
<th>APPNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/10/2014</td>
<td>21.38.28</td>
<td>1414201108</td>
<td>4</td>
<td>F</td>
<td>myproc1.fex</td>
<td>abc</td>
</tr>
<tr>
<td>24/10/2014</td>
<td>21.38.35</td>
<td>1414201115</td>
<td>4</td>
<td>F</td>
<td>myproc2.fex</td>
<td>abc</td>
</tr>
<tr>
<td>24/10/2014</td>
<td>21.37.49</td>
<td>1414201069</td>
<td>4</td>
<td>D</td>
<td>myapp1</td>
<td>abc</td>
</tr>
<tr>
<td>24/10/2014</td>
<td>21.32.36</td>
<td>1414200756</td>
<td>0</td>
<td>D</td>
<td>myapp2</td>
<td>abc</td>
</tr>
</tbody>
</table>

Note that APP QUERY ... HOLD returns a slightly extended type of information. Whitespace has selectively been removed from the above output for readability (the FILENAME column is actually 70 characters wide).

The following practical example of using the APP QUERY HOLD command checks the existence of the file *myproc1.fex* in application *abc*. If the file does not exist, the procedure exits. If the file does exist, the procedure continues.

```sql
APP QUERY abc HOLD
TABLE FILE FOCAPPQ
PRINT * ON TABLE HOLD
WHERE APPNAME = 'abc'
WHERE FILENAME = 'myproc1.fex'
END
-IF &LINES GT 0 THEN GOTO RESUME
-TYPE Procedure Not Found ... exiting!
-EXIT
-RESUME
```

**Retrieving Extended Catalog Information**

**In this section:**
- catalog/sysapps
- catalog/sysfiles

This section provides basic information about querying the server catalogs.

**catalog/sysapps**

**Example:**

Listing Files in an APP

The catalog/sysapps table contains metadata for physical objects on path.
This section only touches on basic uses typically needed by a developer. The Master File on disk robustly describes more attributes than are described here. You can directly study the Master File in order to understand other uses. The catalog/sys* group of files are subject to change (and are usually upwardly compatible). You should never write applications that have specific dependencies (typically on object size), which tend to cause upward compatibility issues.

**Example:**  
**Listing Files in an APP**

The following request lists the application name, application location, file names, and file extensions in the application named `abc`.

```sql
TABLE FILE SYSAPPS
PRINT APPNAME APPLCD FNAME FEXT
WHERE APPNAME EQ 'abc';
END
```

The output (with whitespace selectively removed for readability) is:

<table>
<thead>
<tr>
<th>APPNAME</th>
<th>APPLCD</th>
<th>FNAME</th>
<th>FEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>/usr/wf/ibi/apps/abc</td>
<td>myproc1</td>
<td>fex</td>
</tr>
<tr>
<td>abc</td>
<td>/usr/wf/ibi/apps/abc</td>
<td>myproc2</td>
<td>fex</td>
</tr>
</tbody>
</table>

The following practical example of using the SYSAPPS table to check file existence checks the existence of the file `myproc1.fex` in the application `abc`. If it does not exist, the procedure exits. If the file does exist, the procedure transfers to the next step in order to continue:

```sql
TABLE FILE SYSAPPS
PRINT * ON TABLE HOLD
WHERE APPNAME = 'abc';
WHERE FNAME = 'myproc1';
WHERE FEXT = 'fex';
END
-IF &LINES GT 0 THEN GOTO RESUME
-TYPE Procedure Not Found ... exiting!
-EXIT
-RESUME
```
catalog/sysfiles

Example:

Listing APP MASTER Objects

Listing APP FOCEXEC Objects

Using the SYSFILES Table to Check File Existence

The catalog/sysapps table contains metadata for app name objects on a path for a select object type. The default is for file type MASTER (Master Files), but is settable for other types. Unless limited in some way, all objects (of the selected type) are displayed.

This section only touches on basic uses typically needed by a developer. The Master File on disk robustly describes more attributes than are described here. You can directly study it in order to understand other uses. The catalog/sys* group of files are subject to change (and are usually upwardly compatible). You should never write applications that have specific dependencies (typically on object size), which tend to cause upward compatibility issues.

Example: Listing APP MASTER Objects

The following request lists file names, file names with their application paths, and extensions of files with file type MASTER (the default):

```
TABLE FILE SYSFILES
PRINTFILENAMELGNAMEPHNAMEEXTENSION
END
```

The output (with some records and whitespace selectively removed for readability) is:

<table>
<thead>
<tr>
<th>FILENAME</th>
<th>LGNAME</th>
<th>PHNAME</th>
<th>EXTENSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>mydata</td>
<td>MASTER</td>
<td>baseapp/mydata.mas</td>
<td>mas</td>
</tr>
<tr>
<td>mdschema</td>
<td>MASTER</td>
<td>_edahome/catalog/mdschema.mas</td>
<td>mas</td>
</tr>
</tbody>
</table>

Example: Listing APP FOCEXEC Objects

The following request sets the file type to FOCEXEC and then prints the file names, file names with their application paths, and extensions of files with file type FOCEXEC:

```
SQL FMI SET SYSFILES FOCEXEC
TABLE FILE SYSFILES
PRINTFILENAMELGNAMEPHNAMEEXTENSION
END
```
The output (with some records and whitespace selectively removed for readability) is:

<table>
<thead>
<tr>
<th>FILENAME</th>
<th>LGNAME</th>
<th>PHNAME</th>
<th>EXTENSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>myproc1</td>
<td>FOCEXEC</td>
<td>baseapp/myproc1</td>
<td>fex</td>
</tr>
<tr>
<td>myproc2</td>
<td>FOCEXEC</td>
<td>baseapp/myproc2</td>
<td>fex</td>
</tr>
</tbody>
</table>

**Note:** The value for LGNAME will switch to DEFAULT if the data is limited and only one object returns.

A valid value for the SQL FMI SET SYSFILES command is any valid server file type. Some examples are FOCUS, FOCEXEC, STY, PDF, or ACCESS. For a full list of valid file types, see *Designating File Types for APP Commands* on page 240.

**Example:** Using the SYSFILES Table to Check File Existence

The following practical example of using the SYSFILES table to check file existence prints the filename *myproc1* with extension *fex* (with the file type set to FOCEXEC). If no lines are returned, the file does not exist and the procedure exits. If the file exists, the procedure transfers to the point at which processing continues.

```sql
SQL FMI SET SYSFILES FOCEXEC TABLE FILE SYSFILES PRINT FILENAME ON TABLE HOLD WHERE FILENAME = 'myproc1' ; WHERE EXTENSION = 'fex' ; END -IF &LINES GT 0 THEN GOTO RESUME -TYPE Procedure Not Found ... exiting! -EXIT -RESUME
```

**Help Information: APP HELP**

**How to:**

Request Help for an APP Command

The APP HELP command provides help information for all of the APP commands.
Syntax: How to Request Help for an APP Command

APP HELP command parameters

where:

command

Is any valid APP command.

parameters

Are parameters that are available to or required by the command.

Restricting the Use of APP Commands

Server administrators can restrict the ability of other classes of users to change the APP environment. This setting is configurable for Application Administrators and Basic Users.

When this restriction is set, all user interfaces affected by this server setting, such as the Web Console, the Data Management Console, Developer Studio, and Managed Reporting, display only applications that are in the effective application search path, instead of displaying all applications defined by the server approot setting. In addition, the use of certain APP commands that users might otherwise issue to bypass the intended controls is restricted.

To ensure full administrative capabilities, the restriction is dynamically switched off when a user who has server administration rights logs on from client software or to the Web Console.

This capability is supported with all security settings.

Procedure: How to Restrict the Use of APP Commands

The server administrator can restrict the use of APP commands by other users.

1. From the Workspace menu, select Access Control.
2. Expand the Roles folder for Application Administrator or Basic user.
3. Right-click a user or group and choose Properties.
4. Select the General Privileges tab.
5. By default Change Own Application Path (No applock) is selected. Deselect this check box to restrict the current user or group ability to use the APP commands listed below.
6. Click Apply to confirm the setting.
Once modification of the application path is blocked, use of the following APP commands is restricted for the designated user or group:

- The following commands generate an error message:
  - APP CREATE
  - APP DELETE
  - APP RENAME

- Although no error message is explicitly generated, the following commands are restricted if they reference an application outside of the current application path:
  - APP APPENDPATH
  - APP HOLD
  - APP HOLDDATA
  - APP HOLDMETA
  - APP MAP
  - APP PATH
  - APP PREPENDPATH
  - APP COPY
  - APP COPYF[ILE]
  - APP DELETEF[ILE]
  - APP MOVEF[ILE]
  - APP RENAMEF[ILE]
Accessing Metadata and Procedures

In this section:

Search Rules
Creation Rules for Procedure Files
Locating Master Files and Procedures
Accessing Existing Data Files
Creation Rules for Data Files
Data Set Names

Permanent files include metadata and procedures that were either created before the session by another application or remain after the session is over for use by another application.

Search Rules

Example: Search Paths

Unless a file name is fully qualified with the application name, the search sequence is:

1. Current directory of the agent, which is edatemp/tnnnnn.
2. Applications set using APP HOLDMETA for metadata files, and APP HOLDDATA for hold data files.
3. Applications set in APP PATH (including MVSAPP for z/OS).
4. The baseapp application.
5. The EDAHOME/catalog.
6. For stored procedures only: if the file is not found, the server checks to see if the file was allocated with a FILEDEF or DYNAM command, and if so, tries to execute it.

Example: Search Paths

The following commands follow the search path, starting with the application set by the APP HOLDMETA command:

APP HOLDMETA APP1
When a procedure is executed, and referred to by a one-part name

```
EX ABC
```

the following is executed

```
profile.fex in APP1 application
```

followed by

```
EX APP1/ABC
```

If the procedure ABC is not found in APP1, the server follows the standard search path for procedures to find and execute it.

**Creation Rules for Procedure Files**

Unless a file name is fully qualified or redirected to another location using an APP HOLD, APP HOLDMETA, APP HOLDDATA, FILEDEF, or DYNAM command, it is created in the temporary application area of the agent and disappears after the agent is released.

For example, on z/OS if DYNAM allocation for HOLDMAST or HOLDACC is present, the metadata files are created in the corresponding PDSs (for example, for a CREATE SYNONYM or TABLE FILE file with HOLD).

For related information, see *Output Redirection Commands* on page 244.

**Locating Master Files and Procedures**

**How to:**

Locate Master Files and Procedures

Once your path is set, you can locate Master Files and procedures using the WHENCE command.

**Syntax:**

**How to Locate Master Files and Procedures**

To locate a Master File or procedure, issue the following command

```
WHENCE filename filetype
```

where:

```
filename
```

Is the name of the file you are trying to locate.

```
filetype
```

Is the type of file you are trying to locate.
Accessing Existing Data Files

You can allocate existing data files using the following methods:

- DATASET keyword in the Master File.
- FILEDEF command for non-FOCUS data sources (FIXED, RMS, VSAM, XML).
- USE command for FOCUS data sources.
- For the z/OS Server, native operating system services, when supported.
- DYNAM command as a USS equivalent for the MVS ALLOCATE command.
- Superseded by JCL DD card.

It is recommended that you use only one method for each allocation.

Creation Rules for Data Files

**How to:**

Issue a FILEDEF Command

Issue a FILEDEF Command for a Native MVS Data Set

**Example:**

Sample Allocations by JCL
Sample DYNAM Commands
Sample USE Commands

For a newly created data file, the location is determined as follows:

1. An application set by APP HOLDDATA applies to all HOLD files.
2. For FILEDEF command, one for each data file.
3. For z/OS, native operating system allocations when supported.

The request that caused the file to be created determines the file DCB parameters, such as record length, record format, and so on.

For related information, see *Output Redirection Commands* on page 244.
**Example:**  **Sample Allocations by JCL**

The following table contains sample allocations by JCL.

<table>
<thead>
<tr>
<th>Allocation Type</th>
<th>JCL Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSAM</td>
<td><code>//VSAM01 DD DISP=SHR, DSN=qualif.DATA.VSAM</code></td>
</tr>
<tr>
<td></td>
<td>This type of allocation requires the <code>szero = y</code> parameter in the <code>edaserve.cfg</code> file to support sharing of BufferPool Zero.</td>
</tr>
<tr>
<td>Fixed</td>
<td><code>//FIX01 DD DISP=SHR, DSN=qualif.FIXED.DATA</code></td>
</tr>
<tr>
<td>PDS</td>
<td><code>//MASTER DD DISP=SHR, DSN=qualif.MASTER.DATA</code></td>
</tr>
<tr>
<td>FOCUS</td>
<td><code>//CAR DD DISP=SHR, DSN=qualif.CAR.FOCUS</code></td>
</tr>
</tbody>
</table>

**Example:**  **Sample DYNAM Commands**

The following table contains samples of the DYNAM command.

<table>
<thead>
<tr>
<th>Allocation Type</th>
<th>JCL Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSAM</td>
<td><code>DYNAM ALLOC FILE QVASM DA qualif.QVSAM.VSAM SHR REUSE</code></td>
</tr>
<tr>
<td>Fixed</td>
<td><code>DYNAM ALLOC FILE FILE1 DA qualif.FILE1.DATA SHR REUSE</code></td>
</tr>
<tr>
<td>PDS</td>
<td><code>DYNAM ALLOC FILE MASTER DA qualif.MASTER.DATA SHR REUSE</code></td>
</tr>
<tr>
<td>FOCUS</td>
<td><code>DYNAM ALLOC FILE CAR DA qualif.CAR.FOCUS SHR REUSE</code></td>
</tr>
</tbody>
</table>

**Syntax:**  **How to Issue a FILEDEF Command**

```
FI filedes DISK app/[appa...]/physfile.ftm
```

where:

*`filedes`*  
Is a file designation.

*`app/[appa...]`*  
Is an application name. It can be a nested application name.

*`physfile.ftm`*  
Is a physical file located in the application.
Syntax: How to Issue a FILEDEF Command for a Native MVS Data Set

```plaintext
FILEDEF DISK "//NATIVE.MVS.DATASET"
```

where:

- `filedes` Is a file designation.
- `NATIVE.MVS.DATASET` Is a Native MVS data set. It can contain any number of qualifiers, up to 44 characters long.

Example: Sample USE Commands

The USE command supports renaming of Master Files and concatenation of data sets. The USE command is the only mechanism for accessing files on the sink machine.

**Renaming a Master File**

```plaintext
USE
  CAR1 ON CAR
END
```

**Concatenating Master Files**

```plaintext
USE
  CAR1 as CAR
  CAR2 as CAR
END
```

**Accessing Files on a Sink Machine**

```plaintext
USE
  CAR1 AS FOCSU01
END
```

Data Set Names

**How to:**

Define a Data Set

If a data set name satisfies one of the following conditions, the server assumes that it is an MVS file name:

- Data set name starts with "/".
- Data set name contains no "/" and contains at least one "."
In all other cases, the name is interpreted as an HFS file name.

**Syntax:**

**How to Define a Data Set**

The following syntax is supported:

- `DATASET=APP1/physfile.ftm`
- `DATASET='qualif.car.data'`
- `DATASET=qualif.car.data`

In addition, on z/OS, you can use the following:

<table>
<thead>
<tr>
<th>Type</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDG files</td>
<td><code>FILENAME=CARGDG,SUFFIX=FOCUS, DATASET='qualif.CARGDG.FOCUS(0)'</code></td>
</tr>
<tr>
<td>PDS members</td>
<td><code>FILENAME=CARMEMB,SUFFIX=FOCUS, DATASET=qualif.CARPDSDATA(CARMEMB)</code></td>
</tr>
<tr>
<td>FOCUS, VSAM, Fixed</td>
<td><code>FILENAME=CAR,SUFFIX=FOCUS, DATASET=//'qualif.CAR.FOCUS'</code></td>
</tr>
</tbody>
</table>

**Allocating Temporary Files**

**How to:**

- Allocate Temporary Files
- Allocate Temporary Files to MVS Data Sets
- Support Long Synonym Names Using DYNAM SET LONGSYNM

**Reference:**

- Usage Notes for Allocating Temporary Files
- System Defaults for Allocating Temporary Files to MVS Data Sets

Temporary files are transient files that disappear after you end a session.

By default, all temporary data files (for HOLD and FOCSORT files) and temporary metadata files, such as temporary Master Files and Access Files, are created in the temporary area of an agent, which corresponds to your TSCOM ID. For example, if your TSCOM ID is TS000001, your temporary files are located in //edatemp/ts000001.

For z/OS, you can control the size and location of these temporary metadata files and data files. You can specify that the temporary files reside in the hierarchical file system, MVS data sets, or in hiperspace.
How to Allocate Temporary Files

**Syntax:**

To specify the allocation of your temporary files, issue the following command

```
DYNAM SET TEMP [ALLOC] {HFS|MVS|HIPER}
```

where:

- **HFS**
  - Allocates temporary files to the hierarchical file system. HFS is the default value.

- **MVS**
  - Allocates temporary files to MVS data sets.

- **HIPER**
  - Allocates temporary files to hiperspace.

**Reference:**

**Usage Notes for Allocating Temporary Files**

For z/OS, temporary metadata files can be allocated using a similar procedure to allocating permanent metadata files:

- If DYNAM allocation for HOLDMAST or HOLDACC is present, temporary files are stored in the designated PDSs.
- If DYNAM SET TEMP[ALLOC] MVS is issued, in the default temporary PDSs.
- If DYNAM SET TEMP[ALLOC] HIPER is issued, in the HIPERSPACE.

**Syntax:**

**How to Allocate Temporary Files to MVS Data Sets**

To alter the default allocation parameters for temporary files for MVS data sets, issue the following command

```
DYNAM SET TEMP [ALLOC] FOR type dynam parms
```

where:

- **type**
  - Is one of the following: HOLDACC, HOLDMAST, HOLD SAVE, REBUILD, FOCUS, FOCSORT, OFFLINE, or FOC$HOLD.

- **dynam parms**
  - Are regular DYNAM ALLOC parameters to be used as default for that type. Note that DCB parameters, if provided here, will be ignored, since they must be compatible with the file type being written.
This is similar to the functionality of IBITABLA in the SSCTL Server. The defaults should be overwritten for all cases when, in older versions, a private copy of IBITABLA existed containing different values.

**Reference:** System Defaults for Allocating Temporary Files to MVS Data Sets

System defaults for HOLDMAST and HOLDACC are:

```
TRKS 5  5 DSORG PO DIR 36 NEW REU
```

System defaults for all other types are:

```
CYLS 5 10 DSORG PS NEW REU
```

**Syntax:** How to Support Long Synonym Names Using DYNAM SET LONGSYNM

The server supports synonym names up to 64 characters. However, PDS member names cannot exceed eight characters. The server accounts for this operating environment limitation with the command DYNAM SET LONGSYNM.

A synonym comprises a Master File and, usually, an Access File. When you create a synonym with a name exceeding eight characters, the LONGSYNM setting currently in effect determines how the long name of the Master File and of the Access File will be handled.

You can issue DYNAM SET LONGSYNM anywhere SET commands are valid, including the global server profile (edasprof.prf) and a stored procedure (FOCEXEC).

DYNAM SET LONGSYNM, on servers running on z/OS, corresponds functionally to the server configuration file keyword LONGSYNM on servers running on MVS.

The syntax is

```
DYNAM SET LONGSYNM {HFS|MVS.MATCH}
```

where:

- **HFS**
  
  Specifies that each synonym whose name is longer than eight characters will be created in an HFS directory. This is the default.

- **MVS**
  
  Specifies that when you save a synonym with a name exceeding eight characters, the server truncates the name, preserving up to the first six characters, followed by a left curly brace (I) and a suffix number that ensures the name is unique. (The server preserves the original long name within the synonym files.)

  For example, if you create a Master File named VERYLONGNAMETEST, it will be saved as VERYLO{0. If you then create a Master File named VERYLONGNAMEPROD, it will be saved as VERYLO{1.
The server chooses a suffix number by taking the next unused number in the sequence for that truncation of a Master File or Access File name. If the next number available for the Master File is different than that available for the Access File, the files will be created with different numbers. For example, if the highest Master File name truncated to VERYLO is VERYLO{8, and the highest Access File name truncated to VERYLO is VERYLO{5, and you create a synonym specifying the name VERYLONGNAMEAGAIN, the new Master File will be saved as VERYLO{9, and the new Access File will be saved as VERYLO{6.

**MATCH**

Works the same as the MVS setting, except that it ensures that the truncated names of a Master File and Access File synonym will always match. That is, they will be named using the same suffix number.

In the example provided for the MVS setting, if SET LONGSYNM had instead been set to MATCH, both the new Master File and the new Access File would have been named VERYLO{9.

Matching names may be a convenience for some people if they manually manage synonym files. It is less efficient than the MVS setting, however.

**Temporary Space Usage and Location**

The server uses temp space for the various processes. This space may be used for anything from logs and traces to transient work files (such as HOLD files). This temp space uses real disk space, but is recycled and cleaned up based on server configuration (for example, secured servers clean agent directories upon disconnect). Ultimately, a server restarts also cleans up this temporary space. If a server has been turned off, and a restart is not planned (possibly because it was a test configuration), the space may be recovered by the server admin with the following command:

```
edastart -cleardir
```

**Temporary Disk Space Usage for Non-PDS Deployment**

<table>
<thead>
<tr>
<th>How to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the EDATEMP Variable</td>
</tr>
<tr>
<td>Pre-Allocate Temporary Files</td>
</tr>
<tr>
<td>Dynamically Allocate FOCUS Files on z/OS</td>
</tr>
</tbody>
</table>

Temporary space, by default, is created under the configuration directory (ffs, wfs, or dm) in the file system used to install the product. The edatemp directory is two levels deep.

The first level directory is used for trace files if tracing is active. By default, the directory is named edatemp and is also generally referred to as the edatemp directory of EDACONF.
The subdirectory is used for temporary files and traces created by various processes, such as the TCP and HTTP listeners, the Workspace Manager, and the end-user agent processes. Each connecting user is assigned to a private data agent directory to isolate their work from other users, and that directory is cleaned up upon disconnect. The agent subdirectories are named tsnnnnnnn, where nnnnnn is the ID number assigned to the data agent.

The edatemp directory can be configured to use a separate file system by setting the EDATEMP variable to point at the alternate location. The steps and syntax vary by platform, and may be done as an operating system variable or as a variable in the server configuration file (edaserve.cfg) before server start up.

If you are using the server configuration file, the best method is to edit edaserve.cfg from the Web Console Workspace folder, adding the line:

```
edatemp = directory
```

where

```
directory
```

Is a full path directory name, using the appropriate platform syntax. After saving, restart the server.

**Note:** Editing the server configuration file (edaserve.cfg) is the only method available for Windows.

**Syntax:**

**How to Specify the EDATEMP Variable**

**For UNIX and Linux,** the edatemp variable can be coded in the edastart.sh file:

```
export EDATEMP=/u/iway/edatemp
```

**Note:** This also applies to IBM i, VMS, and Windows.

For OpenVMS, the edatemp variable can be coded in the edastart.com file:

```
DEFINE EDATEMP TMP:[TMP.EDATEMP]
```

For UNIX System Services, it can be coded in the ISTART JCL member under the EDAENV dd statement:

```
//EDAENV      DD   *
EDATEMP=/u/iway/edatemp
```

For z/OS UNIX System Services only, you can set the temporary area to MVS by using the following command in edasprof.prf or user profile.

```
DYNAM SET TEMPALLOC MVS
```

The above are global settings which affect temporary file allocations for all users.
Syntax: How to Pre-Allocate Temporary Files

You can pre-allocate an individual file for a user, using the following techniques:

- **For UNIX and Linux:**
  
  ```
  FILEDEF XXX DISK /u/another/area/xxx.dat
  where:
  /u/another/area
  Has enough free space to hold the file.
  ```

- **For Windows:**
  
  ```
  FILEDEF XXX DISK C:\tmp\another\area\xxx.dat
  where:
  tmp\another\area
  Has enough free space to hold the file.
  ```

- **For OpenVMS:**
  
  ```
  FILEDEF XXX DISK TMP:\[ANOTHER.AREA\]xxx.DAT
  where:
  TMP:\[ANOTHER.AREA\]
  Has enough free space to hold the file.
  ```

- **For z/OS UNIX System Services:**
  
  You can use the same filedef syntax indicated for UNIX, or you can use the DYNAM command to direct the temporary file to MVS.

  ```
  DYNAM ALLOC FILE XXX SPACE
  ```

  Note that, for the DYNAM command, you must to specify the amount of space required.

- **For FOCUS files:**
  
  You can use the FILEDEF and USE commands to create a FOCUS file outside the edatemp area.

  ```
  FILEDEF NAME DISK /{pathname}{filename}.foc .......
  USE NAME NEW
  END
  ```
**Syntax:**  

How to Dynamically Allocate FOCUS Files on z/OS

You can dynamically allocate FOCUS files on z/OS with the USE command. The command is

```
DYNAM ALLOC FILE ddname SPACE
USE ddname AS masterfile
END
```

where:

- `ddname`  
  Is the DDNAME.

- `masterfile`  
  Is the Master File name.

If the DDNAME and Master File name are the same, use just the command:

```
DYNAM ALLOC
```

Application Tools

**In this section:**  

EX Procedure and Amper Variables

An application program may be as simple as a TABLE FILE ... END request or as elaborate as a series of replaceable variables (known as amper variables) controlled by dynamic inputs, GOTO statements, and/or looping logic (known collectively as Dialogue Manager). While Dialogue Manager is fully detailed in the Stored Procedure Reference manual, a limited set of these commands and tools are also noted here due to their integral use in APP management.

**EX Procedure and Amper Variables**

**In this section:**  

EX EDAMAIL

The EX procedure executes another procedure, as found on the application path. The procedure extension (on non-PDS platforms) is not required, and is assumed to be .fex. The full syntax is:

```
EX[EX] [appname/]procedure[.fex] [parameter=value[,parameter=value][,...]
```
Parameters may be names (such as LASTNAME) or numeric (such as 1), and may be mixed within the list. A specific APP name can be referenced and does not require the APP to be on the application path prior to execution. Numerics can also be assumed positionally, as in this example:

```
EX mytest DETAIL=ALL,QUARTERLY,PERSON=JAMES MADISON, 5=MANAGER
```

and the procedure would contain amper variables (parameters) for &DETAIL, &2, and &PERSON, and would use the context of:

```
TABLE FILE ...
WHERE PERSON IS '&PERSON' AND PERIOD EQ '&2'
... 
END
```

There are two types of amper variables, single and double. Single amper variables are only active within the procedure they are created in. Double amper variables are good for the life of the session. Additionally, there are predefined, single amper variables, such as &LINES (records returned from a request), &FOCUSER (current user ID), &FOCCFOCEXEC (name of the current executing procedure), &FOCCODEPAGE (the server NLS code page), and many others. See the Stored Procedure Reference manual for a detailed listing of other pre-defined amper variables.

**EX EDAMAIL**

**How to:**

Use EX EDAMAIL in the Positional Parameter Form

Use EX EDAMAIL in the Extended Form

**Example:**

- Mailing an HTML File as Message Body
- Mailing an HTML File as a Message Attachment
- Mailing a Multi-line Inline Message
- Mailing an HTML File as a Message Body Using Multiple Addresses and Extended Form

EDAMAIL is an internal procedure that allows you to send emails from a procedure with the content of a specific file included in the email body or as an attachment. This is useful for sending email alerts for events ranging from special error conditions to simple report completion. EDAMAIL requires a configured (and working) email SMTP Server node for the server workspace.

There are two forms of syntax for EDAMAIL:

- The original form uses positional parameters, and is limited to the original specification.
The extended form uses non-positional, name-value pair parameters. The extended form supports additional SMTP email client features such as Reply To and Importance.

The extended form is assumed if the first parameter contains an equal sign (=) indicating that a name-value pair is being passed.

Most forms of email addresses are acceptable, including support@ibi.com, support1 <support@ibi.com>, and "support1" <support@ibi.com>. A semi-colon is used as the address separator for parameters that allow multiple email addresses. A comma is also allowed as a separator if the overall address string is enclosed in single quotation marks.

The actual use and display of the email headers created by EDAMAIL are a function of the SMTP Server in use (and any intervening SMTP hops), plus the user email client (such as Outlook, Gmail, Hotmail, and so on). They are not directly controlled by the sender email headers. Therefore, an email may not always exhibit the expected behavior in all email client environments. For example, older email clients may not recognize newer header types, and may ignore Reply To. Any functional issues should first be investigated by an experienced SMTP/Email administrator to determine if they are client-related.

**Syntax:**

**How to Use EX EDAMAIL in the Positional Parameter Form**

The syntax is:

```
EX EDAMAIL to, from, subject, [flag], filetype, data
```

where:

- **to**
  
  Is the email recipient. Multiple addresses are allowed, using a semi-colon as the address separator.

- **from**
  
  Is the email sender.

- **subject**
  
  Is the email subject string. If the subject string contains a comma, the string must be enclosed in quotation marks.

- **flag**
  
  If set to a or A, the file is sent as an attachment. Otherwise, it is included as the body of the email. All other values are ignored. The value is also ignored if the filetype parameter is blank.

- **filetype**
  
  Defines the data file type for an email message body that uses a file. Any application file type is valid, including MASTER, FOCEXEC, HTML, and TEXT. Leave the parameter empty to use the inline email message body feature.
Is the inline data stream for the email message body or the [app/]filename file containing the email message body. The inline data stream feature requires an empty filetype parameter. The EDAMAIL feature can also spread an inline email message body onto multiple lines using the -LINES {n}* feature.

If an inline data stream message body is spread across multiple lines in the procedure, the resulting email is a single line of output. Multi-line message bodies are respected when the message body from a file option is used.

**Example:** Mailing an HTML File as Message Body

TABLE FILE file1
PRINT A B C
ON TABLE HOLD AS MYFILE FORMAT HTML
END
EX EDAMAIL user1@corp1.com, user2@corp1.com, File1 Report,,HTML, MYFILE

**Example:** Mailing an HTML File as a Message Attachment

TABLE FILE file1
PRINT A B C
ON TABLE HOLD AS MYFILE FORMAT HTML
END
EX EDAMAIL user1@corp1.com, user2@corp1.com, File1 Report,a,HTML, MYFILE

**Example:** Mailing a Multi-line Inline Message

... 
EX -LINES * EDAMAIL user1@corp1.com, user2@corp1.com, &SUBJECT,,, 
Run result for &TESTNAME is:
&RESULT
EDAMAIL*

**Syntax:** How to Use EX EDAMAIL in the Extended Form

The EDAMAIL extended form using name-value pairs is activated by the detection of an equal sign (=) in the first parameter. Parameter names are not case sensitive and may be in any order, but the message parameter (if used) must be last.

The syntax is:

EX EDAMAIL to=addresslist, [toaddr=addresslist,] [from=address,] 
[fromaddr=address,] [replyto=address,] [importance=low|normal|high,] 
[subject=string,] [flags=value,] [filetype=extension,] 
[filename=file,] [message=body message]
where:

**to=addresslist**
Is the email recipient displayed by the user email client (and used in an email client Reply To All, if a toaddr header is not supplied). Multiple addresses are allowed, using a semi-colon as the address separator. A comma is also allowed as a separator, if the overall address string is enclosed in single quotation marks.

If the to parameter is used in conjunction with toaddr, the value of to may be an arbitrary string, such as "Group Managers", which most email clients will display as a pseudo-title in the To field without displaying the actual addresses used in the toaddr parameter. A forced blank can be supped for the To field by using to="".

**toaddr=addresslist**
Is the email recipient. If not supplied, SMTP servers will use the to header. Email clients will use the toaddr value in an email client Reply To All. Multiple addresses are allowed, using a semi-colon as the address separator. A comma is also allowed as a separator, if the overall address string is enclosed in single quotation marks.

**from=address**
Is the email sender displayed by the email client (and used in an email client Reply, unless overridden by a fromaddr or Reply To header). If the from parameter is used in conjunction with fromaddr, the from value may be an arbitrary string, such as The Boss, which most email clients will display as a pseudo title in the From field, and will not display the actual address used in the fromaddr parameter.

**fromaddr=address**
Is the email sender. If not supplied, most email clients will use the From header when doing a reply.

**replyto=address**
Is the email sender. If not supplied, most email clients will use the fromaddr or from parameter value.

**importance=low|normal|high**
Is the email importance level for email clients that support importance flags. Valid values are high, normal, and low.

**subject=string**
Is the email subject string. If the subject string contains a comma, the string must be enclosed in quotation marks.

**flags=value**
If set to a or A, the file is sent as an attachment. Otherwise, it is included as the body of the email.
filetype=extension
Defines the data file type for an email message body that uses a file as the body. Any application file type is valid, including MASTER, FOEXEC, HTML, TEXT, and so on. Leave the parameter out to use the inline email message body feature.

filename=file
Defines the data file for an email message body that uses a file as the body. Leave the parameter out to use the inline email message body feature.

message=body message
Is the inline data stream containing the email message body. If used, it must be the last parameter in the EDAMAIL command. To use the inline data stream feature, the filetype and filename parameters cannot be supplied. The data stream may also be spread onto multiple lines if EDAMAIL is used with the EX-LINES {n|*} feature.

If an inline data stream message body is spread across multiple lines in the procedure, the resulting email is a single line of output. Multi-line message bodies are respected when the message body from a file option is used.

**Example:** Mailing an HTML File as a Message Body Using Multiple Addresses and Extended Form

TABLE FILE file1
PRINT A B C
ON TABLE HOLD AS MYFILE FORMAT HTML
END
EX EDAMAIL to=Managers,toaddr=user1@corp1.com;user2@corp1.com,
from=support1@corp1.com,subject=File1 Report, filetype=HTML,
filename=MYFILE
Adapters must be configured to allow a Full Function Server, a WebFOCUS Reporting Server, or a DataMigrator Server to access data in different types of databases. You must add and configure an adapter for every database type you want to access.

This topic describes briefly how to declare connection attributes and authentication information, when required, using the Web Console or the Data Management Console.
Changing Common Adapter Settings

The Web Console Adapters page has a button in the Troubleshooting group labeled Change common adapter settings that allows you to customize data type mappings and other miscellaneous settings that are common to all adapters, as shown in the following image.

![Change Settings for Common Adapter](image)

Adapter-specific settings are customizable as well, and can be accessed by right-clicking a configured adapter folder and selecting Change Settings from the context menu.

Configuring an Adapter

**How to:**

Declare Connection Attributes

Test an Adapter Connection

You can configure any supported adapter for use with a Full-Function Server, WebFOCUS Reporting Server, or DataMigrator Server from the Web Console or the Data Management Console.
If an adapter has already been configured, it is listed in the Configured folder of the Adapters page navigation pane. Adapters that have not been configured are listed in the Available folder. Adapters are grouped as follows:

- SQL
- XML Based
- ERP
- OLAP
- Procedures
- Sequential and Indexed
- DBMS
- Social Media
- Other

For general instructions about adding an adapter and declaring connection attributes, see How to Declare Connection Attributes on page 279.

**Note:** Although all database configuration panes have the same look and feel, the parameters are specific to each database. To obtain detailed configuration information for an adapter, click the ? next to each parameter.

Most of the adapter configuration information is contained in two configuration files, EDASPROF.PRF and EDASERVE.CFG.

- EDASPROF.PRF, or the global profile, contains data adapter connection information.
- EDASERVE.CFG contains database release and access method information.

Your entries on the Web Console or the Data Management Console populate these files.

**Procedure: How to Declare Connection Attributes**

You can configure the adapter from either the Web Console or the Data Management Console.

1. From the Web Console menu bar, click Adapters.
   
   or
   
   From the Data Management Console, expand the Adapters folder.
   
   The Adapters folder opens.

2. Expand the Available folder, if it is not already expanded.
3. Expand the appropriate group folder and the specific adapter folder. The group folder is described in the connection attributes reference.

4. Right-click the adapter name and/or version and select Configure.
   The Add Adapter to Configuration pane opens.

5. Enter values for the parameters required by the adapter, as described in the connection attributes reference.

6. Click Configure. The configured adapter is added to the Adapters list in the navigation pane.

Once an adapter is configured, you can click the adapter name or connection to perform a variety of other tasks, including creating synonyms, testing or deleting the connection, and changing or viewing the connection properties. Specific options vary by adapter.

**Procedure: How to Test an Adapter Connection**

1. From the Web Console menu bar, click Adapters.
   or
   from the Data Management Console, expand the Adapters folder.
   The Adapters folder opens.

2. Expand an adapter in the navigation pane.

3. Right-click the adapter connection and, if available for the selected adapter, select Test.
   The test results appear in the right pane. Test results vary, depending on adapter.

**Changing the Adapter Configuration**

The Configured folder of the Adapters page navigation pane lists the adapters that have already been configured for the current operational instance.

The following general information applies.

- Right-click an Adapter folder in the navigation pane and choose from the tasks that are available for that adapter. The following table lists and describes the available tasks, or functions.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add connection</td>
<td>Adds a connection for adapters that have the functionality to support multiple connections. These can be created in any level profile.</td>
</tr>
</tbody>
</table>
Open the Adapter folder in the navigation pane and right-click a version or connection to choose from the tasks that are available for the selected adapter. The following table lists and describes the available tasks or functions.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Settings</td>
<td>Displays the Change Setting page, where you can change a variety of settings in effect for the selected adapter.</td>
</tr>
<tr>
<td>Properties</td>
<td>Allows you to change properties. Available for all JDBC-based adapters.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the adapter configurations and all connection settings from the list of configured adapters.</td>
</tr>
<tr>
<td>Help</td>
<td>Provides specific information for the adapter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>Enables you to view and change connection parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Duplicate entries are not verified.</td>
</tr>
<tr>
<td>Create or Update Synonym</td>
<td>Opens the first Create Synonym pane, where you can begin to enter the information required to create a synonym. These panes vary for different adapters. For information, click the ? next to each parameter.</td>
</tr>
<tr>
<td>Test</td>
<td>Runs a select statement for name/owner against a catalog table with a limit of up to 15 records. See <a href="#">How to Test an Adapter Connection</a> on page 280.</td>
</tr>
<tr>
<td>Impact Analysis</td>
<td>Produces a report of the synonyms that use the connection.</td>
</tr>
<tr>
<td>Delete/Remove</td>
<td>Deletes connection settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Entries are deleted from the profile in which they were created.</td>
</tr>
</tbody>
</table>
Configuring a Remote Server

Configuring remote servers allow you to add nodes to the communications configuration. The connection attributes for a remote server are written to the server, user, group, or role profile, which can be chosen during configuration.

Remote servers can be configured from the navigation pane of the Adapters page. Right-click Remote Servers and select Configure. The Remote Server Configuration page opens. For configuration information, click the ? next to each parameter.

This adapter allows applications to access data sources that reside on a remote server.

SQL Automatic Passthru Status

**How to:**

Display the SQL APT Status Report

You can find the Automatic Passthru (APT) status for a function or keyword from a report available from the Web Console.

**Procedure:** How to Display the SQL APT Status Report

1. Select Adapters from the main menu.
2. From the Information section of the ribbon, click the SQL APT Status icon.

The SQL APT Status Report is displayed, as shown in the following image.
The report lists the APT status for each function and keyword by each SQL adapter. The possibilities are:

- **Pass as is.** Do not convert, pass to the DBMS as is.
- **Convert.** Convert into a DBMS-specific implementation and pass to the DBMS.
- **FOCUS.** Force the SQL to be processed by FOCUS.

**Determining SQL Optimization**

**How to:**
Display the SQL Optimization Report

You can determine which functions are optimized to their SQL counterparts by adapter in the SQL Optimization Report available from the Web Console.

**Procedure: How to Display the SQL Optimization Report**

1. Select *Adapters* from the main menu.
2. From the Information section of the ribbon, click the *SQL Optimization Report* button.
The Filter SQL Optimization Report page opens, as shown in the following image.

3. Optionally, select an Adapter Subcategory from the corresponding list box.
4. Optionally, select a Function Category from the corresponding list box.
5. Optionally, select the Show Function Description, Show DBCS Configuration, or Show Requirement on parameter value(s) check boxes.
6. Click Show Report.
The SQL Optimization Report is displayed, as shown in the following image.

Determining Function Parameters

**How to:** Display the Function Parameters Report

You can determine the parameters for a particular function from the Function Parameters Report available from the Web Console. The report also includes a brief description of the function.

**Note:** A report on System and Security Functions is available from the Access Control page and, therefore can only be viewed by users with server administrator privileges. These functions are not included in the reports available on the Adapters page.

**Procedure: How to Display the Function Parameters Report**

1. Select *Adapters* from the main menu.
2. From the Information section of the ribbon, click the *Function Parameters Report* button.
The Filter Function Parameters Report page opens, as shown in the following image.

3. Optionally, select a Function Category from the corresponding list box.
4. Click Show Report.

The Filter Function Parameters Report is displayed, as shown in the following image.

Data Type Support Report

**How to:**
Access the Data Type Report

SQL Data Type mapping options are available in a report available from the Web Console.
**Procedure: How to Access the Data Type Report**

To access the Data Type Report:

1. Select *Adapters* from the main menu.
2. From the Troubleshooting section of the Ribbon, click the *Data Types* button.

   The Filter Data Types Report page opens, as shown in the following image.

3. Select an *Adapter Subcategory* from the corresponding list box.
4. Select an *Adapter* from the corresponding list box.
5. Select a *Server Data Type* from the corresponding list box.
6. Click *Show Report*. 
The Filter Data Types Report is displayed, as shown in the following image.

![SQL Data Types Table]

**Note:** You can also display the report as a PDF by selecting the *Show Report in PDF* check box.

**Social Media Adapters**

For information about the Social Media Adapters, see the *WebFOCUS Social Media Integration Guide*.
The data source being used determines the type of metadata that is required. For example,

- When the server accesses a relational data source, it needs to know how to interpret the data stored there. You must create a synonym that describes the structure of the data source and the server mapping of the data types.

- When the server invokes a transaction or procedure, it needs to know how to build the request, what parameters to pass, and how to format an answer set from the response. You must create a synonym that describes the layout of the request/response area.

Whatever your data source, the adapter you are using manages the synonym creation process for you, creating a synonym that meets your specific requirements.

This topic describes briefly how to create, test, and otherwise manage a synonym, using the Web Console or the Data Management Console.

**Topics:**
- Creating Synonyms
- Testing Synonyms
- Managing Synonyms
- Using the Wizards
Creating Synonyms

**How to:**
Create a Synonym

Synonyms define unique names (or aliases) for each table, view, transaction or procedure that is accessible from the server. Synonyms are useful because they hide the underlying data source location, identity, transaction or procedure from client applications. They also provide support for extended metadata features of the server, such as virtual fields and additional security mechanisms.

You can create synonyms for supported adapters from the Web Console or the Data Management Console.

**Note:** Although all synonym creation panes have the same look and feel, the parameters are specific to each adapter. To obtain detailed information for an adapter, click a ? next to a parameter.

**Procedure: How to Create a Synonym**

To create a synonym, you must have previously configured the adapter. You can create a synonym from the Applications or Adapters pages of the Web Console.

1. From the Web Console menu bar, click **Applications**.
   
   The Applications page opens.

2. Click the **New** button and select **Synonym** from the drop-down menu.

   The **Select adapter to configure or Select connection to create synonym** pane opens.

3. Click a connection for the configured adapter.

   The first of a series of synonym creation panes opens.

4. Enter values for the parameters required by the adapter as described in the synonym creation parameters reference.

5. After entering the parameter values, click **Create Synonym**.

   The Status pane indicates that the synonym was created successfully.
Note:

- You can also create a synonym from the Adapters page by right-clicking a configured adapter connection and selecting Create Synonym. For some adapters, the option is Create or Update Synonym.

- Right-clicking an application also provides an New/Synonym via Synonym Editor option, which enable you to create a synonym using that tool. For more information, see the iWay DataMigrator User's Guide.

Reference: Checking Synonyms

Once you have created a synonym, you can view its properties by right-clicking the synonym and selecting Properties from the context menu.

The Properties page opens and shows the location, adapter, date last modified, and privileges of the connected user for this synonym.

Clicking the Check File button displays the number of errors, number of segments, number of fields, and length of all fields for the synonym.

Testing Synonyms

How to: Test a Synonym

After you have created a synonym, it is good practice to ensure that it can retrieve data from a data source. You can quickly test this functionality on a sample of up to 20 rows.

Procedure: How to Test a Synonym

You can test a synonym from either the Web Console or the Data Management Console.

1. From the Web Console menu bar, click Applications
   or
   from the Data Management Console, expand the Server node folder.
   On the Web Console, the Applications page opens.

2. Expand an application folder.
3. Right-click a synonym and select Sample Data.

The sample data is displayed.

<table>
<thead>
<tr>
<th>Product Number</th>
<th>Product Name</th>
<th>Quantity in Stock</th>
<th>Sale Price</th>
<th>Our Cost</th>
<th>Product Category</th>
<th>Product Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1004</td>
<td>2 HD VCR LCD Menu</td>
<td>43,068</td>
<td>179.00</td>
<td>129.00</td>
<td>VCRs</td>
<td>Analog</td>
</tr>
<tr>
<td>1006</td>
<td>Combo Player - 4 Hd VCR + DVD</td>
<td>13,627</td>
<td>399.00</td>
<td>289.00</td>
<td>DVD</td>
<td>Digital</td>
</tr>
<tr>
<td>1008</td>
<td>DVD Upgrade Unit for Cnt. VCR</td>
<td>199</td>
<td>199.00</td>
<td>139.00</td>
<td>DVD</td>
<td>Digital</td>
</tr>
<tr>
<td>1010</td>
<td>7505L Digital Camcorder 300 X</td>
<td>10,758</td>
<td>999.00</td>
<td>750.00</td>
<td>Camcorders</td>
<td>Digital</td>
</tr>
<tr>
<td>1012</td>
<td>e500L Digital Camcorder 150 X</td>
<td>2,572</td>
<td>899.00</td>
<td>710.00</td>
<td>Camcorders</td>
<td>Digital</td>
</tr>
<tr>
<td>1014</td>
<td>3405X Digital Camera 65K P</td>
<td>990</td>
<td>249.00</td>
<td>199.00</td>
<td>Cameras</td>
<td>Digital</td>
</tr>
</tbody>
</table>
### Managing Synonyms

Once you have created a synonym, you can click the synonym name in the navigation pane of either the Web Console or the Data Management Console to access the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Opens the Master File for viewing and editing using a graphical interface. If an Access file is used it will be also available.</td>
</tr>
<tr>
<td>Edit as Text</td>
<td>Enables you to view and manually edit the Master File synonym.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To update the synonym, it is strongly recommended that you use the graphical interface provided by the <em>Open</em> option, rather than manually editing the Master File.</td>
</tr>
<tr>
<td>Edit Access File as Text</td>
<td>Enables you to view and manually edit the Access File synonym.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is available only when an Access File is created as part of the synonym.</td>
</tr>
<tr>
<td>Sample Data</td>
<td>Retrieves up to 20 rows from the associated data source.</td>
</tr>
<tr>
<td>Data Profiling</td>
<td>Data Profiling provides the data characteristics for synonym columns.</td>
</tr>
<tr>
<td></td>
<td>Alphanumeric columns provide the count of distinct values, total count, maximum, minimum, average length, and number of nulls.</td>
</tr>
<tr>
<td></td>
<td>Numeric columns provide the count of distinct values, total count, maximum, minimum, average value, and number of nulls.</td>
</tr>
<tr>
<td>Refresh Synonym (if applicable)</td>
<td>Regenerates the synonym. Use this option if the underlying object has been altered.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data Management</td>
<td>Followed by these options, if applicable:</td>
</tr>
<tr>
<td></td>
<td><strong>Recreate DBMS Table.</strong> Recreates the data source table. You are asked to confirm this selection before the table is regenerated.</td>
</tr>
<tr>
<td></td>
<td>(Note that the table will be dropped and recreated. During the process, data may be lost.)</td>
</tr>
<tr>
<td></td>
<td><strong>Delete All Data.</strong> Deletes all existing data. You are asked to confirm this selection before the data is deleted.</td>
</tr>
<tr>
<td></td>
<td><strong>Drop Table.</strong> Drops the table so that it is removed from the DBMS.</td>
</tr>
<tr>
<td></td>
<td><strong>Insert Sample Data.</strong> Inserts specified number of sample records, populating all fields with counter values.</td>
</tr>
<tr>
<td></td>
<td><strong>Show/Modify Data.</strong> Opens a window that shows the data in the data source with buttons you can click to insert values, filter values,</td>
</tr>
<tr>
<td></td>
<td>reload the data source, and customize the view.</td>
</tr>
<tr>
<td></td>
<td><strong>Reorganize.</strong> Recreates the data source table preserving original data.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is not available in the Web Console.</td>
</tr>
<tr>
<td>Impact Analysis</td>
<td>Generates a report showing where this synonym is stored and used, with links to the synonym instances. Impact Analysis reports enable you to evaluate changes before they are made by showing which components will be affected. See the Server Administration manual for details about Impact Analysis reports.</td>
</tr>
<tr>
<td>Dependencies Analysis</td>
<td>Generates a report showing information about the synonym and other synonyms and objects that are referenced within it.</td>
</tr>
<tr>
<td>Copy</td>
<td>Copies the synonym to the clipboard.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the synonym. You are asked to confirm this selection before the synonym is deleted.</td>
</tr>
<tr>
<td>Cut</td>
<td>Deletes the synonym and places it on the clipboard.</td>
</tr>
<tr>
<td>Privileges</td>
<td>Shows the security subjects on the server and the privileges they have to this synonym.</td>
</tr>
<tr>
<td>Properties</td>
<td>Displays the properties of the synonym, including physical location, last modified date, description, and privileges.</td>
</tr>
</tbody>
</table>
Using the Wizards

**In this section:**
- SQL Wizard
- Upload Wizard

The SQL Wizard leads you through the creation of metadata. The Upload Wizard leads you through the process of uploading a file from your local machine to the server. The Quick Copy Wizard lets you load a new file, replace an existing file, or append a new file to an existing file.

After each process is complete, the wizard lets you run or save a test query and schedule or email the final output.

For information about the Quick Copy Wizard, see the *DataMigrator User’s Guide*.

**SQL Wizard**

**How to:**
- Access the SQL Wizard
- Use the SQL Wizard to Configure an Adapter, Create a New Connection, or Change a Connection
- Use the SQL Wizard to Import Metadata
- Use the SQL Wizard to Select One or More Tables
- Use the SQL Wizard to Categorize Fields
- Use the SQL Wizard to Generate a Test Query
- Use the SQL Wizard to Run, Email or Schedule a Report

The SQL Wizard provides a step-by-step process for creating a summary table or cluster synonym and running a report. The wizard enables you to:

1. Configure an adapter, create a new connection, or change connection parameters.
2. Import metadata.
3. Select a Fact Table to create Joins.
4. Categorize dimensions and measures to create summary table or cluster synonyms.
5. Generate a test query.
6. Run, submit with email or schedule the report.
7. Return to the console.

The SQL Wizard displays these steps on the ribbon or in the navigation pane, as shown in the following image.

![SQL Wizard steps](image)

When you complete a task, the wizard automatically moves to the next step.

To exit the wizard and return to the full console, click *Full Console*.

**Procedure: How to Access the SQL Wizard**

1. Access the SQL Wizard by clicking the *Wizards* icon.

![Wizards pane](image)

The Wizards pane opens, as shown in the following image.

![Wizard options](image)

2. Select the SQL Wizard.

**Procedure: How to Use the SQL Wizard to Configure an Adapter, Create a New Connection, or Change a Connection**

1. Select one of the following options:

   - *New Adapter/Connection*
2. If you select *New Adapter/Connection*, the Configure Adapter pane opens. Select the radio button for the adapter and click *Next*.

**Note:** You can click any of the column headings to sort the available adapters.

The Add Adapter to Configuration pane opens. Enter the parameters for the specific adapter and click *Configure*. For information on the parameters, see the *Adapter Administration* manual.
3. If you select *Add Connection*, the Add Connections pane opens. Select an radio button for an available adapter and click *Next*.

The Add Connection pane opens. Enter the parameters for the specific adapter and click *Configure*. For information on the parameters, see the *Adapter Administration* manual.
4. If you select Change Connection, the Edit Connections pane opens. Select the radio button for the connection and click Next.

![Edit Connections Pane]

**Note:** You can click any of the column headings to sort the available connections. The Change Connect Parameters pane opens. Change the parameters for the specific connection and click Configure.

5. Click Next to move to the Import Metadata step.
Procedure: How to Use the SQL Wizard to Import Metadata

After completing the Connection step, the wizard moves to the Import Metadata step where you can create one or more synonyms.

The Select connection to create synonyms pane opens, as shown in the following image.

1. Select the radio button for the adapter and click Next.

   Note: You can click the Adapter or Connection column to sort the available adapters.
The Select Synonym Candidates pane opens.

Select Synonym Candidates for MS SQL Server (wfretail)

- **Restrict object typ...** Tables, Views and Other Objects

**Further restrict search to:**
- Tables
- Views
- Synonyms

- **Select database** Default database

- **Filter by owner/schema and object name**

2. Select or enter the object types, database, and filtering conditions, and click Next. For additional information on the parameters, see the Adapter Administration manual. The Create Synonym page opens.
3. Select one or more tables,

You can select or enter values for:

- Miscellaneous parameters such as cardinality (whether to reflect the number of rows in a table) and whether to use dynamic columns (retrieve metadata dynamically from the data source).
- Data type mappings.
- Whether to decompose date fields into their components (precision for integer and floating point fields, and scale for floating point fields).
- The date format to use.
- The target application.
- Whether to create or update the synonym.
- Whether to overwrite existing synonyms with the same name.
- The synonym name.

**4.** Click Next.

The synonyms are created in the application directory, as indicated on the Create Synonym Status page.

For more information about synonym creation parameters, see the chapter for your adapter in the *Adapter Administration* manual.

**5.** Click Next.

The wizard moves to the Joins step.

**Procedure: How to Use the SQL Wizard to Select One or More Tables**

After you have created synonym(s), the wizard moves to the *Joins* step where you can select one or more fact tables or a single table, as shown in the following image.

![Select Fact Table](image)

1. Select one or more check boxes for particular synonyms and click Next.
The Select Synonyms to be added for the Star Schema pane opens, as shown in the following image.

![Select Synonyms to be added for the Star Schema](image)

2. Select check boxes for one or more synonyms, and click Next. If you are not creating a star schema, but are creating a synonym for a single table, just click Next.

The wizard moves to the Measures and Dimensions step.

**Procedure: How to Use the SQL Wizard to Categorize Fields**

After completing the Import Metadata and Joins steps, the wizard moves to the Measures and Dimensions step. This step creates measure groups for the selected fact tables and dimension hierarchies, based on name pattern matching and date-time analysis.
The Categorize Fields into Measures, Dimensions and Hierarchies pane opens, as shown in the following image.

To show both the Column/Table View and the Measure/Dimension/Hierarchy View, click Show Hidden. This view is shown in the following image.
The alphanumeric columns are categorized as dimensions and hierarchies, and the numeric columns are categorized as measure groups and measures.

1. Use right-click options on the Data pane to delete items, insert child tables, change the join condition, and see sample data. Use right-click options on the Measures/Dimensions/Hierarchies pane to insert new measure groups and dimensions, hide or rename items, delete hierarchies, and assign a geographic role.

All of the options are described in the help text on the page.

2. Click Next.

   The Save As dialog box opens.

3. Enter a name for the synonym in the File Name field and click OK.

   The Create Test Query pane opens.

**Procedure: How to Use the SQL Wizard to Generate a Test Query**

The Create a Test Query page has two panes, as shown in the following image.

The left pane lists the data available for the query. The right pane has categories in which you can place the data for summation, sorting, and filtering.

1. Drag fields from the Data list to the Query list in the appropriate categories for the query you are designing.
Right-click a filter field to select values and a relational operator to use in the filter.

2. Click Save As, to save the query, or Run, to run the query immediately.

If you clicked Save As, the Save As dialog box opens. Assign a name for the query, and click OK.

If you selected Run, the query runs and the results display in a new tab.

Procedure: How to Use the SQL Wizard to Run, Email or Schedule a Report

1. Click Run, E-Mail, Schedule from the ribbon or the navigation pane.

The Run, E-Mail, Schedule pane opens, as shown in the following image.

2. Select the radio button for a report.

3. Click Run to run the report.

4. Click Submit with E-Mail to submit the procedure and specify start or completion email.
The Submit procedure with E-Mail pane opens, as shown in the following image.

5. To schedule the procedure, click *Manage Schedule and Email*. 

---

*Using the Wizards*
The Manage Schedule and E-Mail for procedure pane opens, as shown in the following image.

For information on email and scheduling options, see Sending an E-mail Notification for a Procedure on page 340 and Scheduling a Procedure on page 329.

**Upload Wizard**

**How to:**
- Use the Upload Wizard to Upload a File and Create a Synonym
- Use the Upload Wizard to Categorize Data
- Use the Upload Wizard Create a Test Query
- Use the Upload Wizard to Run, Email, or Schedule a Procedure

The Upload Wizard enables you to upload files from your local machine to server application folders and to load them into a DBMS for use in creating synonyms and reports. You can then run a report with or without email, or schedule it.
The wizard enables you to:

- Upload files.
- Create cluster synonyms using dimensions and measures.
- Create test queries.
- Run, submit with email, or schedule the procedure.
- Return to the console.

The Upload Wizard displays these steps on the ribbon or in the navigation pane, as shown in the following image.

![Wizard Steps Image](image)

When you complete a task, the wizard automatically moves to the next step.

**Procedure: How to Use the Upload Wizard to Upload a File and Create a Synonym**

1. From the Web Console, click the Wizards icon, as shown in the following image.

![Wizards Icon](image)

The Wizards pane opens, as shown in the following image.

**Please select one of the following wizards**

- SQL Wizard, Connect to SQL -> Import Metadata -> Joins -> Measures and Dimensions -> Test Query
- Upload Wizard, Upload Desktop File -> Measures and Dimensions -> Test Query
- Quick Copy Wizard, Quick ETL Copy -> Test Query

2. Select *Upload Wizard*. 
The Upload Wizard opens to the Upload pane, as shown in the following image.

3. Drag and drop a file or click Select Upload File and navigate to a file on your file system, as shown in the following image.
4. Click Open. The upload is confirmed, as shown in the following image.

![Upload Confirmation Image]

**Note:** Wait until the file is completely uploaded before trying to use it. The upload progress is indicated by the progress bar.

5. Click Next.

The synonym creation screens will vary, depending on the type of file uploaded.

a. If you uploaded an Excel file, the Select Worksheets page opens, as shown in the following image.
Select Worksheet(s) from employees.xls

Select the Excel worksheet(s) to upload by selecting the corresponding checkbox(s).

- **Row scan limit**: 3000 (Enter number of rows to scan to determine field formats or 0 to scan all rows.)
- **Number of header rows**: 1 (Enter number of first rows containing column headers.)
- **Error check Excel columns**
- **Customize data type mappings**

### Select Target Parameters

- **Target Application**: bemanco
- **Target Adapter**: disk File

- **Prefix**: 
- **Suffix**: 
- **Overwrite existing synonyms**

<table>
<thead>
<tr>
<th>Default Name (editable)</th>
<th>Worksheet Name</th>
<th>Named Range</th>
<th>Rows/Columns</th>
<th>Display Worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>magnifcenturyemployees</td>
<td>MagnifcenturyEmployees</td>
<td>MagnifcenturyEmployees</td>
<td>116/12</td>
<td>Data</td>
</tr>
<tr>
<td>magnifcenturyemployees</td>
<td>MagnifcenturyEmployees</td>
<td>MagnifcenturyEmployees</td>
<td>116/21</td>
<td>Data</td>
</tr>
</tbody>
</table>

You can select or enter values for the following attributes:

- The number of rows to scan in order to set field data types.
- The number of header rows.
- Whether to decompose date fields into their components.
- Whether to error check the columns (using the first data row to set field data types).
- The date format to use.
- The target application for the file.
- The target adapter.

The Target Parameters that display depend on the target adapter you select. If the target adapter is a relational data source, a Target Connection parameter will appear and, if supported by the adapter, a bulk load option. If the target adapter is a delimited flat file, Field Delimiter, Enclosure, and Header parameters will appear.
- Whether to overwrite existing synonyms with the same names
- The worksheets to be processed.
- The synonym names.

b. If you uploaded a delimited file, the Text file delimited records specification page opens, as shown in the following image.

Text file delimited records specification for car_country_centroid.csv

You can enter or select values for the following attributes:

- The delimiter character.
- The enclosure character.
- Whether the first row contains column headings.
- Whether to preserve leading blanks.
- Whether to enable null support.
- The code page.
- How many rows to use to determine field formats.
- Whether to decompose date fields into their components.
The date format to use.

Whether to recreate the file and metadata, append the new data (keeping the existing metadata), or replace the data (keeping the existing metadata).

The target application for the file.

The target adapter.

The Target Parameters that display depend on the target adapter you select. If the target adapter is a relational data source, a Target Connection parameter will appear and, if supported by the adapter, a bulk load option. If the target adapter is a delimited flat file, Field Delimiter, Enclosure, and Header parameters will appear.

Whether to overwrite existing synonyms.

The synonym name.

6. Enter parameters for the synonym, and click Next.

The synonym is created.

7. Click Next.

The Measures and Dimensions pane opens.

To exit the Upload Wizard, click Full Console.

**Procedure:** How to Use the Upload Wizard to Categorize Data

The Upload Wizard categorizes the objects in the synonym into measures, dimensions, and hierarchies.

1. Click Show Hidden to show the Column View on the left and the Measure/Dimension/Hierarchy View on the right.
The Column View on the left shows the uploaded file, as shown in the following image.

On the right, the columns have been categorized as measures, dimensions, and hierarchies.

2. Use right-click options on the Column View pane to see sample data and rename items. Use right-click options on the Measures/Dimensions/Hierarchies pane to insert new measure groups and dimensions, hide or rename items, delete hierarchies, assign a geographic role, and see sample data.

3. Click Next.

The Save As dialog box opens.

4. Enter a name for the synonym in the File Name field and click OK.

5. Click Next.

The wizard moves to the Test Query step and opens the Create Test Query pane.
Procedure: How to Use the Upload Wizard Create a Test Query

When the Wizard moves to the Test Query step, the Create Test Query pane opens, as shown in the following image.

1. Create a query by dragging objects from the Data section on the left to the appropriate query category in the Query section on the right, as shown in the following image.
You can move the query pane to the bottom or right by selecting the location from the Output drop-down list.

You can use the Modeling View tab to create a join and the Output Format tab to select an output format for the query.

2. Click Save As or Run.

If you clicked Save As, the Save As dialog box opens so that you can save the query. A status page shows whether the query was saved successfully.

If you clicked Run, the report output is displayed, as shown in the following image.

---

### Procedure: How to Use the Upload Wizard to Run, Email, or Schedule a Procedure

After you have created a test query with the Upload Wizard, you can run the procedure, submit it to run with email, or schedule it.

1. Click **Run, E-Mail, Schedule** from the ribbon or navigation pane.
The Run, E-Mail, Schedule page opens, as shown in the following image.

2. Click Run to run the report.

3. Click Submit with E-Mail to submit the procedure and specify start or completion email.
   The Submit procedure with E-Mail pane opens.

4. To schedule the procedure, click Manage Schedule and Email.
   For information on email and scheduling options, see Sending an E-mail Notification for a Procedure on page 340 and Scheduling a Procedure on page 329.

   To exit the Upload Wizard, click Full Console.
Procedures are reusable components of application logic which can include reporting or extract syntax, and are usually written in the native 4GL language of the server (TABLE). The native language of the server also includes syntax for controlling the execution of events within the request, and is known as Dialogue Manager. Procedures that contain TABLE and Dialogue Manager commands are called FOCEXECs.

Procedures may also be written in compiled and linked 3GL languages, such as C, COBOL, Fortran, Assembler, RPG, and others, and then can be called from the native 4GL language of the server.

This chapter discusses use of tools to create 4GL procedures plus an introduction to the general use of the Dialogue Manager language. The Stored Procedure Reference manual discusses the creation of procedures using 3GL languages.
Working With Stored Procedures

Procedures are available from the navigation pane of Application page. You can:

- Create and edit stored procedures.
- Run procedures at the present time, at a later time, or under stress conditions (Web Console only).
- Run a variety of reports that monitor many aspects of procedure performance.

Creating a Stored Procedure

How to:
Create a Stored Procedure

You can code a stored procedure in the text editor feature that is easily accessible from the Web Console and the Data Management Console.

The contents of a procedure can vary greatly. Reports can be created that go to a user’s browser, a configured printer, or held as a data extract in various formats. The reporting and extract language is called TABLE. Additionally, syntax is available to parameterize a request and control the flow of execution in a request. Parameters (called amper variables) and flow of control within a procedure are part of the Dialogue Manager language.

For complete information about TABLE, see the Creating Reports With WebFOCUS Language manual. For complete information about Dialogue Manager commands, see the Developing Reporting Applications manual. While the entire syntax of these features is not within the scope of this manual, it is necessary to provide information about basic run-time essentials. For information, see Procedure Run-Time Processing Essentials on page 342.

The following is small representative example that embodies reporting (TABLE), parameters (Amper Variables) and execution flow (Dialogue Manager):

```
-DDEFAULT &COUNTRY = ENGLAND
-IF &COUNTRY EQ '' THEN GOTO NOPARM ;
TABLE FILE CAR
PRINT COUNTRY CAR
WHERE COUNTRY = '&COUNTRY';
END
-EXIT
-NOPARM
TABLE FILE CAR
PRINT COUNTRY CAR
END
```
Procedure: How to Create a Stored Procedure

You can create procedures from the Web Console or the DMC.

1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Applications page opens.

2. Right-click an application folder, select New, and then Procedure.

   A text editing window opens.

3. Type the procedure code, which may be either FOCUS syntax or SQL Passthru syntax.

   For example:

   ```sql
   SQL DB2 SELECT x FROM y 
   END
   ```
When using a pure editor environment, you are responsible for the accuracy of the syntax you enter. However, any errors that are generated will be displayed in the right pane, as well as in the Session Log, which you can access from the My Console option on the menu bar.

4. Click the Run or Save As icon.

When you Run the procedure, the output is displayed in the right pane.

When you Save the procedure, the Save As pane opens.

5. Select an application folder, as show in the following image.

![Save As Window](image)

6. Enter a name in the File Name field.

7. Click OK.

The procedure is added to the application folder in the navigation pane.
**Sending Stored Procedure Report Output to Server-Side Printers**

A report is spooled to print using a combination of commands. You must issue a FILEDEF (or ALLOCATE on z/OS) command to point to a specific printer, the OFFLINE command to redirect the report request output to the device, the report request itself, and the OFFLINE CLOSE command to close the spooling session (as multiple requests may be spooled as part of a single print output). For details, see *Server Side OFFLINE Printing* on page 402.

**Editing a Stored Procedure**

**How to:**

*Edit a Procedure*

Once you have created a procedure, you can open the text editor to view or revise it.

**Tip:** In addition to editing procedure code, you can copy, delete, or move a procedure component using options on the *Applications* navigation pane.

**Procedure:**  **How to Edit a Procedure**

You can edit procedures from the Web Console or the DMC.

1. From the Web Console menu bar, click *Applications*, or from the Data Management Console, expand the Server node folder.
   
   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a procedure, and select *Open*.
   
   The procedure opens in the text editor.

   **Tip:** Double-clicking the procedure will also open the text editor.

4. When you have made your changes, click the *Save*, *Save As*, or *Run* icon.
Running a Stored Procedure

In this section:
- Running a Stored Procedure
- Running a Procedure With Different Variables
- Prompting for Amper Variables in Procedures

You can run a procedure from the Web Console or the DMC with the following variations:

- **Run.** Runs the procedure immediately.
- **Run Advanced.** Has the following options:
  - **Submit with E-Mail.** Allows you to set up email notification when the procedure starts and/or completes, and to change default values of amper variables.
  - **Run Stress.** Records the exact sequence of user actions into a script. For information, see *Stress Testing a Procedure* on page 406.
  - **Debug.** Enable you to run the procedure in debug mode. You can step through the code, viewing the result for each line.

Running a Stored Procedure

How to:
Run a Procedure

You can run a stored procedure from an application folder in the navigation pane of the Applications page.

In addition, when you create or edit a stored procedure in the text editor, you can run the procedure directly from that window, with or without first saving it.

**Procedure: How to Run a Procedure**

You can run procedures from the Web Console or the DMC.

1. From the Web Console menu bar, click *Applications*, or from the Data Management Console, expand the Server node folder.
   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a procedure, and select *Run.*
Running a Procedure With Different Variables

How to: Run a Procedure With Different Variable Values

You can run a stored procedure with amper variable values that differ from those originally specified in the procedure.

Procedure: How to Run a Procedure With Different Variable Values

You can run procedures from the Web Console or the DMC.

1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.
   
   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a procedure, select Run Advanced, and then Submit with E-Mail.
The Submit procedure page opens.

4. Select the *Submit changing defaults* check box and click *Submit*.
5. Enter values for the variables and click *Run*.

The output is displayed in the right pane.

**Prompting for Amper Variables in Procedures**

First-level (non-nested) procedures can prompt for Dialogue Manager amper variables with the following exceptions: -IF THEN ELSE branching, -GOTO branching, and -PROMPT with a list amper variable values. (These commands may produce unexpected results.)
Scheduling a Procedure

**How to:**
- Schedule a Request to Run Once
- Schedule a Recurring Request to Run
- Schedule a Request to Run on Multiple Days
- Schedule a Request to Run When the Server Starts

You can control when and how often a procedure is run using the *Schedule/E-mail* option on the navigation pane of the Applications page.

**Procedure:**  **How to Schedule a Request to Run Once**

You can schedule procedures from the Web Console or the DMC.

1. From the Web Console menu bar, click *Applications*, or from the Data Management Console, expand the Server node folder.
   
   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a procedure, select *Schedule/E-mail*, and then *Manage*.
The Manage Schedule and E-mail for procedure page opens, as shown in the following image.

4. Select the Active from the Scheduler Status drop-down menu.
The Start and stop range section open, as shown in the following image.

![Manage Schedule and E-Mail for procedure ibisamp/proc1](image_url)

5. To set a start date, click the Start Date drop-down menu to open a calendar, and select a date, as shown in the following image.

![Start and stop range](image_url)

6. To select a start time, select an hour and minute from the Start Time drop-down menus. Hours are listed for a 24-hour clock.

7. Optionally, you can set up email notification when the procedure starts and/or ends in the E-Mail on Start and E-Mail on Completion sections.

   **Note:** To use email notification, the E-mail SMTP Server must be configured from workspace. For information, see *E-mail SMTP Server Settings* on page 429.

8. Click Set or Set and Test Run.
Procedure: How to Schedule a Recurring Request to Run

You can schedule procedures from the Web Console or the DMC.

1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a procedure, select Schedule/E-mail, and then Manage.

   The Manage Schedule and E-mail for procedure page opens.

4. Select the Active from the Scheduler Status drop-down menu.

5. In the General section, select Recurring from the Schedule Type drop-down menu.
Additional parameters become available in the General Section, as shown in the following image.

6. Select an interval from the Interval Type drop-down menu. The choices are Minutes, Hourly, Daily, Weekly, Monthly and Yearly.

7. Enter a value in the Interval value field. This specified the frequency at which the procedure will run. For example, if you chose Weekly as the Interval Type, entering 2 will execute the procedure every two weeks.
8. To set a start date, click the Start Date drop-down menu to open a calendar, and select a date, as shown in the following image.

9. To select a start time, select an hour and minute from the Start Time drop-down menus. Hours are listed for a 24-hour clock.

10. Optionally, you can select the Specify End Date check box, and select an end date and time.

11. Optionally, you can select days of the week or month, intraday start and/or end, as well as how to handle holidays, from the Special date/time ranges section, as shown in the following image.
The Run on Holidays drop-down menu allows you to skip, run, or only run the report on holidays.

12. Optionally you can expand from the Log and output destinations section and select destinations, as shown in the follow image.

![Log and output destinations](image)

13. Optionally, you can set up email notification when the procedure starts and/or ends in the E-Mail on Start and E-Mail on Completion sections.

   **Note:** To use email notification, the E-mail SMTP Server must be configured from workspace. For information, see *E-mail SMTP Server Settings* on page 429.

14. Click Set or Set and Test Run.

**Procedure:**  **How to Schedule a Request to Run on Multiple Days**

You can schedule procedures from the Web Console or the DMC.

1. From the Web Console menu bar, click *Applications*, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a procedure, select *Schedule/E-mail*, and then *Manage*.

   The Manage Schedule and E-mail for procedure page opens.

4. Select the *Active* from the Scheduler Status drop-down menu.

5. In the General section, select *Multi-Day* from the Schedule Type drop-down menu.
The Special date/time ranges section opens, as shown in the following image.
6. To set a start date, click the Start Date drop-down menu to open a calendar, and select a date, as shown in the following image.

7. To select a start time, select an hour and minute from the Start Time drop-down menus. Hours are listed for a 24-hour clock.

8. Optionally, you can select the Specify End Date check box, and select an end date and time.

9. Optionally, you can select days of the week or month, as well as how to handle holidays, from the Special date/time ranges section, as shown in the following image.
The Run on Holidays drop-down menu allows you to skip, run, or only run the report on holidays.

10. Optionally you can expand from the Log and output destinations section and select destinations, as shown in the follow image.

11. Optionally, you can set up email notification when the procedure starts and/or ends in the E-Mail on Start and E-Mail on Completion sections.

   **Note:** To use email notification, the E-mail SMTP Server must be configured from workspace. For more information, see *E-mail SMTP Server Settings* on page 429.

12. Click Set or Set and Test Run.

**Procedure: How to Schedule a Request to Run When the Server Starts**

You can schedule procedures from the Web Console or the DMC. This procedure will run on every server start.

1. From the Web Console menu bar, click **Applications**, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a procedure, select **Schedule/E-mail**, and then **Manage**.

   The Manage Schedule and E-mail for procedure page opens.

4. Select the **Active** from the Scheduler Status drop-down menu.
5. In the General section, select *Run when server starts* from the Schedule Type drop-down menu.

6. Optionally, you can set up an email notification when the procedure starts and/or ends in the E-Mail on Start and E-Mail on Completion sections.

**Note:** To use the email notification option, the E-mail SMTP Server must be configured from the workspace. For information, see *E-mail SMTP Server Settings* on page 429.
7. Optionally, you can expand from the Log and output destinations section and select destinations, as shown in the following image.

![Log and output destinations](image)

8. Click Set or Set and Test Run.

Sending an E-mail Notification for a Procedure

**How to:**

Send an E-mail Message for a Request

You can set up your server to send an email message that notifies recipients of the successful completion or failure of every procedure execution. In addition, you can request that an email message be sent to a designated recipient at the start or end of the request execution.

**Prerequisites:** This procedure assumes that the E-mail SMTP Server has been configured. For information, see E-mail SMTP Server Settings on page 429.

**Procedure:** How to Send an E-mail Message for a Request

You can set up email for procedures from the Web Console or the DMC.

1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a procedure, select Schedule/E-mail, and then Manage.

   The Manage Schedule and E-mail for procedure page opens.

4. Optionally, expand the E-Mail on Start section and enter an email address in the Mail to field.

5. In the E-Mail on Completion section, enter an email address in the Mail to field.

6. Optionally, select the Advanced check box in either E-Mail section.
Additional parameters become available, as shown in the following screen.

7. To provide advanced parameters:
   - Select an option from the Importance drop-down menu, either Normal, Low or High.
   - Enter information in the Subject field.
   - Enter in information in the E-Mail Message field.
   - Select the Send HTML output as inline message check box (only available for E-Mail on Completion).

   **Note:** This option will use the report as the email body. Any content in the E-Mail Message field will not be included.

8. Click Set or Set and Test Run.
A stored procedure is a file of commands that resides on a server and is also known as a FOCEXEC procedure. The procedure typically includes any combination of Dialogue Manager control statements, Dialogue Manager variables, SET commands, SQL syntax, TABLE syntax and other syntax that perform tasks such as report generation or file maintenance, or it simply generates messages.

This section is intended as a basic reference for Dialogue Manager and how it integrates to some basic TABLE tasks. Complete information about Dialogue Manager, see the Stored Procedures Reference manual and Managing Flow of Control in an Application in the WebFOCUS Developing Reporting Applications manual.

**Commands in a Stored Procedure**

A procedure must reside on disk in an APP location, which may be an APP directory or an APP MAPped directory (or PDS on z/OS PDS deployment). Additionally, a procedure may reside elsewhere and be "sent" to the server by a client application such as the WebFOCUS mid-tier.

With the EXEC (or EX) command, a stored procedure may be called by another stored procedure or by a client application. This is illustrated below.
In addition to Dialogue Manager commands that control execution flow, and messages (such as the -TYPE above), the following may be included in a procedure:

- SQL and TABLE statements allowed by the server platform.
- Server commands, for example, CALLPGM, EXEC, and END. For details on CALLPGM and EXEC when used to call a compiled 3GL program, see the Stored Procedures Reference manual. This chapter discusses the use of EXEC to call other FOCEXEC procedures.
- Commands allowed in a server profile, such as SET. For details on the profile and its allowable commands, see Server Introduction on page 17.
- Commands that enable portions of a procedure to be executed on a remote alternate server. See the Stored Procedures Reference manual for details on the syntax and use of those commands. Also see the Server Administration manual for commands that connect to a target server, such as SQL EDA SET SERVER.
- The ON TABLE HOLD command, which holds an answer set in a temporary file on a server. See ON TABLE HOLD on page 373 for details on syntax and use.
- The ON TABLE PCHOLD command, which sends an answer set to a client application. See ON TABLE PCHOLD on page 374 for details on the syntax and use.
- Platform-specific commands such as file allocation (that is, DYNAM on z/OS or FILEDEF on other platforms).

### Dialogue Manager Commands and Processing

**In this section:**
Dialogue Manager Command Processing in a Procedure

The following table summarizes the available Dialogue Manager commands. Note that every command begins with a hyphen (-), and this is what differentiates Dialogue Manager syntax from other syntax within a procedure.

The following sections describe the syntax and use of the commands. For an alphabetical list, see the Stored Procedures Reference manual.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>-*[text]</td>
<td>Comments within a procedure.</td>
</tr>
<tr>
<td>-?</td>
<td>Displays the value of local variables.</td>
</tr>
<tr>
<td>Command</td>
<td>Function</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-UNIX cmd</td>
<td>Executes an operating system command for the respective operating system, and the command is ignored when encountered on a non-applicable operating system, except -SYSTEM which runs on all platforms.</td>
</tr>
<tr>
<td>-WINNT cmd</td>
<td>Note that some platforms use a prior version of the platform name (that is, -AS/400 is for IBM i and -WINNT is for Windows). There are also non dash versions of these commands (and ! is the equivalent of -SYSTEM), but they are not ignored when run on a platform for which they are not relevant.</td>
</tr>
<tr>
<td>-DOS cmd</td>
<td></td>
</tr>
<tr>
<td>-VMS cmd</td>
<td></td>
</tr>
<tr>
<td>-AS/400 cmd</td>
<td></td>
</tr>
<tr>
<td>-TSO RUN cmd</td>
<td></td>
</tr>
<tr>
<td>-SYSTEM cmd</td>
<td></td>
</tr>
<tr>
<td>-CLOSE</td>
<td>Closes an external file opened for reading or writing (an external file is a sequential file in the platform's file system).</td>
</tr>
<tr>
<td>-DEFAULT</td>
<td>Sets a variable to an initial value.</td>
</tr>
<tr>
<td>-DEFAULTS</td>
<td></td>
</tr>
<tr>
<td>-EXIT</td>
<td>Executes stacked commands and terminates the procedure. For a definition of stacked commands, see Commands in a Stored Procedure on page 342.</td>
</tr>
<tr>
<td>-GOTO</td>
<td>Forces an unconditional branch to a label.</td>
</tr>
<tr>
<td>-IF</td>
<td>Determines the execution flow based on the evaluation of an expression (a conditional branch).</td>
</tr>
<tr>
<td>-INCLUDE</td>
<td>Calls another Dialogue Manager FOCEXEC procedure.</td>
</tr>
<tr>
<td>-label</td>
<td>Identifies a section of code that is the target of a -GOTO or -IF.</td>
</tr>
<tr>
<td>-PASS</td>
<td>Directly issues and controls passwords.</td>
</tr>
<tr>
<td>-PROMPT</td>
<td>Types a message to the terminal (if edastart -t is in use) or creates an input window with the message in a browser if the connection type is HTTP and reads the reply from the user. This reply assigns a value to the variable named.</td>
</tr>
<tr>
<td>-QUIT</td>
<td>Terminates the procedure without executing stacked commands.</td>
</tr>
<tr>
<td>-READ</td>
<td>Reads data from an external file.</td>
</tr>
<tr>
<td>-REMOTE BEGIN</td>
<td>Signals the start of commands on an originating server that are to be sent to a target server. Only available with Hub Services.</td>
</tr>
<tr>
<td>Command</td>
<td>Function</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-REMOTE END</td>
<td>Signals the end of commands from an originating server.</td>
</tr>
<tr>
<td>-REPEAT</td>
<td>Executes a loop.</td>
</tr>
<tr>
<td>-RUN</td>
<td>Executes stacked commands and closes any external files opened with -READ or -WRITE.</td>
</tr>
<tr>
<td>-SET</td>
<td>Sets a variable to a literal value or to a value computed in an expression.</td>
</tr>
<tr>
<td>-TYPE</td>
<td>Sends a message to a client application.</td>
</tr>
<tr>
<td>-WRITE</td>
<td>Writes data to an external file.</td>
</tr>
<tr>
<td>-</td>
<td>Line continuation of a prior Dialogue Manager command.</td>
</tr>
</tbody>
</table>

**Dialogue Manager Command Processing in a Procedure**

**Example:**

Issuing an EXEC (or EX) Call

A procedure processes as follows:

- Dialogue Manager reads each line of the procedure, one by one. Values are substituted for variables encountered in any line.

- All Dialogue Manager commands (commands that start with a ":") execute as they are encountered.

- Other commands are temporarily stored (stacked) for subsequent execution and are referred to as stacked commands.
The Dialogue Manager commands -RUN and -EXIT force the execution of any stacked commands.

**Example:** **Issuing an EXEC (or EX) Call**

The following is an example of executing a procedure (SLRPT), with an explanation of the way it processes.

To execute this procedure, the requesting application issues an EXEC (or EX) with the procedure name and supplies values for the required parameters. For example:

```
EX SLRPT COUNTRY=ENGLAND, CAR=JAGUAR
```
The following procedure has been enumerated into sections, and its behavior explained (the numbers on the left are not part of the actual procedure, but are simply supplied as reference points for the explanations):

1. \(-\text{IF } \&\text{COUNTRY EQ 'DONE'} \text{ THEN GOTO GETOUT;}

2. \(\text{SQL}
   \begin{align*}
   &\text{SELECT COUNTRY, CAR, MODEL, BODY } \\
   &\text{FROM CAR } \\
   &\text{WHERE COUNTRY='}&\&\text{COUNTRY'} \text{ AND CAR='}&\&\text{CAR'} \\
   &\text{ORDER BY CAR;}
   \end{align*}
\)

3. \(\text{TABLE}
   \begin{align*}
   &\text{ON TABLE PCHOLD } \\
   &\text{END}
   \end{align*}
\)

4. \(\text{-RUN}

5. \(\text{-EXIT}

\begin{align*}
&\text{-GETOUT } \\
&\text{-TYPE NO PROCESSING DONE: EXITING SP}
\end{align*}
\)

The procedure processes as follows:

1. Values for the variables \&COUNTRY and \&CAR are passed to the procedure before the first line executes. Dialogue Manager substitutes the value ENGLAND for the variable \&COUNTRY in the first line and tests for the value DONE. The test fails, so Dialogue Manager proceeds to the next line.

   If the value were DONE instead of ENGLAND, control would pass to the label -GETOUT, and the message NO PROCESSING DONE: EXITING SP would be sent to the client application. (Dialogue Manager would skip the intervening lines of code.)

2. The next five lines are SQL. Dialogue Manager scans each for the presence of variables, substituting the value ENGLAND for \&COUNTRY and the value JAGUAR for \&CAR (remember, those values were passed by EDARP). As each line is processed, it is placed on a stack to be executed later by the server.

3. The command ON TABLE PCHOLD sends the answer set to the client application.
   The command END delimits ON TABLE PCHOLD.
After Dialogue Manager processes the command END, the stacked commands look like this:

```
SQL
SELECT COUNTRY, CAR, MODEL, BODY
FROM CAR
WHERE COUNTRY='ENGLAND' AND CAR='JAGUAR'
ORDER BY CAR;
TABLE
ON TABLE PCHOLD
END
```

The next line is then processed by Dialogue Manager.

4. The Dialogue Manager command -RUN forces the stacked commands to execute.

5. The Dialogue Manager command -EXIT terminates the procedure.

### Using Variables

**In this section:**

- Naming Conventions
- Local Variables
- Global Variables
- Predefined System Variables

This section describes how to use variables in a procedure.

Variables fall into two categories:

- Local and global variables, whose values must be supplied by the procedure at run time.
- System and statistical variables, whose values are automatically supplied by the system when referenced.

The following features apply to all variables:

- A variable stores numbers or a string of text, and is placed anywhere in a procedure.
- A variable refers to a command, a database field, a verb, or a phrase.
- The maximum number of variables allowed in a procedure is 1,024. Because approximately 30 are reserved for server use, the maximum number of user-named variables allowed in a procedure is 994.
Naming Conventions

**How to:**
Use Variables in a Procedure

This section describes how to use variables in a procedure.

Variables fall into two categories:

- Local and global variables, whose values must be supplied by the procedure at run time.
- System and statistical variables, whose values are automatically supplied by the system when referenced.

Local and global variable names are user-defined, while system and statistical variables have predefined names.

The following rules apply to the naming of local and global variables:

- A local variable name is always preceded by an ampersand (&).
- A global variable name is always preceded by a double ampersand (&&).
- Embedded blanks are not permitted.
- If an anticipated value for a variable might contain an embedded blank, enclose the variable in single quotation marks when you refer to it.
- A variable name may be any combination of the characters A through Z, 0 through 9, and the underscore (_). The first character of the name must be A through Z.
- Assign a number to a variable, instead of a name, to create a positional variable.

**Syntax:**

**How to Use Variables in a Procedure**

```plaintext
&[&] name
```

where:

```plaintext
&name
```

Is the user-defined name of a local variable. The first character of `name` must be A through Z.

```plaintext
&&name
```

Is the user-defined name of a global variable. The first character of `name` must be A through Z.
The following variables are properly named:

-&WHICHPRODUCT
-&WHICH_CITY
'&CITY'
&&CITY

The following variables are improperly named for the reason given:

<table>
<thead>
<tr>
<th>Invalid</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;WHICH CITY</td>
<td>Contains embedded blank.</td>
</tr>
<tr>
<td>&amp;WHICH-CITY</td>
<td>Contains a hyphen (-).</td>
</tr>
<tr>
<td>WHICHCITY</td>
<td>Leading ampersand(s) is missing.</td>
</tr>
</tbody>
</table>

### Local Variables

#### Example: Using Local Variables

Once supplied, values for local variables remain in effect throughout a single procedure. The values are lost after the procedure finishes processing and are not passed to other procedures that contain the same variable name.

**Example: Using Local Variables**

Consider the following procedure in which &CITY, &CODE1, and &CODE2 are local variables.

```sql
SQL
SELECT SUM (UNIT_SOLD),
      SUM (RETURNS)
FROM SALES
WHERE CITY = '&CITY'
AND PROD_CODE >= '&CODE1'
AND PROD_CODE <= '&CODE2'
```
Assume you supply the following values when you call the procedure:

\[ \text{CITY=STAMFORD, CODE1=B10, CODE2=B20} \]

Dialogue Manager substitutes the values for the variables as follows:

\[
\text{SQL}
\text{SELECT SUM (UNIT_SOLD),}
\text{SUM (RETURNS), CITY}
\text{FROM SALES}
\text{WHERE CITY = STAMFORD}
\text{AND PROD_CODE} \geq 10
\text{AND PROD_CODE} \leq 20
\text{GROUP BY CITY, PROD_CODE}
\]

After the procedure executes and terminates, the values STAMFORD, B10, and B20 are lost.

**Global Variables**

**Example:**

**Using Global Variables**

Once a value is supplied for a global variable, it remains in effect throughout the session of a processing service, unless cleared by the server. All procedures that contain the same global variable name receive the supplied value until you terminate the session.
**Example:** Using Global Variables

The following example illustrates the use of three global variables: &\&CITY, &\&CODE1, &\&CODE2.

```sql
SELECT SUM (UNIT_SOLD),
      SUM (RETURNS)
FROM SALES
WHERE CITY = &\&CITY
AND PROD_CODE >= &\&CODE1
AND PROD_CODE <= &\&CODE2
```

**Predefined System Variables**

**Example:**

Using Predefined Run-Time System Variables

There are predefined run-time system variables that you can use in a procedure. Dialogue Manager automatically supplies values for these variables whenever the variables are encountered.

The list within this section shows only the commonly used variables. Additional variables exist for other specific features and are documented in the sections for those features.

Unless otherwise noted in the table, you may override run time values by replacing or adding the parameter values specified.

<table>
<thead>
<tr>
<th>System Variable</th>
<th>Description</th>
<th>Format or Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;APPROOT</td>
<td>Physical location of the APPROOT directory.</td>
<td>Directory name.</td>
</tr>
<tr>
<td>&amp;DATE</td>
<td>Current date.</td>
<td>MM/DD/YY</td>
</tr>
<tr>
<td>&amp;DATEfmt</td>
<td>Current date.</td>
<td>fmt is any combination of YYMD, MDYY, and so on.</td>
</tr>
<tr>
<td>&amp;MDY</td>
<td>Current date. Useful for numerical comparisons.</td>
<td>MMDDYY</td>
</tr>
<tr>
<td>System Variable</td>
<td>Description</td>
<td>Format or Value</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>&amp;MDYY</td>
<td>Current date (four-digit year).</td>
<td>MMDDCCYY</td>
</tr>
<tr>
<td>&amp;DMY</td>
<td>Current date.</td>
<td>DDMMYY</td>
</tr>
<tr>
<td>&amp;DMMY</td>
<td>Current date (four-digit year).</td>
<td>DDMMCCYY</td>
</tr>
<tr>
<td>&amp;YMD</td>
<td>Current date.</td>
<td>YYMMDD</td>
</tr>
<tr>
<td>&amp;YYMD</td>
<td>Current date (four-digit year).</td>
<td>CCYMMDD</td>
</tr>
<tr>
<td>&amp;FOCFOCEXEC</td>
<td>Current running procedure.</td>
<td>Manages reporting operations involving many similarly named requests that are executed using EX. &amp;FOCFOCEXEC enables you to easily determine which procedure is running. &amp;FOCFOCEXEC is specified within a request or in a Dialogue Manager command to display the name of the currently running procedure.</td>
</tr>
<tr>
<td>&amp;FOCINCLUDE</td>
<td>Current included procedure.</td>
<td>Manages reporting operations involving many similarly named requests that are included using -INCLUDE. &amp;FOCINCLUDE is specified within a request or in a Dialogue Manager command to display the name of the currently running procedure.</td>
</tr>
<tr>
<td>&amp;ECHO</td>
<td>Current echo tracing value.</td>
<td>ON, OFF, or ALL</td>
</tr>
</tbody>
</table>
| &FOCMODE | Operating environment. | AS/400, MSO, UNIX, VMS or WINNT. You cannot override the system-supplied value. MSO is the value returned on z/OS. If it is necessary to further test for server PDS verses HFS Deployment. The following may be used:  
- SET TEMP &XYZ  
- SET &XYZ = IF &XYZ EQ 'MVS' THEN 'PDS' ELSE 'HFS' ; |
| &FOCPRINT | Current print setting. | ONLINE OFFLINE |
| &FOCREL | Source code release number. | Release number (for example, R727706D). |
| &IORETURN | Value returned after the last Dialogue Manager -READ or -WRITE operation. | 0 Successful operation.  
1 End or failure. |
### System Variable | Description | Format or Value
--- | --- | ---
&RETCODE | Return code value from execution of a server or operating system command. Referencing &RETCODE forces the execution of all stacked commands, like the command -RUN. | Any value returned by a command is valid (for example, CALLPGM flag values), but zero is considered normal (successful) execution. The one exception is the &RETCODE value of dash operating system commands, such as -DOS, -UNIX, -VMS, -AS/400, and -WINNT, represent the success, not of the command they are running, but of the ability of the server to spawn out to the OS and run the command. In this case, the &RETCODE value is normally zero because it reflects that the spawn executes normally regardless of the results of the specific command. For this case, the amper variable &EXITRC should be used to check the command result or the non-dash version of the command should be used.

&EXITRC | Return code value from execution of an operating system command. Referencing &EXITRC forces the execution of all stacked commands, like the command -RUN. | Any value returned by a command is valid, but zero is considered normal (successful) execution.

&TOD | Current time. When you enter FOCUS, this variable is updated to the current system time only when you execute a MODIFY, SCAN, or FSCAN command. To obtain the exact time during any process, use the HHMMSS subroutine. | HH.MM.SS

&FOCCODEPAGE | Code page of the server when NLS is configured else varies by platform when not configured. | Numeric, such as 297, not changeable.

&FOCLANGCODE | Language of the server when NLS is configured, else blank. | String, such as FRE, not changeable.

&LINES | Number of lines printed in last TABLE. | Numeric, not changeable.

&RECORDS | Number of records retrieved for last TABLE/GRAPH. | Numeric, not changeable.

&TRANS | Number of transactions processed. | Numeric, not changeable.

&ACCEPTS | Accepted transactions. | Numeric, not changeable.
<table>
<thead>
<tr>
<th>System Variable</th>
<th>Description</th>
<th>Format or Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;NOMATCH</td>
<td>Nomatch rejects.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;FORMAT</td>
<td>Format errors.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;INVALID</td>
<td>Invalid conditions.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;DUPLS</td>
<td>Duplicates rejected.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;INPUT</td>
<td>Segments input.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;CHNGD</td>
<td>Values updated.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;DELTD</td>
<td>Segments deleted.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;RETCODE</td>
<td>Value after DOS command.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;BASEIO</td>
<td>Number of input/output operations.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;READS</td>
<td>Read operations from external file.</td>
<td>Numeric, not changeable.</td>
</tr>
<tr>
<td>&amp;REJECTS</td>
<td>Number of rejected transactions.</td>
<td>Numeric, not changeable.</td>
</tr>
</tbody>
</table>

**Example:**  Using Predefined Run-Time System Variables

The following example incorporates the system variable &DATE into an SQL request, testing a user-supplied variable (IDATE) against it.

```
SQL
SELECT '&DATE', IDATE
FROM filename
WHERE IDATE < '08/08/2004'
-EXIT
```
Supplying Values for Variables

In this section:
General Rules
Supplying Values in the EXEC Command
Displaying Execution Flow
-DEFAULT[S] Command
-SET Command

You must supply values for variables in a procedure even if the value is a blank. For instance, some server commands are invalid without values but process normally with blanks.

Supply values for variables in the following ways:

- With the EXEC command as parameters.
- With a command such as -DEFAULTS, -SET, or -READ.

This section describes these methods.

General Rules

The following general rules apply to values for variables:

- The maximum length is 32,000 characters when using the -TYPE or -WRITE command.
- Once a value is supplied for a local variable, it is used throughout the procedure unless it is changed with a command such as -SET or -READ.
- Once a value is supplied for a global variable, it is used throughout the session in all procedures unless it is changed with -SET, -READ, or another command.
Supplying Values in the EXEC Command

**How to:**

- Pass Keyword Parameters
- Pass Positional Parameters

**Reference:**

Combining Positional and Keyword Parameters

The command EXEC enables you to call one procedure from another and set values for variables in the called procedure, using:

- Keyword parameters.
- Positional parameters.
- A combination of keyword and positional parameters.

**Syntax: How to Pass Keyword Parameters**

```
EX[EC] procedurename=value[, ...]
```

where:

- `procedure`
  Is the name of the called procedure.

- `name=value`
  Is a keyword parameter.

  If `value` contains an embedded comma, blank, or equal sign, it must be enclosed in single quotation marks. For example:

  ```
  EX SLRPT AREA=S, CITY='NY, NY'
  ```

  Name=value pairs must be separated by commas. You do not need to enter pairs in the order in which they are encountered in the procedure.

  A procedure with a long list of variables or long values for parameters may be broken onto multiple lines by inserting a comma as the last character on the line and entering the rest of the list on the following line.

**Syntax: How to Pass Positional Parameters**

```
EX[EC] procedure parm1[, ...]
```
where:

procedure

Is the name of the called procedure.

parm1

Is a positional parameter. You do not need to specify the number in the parameter list. Dialogue Manager matches the values, one by one, to the positional variables as they are encountered in the called procedure.

However, you must specify the parameters in the order in which the numeric ampers are used in the procedure.

Consider the following procedure:

```
SQL
SELECT SUM(UNIT_SOLD),SUM(RETURNS),RETURNS/UNIT_SOLD FROM SALES
WHERE PROD_CODE BETWEEN '&1' AND '&2' AND CITY = '&3' ;
END
```

The calling procedure would be:

```
EX SLRPT B10,B20,STAMFORD
```

**Reference:** Combining Positional and Keyword Parameters

Consider a procedure with:

```
SQL
SELECT &1, &2, &FIELD1, &3 FROM CAR;
END
```

If it is called from another procedure using EXEC, the EXEC command and parameters might look like:

```
EXEC PPARAM1 MODEL,MPG,FIELD1=CAR,COUNTRY
```

**Displaying Execution Flow**

**How to:**

Display Command Lines While Executing

Dialogue Manager implements IF THEN ELSE and other flow logic such as -GOTO. The flow logic and other syntax may be displayed (typically for debugging purposes) by using the &ECHO variable.
### Syntax: How to Display Command Lines While Executing

EX xxx ECHO=value
-DEFAULTS &ECHO = value
-SET &ECHO = value

Valid values are:

**ON**

Displays lines that are expanded and stacked for execution.

**ALL**

Displays Dialogue Manager commands as well as lines that are expanded and stacked for execution.

**OFF**

Suppresses display of both stacked lines and Dialogue Manager commands. OFF is the default value.

Note that if the procedure is encrypted, &ECHO automatically receives the value OFF, regardless of the value that is assigned explicitly.

### -DEFAULT[S] Command

#### Syntax:

-DEFAULT[S] &[&]name=value [...]

where:

- **&name**
  
  Is the name of the variable.

- **value**
  
  Is the default value assigned to the variable.
**-SET Command**

**How to:**
Supply Values With the -SET Command

The -SET command is used to assign a value or computed value to a variable.

**Syntax:**

**How to Supply Values With the -SET Command**

```plaintext
-SET &[&]name={expression|value};
```

where:

- **&name**
  
  Is the name of the variable. A double amper indicates that the variable is global.

- **expression**
  
  Is a valid expression. An expression may occupy several lines. Each continuation line requires a leading dash (-) in the first character position to indicate that it is a continuation. A -SET always end with a semi-colon.

- **value**
  
  Is a value such as a number or string (enclose the string in single quotation marks if contains an embedded space).

The following are some examples:

<table>
<thead>
<tr>
<th>Example</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>~SET &amp;NUM = 1 ;</td>
<td>Set value</td>
</tr>
<tr>
<td>~SET &amp;FN = JOHN ;</td>
<td>Set value</td>
</tr>
<tr>
<td>~SET &amp;LN = 'JOHN';</td>
<td>Set value with quotes</td>
</tr>
<tr>
<td>~SET &amp;NAME = 'JOHN DOE';</td>
<td>Set value with quotes required by embedded space</td>
</tr>
<tr>
<td>~SET &amp;NAME = &amp;FN</td>
<td>' '</td>
</tr>
<tr>
<td>~SET &amp;NAME = &amp;LN</td>
<td></td>
</tr>
</tbody>
</table>
Branching

**In this section:**
Screening Values With \-IF Tests

**How to:**
Use the \-GOTO Command for Unconditional Branching
Use the \-IF...GOTO Command for Conditional Branching

The execution flow of a procedure is determined using the following commands:

- \-GOTO. Used for unconditional branching, \-GOTO transfers control to a label.
- \-IF...GOTO. Used for conditional branching, \-IF...GOTO transfers control to a label depending on the outcome of a test.

**Syntax:**

**How to Use the \-GOTO Command for Unconditional Branching**

\-GOTO label

\where:

**label**

Is a user-defined name of up to 64 characters. Embedded blanks in labels or using other Dialogue Manager commands as labels is not allowed. It is also advised to not use words that may be confused with functions or arithmetic or logical operations. If a label is not found by search downward in the procedure, it is searched from the beginning a single time (if still not found a user error will occur).

**TYPE text**

Optionally sends a message to the application.
How to Use the -IF...GOTO Command for Conditional Branching

Syntax:
-IF expression [THEN] GOTO label ;
-IF expression [THEN] GOTO label ELSE GOTO label ;
-IF expression [THEN] GOTO label ELSE IF... ;

where:

label

Is a user-defined name of up to 64 characters. Embedded blanks in labels, or using other Dialogue Manager commands as labels is not allowed. It is also advised to not use words that may be confused with functions or arithmetic or logical operations. If a label is not found by search downward in the procedure, it is searched from the beginning a single time (if still not found a user error will occur).

expression

Is a valid expression. Literals need not be enclosed in single quotation marks unless they contain embedded blanks or commas.

THEN

Is an optional keyword that increases readability of the command.

ELSE GOTO

Optionally passes control to label2 when the -IF test fails.

ELSE IF

Optionally specifies a compound -IF test.

TYPE text

Optionally sends a message to a client application.

Continuation lines must begin with a hyphen (-) and lines must break between words. A space after the hyphen is not required, but it adds to readability.
Screening Values With -IF Tests

**How to:**

Test for the Presence of a Value
Test for the Length of a Value
Test for the Type of a Value

To ensure that a supplied value is valid in a procedure, test for its:

- Presence
- Type
- Length

For instance, you would not want to perform a numerical computation on a variable for which alphanumeric data has been supplied.

**Syntax:**  
**How to Test for the Presence of a Value**

```
-IF &name.EXIST GOTO label...;
```

where:

- `&name`
  
  Is a user-supplied variable.

- `.EXIST`
  
  Indicates that you are testing for the presence of a value. If a value is not present, a zero (0) is passed to the expression. Otherwise, a non-zero value is passed.

- `GOTO label`
  
  Specifies a label to branch to.

**Syntax:**  
**How to Test for the Length of a Value**

```
-IF &name.LENGTH expression GOTO label...;
```

where:

- `&name`
  
  Is a user-supplied variable.
.LENGTH

Indicates that you are testing for the length of a value. If a value is not present, a zero (0) is passed to the expression. Otherwise, the number of characters in the value is passed.

expression

Is the remainder of a valid expression, such as GT 8.

GOTO label

Specifies a label to branch to.

Syntax: How to Test for the Type of a Value

-IF &name.TYPE expression GOTO label...;

where:

&name

Is a user-supplied variable.

.TYPE

Indicates that you are testing for the type of a value. The letter N (numeric) is passed to the expression if the value is interpreted as a number up to 10^{31}-1 and is stored in four bytes as a floating point format. In Dialogue Manager, the result of an arithmetic operation with numeric fields is truncated to an integer after the whole result of an expression is calculated. If the value could not be interpreted as numeric, the letter A (alphanumeric) is passed to the expression.

expression

Is the remainder of a valid expression, such as EQ A.

GOTO label

Specifies a label to branch to.
Calling Another Procedure

In this section:
- Nesting
- The EXEC Command

How to:
- Use the -INCLUDE Command

One procedure calls another procedure using:

- The -INCLUDE file command, which incorporates a whole or partial procedure into the current procedure and executes it immediately when encountered. Unlike EXEC, no parameters may be passed with -INCLUDE, but they may be -SET on lines prior to the -INCLUDE. A -INCLUDE procedure can be a partial procedure that may contain header text or code to include at run time based on a step in the originating procedure.

- The command EXEC. The command is stacked and executed when the appropriate Dialogue Manager command is encountered. The called procedure must be fully executable.

Syntax: How to Use the -INCLUDE Command

Lines incorporated with a -INCLUDE are processed as though they had been placed in the calling procedure originally.

```
-INCLUDE filename
```

where:

```
filename
```

Is the name of the called procedure.

A calling procedure cannot branch to a label in a called procedure, and vice versa.

Nesting

Any number of different procedures may be invoked as a -INCLUDE from within a single calling procedure. Called procedures can also call (nest) additional procedures. The same procedure may even call itself recursively. However, recursive calls are limited to four levels deep.
The EXEC Command

How to:

Use the EXEC (or EX) Command

A procedure also calls another one with the command EXEC. The called procedure must be fully executable.

See Supplying Values for Variables on page 356 for additional information about passing parameter values.

Syntax:

How to Use the EXEC (or EX) Command

Procedure lines with EXEC (or EX) commands temporarily stop execution of the current procedure and call the new procedure. The new procedure may be passed current variables that are available as parameter values to the new procedure, but must do so explicitly unless those variables are global variables.

EXEC [appname/]filename [parm[, ...]]

where:

appname

Is the location of the called procedure.

filename

Is the name of the called procedure.

parm[, ...]

Are one or more parameters being passed, either positionally or by name.

Creating Expressions

In this section:

Arithmetic Expressions
Alphanumeric Expressions
Logical Expressions
Compound Expressions

An expression consists of variables and literals (numeric or alphanumeric constants) that are combined arithmetically, logically, or in some other way to create a new value.
This section describes how to create:

- **Arithmetic Expressions** on page 367.
- **Alphanumeric Expressions** on page 368.
- **Logical Expressions** on page 370.
- **Compound Expressions** on page 372.

### Arithmetic Expressions

#### Example:

Using Arithmetic Expressions

#### Reference:

Guidelines for Using Arithmetic Expressions

An arithmetic expression is:

- A numeric constant, for example, 1.
- Two variables joined by one of the following arithmetic operators:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Addition</td>
</tr>
<tr>
<td>-</td>
<td>Subtraction</td>
</tr>
<tr>
<td>*</td>
<td>Multiplication</td>
</tr>
<tr>
<td>/</td>
<td>Division</td>
</tr>
<tr>
<td>**</td>
<td>Exponentiation</td>
</tr>
</tbody>
</table>

An example is:

`&DELIVER_AMT / &OPENING_AMT`

- Two or more arithmetic expressions, joined by one of the operators in the preceding list. An example is:
  
  `(>&RATIO - 1) ** 2`

- A compound expression or function that gives an arithmetic result.
**Example:** Using Arithmetic Expressions

Following are some arithmetic expressions used in the command -SET:

- `SET &COUNT = 1;`
- `SET &NEWVAL = (&RATIO - 1) ** 2;`
- `SET &RATIO = (&DELIVER_AMT * 100) / (&OPENING_AMT);`

**Reference:** Guidelines for Using Arithmetic Expressions

Keep the following in mind as you create arithmetic expressions:

- If you attempt to divide by 0, Dialogue Manager sets the result to 0.

Arithmetic operations are performed before logical operations, in the following order:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>**</td>
<td>Exponentiation</td>
</tr>
<tr>
<td>/ *, +,-</td>
<td>Division and multiplication, Addition and subtraction</td>
</tr>
</tbody>
</table>

- For operations on the same level (for example, division and multiplication), the evaluation is performed from left to right.
- An expression in parentheses is evaluated before any other expression.
- Values for local and global variables (amper variables) are stored internally as character strings, including numeric values. If a calculation is performed on an amper variable, the variable is first converted from a character string into a numeric. After the whole result is calculated, the result of arithmetic operations with numeric fields is truncated to the integer field. Finally, the result is converted back into a character string.

**Alphanumeric Expressions**

**How to:**

Concatenate Alphanumeric Variables and Literals

**Example:**

Concatenating Alphanumeric Variables and Literals

An alphanumeric expression is:
A literal enclosed in single quotation marks, for example 'Smith John'.

- A logical expression that yields an alphanumeric result.
- A function that yields an alphanumeric result.
- Two or more alphanumeric variables or literals combined into a single string. See How to Concatenate Alphanumeric Variables and Literals on page 369 for the syntax and an example.

**Syntax:** How to Concatenate Alphanumeric Variables and Literals

```verbatim
variablename = {alphaexp1|'literal'} concatenation
{alphaexp2|'literal'} [...] 
```

where:

- `variablename` Is the name of the variable assigned to the result of the concatenation.
- `alphaexp1, alphaexp2` Are local or global variable that forms part of the concatenation.
- `literal` Is a literal that forms part of the concatenation. It must be enclosed in single quotation marks.
- `concatenation` Is one of the following symbols:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`</td>
<td></td>
</tr>
<tr>
<td>`</td>
<td>`</td>
</tr>
</tbody>
</table>

**Example:** Concatenating Alphanumeric Variables and Literals

```verbatim
-SET &NAME = &LASTNAME || ',' || &FIRST_INIT;
```

If &LASTNAME is equal to Doe and &FIRST_INIT is equal to J, &NAME is set to:

Doe, J
Logical Expressions

Example: Forming a Logical Expression

Reference: Guidelines for Alphanumeric and Logical Expressions

A logical expression contains logical and relational operators and is evaluated to a value that is true or false.

Example: Forming a Logical Expression

This example shows various elements that are used to form a logical expression. The abbreviation exp stands for expression.

{arithmetic exp|alphanumeric exp} operator1 {numeric lit|alphanumeric lit} OR...

expressionoperator2expression

logical exp {AND|OR} logical exp

NOT logical exp

where:

operator1
Is one of the following: EQ, NE, OMITS, or CONTAINS.

expression
Is either an arithmetic, alphanumeric, or logical expression.

operator2
Is one of the following: EQ, NE, LE, LT, GE, or GT.

The following table defines valid operators (EQ, NE, and so on) used in this example.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EQ</td>
<td>Tests for a value equal to another value.</td>
</tr>
<tr>
<td>NE</td>
<td>Tests for a value not equal to another value.</td>
</tr>
<tr>
<td>OMITS</td>
<td>Tests for a value that does not contain a matching character string.</td>
</tr>
<tr>
<td>CONTAINS</td>
<td>Tests for a value that does contain a matching character string.</td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>LE</td>
<td>Tests for a value less than or equal to another value.</td>
</tr>
<tr>
<td>LT</td>
<td>Tests for a value less than another value.</td>
</tr>
<tr>
<td>GE</td>
<td>Tests for a value greater than or equal to another value.</td>
</tr>
<tr>
<td>GT</td>
<td>Tests for a value greater than another value.</td>
</tr>
<tr>
<td>AND</td>
<td>Returns a value of true if both of its operands are true.</td>
</tr>
<tr>
<td>OR</td>
<td>Returns a value of true if either of its operands is true.</td>
</tr>
<tr>
<td>NOT</td>
<td>Returns a value of true if the operand is false.</td>
</tr>
</tbody>
</table>

**Reference:** Guidelines for Alphanumeric and Logical Expressions

Keep the following in mind:

- An alphanumeric literal with embedded blanks or commas must be enclosed in single quotation marks. For example:
  
  ```-IF &NAME EQ 'JOHN DOE' GOTO QUIT;```
  
  To produce a single quotation mark within a literal, place two single quotation marks where you want one to appear:
  
  ```-IF &NAME EQ 'JOHN O''HARA' GOTO QUIT;```

- A computational field may be assigned a value by equating it to a logical expression. If the expression is true, the field has a value of 1; if the expression is false, the field has a value of 0.

- Use OR to connect literals or other expressions. You must also use parentheses to separate expressions connected with OR.

- Logical operations are done after arithmetic operations, in the following order:
  
  `EQ NE LE LT GE GT NOT CONTAINS OMITS AND OR`

- Separate a collection of test values with OR:
  
  ```-IF &STATE EQ 'NY' OR 'NJ' OR 'WA' GOTO QUIT;```
  
  In this case, OR and EQ are evaluated at the same level.
Use parentheses to specify a desired order. An expression in parentheses is evaluated before any other expression. For example, the command

-IF &STATE EQ 'NY' AND &COUNTRY EQ 'US' OR 'UK' THEN...

is evaluated as:

IF &STATE EQ 'NY' IF &COUNTRY EQ 'US'...

Dialogue Manager then evaluates the phrase OR UK and indicates that it is a syntax error.

To write the command correctly, add parentheses:

-IF ((&STATE EQ 'NY') AND (&COUNTRY EQ 'US' OR 'UK')) THEN...

**Compound Expressions**

**Example:**

Using Compound Expressions

A compound expression has the following form:

-IF expression THEN expression ELSE expression;

The following restrictions apply:

- Each of the expressions may itself be a compound expression, although the expression following -IF may not be a -IF...THEN...ELSE expression (for example, -IF...-IF...).
- If the expression following THEN is itself a compound expression, it must be enclosed in parentheses; this rule does not apply to an expression following ELSE.
- Compound expressions only have up to 16 -IF commands.

**Example:** Using Compound Expressions

If the following example is executed without an input parameter list, the client application receives the message NONE. If it executes with the parameter BANK='FIRST NATIONAL', the client application receives the message FIRST NATIONAL.

-DEFAULTS &BANK = ''
-SET &BANK = IF &BANK EQ '' THEN 'NONE'
-ELSE &BANK;
-TYPE &BANK
The next example uses a compound expression to define a truth condition (1 is true and 0 is false).

-DEFAULTS &CURR_SAL = 900,&DEPARTMENT=MIS
-SET &MYTEST = (&CURR_SAL GE 1000) OR (&DEPARTMENT EQ MIS);
-IF &MYTEST EQ 1 THEN GOTO YES ELSE GOTO NO;
-YES
-TYPE YES
-EXIT
-NO
-TYPE NO

When this code is executed, the client application receives the message YES.

**ON TABLE HOLD**

**How to:**

Use the ON TABLE HOLD Command

When a server receives the results of an SQL request (an answer set) from another server, the answer set will either:

- Be returned to the client application using ON TABLE PCHOLD. That command is described in *ON TABLE PCHOLD* on page 374.

- Be held on the initiating server, without sending it back to the client application, using ON TABLE HOLD. A corresponding Master File for the file that holds the answer set is also created.

**Syntax:**

**How to Use the ON TABLE HOLD Command**

```
SQL
SQL request;
ON TABLE HOLD [AS filename] FORMAT format
END
```

where:

*filename*

Is the name of the file that holds the answer set. If *filename* is omitted, the name of the held file on the server is HOLD, and subsequent creations of HOLD files overlay each other. The file name is a symbolic name known to the operating system for the server environment.
format

A valid format option for the server. The following is a list of commonly used values are:

ALPHA, BINARY, COMMA, COMT, DB2, DIF, DOC (WebFOCUS ONLY), EXCEL, EXL2K (WebFOCUS ONLY), EXL2K PIVOT (WebFOCUS ONLY), FOCUS, HTML, HTMTABLE, INGRES, INTERNAL, LOTUS, PDF, POSTSCRIPT, REDBRICK, SQL, SQLDBC, SQLINF, SQLMAC, SQLMSS, SQLODBC, SQLORA, SQLSYB, SYLK, TABT, WK1, and WP.

The above list is not intended to be a complete list, and the use of some of these formats is limited to use with a configured adapter.

END

Is required on a separate line.

ON TABLE PCHOLD

How to:

Use the ON TABLE PCHOLD Command

Example:

Using the ON TABLE PCHOLD Command

In order for a Dialogue Manager procedure to return an answer set to a client application, a certain set of commands must be issued directly after the SQL request in the syntax of the procedure.

Syntax: How to Use the ON TABLE PCHOLD Command

SQL
SQL request;
TABLE
ON TABLE PCHOLD [FORMAT ALPHA]
END

where:

SQL request;

Is a valid SQL request, ending with a semicolon.

FORMAT ALPHA

Optionally specifies that the hold file on the client is a text file. Use any valid format available on the client, but the underlying transfer is in alpha format. FORMAT ALPHA is the default value.
Is required on a separate line.

**Example:**  **Using the ON TABLE PCHOLD Command**

This example shows how the ON TABLE PCHOLD command requests information from a table in a catalog.

```sql
SELECT NAME, CREATOR, COLCOUNT, RECLENGTH FROM SYSTABLE;
TABLE ON TABLE PCHOLD FORMAT ALPHA
END
```

The result of the request is an answer set sent to the client application by the server.

**Platform-Specific Commands and Features**

This topic describes platform-specific commands that may be included in a procedure for various purposes. However, it always best to avoid the use of platform-specific commands, as they can affect the portability of an application to new environments.

The nature of z/OS, PDS Deployment, and security requires operating system commands to be a limited command set, and use of the keyword DYNAM to preface commands, where other environments are free to simply jump to the operating system command level and executable anything the application user has access to. DYNAM commands are also allowed in z/OS HFS Deployment.

On platforms other than z/OS PDS Deployment, native commands are directly available using the -SYSTEM, -UNIX, -VMS, -WINNT, and -AS/400 series of commands.

File references that are symbolic logical names for the purpose of -READ, -WRITE, TABLE (using external files), and HOLD AS require a DYNAM ALLOC (PDS) or FILEDEF to create the logical reference.

For more information about reporting, see the *Creating Reports With WebFOCUS Language* manual. For more information about Dialogue Manager, see the *Developing Reporting Applications* manual.
DYNAM Command (z/OS PDS and HFS Deployments)

In this section:
- Use of Data Sets
- DYNAM Allocation User Exit
- The ALLOCATE Subcommand
- The CONCAT Subcommand
- The FREE Subcommand
- The CLOSE Subcommand
- The COPY Subcommand
- The COPYDD Subcommand
- The DELETE Subcommand
- The RENAME Subcommand
- The SUBMIT Subcommand
- The COMPRESS Subcommand

How to:
- Use the DYNAM Command

This section describes the DYNAM command and its subcommands.

Syntax:  
**How to Use the DYNAM Command**

The DYNAM command manipulates data sets under MVS.

*DYNAM*  
**subcommand** *operand [operand]...*

where:

**subcommand**

Is required, and specifies one of the operations (subcommands) in the list below. The abbreviated form of the subcommand’s syntax is given under the full form. Details on each subcommand are provided in the following sections as noted.

<table>
<thead>
<tr>
<th>ALLOCATE</th>
<th>Allocates a data set. See <em>The ALLOCATE Subcommand</em> on page 379.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALLOC</td>
<td></td>
</tr>
<tr>
<td>ALLO</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>CONCAT</td>
<td>Concatenates data sets. See <em>The CONCAT Subcommand</em> on page 387.</td>
</tr>
<tr>
<td>FREE</td>
<td>Frees data sets specified by ddnames or dsnames. Names may contain wildcard characters. See <em>The FREE Subcommand</em> on page 388.</td>
</tr>
<tr>
<td>CLOSE</td>
<td>Closes data sets. Use this subcommand when data sets cannot be freed because of being open. See <em>The CLOSE Subcommand</em> on page 389.</td>
</tr>
<tr>
<td>COPY</td>
<td>Copies an entire data set or selected partitioned data set (PDS) members. This subcommand provides features such as record format conversion, either automatic or option controlled. See <em>The COPY Subcommand</em> on page 390.</td>
</tr>
<tr>
<td>COPYDD</td>
<td>Copies a sequential data set or PDS member. COPY handles all the features of COPYDD, and is recommended for use instead of COPYDD. See <em>The COPYDD Subcommand</em> on page 392.</td>
</tr>
<tr>
<td>DELETE</td>
<td>Deletes an entire data set or selected PDS members. See <em>The DELETE Subcommand</em> on page 393.</td>
</tr>
<tr>
<td>RENAME</td>
<td>Renames an entire data set or selected PDS members. See <em>The RENAME Subcommand</em> on page 394.</td>
</tr>
<tr>
<td>SUBMIT</td>
<td>Submits MVS jobs. See <em>The SUBMIT Subcommand</em> on page 396.</td>
</tr>
<tr>
<td>COMPRESS</td>
<td>Compresses a PDS. See <em>The COMPRESS Subcommand</em> on page 397.</td>
</tr>
</tbody>
</table>

**operand**

May be a keyword, a keyword followed by its parameter, or a parameter without a keyword.

The following rules apply to the DYNAM command:

- The subcommand, keywords, and parameters are separated with one or more blanks. Keywords are coded in free format.

- A parameter may be a list of subparameters (for example, VOLUME for a multi-volume data set). Separate subparameters in the list using commas. To include blanks between subparameters (with or without the comma), enclose the entire list in parentheses. For example:

  \[ A, B \ (A, B) \ (A, B) \ (A, B, C, D) \]
A DYNAM command may span several lines. Enter a hyphen (-) at the end of each line to be continued. When the lines are concatenated, blanks after the hyphen and leading blanks from the next line are removed. Blanks before the hyphen are removed if they are preceded by a comma. The total length of a DYNAM command may not exceed 2,048 characters.

Most keywords may be truncated up to the shortest unambiguous length. The commonly used abbreviations are fixed. Note that the unique truncation of a keyword may not always be valid as new keywords are added. It is recommended that the full keyword be used in files.

Fixed abbreviations are given in the following sections on the subcommands. For example, DDNAME may be abbreviated as DD, DDN, DDNA, DDNAM, or DDNAME.

Certain keywords have synonyms. For example, the keywords FILENAME and DDNAME are synonyms, and so are DATASET and DSNAME.

As in TSO, a data set name is enclosed in single quotation marks. Prefix substitution is not supported; specify only the fully qualified data set names in JCL.

Some DYNAM commands accept either the ddname or data set name (dsname) as the same parameter. In such cases, the parameter is considered a ddname if it is not longer than 8 bytes, does not contain periods (.), and is not enclosed in single quotation marks ('). Otherwise, the parameter is considered a data set name. Thus, to specify an unqualified data set name, enclose it in single quotation marks.

**Use of Data Sets**

z/OS PDS Deployment obtains a lock for any allocated data set name; a shared lock for those specified as SHR, and an exclusive lock for OLD, NEW, or MOD.

Although data sets are allocated more than once in a job step, only one type of lock may be obtained. For example, if the data set is initially allocated as SHR and is then allocated as OLD in the same step, the MVS lock changes from shared to exclusive, and the data set is not available for use by other jobs until all allocations in the job are freed.

The DYNAM commands that manipulate data sets use an improved locking mechanism, similar to that implemented in ISPF:

- Any output PDS is allocated by DYNAM (or pre-allocated by the user) as SHR. This avoids exclusive MVS locking, which lasts until all data set allocations are freed.

- To protect from simultaneous updating, DYNAM obtains an exclusive lock as used by ISPF (and other programs, including LINKEDIT), but only during the actual update time. This lock controls access to the data set between users, even from within the same job step.
Note: The DYNAM locking mechanism protects from simultaneous updating and possible
corruption of data, but does not protect from updating and simultaneous reading. For example,
it is possible to continue to read a PDS member recently deleted by another user.

DYNAM Allocation User Exit

The DYNAM allocation user exit is an optional site-supplied routine that may be called for
each data set allocation made by DYNAM. The routine may test, alter, or reject the allocation
request. For more information, see Information Builders Technical Memo 7860.1, The DYNAM
User Exit.

The ALLOCATE Subcommand

How to:
Use the ALLOCATE Subcommand

The DYNAM ALLOCATE command allocates a data set.

Syntax: How to Use the ALLOCATE Subcommand

DYNAM ALLOCATE [disposition] [CLOSE]
DDNAME ddname [DEFER] [DSNAME dsname[(memname)]] [DUMMY]
[EXPD T date]
[HIPER OFF]
[INPT|OUTPT]
[LABEL type]
[MEMBER memname] [status] [MSVGP msvgp]
[PARALLEL] [PASSWORD password] [PERM] [POSITION nnnn]
[REFVOL dsname] [RETPD days] [REUSE]
[UNIT unit]
[VOLUME volser]

Space operands are:

[format]
[parameter]
[DIR n]
[PRIMARY n1]
[RELEASE] [ROUND]
[SECONDARY n2] [SPACE space]
DCB operands are:

- **[BLKSIZE n]**
- **[BUFNO n]**
- **[DEN n]**
- **[DSORG dsorg]**
- **[LRECL n]**
- **[RECFM recfm]**
- **[REFDD ddname]**
- **[REFDSN dsname]**

SMS and VSAM operands are:

- **[DATACLASS name]**
- **[DSNTYPE {LIBRARY | PDS}]**
- **[KEYOFF n]**
- **[LIKE dsname]**
- **[MGMTCLASS name]**
- **[RECORGS recorg]**
- **[SECMODEL name]**
- **[STORCLASS name]**
- **[BUFND m]**
- **[BUFNI n]**

Output printing operands are:

- **[DEST dest[.user]]**
- **[FCB name [ALIGN | VERIFY]]**
- **[FORMS name]**
- **[HOLD]**
- **[OUTLIM n]**
- **[OUTPUT name]**
- **[SYSOUT class]**
- **[USER user]**
- **[WRITER name]**

**where:**

- **ALLOCATE**
  - Can be abbreviated as ALLOC or ALLO.

- **disposition**
  - Is one of the following:

<table>
<thead>
<tr>
<th>CATALOG</th>
<th>DELETE</th>
<th>KEEP</th>
<th>UNCATALOG</th>
</tr>
</thead>
<tbody>
<tr>
<td>By default, for a data set status of NEW, if dsname is specified, the disposition is CATALOG; otherwise, the disposition is DELETE. Is incompatible with SYSOUT. CATLG and UNCAT are also valid as synonyms for CATALOG and UNCATALOG. DELETE, KEEP, and UNCATLOG follow the standard MVS meanings of delete after free, keep as is after free, and keep uncataloged.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **CLOSE**
  - Is deallocation of the data set at close, rather than at the end of the step. The JCL analogy is FREE=CLOSE.
DDNAME  

Is the DDNAME to be associated with an allocation; it must be specified. Synonym is FILENAME.

DEFER

Assigns device(s) to the data set but defers mounting of the volume(s) until the data set is opened. The JCL analogy is DEFER in UNIT.

DSNAME  

The member name is specified either in parentheses after dsname or using keyword MEMBER (see also MEMBER). If dsname is specified as an asterisk (*), terminal is allocated. This is used for output only. Synonym is DATASET.

DUMMY

Allocates a dummy data set.

EXPDT date

Is the expiration date in format YYDDD, YYYY/DDD, or YYYYDDD. Is incompatible with RETPD and SYSOUT.

HIPER OFF

Prohibits allocation in a hiperspace. Is equivalent to UNIT NOHIPER, and is used when UNIT is also to be specified. For example, UNIT VIO HIPER OFF.

INPT

Data set is to be processed as input only (INPT) or output only (OUTPUT). The JCL analogy is IN in LABEL. Is incompatible with SYSOUT.

OUTPT

Data set is to be processed as input only (INPT) or output only (OUTPUT). JCL analogy: IN in LABEL. Is incompatible with SYSOUT.

LABEL type

Specifies type of volume labels. Can be one of the following: NL, SL, NSL, SUL, BLP, LTM, AL, or AUL. Is incompatible with SYSOUT.

MEMBER  

Is the name of a PDS member to be allocated. See also DSNAME.

status

Is the data set status. Possible values are:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW</td>
<td>is the default data set status. Incompatible with SYSOUT.</td>
</tr>
<tr>
<td>MOD</td>
<td>is an extended data set.</td>
</tr>
<tr>
<td>OLD</td>
<td>is exclusive control of the data set.</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>SHR</td>
<td>is shared access to the data set.</td>
</tr>
</tbody>
</table>

**MSVGP msvgp**

Is the identification of a group of mass storage system (MSS) virtual volumes. Is incompatible with SYSOUT and VOLUME.

**PARALLEL**

Each volume is to be mounted on a separate device. The JCL analogy is P in UNIT.

**PASSWORD password**

Password for a password-protected data set.

**PERM**

The allocation is to be permanent—that is, protected from being freed or concatenated by any DYNAM command issued by an MSO user. The operand is valid only in an MSO server initialization profile.

**POSITION nnnn**

Data set sequence number on a tape volume, up to 9999. The JCL analogy is the first subparameter in LABEL.

**REFVOL dsname**

Volume serial information is to be obtained from the named cataloged data set. The JCL analogy is VOL=REF=dsname. Is incompatible with SYSOUT and VOLUME.

**RETPD days**

Is the retention period, up to 9999 days. Is incompatible with EXPDT and SYSOUT.

**REUSE REU**

If the ddname to be allocated is already in use, it is to be freed.

**UNIT unit**

Is the device group name, device type, specific unit address, or NOHIPER. NOHIPER prohibits allocation in a hiperspace, and is meaningful for a temporary (NEW, DELETE) data set; see also HIPER OFF.

**VOLUME volserVOL**

Are volume serial numbers. Are incompatible with REFVOL and SYSOUT. Synonyms are VOLUME and VOLser.
Space operands may be:

**format**

The format of the primary space to be allocated. Possible values are:

- **ALX** is up to five contiguous areas.
- **CONTIG** is one contiguous area.
- **MXIG** is one maximal contiguous area.

JCL analogy: ALX/CONTIG/MXIG in SPACE.

**n**

Represents units of primary and secondary space allocation.

**parameter**

The parameter for space allocation. Possible values are:

- **BLOCKS [n]**
- **CYLINDERS**
- **MEGABYTES**
- **PAGES**
- **TRACKS**

**n** represents units of primary and secondary space allocation. If the parameter for BLOCKS is omitted, the average block length is copied from BLKSIZE. If the space unit is omitted but SPACE and BLKSIZE are specified, BLOCKS equal BLKSIZE is used. For PAGES, BLOCKS 4096 is used. BLKSIZE must be specified if the BLOCKS parameter is specified.

Synonyms are CYLs for CYLINDERS and TRKs for TRACKS.

**DIR n**

The number of 256-byte records for the directory of a PDS.

**PRIMARY n1**

The primary space quantity. See also **SPACE**.

**RELEASE**

The unused space is to be released when the data set is closed. Synonym is RLSE.

**ROUND**

If space is requested in BLOCKS, MEGABYTES, or PAGES, it is to be rounded to whole cylinder(s).

**SECONDARY n2**

Is the secondary space quantity. See also **SPACE**.
### SPACE space SP

The primary (n1) and/or secondary (n2) space quantity in one of the following formats:

\[ n1/(n1)/n1, n2/(n1, n2)/n1, n2/(n1 n2)/n1, n2/(, n2) \]

See also PRIMARY and SECONDARY.

DCB operands may be:

**BLKSIZE n**

The block size, up to 32760. See also BLOCKS.

**BUFNO n**

The number of buffers, up to 255.

**DEN n**

n represents magnetic tape density: 0, 1, 2, 3, or 4 for 200, 556, 800, 1600, 6250 bpi respectively.

**DSORG dsorg**

The data set organization. Default, for NEW only: PO if DIR or DSNTYPE specified; PS otherwise. Following values are syntactically correct:

<table>
<thead>
<tr>
<th>DSORG</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VS</td>
<td>VSAM</td>
</tr>
<tr>
<td>PO/POU</td>
<td>PDS or PDS unmovable.</td>
</tr>
<tr>
<td>DA/DAU</td>
<td>Direct access or direct access unmovable.</td>
</tr>
<tr>
<td>PS/PSU</td>
<td>Physical sequential or physical sequential unmovable.</td>
</tr>
</tbody>
</table>

**LRECL n**

The logical record length, up to 32760.

**RECFM recfm**

The record format. The first letter must be D, F, U, or V, which may be followed by any valid combination of A, B, M, S, or T:

<table>
<thead>
<tr>
<th>RECFM</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Records with ISO/ANSI control characters.</td>
</tr>
<tr>
<td>B</td>
<td>Blocked records.</td>
</tr>
<tr>
<td>D</td>
<td>Variable-length ISO/ANSI tape records.</td>
</tr>
<tr>
<td>F</td>
<td>Fixed-length records.</td>
</tr>
</tbody>
</table>
### Records with machine code control characters.

### Standard fixed-length or spanned variable-length records.

### Track overflow.

### Undefined-length records.

### Variable-length records.

**REFDD** *ddname*

DCB attributes are to be copied from the specified *ddname*. Under TSO, EXPDT and INPT/OUTPT specifications are also copied. Any of those can be overridden by the appropriate keyword on the same command. The JCL analogy is DCB=*. *ddname*. Is incompatible with REFDSN.

**REFDSN** *dsname*

DCB attributes (DSORG, RECFM, OPTCD, BLKSIZE, LRECL, RKP, KEYLEN) and EXPDT are to be copied from the specified cataloged data set. Any of those can be overridden by the appropriate keyword on the same command. The JCL analogy is DCB=dsname. Is incompatible with REFDD.

**SMS and VSAM operands are:**

**DATACLASS** *name*

The name of a data class for an SMS-managed data set.

**DSNTYPE {LIBRARY|PDS}**

LIBRARY is for a new partitioned extended (PDSE), and PDS is for a new partitioned data set. A PDSE cannot contain load modules, should be SMS-managed, and allows concurrent updating of different members.

**KEYOFF** *n*

The offset of the key in each logical record for a new VSAM key-sequenced (RECORG KS) data set.

**LIKE** *dsname*

Allocation attributes (DSORG, RECORG, or RECFM, LRECL, KEYLEN, KEYOFF, SPace, DIR) are to be copied from the specified cataloged data set (model). Any of those can be overridden by the appropriate keyword on the same command.

**MGMTCLASS** *name*

The name of a management class for an SMS-managed data set.
The VSAM record organization: KS, ES, RR, or LS for key-sequence, entry-sequence, relative record, or linear space data sets, respectively.

The data set RACF profile is to be copied from the named existing RACF profile.

The name of a storage class for an SMS-managed data set.

The number of VSAM DATA buffers.

The number of VSAM INDEX buffers.

The remote destination for a SYSOUT data set. In conjunction with user ID, it is a node and a user at that node; the user ID is coded after the period (.) or using the USER keyword.

The name of an FCB (forms control buffer) image to be used for printing of a data set. The operator may be asked to check the printer forms alignment (ALIGN), or to verify the FCB image name displayed on the printer (VERIFY).

A SYSOUT form name. JCL analogy: third subparameter in SYSOUT, FORMS in OUTPUT JCL.

A SYSOUT data set is to be placed on the hold queue.

A limit for the number of logical records in a SYSOUT data set.

The name(s) of OUTPUT JCL statement(s) to be associated with a SYSOUT data set.

A SYSOUT data set is to be allocated and the specified output class (A-Z, 0-9) is to be assigned. If an asterisk (*) or NULL is coded, the class is copied either from CLASS in OUTPUT JCL if it is specified, or otherwise from MSGCLASS in JOB.
**USER user**

A SYSOUT data set is to be routed to the specified user ID. DEST is required to specify a user's node.

**WRITER name**

The name of an installation-written system output printing routine. The JCL analogy is the second subparameter in SYSOUT. Is incompatible with USER.

In addition to the shown fixed abbreviations and synonyms, keywords may be abbreviated up to the unique truncation. Those abbreviations are not fixed and may be changed when new keywords are added. They may be used interactively to save some keystrokes, but when a command is saved in a file, it is recommended that you use unabbreviated keywords.

**Examples:**

Allocate an existing data set:

```
DYNAM ALLOC DD MYDD DS MYID.DATA.SET SHR REU
```

Allocate a new data set. Defaults are NEW, CATALOG (dsname present), and DSORG PO (not-zero DIR present):

```
DYNAM ALLOC DD MYDD DS MYID.DATA.SET SPACE 6,2 TRACKS DIR 4 UNIT SYSDA - RECFM FB LRECL 80 BLKSIZE 1600
```

Allocate a terminal:

```
DYNAM ALLOC DD MYDD DS *
```

Allocate a SYSOUT data set with default output class. Upon freeing, the data set is sent to the user ID U1234 at node SYSVM:

```
DYNAM ALLOC DD MYDD SYSOUT * DEST SYSVM.U1234
```

**The CONCAT Subcommand**

**How to:**

Use the CONCAT Subcommand

The DYNAM CONCAT command concatenates up to 16 data sets.

**Syntax:**

**How to Use the CONCAT Subcommand**

```
DYNAM CONCAT [PERM] DDNAME ddname1 ddname2 [ddname3...]
```

where:

**CONCAT**

Can be abbreviated as CONC.
PERM

Is optional. This marks the concatenation as permanent—that is, protected from being freed or concatenated again by any DYNAM command issued by an MSO user. Valid only in an MSO server initialization profile.

DDNAME DDN DD

Are required; synonym is FILENAME.

ddname1

Is the first ddname to be concatenated and associated with the resulting concatenated group.

ddname2

Is the second ddname and any subsequent ddname to be concatenated.

For example:

DYNAM CONCAT DDN EDARPC MYEX NEWEX

The FREE Subcommand

How to:

Use the FREE Subcommand

The DYNAM FREE command deallocates any number of specified data sets.

Syntax:

How to Use the FREE Subcommand

DYNAM FREE (DDNAME ddname [ddname...] | DSNAME dsname [dsname...])

where:

DDNAME DDN DD

Are required if there is no dsname; synonym is FILENAME.

ddname

Is the ddname of the data set to be freed.

DSNAME DSN DS

Are required if there is no ddname; the synonym is DATASET.

dsname

Is the name of the data set to be freed. All ddnames associated with this dsname, except concatenated groups, are deallocated.
While at least one ddname or data set name is required, you may specify more than one ddname or data set name. Each specified name may contain asterisks (*) and question marks (?) as wildcards. Wildcards are special characters used to specify a subset of names rather than one name. The wildcards appear anywhere in a name and mean the following:

*  
  Represents any number of characters. For example, *Q* matches any name containing the character Q.

?  
  Represents any single character. For example, ?Q? matches any 3-character name containing the character Q in the middle.

If the ddname is not found, a message is issued only if a single ddname without wildcards is specified. A message is not displayed if a data set or more than one ddname is not found.

**Examples:**

```
DYNAM FREE DDN SYS0* TEMP?
DYNAM FREE DSN MYID.DATA.SET
```

**The CLOSE Subcommand**

**How to:**

Use the CLOSE Subcommand

The DYNAM CLOSE command closes data sets that cannot be freed because they are opened.

**Syntax:**

```
DYNAM CLOSE  {DDNAME ddname [ddname...]|DSNAME dsname [dsname...]}  
```

where:

```
CLOSE  
  Can be abbreviated as CLO.

DDNAME DDN DD  
  Are required if there is no dsname; the synonym is FILENAME.

ddname  
  Is the ddname of the data set to be closed.
```
DSNAME DSN DS

Are required if there is no ddname; the synonym is DATASET.

dsnname

Is the name of the data set to be closed. All ddnames associated with this dsname, except concatenated groups, are closed.

While at least one ddname or data set name is required, more than one ddname or data set name may be specified. Each specified name may contain wildcard characters. The same rules apply to the DYNAM CLOSE command as to the DYNAM FREE command.

The COPY Subcommand

How to:

Use the COPY Subcommand

The DYNAM COPY command copies an entire MVS data set or selected PDS members.

Syntax:

DYNAM COPY dname1 {[TO] dname2 [[MEMBER] members] [[MEMBER] members]} [options]

where:

dname1

Is the dsname or ddname of the input data set. This is a positional parameter. It must precede all other operands.

TO

May be omitted if dname2 does not match a reserved word, the MEMBER keyword, an option, or the TO keyword. To avoid confusion, use the TO keyword whenever dname2 is a ddname.

dname2

Is the dsname or ddname of the output data set. If the output data set is not a PDS and the dsname is specified, it is allocated as OLD. If the ddname is specified, and the status is SHR, ensure that other users do not access the data set during COPY. Unlike ISPF, DYNAM locks a non-PDS data set in order to prevent simultaneous updating by different DYNAM users.

MEMBER

May be omitted if members are specified in parentheses.
members

Can be a single member specification or a list of member specifications. If the members are enclosed in parentheses, blanks before the left parenthesis may be omitted.

options

May be one or more of the following options:

APPEND adds the input to the end of the existing data, if the output is a sequential data set.

FORCE copies input DCB attributes (RECFM, BLKSIZE, LRECL, and KEYLEN) to the output data set. By default, only missing values are assigned.

KEYMOD allows key modification according to input/output KEYLEN: truncation or padding with binary zeros.

REPLACE replaces all output members matching the selected member names.

TRUNCATE allows truncation of input records that are longer than the output record length. Since trailing blanks are truncated automatically when RECFM is different, the keyword is used either to cut records of the same format or to cut non-blank data.

A member specification has the following syntax

\[ mem[, [newmem][,REPLACE]] \]

where:

mem

Is the selected member name.

newmem

Is the optional new name for the output member.

REPLACE

Is optional and specifies an existing member to be replaced in the output PDS.

Since the comma may be used in member specifications, they are separated with one or more blanks when specified in a list. Therefore, a list of member specifications is always enclosed in parentheses. For example:

\( (MEM\ MEM, NEWMEM\ MEM, NEWMEM, R\ MEM, , R) \)
Note:

- All conversions between different DCB attributes (RECFM, BLKSIZE, and LRECL) are performed automatically.

- If the entire PDS is copied or any selected member’s directory entry contains a TTRN in user data (for example, a load module), the IBM utility IEBCOPY is invoked. In this case, all options except REPLACE are ignored, format conversion is not possible, and copying members to the same PDS is not supported. Note that IEBCOPY requires APF authorization in order to be performed.

- If the main member and its alias names are copied, the relationship remains the same on the output PDS.

- If a specified ddname has been allocated with a member name, the data set is treated as sequential.

Examples:

Copies the entire data set, whether it is a PDS or not.

```
DYNAM COPY MYDD MYID.DATA.SET
```

All four commands are equivalent. Either input or output may be a sequential data set, or both are PDSs.

```
DYNAM COPY MYDD MYID.DATA.SET MEMBER MEM
DYNAM COPY MYDD MYID.DATA.SET(MEM)
DYNAM COPY MYDD(MEM) MYID.DATA.SET
DYNAM COPY MYDD MEMBER MEM MYID.DATA.SET
```

Copies and renames one member.

```
DYNAM COPY MYID.DATA.LIB TO MYDD(MEM1,MEM2)
```

Copies two members.

```
DYNAM COPY MYID.DATA.LIB TO MYDD(MEM1 MEM2)
```

Copies two members into same PDS with renaming.

```
DYNAM COPY MYDD(OLD1,NEW1,R OLD2,NEW2)
DYNAM COPY MYDD(OLD1,NEW1 OLD2,NEW2) REPL
```

The COPYDD Subcommand

How to:

Use the COPYDD Subcommand

The DYNAM COPYDD command copies a sequential data set or PDS member.
**Syntax:** How to Use the **COPYDD** Subcommand

DYNAM COPYDD  

\[ \text{ddname}_1[(\text{mem}_1)] \quad \text{ddname}_2[(\text{mem}_2)] \]

where:

- \( \text{ddname}_1 \)  
  Is the ddname of the input data set.

- \( \text{mem}_1 \)  
  Is optional. It is the input member name.

- \( \text{ddname}_2 \)  
  Is the ddname of the output data set.

- \( \text{mem}_2 \)  
  Is optional. It is the output member name.

**Note:**

- If the specified ddname has been allocated with a member name, the data set is treated as sequential.

- Identically named members are always replaced on the output PDS.

- All conversions between different DCB attributes (RECFM, BLKSIZE, and LRECL) are performed automatically.

- Since the DYNAM COPY command has more features than COPYDD, it is recommended that you use COPY instead of COPYDD.

**The DELETE Subcommand**

**Syntax:** How to Use the **DELETE** Subcommand

DYNAM DELETE  

\[ \text{dsname} \]

To delete individual members, use

DYNAM DELETE  

\[ \text{dsname} [\text{MEMBER}] \text{ members} \]

The DYNAM DELETE command deletes an entire MVS data set or selected PDS members.
where:

**DELETE**
Can be abbreviated as DEL.

**dsname**
Is the data set name to be deleted and uncataloged.

**dname**
Is the dsname or ddname of a PDS containing one or more members to be deleted. The ISPF-like lock is obtained.

**MEMBER**
May be omitted if the members are specified in parentheses.

**members**
Can be a single member name or a list of members. If the members are enclosed in parentheses, blanks before the left parenthesis can be omitted.

**Examples:**

DYNAM DELETE MYID.DATA.OLD
DYNAM DEL MYID.DATA.LIB MEMBER OLD1,OLD2
DYNAM DELETE MYDD(OLD1,OLD2)
DYNAM DEL MYDD(OLD1 OLD2 OLD3)

**The RENAME Subcommand**

**How to:**
Use the RENAME Subcommand

The DYNAM RENAME command renames an entire MVS data set or selected PDS members.

**Syntax:** **How to Use the RENAME Subcommand**

DYNAM RENAME dsname1 dsname2
To rename individual members, use
DYNAM RENAME dname [MEMBER] members [REPLACE]
where:

**RENAME**
Can be abbreviated as REN.
dsname1
Is the data set name to be renamed and uncataloged.

dname2
Is the new name to be assigned to the data set and cataloged.

dname
Is the dsname or ddname of a PDS containing one or more members to be renamed. The ISPF-like lock is obtained.

MEMBER
May be omitted if the members are specified in parentheses.

members
Can be a single member specification or a list of members. If the members are enclosed in parentheses, blanks before the left parenthesis can be omitted.

REPLACE
Is optional. This replaces all members matching the specified new names.

A member specification has the following syntax

oldmem,newmem[,REPLACE]

where:

oldmem
Is the original member name.

newmem
Is the new member name.

REPLACE
Is optional and replaces existing members with the same name as newmem.

Since the comma is used in member specifications, each pair of members is separated with one or more blanks when specified in a list; therefore, a list of member specifications is always enclosed in parentheses.

Examples:

DYNAM RENAME MYID.DATA.OLD MYID.DATA.NEW
DYNAM REN MYID.DATA.LIB MEMBER OLD,NEW,R
DYNAM RENAME MYDD(OLD1,NEW1,R OLD2,NEW2)
DYNAM REN MYDD(OLD1,NEW1 OLD2,NEW2) REPL
The SUBMIT Subcommand

How to:
Use the SUBMIT Subcommand

The DYNAM SUBMIT command submits jobs to MVS.

The ddname for DYNAM SUBMIT is normally allocated using a DYNAM ALLOC command. On HFS-deployed servers, if a DYNAM ALLOC is not found for the ddname, DYNAM SUBMIT will check whether a FILEDEF was issued for the ddname.

Syntax:
How to Use the SUBMIT Subcommand

DYNAM SUBMIT dname [MEMBER(members)]

where:

SUBMIT
Can be abbreviated as SUB.

dname
Is the dsname or ddname of the input data set(s) containing JCL to be submitted. The ddname specifies a concatenation of data sets.

MEMBER
May be omitted if the members are specified in parentheses.

members
May be a single member name or a list of members. When a member list is submitted, the resulting job stream is the concatenation of the members. If the members are enclosed in parentheses, blanks before the left parenthesis can be omitted.

Examples:

DYNAM SUBMIT MYDD MEMBER ASM,PROG,LKED
DYNAM SUB MYDD(ASM,PROG,LKED)
DYNAM SUB MYID.DATA.LIB(CREATE LOAD)
DYNAM SUBMIT MYFILE

Note: The DYNAM SUBMIT command provides an interface with the submit user exit IKJEFF10 as described in the IBM TSO Extensions Version 2 Customization manual. For details, see Information Builders Technical Memo 7859, Enabling a Site-Specified Submit Exit Routine.
The COMPRESS Subcommand

**How to:**
Use the COMPRESS Subcommand

The DYNAM COMPRESS command compresses the partitioned data sets (PDS).

**Syntax:**

**How to Use the COMPRESS Subcommand**

DYNAM COMPRESS dname [dname]...

where:

COMPRESS

Can be abbreviated as COMP.

dname

Is the dsname or ddname of a PDS to be compressed. The ISPF-like lock is obtained.

If the dsname is specified, it is allocated as OLD. If the ddname is specified and status is SHR, make sure that another user does not access the PDS during the compress operation.

**Note:** DYNAM COMPRESS uses the IBM utility IEBCOPY, and therefore are only used when running with APF authorization.

**Examples:**

DYNAM COMPRESS MYDD
DYNAM COMPRESS MYID.DATA.LIB
DYNAM COMP MYDD MYID.DATA.LIB

Comparison of TSO Commands, JCL, and DYNAM

**Example:**

Allocating an Existing File
Creating a New Data Set
Freeing Files
Concatenating Files

This section shows examples of TSO commands and JCL, compared to the equivalent DYNAM commands.
### Allocating an Existing File

**Example:**

<table>
<thead>
<tr>
<th>TSO:</th>
<th>TSO ALLOC F(EDARPC) DA('MYUSER.EDARPC.DATA') SHR</th>
</tr>
</thead>
<tbody>
<tr>
<td>JCL:</td>
<td>//EDARPC DD DSN=MYUSER.EDARPC.DATA,DISP=SHR</td>
</tr>
<tr>
<td>DYNAM:</td>
<td>DYNAM ALLOC FILE EDARPC DA MYUSER.EDARPC.DATA SHR</td>
</tr>
</tbody>
</table>

### Creating a New Data Set

**Example:**

<table>
<thead>
<tr>
<th>TSO:</th>
<th>TSO ALLOC F(EDARPC) DA('MYUSER.EDARPC.DATA')-SPACE(5,3) TRACKS CATALOG DIR(2)-UNIT(SYSDA) USING(NEWDCB)-LRECL(80) RECFM(F B) BLKSIZE(1600)</th>
</tr>
</thead>
<tbody>
<tr>
<td>JCL:</td>
<td>//EDARPC DD DSN=MYUSER.EDARPC.DATA,DISP=(NEW,CATLG), // SPACE=(TRK,(5,3,2)),UNIT=SYSDA, // CB=(LRECL=80,RECFM=FB,BLKSIZE=1600)</td>
</tr>
<tr>
<td>DYNAM:</td>
<td>DYNAM ALLOC FILE EDARPC DA MYUSER.EDARPC.DATA -SPACE 5,3 TRACKS CATLG DIR 2UNIT SYSDA -LRECL 80 RECFM FB BLKSIZE 1600</td>
</tr>
</tbody>
</table>

### Freeing Files

**Example:**

<table>
<thead>
<tr>
<th>TSO:</th>
<th>TSO FREE F(EDARPC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DYNAM:</td>
<td>DYNAM FREE FILE EDARPC</td>
</tr>
</tbody>
</table>

### Concatenating Files

**Example:**

<table>
<thead>
<tr>
<th>TSO:</th>
<th>TSO ALLOC F(EDARPC) DA('MYUSER.EDARPC.DATA'- 'MYUSER.PROGRAMS.DATA') SHR</th>
</tr>
</thead>
<tbody>
<tr>
<td>JCL:</td>
<td>//EDARPC DD DSN=MYUSER.EDARPC.DATA,DISP=SHR // DD DSN=MYUSER.PROGRAMS.DATA,DISP=SHR</td>
</tr>
<tr>
<td>DYNAM:</td>
<td>DYNAM ALLOC FILE EDARPC DA MYUSER.EDARPC.DATA SHR DYNAM ALLOC FILE PROGRAMS DA MYUSER.PROGRAMS.DATA SHR DYNAM CONCAT FILE EDARPC PROGRAMS</td>
</tr>
</tbody>
</table>

**Platform-Specific Commands and Features**
A logical name (or ddname) is a shorthand name that points to the physical file name as the operating system actually knows the file. Logical names simplify code by allowing short names to be used in place of the longer physical file name.

The FILEDEF command assigns a logical name (or ddname) to a physical file name and specifies file attributes. FILEDEF assignments are in effect for the duration of a connection (except when a server is running in Pool Mode). They are released when the connection to the server is closed or a FILEDEF CLEAR is issued.

FILEDEF with the device name PRINTER is used in conjunction with OFFLINE requests to control printing attributes (such as the printer assignment and number of copies), and is further detailed in How to Use the FILEDEF Command in UNIX, Windows, IBM i, z/OS, and OpenVMS on page 399.

**Syntax:**

How to Use the FILEDEF Command in UNIX, Windows, IBM i, z/OS, and OpenVMS

FILEDEF ddname devicetype fileid [(LRECL n) [RECFM fm] [APPEND]]

or

FILEDEF ddname DISK app/[appa...]physfile.ftm

FILEDEF ddname CLEAR

where:

- **ddname**
  - Is the logical name. It may contain 1 to 8 alphanumeric characters.

- **devicetype**
  - Identifies the type of device with which to interact. Specifies DISK for a file that resides on disk. Other device types are PRINTER, TRMIN, and TRMOUT, which have special meanings and options. For more information, see Other FILEDEF Features on page 401.

- **CLEAR**
  - Clears the specified ddname.

- **app/[appa...]**
  - Is an application name (APP form of FILEDEF). It can be a nested application name.
physfile.ftm

Is a physical file located in the application (APP form of FILEDEF).

fileid

Is the physical full path name of the file as it is known on the particular operating system using the native style of the operating system (non APP form of FILEDEF).

For instance, for Windows:

c:\mydir\myfile.dat
\mymachine\mydir\myfile.dat

For UNIX, z/OS, and IBM i IFS:

/home/myhome/mydir/mtfile.dat

For OpenVMS:

DISK$MYDISK:[MYHOME.MYDIR]MYFILE.DAT

For IBM i QSYS

QSYS:MYLIB/MYFILE
QSYS:MYLIB/MYFILE(MYMemb)

UNIX, z/OS, and IBM i IFS are case-sensitive file systems where lower case file names are the norm, so appropriate names should be used when coding the fileid option of the FILEDEF. The use of relative file names for server use is not supported, as they are easily confused on some platforms as APP names. The use of an APP MAP command and APP-based naming will let one simulate relative names, yet also be portable to other platforms by simply adjusting the MAP value.

To support physical directory (or file) names with embedded blanks (common on Windows, but also possible on some other operating systems), the complete fileid must be enclosed in single quotation marks. In most instances, a physical operating system name has a unique characteristic that can be used to detect if a physical name is being used so it will not be confused with an APP name. However, IBM i native library names are not always unique enough, so they require an explicit prefix (QSYS:) to ensure proper access.

**Note:** APP usage can handle any number of directories below APPROOT when nested applications are on (internal default or when edaserver.cfg has nested_app=y). APP usage is limited to the number of directory levels allowed by the nested_app configuration of a server. Any other usage is illegal.

LRECL n

Specifies the record length, n, in bytes. This parameter is optional. If you omit it, the default is 80 bytes. Note that the left parenthesis preceding the optional parameters is required.
RECFM \textit{fm}  
Describes the record format. Specifies \textit{F} for fixed format, \textit{V} for variable format. This parameter is optional. If you omit it, the default is fixed format. Note that the left parenthesis preceding the optional parameters is required.

\textbf{APPEND}  
Enables you to open the specified file and add new material at the end of the file. This parameter is optional. If you omit it and the specified file exists, it will be overwritten. Note that the left parenthesis preceding the optional parameters is required.

Note that FOCUS data sources (files with the .foc extension) that do not conform to the default naming conventions are identified using the \textit{USE} command, not FILEDEF.

\textbf{Other FILEDEF Features}  

\texttt{PRINTER} as a device type is used to change the default output file for the \texttt{OFFLINE} print file or set output destinations. For more information, see \textit{Sending Stored Procedure Report Output to Server-Side Printers} on page 325.

FILEDEF \texttt{TRMIN \textit{TERM} LOWER} is used to change the uppercasing behavior of an interactive session (\texttt{edastart -t}) into case sensitive mode. FILEDEF \texttt{TRMIN \textit{TERM} UP} is used to restore default behavior. Interactive session mode is typically used for testing and is not considered a production feature for general use.

FILEDEF \texttt{TRMOUT \textit{DISK} fileid} is used to capture session output into a file and is only valid during an interactive session (\texttt{edastart -t}).

FILEDEF \texttt{TRMOUT \textit{TERM}} is used to restore default behavior after a change to \texttt{DISK}. Interactive session mode is typically used for testing and is not considered a production feature for general use.

For information about FILEDEF \texttt{OFFLINE PRINTER}, see \textit{Sending Stored Procedure Report Output to Server-Side Printers} on page 325.

While command input lines (interactively or in a \texttt{FOCEXEC}) are effectively unlimited, this was not always the case. A feature of FILEDEF to deal with usually long directory/file names and this former limitation was the ability to split the FILEDEF command across several lines. This was done by using a dash (-) after a FILEDEF token to indicate continuation on the next line. While this feature is not needed anymore, it remains a feature for upward compatibility purposes and is documented here as a deprecated feature.
Server Side OFFLINE Printing

Server side printing of formatted reports is accomplished using the `OFFLINE` command, which sets up and issues a default OFFLINE FILEDEF (or DYNAM ALLOC on z/OS PDS deployment) to receive the formatted outputs after an OFFLINE CLOSE is issued.

The following example on UNIX (and Linux) creates an offline.ftm file and calls `lp`, the default print command for UNIX (and Linux). On other platforms an equivalent print command is issued:

```
OFFLINE
TABLE FILE CAR
PRINT COUNTRY
END
OFFLINE CLOSE
```

There may be one or more outputs buffered to the same output file for printing, but they are not released to the file until an OFFLINE CLOSE is issued. If a system level variable for FOCPRINT is available at OFFLINE CLOSE time, it will be used to attempt printing of the actual file.

The FILEDEF (or DYNAM ALLOC on z/OS PDS Deployment) OFFLINE PRINTER `device` feature allows the additional specification of output destinations and, in some cases, additional operating system print command switches for features such as multiple copies. In this way, a request can be customized to the print requirements of a particular site.

Prior behavior was that if the operating system variable FOCPRINT was declared (with an operating system command and a `$1`), it would be called to take an action on the file name which also replaced the `$1` in the string.

The enhanced FILEDEF command is:

```
FILEDEF OFFLINE PRINTER [filename] [ (PRINTER printername )
```
The printer name option is used with the standard print feature of a given platform. If no printer name is declared or is set to blank, then the offline file is created, but the print feature is not called. Since printing is platform specific, each platform is described here individually, however, there are still some common needs that are sometimes best resolved by creating a layer that can act as a proxy between the server and the print system.

**UNIX and z/OS HFS Deployment**

The printer name is dropped in as the "-d" switch value in the "lp -c -d" command. The "-c" switch is used to avoid over-writing of the offline file before actual printing has occurred. If additional lp switches are desired (like multiple copies with the -n switch), they may be stacked into the name by enclosing the string in single quotation marks:

```
FILEDEF OFFLINE PRINTER ( PRINTER '29d1 -n 2'
```

If a site uses lpr instead of lp, then an lp shell script can be created in the $PATH before the standard lp command and can act as a proxy to call lpr instead. The lp script could be as simple as "/usr/bin/lpr $*" to redirect lp to lpr.

**Note:** On z/OS HFS Deployment, the file is spooled to the system and actual disposition will depend on the configuration of the printer spool.

**z/OS PDS Deployment**

A DYNAM ALLOC command for OFFLINE is used to specify spooling attributes.

**OpenVMS**

The printer name is dropped in as the "/QUEUE=" switch value in the "PRINT/QUEUE=" command. OpenVMS always makes a copy of the file to be printed so it does not have an over-writing the offline file problem. If additional PRINT switches are desired (like multiple copies with /COPIES= switch) they may be stacked into the name by enclosing the string in single quotation marks:

```
FILEDEF OFFLINE PRINTER ( PRINTER '29d1 /COPIES=2'
```

Sites rarely use anything but the standard PRINT command, but can be also proxied if necessary by creating an alternate printer command at the OS level or queue / symbiont that routes to the alternate method.

**Windows**

The printer name is a shared printer name and is used to set up (and later drop a NET USE for the LPT1device to a shared name (for example, \\nodename\myprinter), which is then used in a PRINT /D:LPT1 command to print the actual file. As such, additional switch options cannot be done and use of a PRINT.BAT as a proxy is the only method for further manipulation of the output.
IBM i

Note: IBM i was formerly known as i5/OS.

The output is always spooled from the offline file to the print spool using the system QPRINT file (with whatever the standard values are) on the server's library list. If the spool is set to directly print, output will always be routed as directed with no declaration of a printer name using FILEDEF. If output is not automatically routed and a printer name (using FILEDEF) is declared, then a CHGSPLFA command will be issued with the printer name as the OUTQ() value to direct the spool file to a destination. If additional CHGSPLFA parameters are desired (such as multiple copies with the COPIES() parameter), they may be stacked into the name by enclosing the string in single quotation marks:

FILEDEF OFFLINE PRINTER ( PRINTER '29d1 COPIES(2)' )

A user can also set a specific IBM i QPRINT file to use (which may have attributes such as number of copies set within it) for spooled OFFLINE print files by either placing an appropriate QPRINT file (explicitly named QPRINT) on the server library path or issuing a SET command to use an explicit QPRINT file (of any name). Additionally, you may set a spool file SPLUSRDTA attribute (10-character limited string) to assist in identifying outputs. When set, the print spool job will pick up the attribute information and be displayed by the native operating system tools like DSPLSPLF and WRKDSPLF.

The commands are:

SET I5QPRINT = [{library}]{qprintfile}

and

SET I5SPLUSRDTA = string

The internal default for I5QPRINT is QPRINT and may be set to any valid CRTPRTF-created QPRINT file. The QPRINT file and its attributes must be appropriate for the type of file that the OFFLINE command produces (paged plain text) and the capabilities of the actual print device. If no library is supplied, the *LIBL value of the job will be used to locate the file.

Setting I5QPRINT or I5SPLUSRDTA with no value to the right of the equal sign has no affect and leaves the current value unchanged.

Use SET I5SPLUSRDTA = '' to set I5SPLUSRDTA explicitly back to no value (blank). Also use single quotation marks for values with embedded spaces.

An I5QPRINT value of blank is illegal for the i5 spool system, so a value of '' defaults to QPRINT.

Note that the CRTPRTF command for creating printer attribute files does not create a default QPRINT that matches the IBM-delivered standard default that is in QGPL. To create a QPRINT with standard IBM-delivered default values use:

CRTPRTF FILE(*CURLIB/QPRINT) RPLUNPRT(*NO) CHRID(*CHRIDCTL)
Then make any site-specific changes and change the owner attribute rights from *ALL to *CHANGE (to prevent over-writing) with:

```
EDTOBJAUT OBJ(*CURLIB/QPRINT) OBJTYPE(*FILE)
```

The use of an lp script on IBM i as a proxy is not effective because lp is not used. The use of alternate QPRINT files is the closest equivalent to an lp proxy.

**OFFLINE to DISK Versus PRINTER**

The "( PRINTER printername" feature is only valid when the FILEDEF device is PRINTER. There is, however, a difference between the use of DISK versus PRINTER as a device in a FILEDEF for OFFLINE. When the device DISK is used, page breaks are represented by a 1 in the first column of a given line where a page break is to occur. This is the FORTRAN Carriage Control method of page control and is a vestige of the product’s original mainframe roots. When the disk device is PRINTER, the more modern, Control L (^L / Decimal 12 / Hex 0C) form feed method is used.

**Other Printing Information**

Very often, sophisticated laser based printers are "hung" off networks and communicated with various print protocols. While these printers may come from many manufactures, a very common (but not standard) attribute of these types of printers is automatic sensing between a plain clear text file being sent to the printer and a postscript file that contains printer attribute commands as well as the text to print.

OFFLINE files are plain text (vs. HOLD FORMAT PS which do not get spooled using OFFLINE, and it is up to the user to direct them to a printer). Very often, these sophisticated printers can be set up or used improperly, causing a printer to think a plain text file is postscript when it is not, and yielding a page with a postscript error message. This has only been seen so far when printing from Windows, but is in theory possible from any platform.

This problem is not considered to be a server issue because the software is not directly manipulating these printers and uses standard commands supplied by the OS vendor for printing. Generally, this problem can also be reproduced using standard print tools stand-alone from the server environment. A systems administrator for a printer exhibiting an issue like this should be able to track down why this happens in any given environment and take corrective action.

An improper spooling issue may typically also be corrected by creating a proxy script to inject a leading character into the output that resets the printer, so the remaining output properly prints. Generally, this is a control D, but may vary by printer make and model and, as such, specific implementation of such a proxy script is left to the customer since specific needs may vary greatly by site and the various printer models that are available.
Stress Testing a Procedure

Stress testing enables you to simulate request execution in order to ensure that the server will retrieve data satisfactorily under specified conditions.

The mechanism behind stress testing is a record and playback feature in which the exact sequence of user actions applied through a browser are recorded and then reproduced (played back), simulating a single user or multiple users under the same or different conditions. You can use the generated files and the recorded sequences, known as HTI scripts, along with server traces, to test new configurations, and to diagnose problems.

From the Web Console Playback of HTI Scripts pane, you can initiate test runs under the following separate and combined conditions:

- Requests run simultaneously by a number of users (expressed as threads). You can retest using a variety of scenarios. This feature enables you to determine in advance the system ability to grow (that is, its scalability).

- Requests executed at varying intervals. This feature enables you to determine in advance the ability of the system to adjust to increases in workload.

In addition to these basic tests, you can specify a number of advanced conditions to refine the diagnostic process. For example, stress testing generally provides information about the retrieval performance of the Reporting Server going against one or more data sources (also called back end processing). If, however, you are working in a client environment like WebFOCUS, you may wish to test data retrieval performance beginning at a user browser, going through a Web server (front end processing), to the Reporting Server to the data source. You can request that the test be redirected to the Web server to track retrieval over the longer path. Then, by comparing back end test results with front end test results, you can more accurately diagnose the origin of a performance problem based on any other conditions you specify.

For a full list of the basic and advanced stress test conditions you can apply, see Parameters for Playback of HTI Script Files on page 609.
Recording User Actions Into a Script Using Run Stress

**How to:**
Run a Stress Test

**Example:**
Sample Stress Test Log
Sample Performance Reports

The server recording feature can record the exact sequence of user actions applied through a browser into a script. The script can then reproduce that sequence (play it back), simulating single or multiple users under varying conditions to produce execution statistics.

The Run Stress feature uses an existing procedure to produce the script. It also and changes the browser session to the Diagnostics Scalability Playback Start/Stop page for the script.

The files used by playback and the recorded sequences are known as HTI scripts and are saved in the scalability directory. The scripts can be used along with server traces for problem diagnostics, analysis and testing.

One may go back to the Diagnostics Scalability Playback page at any time off the main menu and create a new script by recording a session activity (top menu bar) or an edit session (top menu bar) plus edit or re-run an existing script.

**Procedure: How to Run a Stress Test**

You can run a stress test on a procedure from the Web Console.

1. From the Web Console menu bar, click *Applications*, or from the Data Management Console, expand the Server node folder.
   On the Web Console, the Applications page opens.
2. Expand an application folder.
3. Right-click a procedure, select *Run Advanced*, and then *Run Stress*. 
The Playback of HTI Script Files page opens.

4. Enter basic test conditions: Number of Threads, Interval Parameter, and a Test Description. Click Advanced if you wish to specify additional conditions.

5. Click Start. Results are displayed in a separate window. For an illustration, see Sample Stress Test Log on page 410.

   The script is listed under the tested procedure in the directory C:\ibi\scale.

6. Open the Performance Reports folder on the Playback navigation pane and choose:
   - Basic Report
   - Extended Report
   - Custom Report
If you choose *Custom Report*, the Custom Performance Report Options page opens.

Select the options you want to see and click *Generate Report*. 
**Example: Sample Stress Test Log**

---- Started at 12:57:32 ----
Received: thread=01 request=0001; timing: resp=0.062 sec, transf=0.000 sec, start=06/29/2005 12:57:32
---- Finished at 12:57:32 ----

Total Execution Time: 0.094 sec
Total Number of Requests: 1
Total Number of Threads: 1
Interval Parameters: 500,-1,-1
Average Server Response: 0.062 sec
Average Data Transfer Time: 0.000 sec
Average Request Processing Time: 0.062 sec
Standard Processing Deviation: 0.000 sec
Minimum Processing Time: 0.062 sec
Maximum Processing Time: 0.062 sec
Average DBMS Time: 3.559 sec
terminating main thread

**Example: Sample Performance Reports**

**Basic Report**

### Basic Test Statistics

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Begin Time</th>
<th>End Time</th>
<th>Arrival Rate per minute</th>
<th>Average Response Time (sec)</th>
<th>Average DBMS Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cargraph</td>
<td>2010/10/29 12:36:44</td>
<td>2010/10/29 12:37:04</td>
<td>120.000</td>
<td>9.813</td>
<td>0.000</td>
</tr>
<tr>
<td>dmstarterm</td>
<td>2010/10/29 12:33:33</td>
<td>2010/10/29 12:34:53</td>
<td>120.000</td>
<td>0.306</td>
<td>0.000</td>
</tr>
<tr>
<td>a_aad_bms_time</td>
<td>2010/10/29 11:53:52</td>
<td>2010/10/29 11:54:06</td>
<td>120.000</td>
<td>10.437</td>
<td>3.599</td>
</tr>
<tr>
<td>a_aad_bms_time</td>
<td>2010/10/27 16:33:01</td>
<td>2010/10/27 16:33:02</td>
<td>120.000</td>
<td>.344</td>
<td>.104</td>
</tr>
</tbody>
</table>

**Extended Report**

### Extended Test Statistics

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Test Description</th>
<th>Begin Time</th>
<th>End Time</th>
<th>Total Time</th>
<th>Arrival Rate per minute</th>
<th>Total Number of Requests</th>
<th>Total Number of Threads</th>
<th>Interval Parameters</th>
<th>Average Response Time (sec)</th>
<th>Average Request Processing Time (sec)</th>
<th>Average Processing Deviation (sec)</th>
<th>Minimum Processing Time (sec)</th>
<th>Maximum Processing Time (sec)</th>
<th>Average DBMS Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cargraph</td>
<td></td>
<td>2010/10/29 12:36:44</td>
<td>2010/10/29 12:37:04</td>
<td>19.000</td>
<td>120.000</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>.918</td>
<td>.000</td>
<td>.000</td>
<td>18.75</td>
<td>.000</td>
<td></td>
</tr>
<tr>
<td>dmstarterm</td>
<td></td>
<td>2010/10/29 12:33:33</td>
<td>2010/10/29 12:34:53</td>
<td>19.000</td>
<td>120.000</td>
<td>59</td>
<td>1</td>
<td>1</td>
<td>.918</td>
<td>.000</td>
<td>.000</td>
<td>18.75</td>
<td>.000</td>
<td></td>
</tr>
<tr>
<td>a_aad_bms_time</td>
<td></td>
<td>2010/10/29 11:53:52</td>
<td>2010/10/29 11:54:06</td>
<td>19.000</td>
<td>120.000</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>.918</td>
<td>.000</td>
<td>.000</td>
<td>18.75</td>
<td>.000</td>
<td></td>
</tr>
<tr>
<td>a_aad_bms_time</td>
<td></td>
<td>2010/10/27 16:33:01</td>
<td>2010/10/27 16:33:02</td>
<td>19.000</td>
<td>120.000</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>.918</td>
<td>.000</td>
<td>.000</td>
<td>18.75</td>
<td>.000</td>
<td></td>
</tr>
</tbody>
</table>
Custom Report

Running Impact Analysis Reports

**How to:**

- Run an Impact Analysis Report for an Application
- Run an Impact Analysis Report for an Adapter Connection
- Run an Impact Analysis Report for a Procedure
- Run an Impact Analysis Report for a Synonym

An Impact Analysis report enables you to determine the impact of changing a synonym, synonym column, procedure, or connection. The report shows you how and where the object is used. For example, running the report on a procedure tells you from which applications and procedures the original procedure is run. Running the report on a synonym tells you which tables or other data sources the synonym describes, and in which procedures it is referenced. This enables you to determine how changing the synonym, column, procedure, or connection could affect the rest of your application.

You can run Impact Analysis reports from the Web Console and from the Data Management Console. Reports also provide drill-down links so that you can, for example, run an Impact Analysis report on a synonym, see a procedure listed in the report, and click the procedure to edit it.

In addition to the reports you can run for an individual procedure, synonym, connection, or column, you can select the following standard Impact Analysis reports for an Application folder in the Web Console or the Data Management Console:

- The **Synonyms by Procedure** report lists your procedures and the synonyms that they use, sorted by procedure. The report includes whether the synonym is used as a source or a target, the adapter type, the table name and description, load type and prior to load options, and directory locations.
The **Procedures by Synonym** report lists your synonyms and the procedures they are used in, sorted by synonym. The report includes whether the synonym is used as a source or a target, the adapter type, the table name and description, load type and prior to load options, and directory locations.

The **Columns by Procedure** report lists the columns used in your procedures and their synonyms sorted by data flow. The report includes how the column is used, as well as directory locations.

The **Procedures by Column** report lists your procedures and their synonyms sorted by column. The report includes how the column is used, as well as directory locations.

The **Synonyms by Procedure - Enterprise** report includes the same information as a Synonyms by Procedure report, but for the server and all its subservers in a hub/subserver environment. This report does not appear if the server you are reporting on does not have any remote servers configured.

The **Procedures by Synonym - Enterprise** report includes the same information as a Procedure by Synonym report, but for the server and all its subservers in a hub/subserver environment. This report does not appear if the server you are reporting on does not have any remote server configured.

**Note:** Enterprise reports appear only if you have subservers.

**Procedure:** **How to Run an Impact Analysis Report for an Application**

You can run an Impact Analysis Report from the Web Console or the DMC.

1. From the Web Console menu bar, click **Applications**, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Applications page opens.

2. Right-click an application folder, select **Impact Analysis**, and then either:

   - **Synonyms by Procedure**
   - **Procedures by Synonym**
   - **Columns by Procedure**
   - **Procedures by Column**
Flow Report

The Impact Analysis report opens in the right pane.

**Procedure:**  **How to Run an Impact Analysis Report for an Adapter Connection**

You can run an Impact Analysis Report from the Web Console or the DMC.

1. From the Web Console menu bar, click *Adapters*, or from the Data Management Console, expand the Server node folder.

   On the Web Console, the Adapters page opens.

2. Expand an adapter folder.

3. Right-click a connection, and select *Impact Analysis*.

A report similar to the following image opens in the right pane. The report provides links to the files and lists such information as the connection names, type of file, usage, and application name.
How to Run an Impact Analysis Report for a Procedure

You can run an Impact Analysis Report from the Web Console or the DMC.

1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.
   
   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a procedure, and select Impact Analysis.
   
   The Impact Analysis report opens in the right pane.

How to Run an Impact Analysis Report for a Synonym

You can run an Impact Analysis Report from the Web Console or the DMC.

1. From the Web Console menu bar, click Applications, or from the Data Management Console, expand the Server node folder.
   
   On the Web Console, the Applications page opens.

2. Expand an application folder.

3. Right-click a synonym, and select Impact Analysis.
The Impact Analysis report opens in the right pane.
Server Workspace Manager

The Web Console provides a variety of tools and techniques that you can use to run and monitor your server. The Workspace Manager is the controlling process that controls and oversees the various processes of the server.

Topics:
- Configuring Workspace Manager
- Workspace Configuration Settings
- Editing Configuration Files
- Configuring Java Services
- Cluster Manager
- Monitoring Server Activity
The Workspace Manager is the component of the Reporting Server that is responsible for managing all server administrative tasks. These tasks, generally performed by Server Administrators, include monitoring server activity, configuring and adjusting the server configuration profile, adding users, enabling and creating services, defining deferred execution characteristics, and enabling and disabling email alerts.

The Server Administrator responsible for the installation, configuration, security, and maintenance of the server uses the Web Console to manage and configure the Workspace Manager in order to keep the server available to clients and running at peak efficiency. To use the Web Console, open Internet Explorer and navigate to the HTTP port on the host machine where the Server is running, as in http://host:http_port.

Your Server must be running in order to use Web Console to access the Workspace Manager.

**Tip:** This chapter references a number of Workspace related keywords. Within the help system, you can access detailed information about these keywords by clicking the keyword links in this document. You can also click the question mark (?) icon next to parameters on the Workspace configuration panes.

### Workspace Manager Configuration Privileges

Access to the administrative features of the Web Console can be restricted by defining a list of users with admin privileges and storing the list in a release-independent file called admin.cfg. This file is located, by default, in .../ibi/profiles.

The list of users and user roles defined in admin.cfg defines a list of administrators and users that can be used for authorization and/or authentication according to established security. Administrators are responsible for installing, configuring, and maintaining the Server with varying degrees of responsibility, depending on their administration levels (SRV, APP, OPR). At least one administrator must be defined in the list, although most sites identify other persons to act as backups.
For example, a Server Administrator (SRV) can perform all the administrative tasks available through Web Console operations. If more than one Server Administrator is defined, the first valid member on the list is used to impersonate FOCUS Database Server (FDS) and other special services. An Application Administrator (APP) is limited to the administrative tasks that do not require changing configuration or restarting the server. Both Server Administrators and Application Administrators can edit user profiles in the user.prf file. However, Server Administrators can edit all user.prf files, while Application Administrators can only edit their own profiles.

Any IDs (beyond the original ID used to configure the server) that are used for server or application administration require read/write privileges to the respective locations that the IDs are expected to manage. To assign these privileges, you must establish group rights for the locations at the operating system level. To view and run Resource Governor procedures, for example, IDs must be at least at the Application Administrator level.

**Quiesce Server**

**How to:**

Quiesce the Server and Set a Custom Message

A server administrator can change the server state to quiesce to disable new connections. Existing connections are not terminated, but will finish processing and disconnect, while new connections will be rejected. A server administrator can still connect to the server. This is done to gradually move the server to the state where maintenance can be performed safely or to collect diagnostic information. It can also be used as the first step before stopping the server without terminating any connections.

A server administrator can enter a custom message that will be displayed for a new user connection when the server is in Quiesce mode.
 Procedure: How to Quiesce the Server and Set a Custom Message

Only a server administrator can change the server state. To Quiesce the server, and define a custom message that will be delivered from the server:

1. From the menu bar, click the Console icon, and select Quiesce.

   ![Console Icon]

   The Quiesce Connections page opens.

2. If you want to deliver a message for new user connections, enter it in the quiesce_msg field.

   ![Quiesce Connections]

3. Click Submit.

   You will be asked if you want to disable new connections.
4. Click OK.

**Note:** To restore the server to normal operation, click the Console icon, and select *Enable New Connections*.

### Configuring an Agent Service

**How to:**
View or Edit Data Service Properties

**Reference:**
Data Service Properties

A server configuration requires at least one agent service with the name DEFAULT, defined by a *SERVICE* block. An agent service is an entity used to define the parameters for a group of data access agents, so that a configuration can manage different groups of data access agents for different purposes. Each data access agent runs for a specific Data Service, and each service may have different values for the settings defined on the services configuration panes. These settings include:

- The maximum number of data access agents and the number of agents prestarted at server startup for a service, as defined by *maximum* and *number ready*.

- The lifetime of the agents of a server, which can be limited through *idle agent limit*, *CPU time limit*, and/or *memory limit*.

- Incoming connections for which there is no available data access agent. These can be put in a queue for the service (configured using *maximum_q* and *queue limit*), and after they are connected, their idle time can be limited using *idle session limit*.

- The *deployment mode* of a service, which defines how data access agents are assigned to connections.
**Procedure:**  **How to View or Edit Data Service Properties**

The service agents are available from the *Workspace* folder.

1. From the menu bar, select *Workspace*.
2. In the navigation pane, open the *Data Services* folder.
3. In the navigation pane, right-click a Data Service and select *Properties*.

The properties page for the particular Data Service opens.

**Reference:**  **Data Service Properties**

The server includes four predefined Data Services:

- DEFAULT
- WC_DEFAULT
- SCHED_DEFAULT
- DFM_DEFAULT
The following image shows the parameters for the DEFAULT service.

![Data Service DEFAULT](image)

**Note:** Changing values with an asterisk (*) requires restarting the server.

Data Services have the following parameters:

- **service**
  - Defines the name of the service.

- **maximum**
  - Defines the maximum number of data access agents that the Workspace Manager will allow to run simultaneously for a specific service.
Configuring Workspace Manager

number_ready

Defines the number of data access agents that the Workspace Manager will create at startup for a specific service.

deployment*

Controls resource sharing between users who are connecting to the same agent in this service. The values are:

- **private deployment.** All users are completely independent of each other and have their unique operating system rights, database connections, and FOCUS language settings.

- **connection_pooling.** All users are partially independent by having their own unique FOCUS language settings but sharing operating system rights and database connections.

Queuing*

Controls whether queuing is on or off.

maximum_q

Defines the maximum number of connections that could be queued for a specific service. Only available when queuing is set to on. Set to -1 for an unlimited queue size.

queue_limit

Defines the amount of time in seconds a queued connection will wait before being timed out if an agent is still unavailable. A setting of -1 mean unlimited.

idle_session_limit

Defines the time limit in seconds that connected agents will wait for client input before they are disconnected. A setting of -1 mean unlimited.

idle_agent_limit

Defines the time limit in seconds that disconnected agents in excess of number_ready can stay idle before they are killed. A setting of -1 mean unlimited.

profile*

Specifies a focexec file that will be executed during agent startup.

cpu_limit

Defines the amount of CPU time in seconds an agent is allowed to use before being killed by the Workspace Manager.
memory_limit

Defines the maximum amount of memory in kilobytes an agent is allowed to use. If an agent process grows above this limit, it will be killed by the Workspace Manager.

disk_limit

Defines the maximum amount of disk space in kilobytes an agent is allowed to use. This would add sizes of all files in agent edatemp directory, such as FOCSORT, HOLD files and other temporary files created by requests. If an agent process grows above this limit, it will be killed by the Workspace Manager.

connection_limit

Defines the time limit in seconds allowed for connection. When it is exceeded, the connection will be terminated, and the agent serving this connection will be stopped.

max_connections_per_user*

Restricts the number of concurrent connections for the same userid for a specific service. When a user exceeds the maximum number allowed, additional connections requested by that user are rejected, and the server displays the message

Connection refused due to the max_connections_per_user (n) being exceeded

where \( n \) is the number of allowed connections.

You have the option to queue user connections that are refused by the server, using the queue_max_user_conns property on the Data Service Properties page. That option is available only if the Queuing property for the Data Service is On.

queue_max_user_conns

Enables queuing of concurrent connections for the same userid for a specific service in excess of max_connections_per_user. This setting allows new connections that would otherwise be rejected to be queued for later processing. Only available when queuing is set to on.

agent_refresh

Defines the maximum number of new connections which can be accepted during the life of each agent process. Beyond this limit, additional new connections will be assigned to a fresh agent. Agent processes which have reached the limit will be terminated when the last accepted session disconnects.
sched_priority

Defines the scheduling priority of each agent process running under the specified service entry. The scheduling priority of a process defines how the operating system scheduler treats the process after it gains control of the CPU, and should be set according to the relative importance of the work being done by the service. Values range from -20 (highest priority) to 20 (lowest priority).

Configuring Deployment Modes

**How to:**
Set the Server Deployment Parameter in a Server Profile

The *deployment mode* of a service defines how data access agents are assigned to connections:

- In private deployment, a dedicated application agent is assigned for each connection request. Private deployment retains the behavior of all prior server releases. At connect time, global, as well as user and service level profiles, are executed. At disconnect time, all temporary files are removed and database connections are closed. The privileges of each application agent depend on the security mode of the server.

  With security set to a value other than OFF, authentication is processed for every client logging on to the server. With security OFF, user identification and authentication are not required. The effective user ID becomes the connecting user for the duration of the session.

- In connection_pooled deployment, the global profile and service profiles are executed when an agent is started, and pooled user profiles are executed on each connection. The WebFOCUS context is cleared once the session is established for a new connection, and then the pooled user profile is executed.

  With security set to a value other than OFF, all users have the same rights because the effective pooled user is unique, regardless of the connecting user.

Connection pooled deployment provides significant performance advantages and is recommended when a large number of users share the same operating system and DBMS credentials. It cannot be used when each connecting user has specific operating system and DBMS rights, nor can it be used for the service DEFAULT with the server security mode set to DBMS because, in this situation, the profile is disabled for connection authentication.
**Procedure:** How to Set the Server Deployment Parameter in a Server Profile

To set the server configuration parameter deployment:

1. From the menu bar, select *Workspace*.

2. In the navigation pane, right-click the *Data Services* folder, and select *New*.

   The New Data Service page opens.

   **Tip:** For an existing service (for example, DEFAULT, WC_DEFAULT, DMC_DEFAULT, DEFAULT_CPOOL), right-click the service and choose *Properties* from the menu to open the Services pane.

3. In the deployment field, choose *private* or *connection_pooling*.

   - With private deployment, all profiles are executed on connection. On disconnect, all DBMS connections are dropped. This is the default value.

     With security set to a value other than OFF, the effective user ID is switched to the connecting user for the duration of the connection.

     Skip to step 6.

   - With connection-pooled deployment, the global profile and service profiles are executed when an agent is started, and pooled user profiles are executed on each connection. The WebFOCUS context is cleared once the session is established for a new connection, and then the pooled user profile is executed.

     When you select this option, *pooled_user* and *pooled_password* are displayed.

     With security set to a value other than OFF, all users have the same rights because the effective user is unique (configured using pooled_user and pooled_password) regardless of the connecting user.

     Continue with steps 4 and 5.

4. Select the *pooled user* from the drop-down list. (This list is populated from the admin.cfg file described in *Workspace Manager Configuration Privileges* on page 418.)

   This service level keyword is required for connection_pooling deployment with security mode OPSYS. It defines the user ID under which all agents will run. The DBMS user IDs are determined by the connection setting type.

5. Enter the corresponding *password*. Note that pooled password is only required for connection_pooling deployment on Windows operating systems.

6. Click the *Save* button.
Multiple Cluster Manager Configurations

Advanced parameters have been added for multiple cluster nodes. The parameters include:

- **START_STOP_THRESHOLD.** Defines the number of polls. Cluster Manager will start or stop remote reserved servers if query response time is continuously above or below MAX_RSP_TIME for the last START_STOP_THRESHOLD polls.

- **MAX_RSP_TIME.** Defines the maximum query response time that users expect. If the value is greater than zero, Cluster Manager will attempt to achieve this limit by starting reserved servers or adjusting the configuration of remote servers if AUTO_CONFIG is on.

- **DISPATCH_METHOD.** Defines how Cluster Manager dispatches user queries to remote servers.

These parameters work on the cluster node level and override the values defined in the CLM node.

Workspace Configuration Settings

You can set a variety of general parameters from the Workspace folder in the navigation pane. The parameters are available from a right-click menu, organized under the following categories:
E-mail SMTP Server Settings.

Event Routing.

National Language Support Settings.

Login Message.

Web Console Appearance.

Settings

Profile Settings.

Core Engine Settings.

Core System Variables.

Core Engine Global Variables

Application Settings. For more information, see Nested Application Directories on page 192 and Home Application Directories for Users on page 195.

Miscellaneous Settings.

License Settings.

Migrate Settings.

These settings are saved in the appropriate configuration files.

Tip: If you prefer, you can edit these parameters directly in the associated configuration files. To do so, select Workspace from the menu bar. In the navigation pane, expand the Configuration Files folder, and choose the option that opens the file you wish to edit in a text editor. For details, see Editing Configuration Files on page 473.

E-mail SMTP Server Settings

Reference:

E-mail SMTP Server Settings

You can specify an IP address for the email server and a sender address. If the server is secured, you can specify the credentials for connecting to the server. You can also test your email connection from the E-mail Settings pane.
Reference: E-mail SMTP Server Settings

To access these settings, select Workspace from the menu bar. Click the E-mail SMTP Server icon on the ribbon, or right-click the Workspace folder in the navigation pane, and select E-mail SMTP Server.

The E-Mail SMTP Server page opens, as shown in the following image.

E-Mail SMTP Server

Note: If an antivirus program is running on this computer, please make sure that the sending email.

smtp_host
port 25
smtp_user
smtp_password
sender_email
server_admin_email

Place each email address (id@domain.com), a user ID (myid) or a procedure name (%myfex) on a new line with no separators

The following settings are saved in the odin.cfg file:

smtp_host

Indicates the IP address of the SMTP email server using the notation that is supported for your IP version (for example, for IPv4, use base 256 standard dot notation. When IPv6 is supported on a platform, and enabled, you can use either 256 standard dot notation or IPv6 notation.)

port

Indicates the TCP port number that a client is connecting to. The default value is 25.
smtp_user
Is the user ID to authorize access to the SMTP server.

smtp_password
Is the password for the smtp_user.

sender_email
Is the sender email address (the address that appears in the From field in emails).

server_admin_email
Is a list that can consist of email addresses, user IDs and procedure names (for example, %myfex.fex), each on a separate line, with no delimiters.

**Note:** If email send operations fail, verify that the smtp host is active and/or that a virus scanner is not blocking edachkup.

When you have completed your entries, optionally click the Send Test E-mail button to test your connection, then click Save.

**Event Routing**

**In this section:**
- Setting Workspace Log Properties for Event Routing
  - EVENT_TEXT and EVENT_ID
  - How to:
    - Customize an Event Routing

Event Routing allows you to launch procedures or send email based on different server events (agent or listener crashes, server configuration errors, disk space limitations, and others). All events are classified by type as information, warning, or error. These can be pre-defined or custom-defined events.

The Customize Event Routing page shows the Default and Customized Event Routing.
The Default routings are shown in the following image.

<table>
<thead>
<tr>
<th>Type</th>
<th>Filter</th>
<th>Description</th>
<th>EDAPRINT</th>
<th>Procedure</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>All Information</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>All Warnings</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>All Errors</td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13023 Server</td>
<td>successfully started</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13093 User</td>
<td>password has been changed</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13120 Server</td>
<td>rejected not to accept any new connections</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13121 Server</td>
<td>is requested to accept all connections</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13164 Listener</td>
<td>is enabled</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13165 Listener</td>
<td>is disabled</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13169 Data service</td>
<td>agent has been started</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>4276 DBCTL interface</td>
<td>has been initialized</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>4288 DBCTL interface</td>
<td>is stopped</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>13088 Connection</td>
<td>rejected because userid is invalid</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>13089 Connection</td>
<td>rejected because password is invalid</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>13090 Failed to</td>
<td>change user password</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>13092 Connection</td>
<td>rejected because account is expired</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>13173 Number of</td>
<td>data service agents has reached the maximum</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>40001 No more</td>
<td>available agents for required service (maximum</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>40002 Not enough</td>
<td>disk space in dfin_dir directory to process</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>40003 File listener</td>
<td>warning</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>40004 CLM failed to</td>
<td>query remote server</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>40005 Agent</td>
<td>exceeded CPU limit</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>40006 Agent</td>
<td>exceeded memory limit</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>40007 Agent</td>
<td>exceeded disk space limit</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>40008 Agent</td>
<td>exceeded connection time limit</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>36048 Resource</td>
<td>Governor canceled a request</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>36097 Resource</td>
<td>Management logging did not archive all data</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>36037 Resource</td>
<td>Management has unarchived logs</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>36029 Resource</td>
<td>Management repository is not valid for this</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>60001 Listener,</td>
<td>special service or agent crashed</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>60002 Agent</td>
<td>aborted</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>60003 ETLOG/ETLSTATS</td>
<td>write error</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>13171 Unable to</td>
<td>start server</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>13015 Configuration</td>
<td>error</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error</td>
<td>36154 Agent</td>
<td>failed to log Resource Management session data</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Customized*
Customized routings are shown in the following image.

![Customize Event Routing](image)

<table>
<thead>
<tr>
<th>Type</th>
<th>Filter</th>
<th>Description</th>
<th>EDAPRINT</th>
<th>Procedure</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customized</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13023</td>
<td>Server successfully started</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Information</td>
<td>13164</td>
<td>A listener is enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13169</td>
<td>A data service agent has been started</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>40001</td>
<td>No more available agents for required service</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Warning</td>
<td>40002</td>
<td>Not enough disk space in dlm_dir directory to process</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Warning</td>
<td>40005</td>
<td>Agent exceeded CPU limit</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Warning</td>
<td>40006</td>
<td>Agent exceeded memory limit</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Warning</td>
<td>40007</td>
<td>Agent exceeded disk space limit</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Error</td>
<td>60001</td>
<td>Listener, special service or agent crashed</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Error</td>
<td>60002</td>
<td>Agent aborted</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

**Procedure:** How to Customize an Event Routing

By customizing event routing, you can launch a procedure or send email based on server events.

1. From the menu bar, select **Workspace**.
2. From the ribbon, click the **Event Routing** icon, or right-click the **Workspace** folder in the navigation pane, and select **Event Routing**.

   The Customize Event Routing page opens.

3. Click **Customize New Event Routing**.
The Customize New Event Routing page opens.

4. From the Type drop-down menu, select a message type. The choices are Error, Information, Warning, and Any.
5. Enter a criteria in the Filter field or select a predefined one from the drop-down menu.

6. From the EDAPRINT drop-down menu, select Yes if you want to write the selected event message to the server log.

In z/OS, the selected server messages can be also written to the z/OS system log by selecting Yes from the JESLOG drop-down menu, as shown in the following image.
7. Optionally, enter an email address to send an email when the event occurs.
8. Optionally, enter a procedure to execute in the Procedure field, including the application name, for example, utility/movefiles.
9. Click Add.
   The event is added to the Customize Event Routing Page.

```
Event Routing

An event routing has been modified, but is not saved.

Save and Restart Server  Clear All Changes  Customize New Event Routing
```

<table>
<thead>
<tr>
<th>Type</th>
<th>Filter</th>
<th>Description</th>
<th>EDAPRINT</th>
<th>Procedure</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customized</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>13023</td>
<td>Server successfully started</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

10. Click Save and Restart Server.

**Setting Workspace Log Properties for Event Routing**

**How to:**
Set Workspace Log Properties for Event Routing

Workspace Log properties allow you to specify a suppression interval for email notifications from event routing, and to include a number of lines from the edaprint log file in the email body. The edaprint log file provides information about the events occurring on the server before a triggered event.

**Procedure:** How to Set Workspace Log Properties for Event Routing

The Workspace Log Properties page controls both event routing email and the edaprint log. For information on the edaprint log, see *How to Set Workspace Log Properties to Control the Edaprint Log* on page 576.

1. From the menu bar, select Workspace.
2. Open the Logs and Traces folder.

3. Right-click Workspace Logs and select Properties.

   The Workspace Logs Properties page opens, as shown in the following image.

![Workspace Logs Properties](image)

4. Enter or select values for the Event Email parameters.

   The Event Email parameters are:

   - **email_suppress_interval**
     
     Suppresses duplicate email notifications if the same event occurs again during this time interval (in seconds). Zero disabled suppression. The default value is 1800 (30 minutes).

   - **logging_email_edaprint**
     
     Defines the maximum number of server messages from edaprint.log included in the email. The default value is 20.

5. Click Save and Restart Server.
**EVENT_TEXT and EVENT_ID**

When a procedure is triggered by an event, the ID of the routing event and the text of the event message are automatically available to the procedure as the EVENT_ID and EVENT_TEXT parameters, respectively. The EVENT_TEXT parameter needs to be decrypted using the following user subroutine:

```plaintext
B64DECODE('XXXXXXXXXX', 'Ann');
```

---

**National Language Support Settings**

**In this section:**
- Times New Roman Font Support for Arabic PDF and PostScript Formats
- Tahoma Font Support for Thai PDF and PostScript Formats

**How to:**
- Add a Dynamic Language Switch to the Web Console Menu Bar
- Create a Localized Version of the Web Console Manually

**Example:**
- Localizing the Web Console Into Finnish

**Reference:**
- NLS Settings
- Language and Default Code Pages for Windows and UNIX
- Language and Default Code Pages for IBM i and z/OS

The Web Console provides the parameters that are required for configuring the Server for National Language Support (NLS).

**Times New Roman Font Support for Arabic PDF and PostScript Formats**

Users that want to output Arabic characters in PDF or PostScript formats can now select the Times New Roman font.

**Tahoma Font Support for Thai PDF and PostScript Formats**

Users that want to output Thai characters in PDF or PostScript formats can now select the Tahoma font.
Reference: NLS Settings

To access these settings, select Workspace from the menu bar. From the ribbon, click the NLS icon, or right-click the Workspace folder in the navigation pane, and select NLS.

The following NLS settings are saved in the nlsconfig.err file:

**CODE_PAGE**

Is the code page of the data sources accessed by the server.

Select a code page from the drop-down list of supported code pages, including Unicode.

The default value is 1252 for Windows and UNIX, and 37 for IBM i (formerly known as i5/OS) and z/OS.

The current value of CODE_PAGE is available to applications as the &FOCCODEPAGE variable.

**Locale attributes**

**LANG**

Controls the default value of the code page, and the language of server error messages if available in translation.

Choose a language name or abbreviation from the drop-down list.
The default value is AMENGLISH (American English) on all platforms.

An asterisk to the right of a language, for example, French*, means that the server is localized for that language. Translated server error messages (for example, FOCnnn through FOCnnnnn) are available and the Web Console is fully displayed in that language once you configure and restart the server. For related information, see *How to Add a Dynamic Language Switch to the Web Console Menu Bar* on page 442.

If you choose a language without an asterisk, the server messages and console appear in English. If you would like the messages and console to appear in a language for which the server has not been localized, you can provide translation yourself. To localize the console, translate the file wceng.lng and rename it to wcXXX.lng where 'XXX' is the three-letter language code for the server. For error messages, translate all or any relevant *.err files and append the same three-letter language code to it. All files are located in the \home\nls folder. For related information, see *How to Create a Localized Version of the Web Console Manually* on page 443.

The current value of LANG is available to applications as the &FOCLANGCODE variable. However, it will be blank if it is not configured.

**CURRENCY**

Enter a one-byte character or hexadecimal value that identifies a currency symbol.

Examples of one-byte characters are:

- € for euro
- ¥ for yen
- $ for U.S. dollar
- £ for British pound sterling

You can use any other single character to designate the currency symbol.

Examples of a hexadecimal value on code page 137 are:

- 0x80 for euro
- 0x24 for dollar sign

**DATEOUTPUT**

Selecting *Localized* from the drop-down menu will provide dates in a localized format.

**COLLATION**

Establishes a binary or case-insensitive collation sequence. The values are:

- **CODEPAGE.** Bases the collation sequence on the code page in effect.
- **BINARY.** Bases the collation sequence on binary values.
SRV_CS. Bases the collation sequence on the LANGUAGE setting, and is case-sensitive.

SRV_CI. Bases collation sequence on the LANGUAGE setting, and is case-insensitive.

When code page files are not modified, CODEPAGE is the same as BINARY, except for Danish, Finnish, German, Norwegian, or Swedish in EBCDIC environment.

The SET COLLATION command has the same effect, and overrides this default setting in NLS configuration.

Optional customization

Customize code page conversion tables

Select this check box to display a list of code pages and descriptions for the possible data sources accessed by the server or the client code page.

Several code pages are always selected by default and cannot be deselected. These are:

- 37 –IBM MF United States
- 137 –U.S. English/Western Europe (Latin 1)
- 437 –U.S. English
- 1047 –IBM MF Open Systems (Latin 1)
- 1252 –Windows Latin; 65001 –Unicode (UTF-8)
- 65001 Unicode (UTF-8)
- 65002 Unicode (UTF-EBCDIC)

Other code pages may also be selected by default, depending on the LANG attribute chosen.

The NLS Configuration Wizard creates conversion tables for these code pages to make them available for subsequent conversion.

Select any additional code pages for which you want tables to be created. For example, if you want to designate a particular code page to be generated in synonyms for flat (fixed) files or VSAM files, you must already have created a code page conversion table using the Customize code page conversion table option during NLS configuration.

Recreate FOCUS system files

Check this box if you wish to load FOCUS internal files in the server code page (as defined in the CODE_PAGE field).

This is recommended if the compatibility of the new and prior code pages is unknown.
Recreate FOCUS sample files

Check this box if you wish to load the sample files (which are delivered with your software) in the server code page (as defined in the CODE_PAGE field).

TSGU command

TSGU is a utility program to configure NLS settings. It is usually not required, but in the following cases it must be executed manually.

- **To create PDFXTBL.** When TYPE 1 fonts should be included in PDF format file, the TYPE 1 font transcoding table must be generated using the following syntax:
  
  \[
  \text{PDFX \{font-name\}}
  \]

- **To create PDFYTBL.** When Unicode fonts should be used in PDF format file, the special font information tables (PDFYTBL) must be generated using the following syntax:
  
  \[
  \text{KTBL \{pdfy-name\}}
  \]

Complete the configuration, then click **Save/Rebuild NLS Files and Restart Server**. The server creates the necessary transcoding, sorting, and monocasing tables for the selected code page.

**Procedure:** How to Add a Dynamic Language Switch to the Web Console Menu Bar

When you configure the server for NLS:

1. Choose a language with an asterisk (*) from the LANG drop-down list. The asterisk indicates that the localized version of the Web Console is available for that language.

2. Click **Save/Rebuild NLS Files and Restart Server**.

3. When the server restarts, the Web Console is displayed in the selected language.

   If you selected a Western European language when configuring the code page, the associated group of Western European languages, as well as English, are available on a menu to the left of the Help option.

4. To toggle among these languages, simply select the one you want from this menu.

In this example, Spanish has been chosen from the menu so the Web Console, as well as any translated error messages, are displayed in the selected language.
Procedure: How to Create a Localized Version of the Web Console Manually

Follow this procedure to localize a language that does not have an asterisk next to its name in the LANG drop-down list. This will enable users to see both the Web Console and the Data Management Console in the localized language.

When adding a localized language, the following files must be created for each language. These files are located in the EDAHOME NLS directory (for example, c:\ibi\srv77\home\nls). Each file contains the list of strings that are used in specific product areas.

<table>
<thead>
<tr>
<th>Area</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Console</td>
<td>wc***.lng</td>
</tr>
<tr>
<td>Synonym Editor</td>
<td>nt***.lng</td>
</tr>
<tr>
<td>Data Management Console</td>
<td>wc***.lng and dm***.lng</td>
</tr>
</tbody>
</table>

where:

***

Represents the 3-letter language abbreviation code for the new language you will be translating.

To localize the files listed in the chart, complete the following steps:

1. Identify the abbreviation code of the new language. To obtain a list of available codes, run the `? LANG SET` command as a procedure. The column LANGAB (Language Abbreviation) shows the 3-letter (*** ) codes.

2. Copy the three component files that have the English strings and rename them using the new language code. (The English versions of the files use the eng language abbreviation code.)

3. Translate the files with the new language abbreviation codes. To do so, open each component file in a Text Editor and proceed with the translation using the following guidelines:
   - Translate the strings on the right side of the equal sign (=). (The left side of the equal sign (=) contains the string numbers. Do not change these values.)
   - Some strings contain multiple variables (placeholders), such as %s/%s. Be especially careful to place these strings in context within your translation.

For example, in the string:

4040 = Create Synonym for %s %s
%s %s represents the table name for which you are creating a synonym. In some languages, the table name may be identified in the beginning or the middle of the sentence, therefore the variable must be placed accordingly.

4. Save the translated file in EDAHOME NLS directory (for example, c:\ibi\srv77\home\nls) using an encoding system that is compatible with the default code page of the language. To check the default code page, run the ? LANG SET command as a procedure. The column CODEPG (Code Page) shows the code page.

Once the new language files exist, you can add the localized language to the Dynamic Language Switch menu by including the ADDLANG parameter in the nlscfg.err file.

5. To edit the nlscfg.err file, select Workspace from the menu bar. In the navigation pane, open the Configuration Files and Miscellaneous folders.

6. Right-click NLS - nlscfg.err, and select Edit.

The nlscfg.err file opens in the text editor. Add the following line of code

```
ADDLANG=language_name
```

where:

- `language_name`

  Is the language abbreviation code (LANGAB) or language name (LANGNM) from the ? LANG SET table.

7. To test the new language, configure the WebFOCUS Reporting Server for NLS and select the language you just translated as the LANG=value.

8. Save and restart the Server. When the Server restarts, the localized language option will be available on the Dynamic Language Switch pull-down menu.

9. Choose the desired language and verify that all menus and options are translated and functioning.

Note: For your convenience, two reference charts that contain the output generated by the ? LANG SET command are included in this document. For details, see Language and Default Code Pages for Windows and UNIX on page 445 or Language and Default Code Pages for IBM i and z/OS on page 447.

Example: Localizing the Web Console Into Finnish

For this example, assume that the server is running on Windows and the NLS setting is CODE_PAGE=137 and LANG=AMENGLISH).

Follow these steps:
1. The wceng.lng file contains the original English strings for the Web Console. Copy and rename the file wcfin.lng.

2. Translate wcfin.lng into Finnish and save it as Latin1(ISO8859-1) in the EDAHOME NLS directory (for example, c:\ibi\srv77\home\nls).

3. From the menu bar select Workspace. In the navigation pane, open the Configuration Files and Miscellaneous folders.

4. Right-click NLS - nlscfg.err, and select Edit.

   The nlscfg.err file opens in the text editor. Add the following line of code:

   `ADDLANG=FINNISH`

5. Click the Save and Restart button for the changes to take effect.

6. To apply the Finnish translation, choose FINNISH from the dynamic language switch drop-down list on the Web Console menu bar.

Reference: Language and Default Code Pages for Windows and UNIX

This chart provides information generated by the ? LANG SET command from the Windows and UNIX platforms.

<table>
<thead>
<tr>
<th>Language Code</th>
<th>Language Name</th>
<th>Language Abbreviation</th>
<th>Language ID</th>
<th>Code Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>AMENGLISH</td>
<td>AME</td>
<td>en</td>
<td>1252</td>
</tr>
<tr>
<td>001</td>
<td>ENGLISH</td>
<td>ENG</td>
<td>en</td>
<td>1252</td>
</tr>
<tr>
<td>020</td>
<td>ARABIC</td>
<td>ARB</td>
<td>ar</td>
<td>1256</td>
</tr>
<tr>
<td>10351</td>
<td>B-PORTUGUESE</td>
<td>BRA</td>
<td>br</td>
<td>137</td>
</tr>
<tr>
<td>385</td>
<td>CROATIAN</td>
<td>HRV</td>
<td>hr</td>
<td>1250</td>
</tr>
<tr>
<td>420</td>
<td>CZECH</td>
<td>CZE</td>
<td>cs</td>
<td>1250</td>
</tr>
<tr>
<td>045</td>
<td>DANISH</td>
<td>DAN</td>
<td>da</td>
<td>137</td>
</tr>
<tr>
<td>031</td>
<td>DUTCH</td>
<td>DUT</td>
<td>nl</td>
<td>137</td>
</tr>
<tr>
<td>372</td>
<td>ESTONIAN</td>
<td>EST</td>
<td>et</td>
<td>923</td>
</tr>
<tr>
<td>358</td>
<td>FINNISH</td>
<td>FIN</td>
<td>fi</td>
<td>137</td>
</tr>
<tr>
<td>Language Code</td>
<td>Language Name</td>
<td>Language Abbreviation</td>
<td>Language ID</td>
<td>Code Page</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>033</td>
<td>FRENCH</td>
<td>FRE</td>
<td>fr</td>
<td>137</td>
</tr>
<tr>
<td>033</td>
<td>FRENCH</td>
<td>FRE</td>
<td>fc</td>
<td>137</td>
</tr>
<tr>
<td>049</td>
<td>GERMAN</td>
<td>GER</td>
<td>de</td>
<td>137</td>
</tr>
<tr>
<td>049</td>
<td>GERMAN</td>
<td>GER</td>
<td>at</td>
<td>137</td>
</tr>
<tr>
<td>030</td>
<td>GREEK</td>
<td>GRE</td>
<td>el</td>
<td>1253</td>
</tr>
<tr>
<td>972</td>
<td>HEBREW</td>
<td>HEB</td>
<td>iw</td>
<td>916</td>
</tr>
<tr>
<td>036</td>
<td>HUNGARIAN</td>
<td>HUN</td>
<td>hu</td>
<td>1250</td>
</tr>
<tr>
<td>039</td>
<td>ITALIAN</td>
<td>ITA</td>
<td>it</td>
<td>137</td>
</tr>
<tr>
<td>081</td>
<td>JAPANESE</td>
<td>JPN</td>
<td>ja</td>
<td>942</td>
</tr>
<tr>
<td>081</td>
<td>JAPANESE-EUC</td>
<td>JPE</td>
<td>je</td>
<td>10942</td>
</tr>
<tr>
<td>082</td>
<td>KOREAN</td>
<td>KOR</td>
<td>ko</td>
<td>949</td>
</tr>
<tr>
<td>371</td>
<td>LATVIAN</td>
<td>LVA</td>
<td>lv</td>
<td>1257</td>
</tr>
<tr>
<td>370</td>
<td>LITHUANIAN</td>
<td>LTU</td>
<td>lt</td>
<td>1257</td>
</tr>
<tr>
<td>047</td>
<td>NORWEGIAN</td>
<td>NOR</td>
<td>no</td>
<td>137</td>
</tr>
<tr>
<td>048</td>
<td>POLISH</td>
<td>POL</td>
<td>pl</td>
<td>1250</td>
</tr>
<tr>
<td>351</td>
<td>PORTUGUESE</td>
<td>POR</td>
<td>pt</td>
<td>137</td>
</tr>
<tr>
<td>040</td>
<td>ROMANIAN</td>
<td>ROM</td>
<td>ro</td>
<td>1250</td>
</tr>
<tr>
<td>007</td>
<td>RUSSIAN</td>
<td>RUS</td>
<td>ru</td>
<td>1251</td>
</tr>
<tr>
<td>085</td>
<td>S-CHINESE</td>
<td>PRC</td>
<td>zh</td>
<td>946</td>
</tr>
<tr>
<td>421</td>
<td>SLOVAK</td>
<td>SVK</td>
<td>sk</td>
<td>1250</td>
</tr>
<tr>
<td>034</td>
<td>SPANISH</td>
<td>SPA</td>
<td>es</td>
<td>137</td>
</tr>
<tr>
<td>046</td>
<td>SWEDISH</td>
<td>SWE</td>
<td>sv</td>
<td>137</td>
</tr>
</tbody>
</table>
### Reference: Language and Default Code Pages for IBM i and z/OS

This chart provides information generated by the `? LANG SET` command from the IBM i and z/OS platforms.

<table>
<thead>
<tr>
<th>Language Code</th>
<th>Language Name</th>
<th>Language Abbreviation</th>
<th>Language ID</th>
<th>Code Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>AMENGLISH</td>
<td>AME</td>
<td>en</td>
<td>37</td>
</tr>
<tr>
<td>001</td>
<td>ENGLISH</td>
<td>ENG</td>
<td>en</td>
<td>37</td>
</tr>
<tr>
<td>020</td>
<td>ARABIC</td>
<td>ARB</td>
<td>ar</td>
<td>420</td>
</tr>
<tr>
<td>10351</td>
<td>B-PORTUGUESE</td>
<td>BRA</td>
<td>br</td>
<td>37</td>
</tr>
<tr>
<td>420</td>
<td>CZECH</td>
<td>CZE</td>
<td>cz</td>
<td>870</td>
</tr>
<tr>
<td>045</td>
<td>DANISH</td>
<td>DAN</td>
<td>da</td>
<td>277</td>
</tr>
<tr>
<td>031</td>
<td>DUTCH</td>
<td>DUT</td>
<td>nl</td>
<td>37</td>
</tr>
<tr>
<td>372</td>
<td>ESTONIAN</td>
<td>EST</td>
<td>et</td>
<td>1112</td>
</tr>
<tr>
<td>358</td>
<td>FINNISH</td>
<td>FIN</td>
<td>fi</td>
<td>278</td>
</tr>
<tr>
<td>033</td>
<td>FRENCH</td>
<td>FRE</td>
<td>fr</td>
<td>297</td>
</tr>
<tr>
<td>033</td>
<td>FRENCH</td>
<td>FRE</td>
<td>fc</td>
<td>297</td>
</tr>
<tr>
<td>049</td>
<td>GERMAN</td>
<td>GER</td>
<td>de</td>
<td>273</td>
</tr>
</tbody>
</table>

Server Administration
<table>
<thead>
<tr>
<th>Language Code</th>
<th>Language Name</th>
<th>Language Abbreviation</th>
<th>Language ID</th>
<th>Code Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>049</td>
<td>GERMAN-500</td>
<td>GE5</td>
<td>at</td>
<td>500</td>
</tr>
<tr>
<td>030</td>
<td>GREEK</td>
<td>GRE</td>
<td>el</td>
<td>875</td>
</tr>
<tr>
<td>972</td>
<td>HEBREW</td>
<td>HEB</td>
<td>iw</td>
<td>424</td>
</tr>
<tr>
<td>036</td>
<td>HUNGARIAN</td>
<td>HUN</td>
<td>hu</td>
<td>870</td>
</tr>
<tr>
<td>039</td>
<td>ITALIAN</td>
<td>ITA</td>
<td>it</td>
<td>280</td>
</tr>
<tr>
<td>081</td>
<td>JAPANESE</td>
<td>JPN</td>
<td>ja</td>
<td>939</td>
</tr>
<tr>
<td>10081</td>
<td>JAPANESE-930</td>
<td>JPK</td>
<td>jk</td>
<td>930</td>
</tr>
<tr>
<td>082</td>
<td>KOREAN</td>
<td>KOR</td>
<td>ko</td>
<td>933</td>
</tr>
<tr>
<td>371</td>
<td>LATVIAN</td>
<td>LVA</td>
<td>lv</td>
<td>1112</td>
</tr>
<tr>
<td>370</td>
<td>LITHUANIAN</td>
<td>LTU</td>
<td>lt</td>
<td>1112</td>
</tr>
<tr>
<td>047</td>
<td>NORWEGIAN</td>
<td>NOR</td>
<td>no</td>
<td>277</td>
</tr>
<tr>
<td>048</td>
<td>POLISH</td>
<td>POL</td>
<td>pl</td>
<td>870</td>
</tr>
<tr>
<td>351</td>
<td>PORTUGUESE</td>
<td>POR</td>
<td>pt</td>
<td>37</td>
</tr>
<tr>
<td>040</td>
<td>ROMANIAN</td>
<td>ROM</td>
<td>ro</td>
<td>870</td>
</tr>
<tr>
<td>007</td>
<td>RUSSIAN</td>
<td>RUS</td>
<td>ru</td>
<td>1025</td>
</tr>
<tr>
<td>085</td>
<td>S-CHINESE</td>
<td>PRC</td>
<td>zh</td>
<td>935</td>
</tr>
<tr>
<td>042</td>
<td>SLOVAK</td>
<td>SVK</td>
<td>sk</td>
<td>870</td>
</tr>
<tr>
<td>034</td>
<td>SPANISH</td>
<td>SPA</td>
<td>es</td>
<td>284</td>
</tr>
<tr>
<td>046</td>
<td>SWEDISH</td>
<td>SWE</td>
<td>sv</td>
<td>278</td>
</tr>
<tr>
<td>086</td>
<td>T-CHINESE</td>
<td>ROC</td>
<td>tw</td>
<td>937</td>
</tr>
<tr>
<td>066</td>
<td>THAI</td>
<td>THA</td>
<td>th</td>
<td>838</td>
</tr>
<tr>
<td>090</td>
<td>TURKISH</td>
<td>TUR</td>
<td>tr</td>
<td>1026</td>
</tr>
</tbody>
</table>
Login Message

**How to:**

Customize the Login Screen With a Message

Customize the Connection Result Screen With a Message

Server administrators can customize the login and connection result screens with custom messages. The *Login Message* option is available by right-clicking the *Workspace* folder in the navigation pane.

**Procedure: How to Customize the Login Screen With a Message**

To customize the login screen:

1. Select *Workspace* from the menu bar.
2. From the ribbon, select the *Login Message* icon, or right-click the *Workspace* folder in the navigation pane, and select *Login Message*.

   The Login Message page opens.
3. Enter the text of the message in the HTML Message field in the Before section, as shown in the following image.

4. Click Save.
The message is added to the login page, as shown in the following image.

**Procedure: How to Customize the Connection Result Screen With a Message**

Server administrators can customize the connection result screen for each user type.

1. Select *Workspace* from the menu bar.
2. From the ribbon, select the *Login Message* icon, or right-click the *Workspace* folder in the navigation pane, and select *Login Message*.

   The Login Message page opens.

3. Select a user type from the Role drop-down menu. The options are *Server Administrator*, *Application Administrator*, *Server Operator*, *Basic User*, and *All Users*. 

   For connection issues, contact [Server Administration](mailto:serveradministration).
4. Enter the text of the message in the Message field of the After field, as shown in the following image.

![Login Message](image)

Optionally, you can set the number of times the message will appear by entering a value in the Display field.

5. Click Save.

The message is displayed after a successful connection, as shown in the following image.

![Message Displayed](image)
Web Console Appearance

Reference: Web Console Appearance

The Web Console appearance parameters control the look of the Web Console, as well as accessibility and menu bar customization.

Reference: Web Console Appearance

To access these settings, select Workspace from the menu bar. From the ribbon, click the Web Console Appearance icon, or right-click the Workspace folder in the navigation pane, and select Web Console Appearance.

The Web Console Appearance page opens, as shown in the following image.

![Web Console Appearance](image)

The following Web Console Appearance settings are saved in the edaserv.cfg file.

**Server-Wide Default Appearance**

**Appearance**

Controls the look of the Web Console.
Workspace Configuration Settings

Possible values are RIA-CarbonRounded, RIA-Default, and RIA-OceanRounded. The default value is RIA-Default.

WebFocus 80 compatibility

Matches the console appearance to WebFOCUS 80. The default value is No.

Accessibility

Display Accessibility Option

Allows users to enable or disable an accessibility display.

Menu Bar Appearance

Caption Of The Custom Link

Specifies the text of a custom link that is shown in the menu bar of the Web Console.

URL Of The Custom Link

Specifies the URL of a custom link that is shown in the menu bar of the Web Console.

Banner

Specifies if a banner image should be displayed on top of the menu bar in the Web Console. The image file must be located in EDAHOME/etc/wc directory.

Menu or Ribbon

Specifies whether the Web Console will display a menu bar or a ribbon. The default is Ribbon.

When you have completed your entries, click Save.

Profile Settings

Reference: Profile Settings

You can control aspects of profile execution from the Profile Settings pane.

Reference: Profile Settings

To access these settings, select Workspace from the menu bar. From the ribbon, click the Settings icon, and select Profile Settings, or right-click the Workspace folder in the navigation pane, and select Settings, and then Profile Settings.
The Profile Settings pane opens, as shown in the following image.

![Profile Settings pane](image)

The following Profile Settings are saved in the edaserv.cfg file:

- **profile_parameter**
  - By passing parameters to profiles, you can submit different session parameters at different connection times. When this parameter is activated, any unresolved variables are prompted for during your initial logon to the Web Console.
  - Available settings are `y` and `n`.
  - If the server, user, or group profiles contain any unresolved variables, set the profile parameter keyword to `y`. The default setting is `n`.

- **group_profile**
  - To control the execution of group profiles during logon, choose:
    - **all.** All group profiles for the connecting user are executed in alphabetic order.
    - **select.** If the user exists in more than one group, the Web Console prompts for a group and executes the associated profile.
    - **primary.** Only the primary group profile for the connecting user is executed. (This is the default setting.)

- **profile_no_domain**
  - In the Windows Server, to control whether the domain name is included in or excluded from a user profile name, choose:
    - `n` to add the domain name to the profile name (for example, user `ibi/edaport` becomes `ibi_edaport.prf`). `N` is the default value.
    - `y` to omit the domain name from the profile name (for example, user `ibi/edaport` becomes `edaport.prf`). This setting is required for compatibility with earlier releases of the Server.
**Note:** The y setting can be safely employed if a single domain is in use and there are no local user IDs that could interfere with domain IDs. If there is potential for interference between local user IDs and domain IDs that are connected to the server, the n setting is required to ensure that each user has a unique profile name.

Note that server must be restarted when this parameter is changed.

When you have completed your entries, click Save.

**Core Engine Settings**

**How to:**
Access Core Engine Settings

Core engine settings allow you to control a wide range of services, including Bulk Load, FOCUTL, HLI, Stylesheet, Common, TABLE, and GRAPH, as well as NLS, Tracing, Obsolete Sets and PFKEYs sets.

**Procedure:** How to Access Core Engine Settings

To access Core Engine settings:

1. Select Workspace from the menu bar.

2. From the ribbon, click the Settings icon, and select Core Engine Settings, or right-click the Workspace folder in the navigation pane, and select Settings, and then Core Engine Settings.
The Core Engine Settings pane opens, as shown in the following image.

3. Select a service from the Settings Service list.

4. Optionally, enter a string in the Setting Name field to find specific settings, using % as a wildcard.
   For example, to find settings containing DATE, enter DATE%. All settings are upper case and the Setting Name field is case sensitive.

5. Optionally, enter a string in the Description Contains field to search for settings by their descriptions.

6. Optionally, select a profile from the Select profile drop-down menu.

7. Click Next.
The Change Core Engine Settings pane opens, as shown in the following image.

8. Make your changes and click Save.

The following confirmation message displays:

Core engine settings successfully changed in edasprof.prf

**Core System Variables**

**How to:**

View Core System Variables

Core System variables control the functionality of the server.
The variables fall into the following categories:

- Display Information
- Operating System
- Release Information
- National Language Support
Procedure: How to View Core System Variables

To view Core System variables:

1. Select Workspace from the menu bar.

2. From the ribbon, click the Settings icon, and select Core System Variables, or right-click the Workspace folder in the navigation pane, and select Settings, and then Core System Variables.

The Core System Variable pane opens, as shown in the following image.

3. Select a service from the Settings Service list.

4. Optionally, enter a string in the Setting Name field to find specific variables, using % as a wildcard. Variables are all upper case and all begin with an ampersand (&).

5. Optionally, enter a string in the Description Contains field to search for variables by their descriptions.

6. Click Next.
The Core System Variables are displayed, as shown in the following image.

Core Engine Global Variables

**How to:**
Create Core Engine Global Variables

You can add global variables to a profile on the server to deliver default values or execute SET commands.

*Procedure: How to Create Core Engine Global Variables*

To create Core Engine global variables:
1. Select *Workspace* from the menu bar.

2. From the ribbon, click the *Settings* icon, and select *Core Global Variables*, or right-click the *Workspace* folder in the navigation pane, and select *Settings*, and then *Core Global Variables*.

   The Core Global Variable pane opens, as shown in the following image.

   ![Core Engine Global Variables](image)

3. Optionally, select a profile from the drop-down menu. The default is edaprof.

4. Click *Add New*.

5. On the Core Global Variable pane, select *SET* or *DEFAULT* from the *Command* drop-down menu.
6. Enter a name and value for the variable in the corresponding fields and click Add New, as shown in the following image.

![Core Engine Global Variables](image)

7. Click Save.

**Application Settings**

**Reference:** Application Settings

When you want to be able to reuse data within the same browser session, you can store the data in the form of a HOLD, SAVE, or SAVB file in the foccache directory, which is automatically created when the connection to the server is established. This becomes the first directory in the application path.

As long as the browser session remains active, the stored files remain in the foccache directory and can be referenced in requests using standard two part names. For example, the first request below creates a HOLD file in foccache, which is referenced by the second request:

```
TABLE FILE CAR
PRINT CAR
ON TABLE HOLD AS FOCCACHE/myfile
END
```
When the maximum foccache retention time is reached (180 minutes by default), the foccache directory is removed by the server and can no longer be referenced. (For related information, see Application Settings on page 463.)

This feature provides an important mechanism for caching and running multiple instances of WebFOCUS active and drill-down reports. You can use any WebFOCUS graphical tool to create the request and generate a report.

**Note:** Each time a WebFOCUS user logs into the Managed Reporting (MR) environment, a new session with its own foccache directory is created. Files that were stored in a prior foccache directory are no longer accessible. When the user logs out of MR the foccache directory used within that MR session is no longer accessible.

**Reference:** Application Settings

To access these settings, select Workspace from the menu bar. From the ribbon, click the Settings icon, and select Application Settings, or right-click the Workspace folder in the navigation pane, and select Settings, and then Application Settings.

The Application Settings pane opens, as shown in the following image.

![Application Settings](image)

The following Application Settings are saved in the edaserve.cfg file.

- **foccache_dir**
  Defines the location of the foccache directory. The default is edatemp/foccache/....
**foccache_maxage**

Defines the maximum number of minutes that a foccache directory will last. The default is 180 minutes. When the foccache directory expires, the session also expires.

0 means unlimited (that is, the directory will be remain active as long as the session lasts or the server is running).

**nested_app**

For applications containing subfolders or multiple-level subfolder trees, this parameter controls whether subfolders will be automatically added to the application path.

The valid values are:

- A positive integer - Enable nested application, and only a specific number of subfolder levels in the active application path.
- \( n \) - Disables nested applications. Only applications explicitly in the APP PATH will be used.
- \( y \) - Enables nested applications. The entire application subfolder tree under each application in the APP PATH is included into active application path.

The default value is 5.

**Note:** For z/OS servers, this setting is only applicable to directory-style applications, it is not applicable to PDS-style applications nor to applications mapped as a collection of ddnames.

**homeapps**

If nested_app is set to \( y \) or a number, homeapps defines the location of the home application root directory. With homeapps defined, each connected user will see a *My Home* applications folder on the Application tree. Users can create new applications (home applications) in this folder. These applications will be visible and available only to the connected user and the server administrator. The user will have full access to his home applications.

**Note:** Only available with a DataMigrator or Managed Reporting license. A WebFOCUS Reporting Server requires a homeapps license to enable home applications.
When you have completed your entries, click *Save and Restart Server*.

**Miscellaneous Settings**

**How to:**
Customize the IKJEFF10 Exit for DYNAM SUBMIT From the Web Console (z/OS)

**Reference:**
Miscellaneous Settings

Miscellaneous Settings allow you to set additional Workspace operating parameters, including automatic recovery, transaction coordination, soft and hard kill delays, maximum session log rows, time window for running response time averages, and proxy server settings.

**Reference:**  **Miscellaneous Settings**

To access these settings, select *Workspace* from the menu bar. From the ribbon, click the *Settings* icon, and select *Miscellaneous Settings*, or right-click the *Workspace* folder in the navigation pane, and select *Settings*, and then *Miscellaneous Settings*. 
The Miscellaneous Settings pane opens, as shown in the following image.

![Miscellaneous Settings](image)

The following Miscellaneous Settings are saved in the edaserv.cfg file:

- **automatic_recovery**
  
  Determines whether the server will automatically recover crashed listeners and/or special services. The default is *n*.
transaction_coordination_mode

Selecting y, activates the iWay Transaction Coordinator. A Two-Phase Commit will be used when XA-Compliant databases participate in a transaction. The default is n.

tscom3_kill_delay1

Defines the time (in seconds) allowed for an agent to stop before soft kill is sent. The default is 16.

tscom3_kill_delay2

Defines the time (in seconds) allowed for a soft kill to work before a hard kill is sent. The default is 32.

crashed_cleanup

By default, crashed agents are kept in the agents table for diagnostics purposes, and are only removed when they are explicitly killed. When this set to y, crashed agents are automatically removed from agents list when the Workspace Manager detects a crash. The default value is n.

crashed_max_dump

If crashed_cleanup is set to y, this determines the number of memory dump files retained for later diagnosis.

seslog_max_lines

Defines the upper limit for the number of rows in a session log. When the limit is exceeded, only the latest records will be kept in the session log and the number of records will equal the limit. The default is 500.

stats_runningavg

Defines the time window for the calculation of running response time averages. The default is 600.

proxy_server

Defines a proxy server, which acts as an intermediary on requests for resources from other servers.

proxy_port

Defines the port number of the proxy server.

proxy_user

Defines a user ID for the proxy server.

proxy_password

Defines a password for the user ID connecting to the proxy server.
outbound_ssl_certificate_file
Required for SSL when using self-signed certificates on i5 systems.

outbound_ssl_certificate_passphrase
Required for SSL when using self-signed certificates on i5 systems.

outbound_ssl_certificate_label
Required for SSL when using self-signed certificates on i5 systems.

outbound_ssl_certificate_keyfile
Required for SSL when using self-signed certificates on i5 systems.

outbound_ssl_auth_server
Required for SSL when using self-signed certificates on i5 systems.

htmlencode
Specifies whether to encode HTML tags in data as plain text in order to prevent attacks by inserting executable code into data.

**z/OS Specific Parameters**

tmpalloc_primary
tmpalloc_secondary
Allocation (in CYLs) for temporary Web Console files allocated by the HTTP listener. The default is 5 and 50, respectively.

submit_opt
Customizes the call of the IKJEFF10 exit when submitting jobs with the DYNAM SUBMIT command.

smf_recno
Defines the SMF record number that the server will use to record utilization statistics.

smf_subtype
Defines which pairs of SMF subtype records are cut. The options are:

- all. Cut all records. This is the default.
- logon. Cut logon/logoff subtype only.
- query. Cut query begin/query end subtype only.
privatedd

Defines how server will handle allocations for duplicated ddnames (same ddname allocated both to IRUNJCL and from a customer application using DYNAM) and what the search strategy will be.

When you have completed your entries, click Save.

**Procedure:** **How to Customize the IKJEFF10 Exit for DYNAM SUBMIT From the Web Console (z/OS)**

To change how the server calls the IKJEFF10 exit, set the submit_opt parameter as follows:

1. From the menu bar, select *Workspace*.
2. From the ribbon, click the *Settings* icon, and select *Miscellaneous Settings*, or right-click the *Workspace* folder in the navigation pane, and select *Settings*, and then *Miscellaneous Settings*.

The Miscellaneous Settings page opens.

3. For the submit_opt option, assign a separate value (0 or 1) in each of the three drop-down lists. The default is 000.

The first drop-down list enables the call to IKJEFF10 from DYNAM SUBMIT. By default, the call is disabled.

   0
   
   Does not call IKJEFF10. This is the default setting.

   1
   
   Calls IKJEFF10.

The second drop-down list specifies that SUBMIT is to call IKJEFF10 in problem state, not in supervisor state. The IBM specification for IKJEFF10 requires supervisor state. If the version of IKJEFF10 in use at your site is capable of running in problem state, this option may be changed, thus allowing DYNAM SUBMIT to be used with IKJEFF10 when the server is not running APF-authorized. When you set:

   0
   
   Supervisor state is required for calling IKJEFF10. This is the default setting.

   1
   
   Supervisor state is not required to call IKJEFF10.
The third drop-down list allows SUBMIT to continue in the event that an error occurs while processing an in-stream data set. In-stream data sets are created by the following statements in the job:

```plaintext
//ddname DD *
//ddname DD DATA
/*XMIT
//name XMIT
/*DATASET
```

If an error is found in one of the previous statements (for example, a syntax error in the DLM parameter), the SUBMIT operation is normally cancelled. This option allows submission of the job to continue, although in such a case the results are unpredictable since the JCL contained within the in-stream data set may be erroneously interpreted as part of the job being submitted.

0
Terminates SUBMIT on in-stream data set error. This is the default setting.

1
Does not terminate SUBMIT on in-stream data set error.

4. Click Save.

Your entries are registered in the edaserve.cfg file.

License Settings

Reference:
License Settings

You can view and change the current license code and provide and/or change your site code using the License Management page.

The license code is encoded to determine the configuration, additional products available in the configuration, the number of CPUs on the server, and the number of user seats the configuration supports.

For more information on how to obtain a new license code, contact Customer Support or your local Information Builders sales office.
Reference: License Settings

To access these settings, select Workspace from the menu bar. From the ribbon, click the License icon, or right-click the Workspace folder in the navigation pane, and select License.

The following License Management settings are saved in the edaserv.cfg file:

When you have completed your entries, click Save and Restart Server.

license

Enter the license number (required for the type of server you are using).

license_active_report

Enter the license number for WebFOCUS Active Technologies.

license_rstat

Enter the license number for the RStat scoring feature.

site_code

Enter the site code number (required for support calls).

license_mobile

Enter the license number for the Mobile Favs feature.
Migrate Settings

How to:
Migrate Configuration Information

The Migrate Settings page allows you to migrate a server from a previous release. It is recommended that you migrate configuration information from previous releases after you verify the proper basic installation of the new release.

Procedure: How to Migrate Configuration Information

To migrate from a previous release:

1. From the menu bar, select Workspace.

2. From the ribbon, click the Migrate icon, or right-click the Workspace folder in the navigation pane, and select Migrate.

   The Migrate page opens.

3. Type the full path of the configuration instance directory (EDACONF) or click the ellipsis (...) and navigate to it.

4. Click Continue.
Editing Configuration Files

How to:
Edit Configuration Files

Manually editing configuration files requires extensive knowledge of the inner workings of the server. All files except VERSION.CFG are available for editing in the Web Console text editor. VERSION.CFG is created by the installation/configuration process and is only available for viewing from that page.

Procedure: How to Edit Configuration Files

1. From the menu bar, select Workspace.
2. In the navigation pane, expand the Configuration Files folder. You can open the following files for editing:
   - Workspace. Opens edaserve.cfg
   - Administration. Opens admin.cfg
   - Communication. Opens odin.cfg
   - Version. Opens version.cfg
   - Server Profile. Opens edasprof.prf
   - Trace Profile. Opens ibitrace.fex
   - FDS Profile. Opens suprof.prf
   - User/Group Profiles Folder. Has an option for each defined user and group.
     Note that both Server Administrators and Application Administrators can edit the user.prf file. However, Server Administrators can edit all user.prfs, while Application Administrators can only edit their own profiles.
   - Miscellaneous folder. Has the following options:
     - Server Startup Script. Opens edastart.bat
     - NLS. Opens nlscfg.err
     - Font. Opens fontuser.xml
     - Environment. Opens edaenv.cfg (When the server starts, environment variables are set according to entries in the edaenv.cfg file. If the environment conflicts with an entry in edaenv.cfg, the entry in edaenv.cfg takes precedence.)
Configuring Java Services

In this section:
Fine-Tuning the Server

How to:
Configure Java Services for a JSCOM3 Listener

You can configure Java Services to add JSCOM3 listener, which is required to support and monitor Java-based adapters and functionality, such as GRAPH. You can fine tune server performance.

Procedure: How to Configure Java Services for a JSCOM3 Listener

1. From the menu bar, select Workspace.
2. In the navigation pane, expand the Java Services folder.
3. Right-click DEFAULT and select Properties.

The Java Services Configuration pane opens, as shown in the following image.
4. Enter values for each of the configuration sections.
5. When finished, click Save and Restart Java Services.

Reference: Java Services Configuration Parameters

You can enter values on the Java Services Configuration pane for Basic and Advanced settings, JVM Settings, and the Classpath. For information on JVM Settings, see How to Fine Tune JVM Settings From the Web Console on page 477.

**Basic**

**NODE**
Defines the logical name for the node block.

**PORT**
Defines the TCP port number that the listener is listening on.

**HOST**
Defines the IP address that the listener is listening on.

**REFRESH**
Defines the minimum number of new connections which can be accepted during the life of each Java server process. A Java server which has reached the limit will be terminated, and a new Java server will be started. To use this feature, you must configure more than one Java server (using NUMBER_READY) to prevent service gaps. It is ignored if only one Java server is configured.

**NUMBER_READY**
Defines the number of Java servers that the Workspace Manager will create at startup. The first server will listen on the PORT defined in the node. Each additional server will listen on an incremental port, for example, PORT + 1, PORT + 2, etc.

**Advanced**

**GPOOLSIZE**
Defines the number of Graph Service Agents that each Java server will create at startup.

**FLEX_SUPPORT**
Enables JAVA environment to support Flex. It should be set to "0" ONLY if there is a conflict between the CLASSPATH objects.
**Classpath**

**IBI_CLASSPATH**

Defines the additional Java Class directories or full path jar names which will be available for Java Services.

**Fine-Tuning the Server**

**In this section:**

Using JVM Tuning Options to Improve Memory Usage

You can fine-tune the server to optimize performance.

A Java Services folder on the Workspace Configuration navigation pane enables you to create and manage multiple client connections to JSCOM3, thereby supporting redundancy and load balancing, as well as the ability to refresh JSCOM3 instances while ensuring that at least one connection is always available.

Java exceptions are displayed in the edaprint.log file, and JVM version and path information is displayed in the edaprint.log file and on the Java Services Configuration pane.

**Using JVM Tuning Options to Improve Memory Usage**

**How to:**

Fine Tune JVM Settings From the Web Console

You can obtain better memory usage performance in production servers by properly tuning the JVM heap and stack sizes using three options on the JVM Settings tab of the Java Services Configuration pane. These options set initial Java heap size, maximum Java heap size, and Java thread stack size. The options update the odin.cfg file. For related information, see *Editing Configuration Files* on page 473.

Before setting these parameters, it is useful to understand the following relationships.

**Heap Size**

JSCOM3 is the server interface to the JVM. When you start JSCOM3, you can specify memory allocation for the JVM using the -X options shown in the following table.

<table>
<thead>
<tr>
<th>JVM option passed to JSCOM3</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Xms</td>
<td>Determines the initial (minimum) Java heap size.</td>
</tr>
</tbody>
</table>
Heap size does not determine the amount of memory your process uses. As you monitor your Java process, you may notice that the amount of memory used exceeds the amount you have specified for -Xmx. This occurs because -Xmx limits the Java heap size and may allocate memory for other things, including a stack for each thread. Therefore, the total memory consumption of the JVM may exceed the value of -Xmx.

**Stack Size**

Each thread in the JVM is assigned a stack. The stack size limits the number of threads you can use. If the stack size is too large, you risk running out of memory since each thread is allocated more memory than it needs.

The following chart describes the JVM Option passed to JSCOM3.

<table>
<thead>
<tr>
<th>JVM option passed to JSCOM3</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Xss</td>
<td>Determines the stack size for each thread. You can make this value as low as 1K: -Xss1K. However, if the stack space is too small, you will eventually see an exception class java.lang.StackOverflowError.</td>
</tr>
</tbody>
</table>

**Controlling Heap and Stack Size**

JSCOM3 uses default values for the minimum (initial) and maximum heap sizes and for the stack size of each thread. To improve performance, you can override the JSCOM3 default settings using the initial Java heap size, maximum Java heap size, and Java thread stack size options. For details, see *How to Fine Tune JVM Settings From the Web Console* on page 477.

You can also choose the Force Finalization option on the Java Services menu, which assists in memory management by releasing memory that is not currently in use by the Java Virtual Machine (JVM).

**Procedure:**  *How to Fine Tune JVM Settings From the Web Console*

1. From the Web Console menu bar, select Workspace.
2. In the navigation pane, open the Java Services folder, right-click a service, and select Properties. The Java Services Configuration pane opens.
3. Click the JVM Settings tab and enter values for the following parameters:

   **Initial Java Heap Size**
   
   Defines the initial Java heap size in megabytes (MB), which reflects the minimum amount of memory that is already being used.
   
   Supply a positive integer number.

   **Maximum Java Heap Size**
   
   Defines the maximum Java heap size in megabytes (MB).
   
   Supply a positive integer number.

   **Note:** With server-side Java applications like JSCOM3, it is good practice to set the initial (minimum) and maximum heap sizes to the same value.

   **Java Thread Stack Size**
   
   Defines the Java thread stack size in kilobytes (KB).
   
   Supply a positive integer number.

   **JVM_OPTIONS**
   
   Defines the additional JVM options. This is the parameters that can affect the performance characteristics of the JVM.

   **JVM_PROPERTIES**
   
   Defines the additional JVM properties. This is a platform-independent generalization of the system environment variables.

4. Click **Save and Restart Java Services** to update the odin.cfg file and restart the server with the new settings.
Cluster Manager

How to:
Enable Cluster Manager
Add Remote Servers
Configure a Cluster
Change Cluster Manager Properties

Reference:
Remote Server Configuration Parameters
Remote Cluster Configuration Parameters
Cluster Manager Properties

Cluster Manager enables you to balance workload across a number of servers. It has polling and monitoring capabilities to identify which servers are up-and-running, average query response time, and the number of concurrent tasks running. CLM can also identify which remote servers are down, and appropriately re-route requests, as well as route a user connection to the most efficient remote server to enhance overall performance.

You can enable Cluster Manager, add remote servers, and configure clusters from the Workspace pane.

Note: CLM connections to a remote server do not use the queuing capabilities that may be configured on remote servers that are members of a cluster.

Procedure: How to Enable Cluster Manager
1. From the menu bar, select Workspace.
2. Right-click the Cluster Manager folder and select Enable.
   The Enable Cluster Manager pane opens.
3. Enter your license code in the LICENSE field and click Configure and Restart Server.
4. Click OK in the confirmation message.
   The Workspace will restart.

Procedure: How to Add Remote Servers
To add remote servers, Cluster Manager must be enabled.
1. From the menu bar, select Workspace.

2. Right-click the Cluster Manager folder, select New Remote Server, and then TCP. The Remote Server Configuration pane opens, as shown in the following image.

3. Enter the host name or IP address for the remote server in the HOST field.

4. Enter the remote server port in the PORT and HTTP_PORT fields.

5. Select a security mode from the SECURITY drop-down menu. The options are Trusted, Explicit, or IWA. Explicit will require you to enter a user and password, and a domain for Windows servers.

6. Optionally, enter a description for the server in the DESCRIPTION field.

7. Optionally, expand the Advanced section to set additional parameters. For information, see Remote Server Configuration Parameters on page 481.

8. Click Save.

9. Repeat the procedure to add all the server that will be part of the cluster.
The servers will be added in the Cluster Manager folder, as shown in the following image.

Reference: Remote Server Configuration Parameters

The Remote Server Configuration pane has Basic and Advanced sections.

**Basic**

**NODE**
Assigns a name to the remote server.

**HOST**
Indicates the host name or IP address for the remote server

**PORT**
Defines the TCP port number for the server.

**HTTP_PORT**
Defines the HTTP port number for the server.

**SECURITY**
Defines the security mode. The options are Trusted, Explicit, or IWA. Explicit will require you to enter a user and password, and a domain for Windows servers.

**DESCRIPTION**
Defines a description for the server.

**Advanced**

**SERVICE_NAME**
Indicates the name of the data service used by the remote server.
**COMPRESSION**

Activates data compression for data transfer between client and server.

**ENCRYPTION**

Defines the encryption method used in TCP data transfer between client and server. The options are DES, Advanced, or IBCRYPT.

**CONNECT_LIMIT**

Defines the maximum time that the client will wait for a TCP connection response from the server. The default value is -1, which creates an indefinite wait.

**MAXWAIT**

Defines the time that the client will wait for a response from the server in seconds. The default value is -1, which creates an indefinite timeout.

**REMOTE_EDASTART**

Defines the full name of the edastart command for the remote server.

**REMOTE_USER_PROFILE**

Determines if all commands in the personal $HOME/.profile will be executed before executing the edastart command for the remote server. The default value is y.

**TYPE**

 Defines the type of node. Reserved node will be brought up and down by Cluster Manager to optimize performance.

**Add to Cluster Node**

Enables you to add the server to a cluster.

**Procedure: How to Configure a Cluster**

To configure a cluster, you need to have enabled Cluster Manager, and configured your remote servers.

1. From the menu bar, select *Workspace*.
2. Right-click the *Cluster Manager* folder, select *New Remote Server*, and then *CLUSTER*.
The Remote Cluster Configuration pane opens, as shown in the following image.

3. Enter a name for the cluster in the **NODE** field.
4. Select the check boxes for the remote servers that you want to include in the cluster.
5. Optionally, enter a description for the cluster in the **DESCRIPTION** field.
6. Click **Save**.
7. Optionally, expand the Advanced section to set additional parameters. For information, see *Remote Cluster Configuration Parameters* on page 484.

The cluster will be added in the Cluster Manager folder, as shown in the following image.
Remote Cluster Configuration Parameters

The Remote Cluster Configuration pane has Basic and Advanced sections.

**Basic**

**NODE**

Assigns a name to the cluster.

**ALTERNATE**

Lists the servers that are available for the cluster.

**DESCRIPTION**

Defines a description for the cluster.

**Advanced**

**CLM_MAXWAIT**

Defines the time that the client will wait for a response from the Cluster Manager in seconds. The default value is -1, which creates an indefinite wait.

**DISPATCH_METHOD**

Defines how Cluster Manager dispatches user queries to remote servers. The options are:

- **Adhere to the settings in Cluster Manager.** The cluster will use the option set in the Cluster Manager settings. This is the default value.

- **RANDOM.** The query will be dispatched randomly to a running server in the cluster. Every server will have the same weight. The query will be queued if a queue is available, and there is no available agent in the selected server.

- **ROUND-ROBIN.** The query will be dispatched to a running server according to the order in the cluster list. The query will be queued if a queue is available, and there is no available agent in the selected server.

- **SMART.** The query will be dispatched to the fastest server according to the statistics gathered from remote servers in the cluster. Overall average response time will be minimized.

- **WEIGHTED.** Weight is assigned to each server based on its relative exponentially smoothed response time. A server is then selected based on the weight. If more than one server is available, the query will not be queued even if a queue is available in the selected server.
MAX_RSP_TIME

Defines the maximum query response time that users can expect. If the value is greater than zero, Cluster Manager will attempt to achieve this limit by starting reserved servers or adjusting the configuration of remote servers if AUTO_CONFIG is on.

START_STOP_THRESHOLD

Defines the number of polls. Cluster Manager will start or stop remote reserved servers if query response time is continuously above or below MAX_RSP_TIME for the last START_STOP_THRESHOLD polls. The default value is 2.

Procedure: How to Change Cluster Manager Properties

You can set Cluster Manager properties that apply to all of your clusters.

1. From the menu bar, select Workspace.
2. Right-click the Cluster Manager folder, select Properties.

The Cluster Manager Properties pane opens, as shown in the following image.
3. Makes change the properties.
4. Click *Save and Restart CLM*.
5. Optionally, you can also reset the Cluster Manager settings and server statistics by clicking *Reset CML and Servers Statistics*.

**Reference:** **Cluster Manager Properties**

With the exception of UDP Port Number, changing Cluster Manager settings will require restarting the Cluster Manager.

**UDP Port Number**
- Defines the UPD port number that the Cluster Manager is listening on for alternate node queries from applications.

**Polling History**
- Defines how many statistics are kept for each remote servers. The default value is 100.

**Polling Interval**
- Defines how often the Cluster Manager gathers statistics from remote servers in seconds. The default value is 30.

**User Query Dispatch Method**
- Defines how Cluster Manager dispatches user queries to remote servers. The options are:
  - **Adhere to the settings in Cluster Manager.** The cluster will use the option set in the Cluster Manager settings. This is the default value.
  - **RANDOM.** The query will be dispatched randomly to a running server in the cluster. Every server will have the same weight. The query will be queued if a queue is available, and there is no available agent in the selected server.
  - **ROUND-ROBIN.** The query will be dispatched to a running server according to the order in the cluster list. The query will be queued if a queue is available, and there is no available agent in the selected server.
  - **SMART.** The query will be dispatched to the fastest server according to the statistics gathered from remote servers in the cluster. Overall average response time will be minimized.
  - **WEIGHTED.** Weight is assigned to each server based on its relative exponentially smoothed response time. A server is then selected based on the weight. If more than one server is available, the query will not be queued even if a queue is available in the selected server.
Max Response Time Limit

Defines the maximum query response time that users expect. If the value is greater than zero, Cluster Manager will attempt to achieve this limit by starting reserved servers or adjusting the configuration of remote servers if AUTO_CONFIG is on.

Threshold for starting/stopping servers

Defines the maximum query response time that users expect. If the value is greater than zero, Cluster Manager will attempt to achieve this limit by starting reserved servers or adjusting the configuration of remote servers if AUTO_CONFIG is on.

Running Average Period

Defines the number of pollings used in averaging statistics. The default value is 2.

Cluster Manager Log

Determines whether Cluster Manager will log cluster statistics in the EDACONF/clmprint.log file.

The maximum number of line for each cluster node is defined by the POLLING HISTORY parameter in odin.cfg. Each line contains the following fields, which are separated by commas, in the following order:

- Cluster name.
- Time in yyyy/mm/dd hh:mm:ss format.
- Number of active servers.
- Total number of connections received among servers since they started or statistics were reset.
- Total number of completed connections among servers since they started or statistics were reset.
- Average response time since servers started or statistics were reset.
- Total number of security failures among servers since they started or statistics were reset.
- Total number of resource failures among servers since they started or statistics were reset.
- Total number of FOCUS errors among servers since they started or statistics were reset.
- Running average response time over the last RUNNING_AVG_PERIOD polling.
- Number of connections to this cluster since Cluster Manager started or statistics were reset.
Monitoring Server Activity

You can monitor every server type and change its operation parameters through the Web Console. Those changes can affect the behavior and performance of the server.

This topic describes how to monitor the following:

- Data Services
- Java Services
- Special Services and Listeners

It also describes how to perform certain administrative tasks on a server.

### Monitoring Server Status

You can view the system and system memory status from the Status page.

1. To access the Status page, select **Workspace** from the main menu.
2. From the ribbon, click the **Status** icon, or right-click the **Workspace** folder and select **Status**.
The Status page opens, as shown in the following image.

You can also access the last agent trace by selecting Status from the Monitor section of the ribbon.
Monitoring Data Services

In this section:
Displaying and Customizing a Data Service Agents Page
Displaying Status Statistics and Aggregated Statistics for Data Services
Working With the Connection Queue
Performing Administrative Tasks for Data Services

From the Web Console, you can:

- Display the Data Services Agents page, and customize the page to include only those statistics that you are interested in. The Data Services Agents page displays statistics for the current list of agents monitored by the Workspace Manager.
- Display the Data Service Agents page for a selected service. You can customize the page to include only those statistics that you are interested in.
- Display statistics, including system-extended statistics, for an individual Data Service Agent.
- Display a status report for all Data Services. You can customize the report to include only those statistics that you are interested in.
- Display aggregated statistics for all Data Services.
- Display aggregated statistics for a selected Data Service.
- Display connection statistics.

As you monitor Data Service activity, you can also perform the following administrative tasks from the Web Console:

- Reset aggregated statistics for Data Services and start collecting them from the beginning.
- Kill one or more Data Service Agents.
- Start one or more new Data Service Agents.
- Display an error message for a Data Service Agent.
Displaying and Customizing a Data Service Agents Page

How to:
Display and Customize the Data Services Agents Page
Display and Customize a Data Service Agents Page Associated With a Selected Service
Display Statistics for an Individual Data Service Agent

Reference:
Data Service Agents Performance Parameters
System-Extended Statistics for an Individual Data Service Agent

This topic describes how Server Administrators can display the Data Service Agents page for all Data Services or for an individual Data Service. Server Administrators access the page from the Workspace on the Web Console menu bar, using the Agents menu option for Data Services.

If you are a user other than a Server Administrator, you can access the same page and the same statistics from My Console on the Web Console menu bar. With the Manage My Agents option, you can monitor and manage your own agents, that is, the agents that match your user ID. If granted the applicable privileges, you can also monitor, or monitor and manage, the agents of the other users in your group.

Procedure: How to Display and Customize the Data Services Agents Page

1. From the menu bar, select Workspace.
2. From the ribbon, click the Agents icon, or right-click the Workspace or Data Services folder in the navigation pane, and select Agents.
   The Data Services Agents page opens on the right.
   The table in Data Service Agents Performance Parameters on page 496 describes all the statistics that you can display on the page.
3. To choose specific statistics that you want to display on the report, click Choose Columns.
   The pane that opens lists the available statistics, grouped by category, such as General, Client Information, and FOCUS Information. A description of each statistic is provided in the right column of the pane, to help you tailor the page for your needs.
   Select the check box for each statistic that you want to display on the page, and deselect the check box for each statistic that you do not want to display.

Server Administration 491
Optionally, you can:

- Use the arrow buttons to the left of a category to open (expand) the category or close it.
- Select the check box to the left of a category (for example, to the left of General), to select all the statistics in that category.

Click OK when you have made your selections.

The following image shows the General and Client Information sections.
The following image shows the FOCUS Information, Adapter Information, and Change Data Capture Info sections.

<table>
<thead>
<tr>
<th>Category/Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOCUS Information</td>
<td></td>
</tr>
<tr>
<td>Query Time</td>
<td>Last time a request was made to the agent</td>
</tr>
<tr>
<td>Command</td>
<td>Last instruction executed by the agent</td>
</tr>
<tr>
<td>Procedure</td>
<td>Last Procedure processed by the agent</td>
</tr>
<tr>
<td>Top Level Procedure</td>
<td>Last Top Level Procedure processed by the agent</td>
</tr>
<tr>
<td>Master File</td>
<td>Last Master file processed by the agent</td>
</tr>
<tr>
<td>Executed Class</td>
<td>Last Java class executed</td>
</tr>
<tr>
<td>Response Time</td>
<td>Last response time measured from request initiation to completion</td>
</tr>
<tr>
<td>Server Time</td>
<td>Last response time excludes time spent in DBMS processing</td>
</tr>
<tr>
<td>Error Number</td>
<td>Last FOCUS error</td>
</tr>
<tr>
<td>FOCUS I/O</td>
<td>The number of FOCUS I/O operations and External input operations performed in last request</td>
</tr>
<tr>
<td>Foccache Ticket</td>
<td>Unique identifier assigned to the last request utilized foccache directory</td>
</tr>
<tr>
<td>Number of Transactions</td>
<td>The number of Transactions or HLI commands performed in last request</td>
</tr>
<tr>
<td>Adapter Information</td>
<td></td>
</tr>
<tr>
<td>DBMS I/O</td>
<td>The number of external I/O operations performed in last request</td>
</tr>
<tr>
<td>DBMS Time</td>
<td>The time spent in DBMS processing in last request</td>
</tr>
<tr>
<td>Change Data Capture Info</td>
<td></td>
</tr>
<tr>
<td>Source DBMS Adapter</td>
<td>Suffix of the listening Adapter</td>
</tr>
<tr>
<td>Source Table Name</td>
<td>Data source to be listened on</td>
</tr>
<tr>
<td>Status</td>
<td>Adapter current status</td>
</tr>
<tr>
<td>Processed Transactions</td>
<td>Number of processed LLWs (files)</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Polling interval</td>
</tr>
<tr>
<td>Timeout Interval</td>
<td>Non-activity time-out interval</td>
</tr>
<tr>
<td>Transactions Processing Limit</td>
<td>Maximum number of LLWs (files) to be processed by Adapter in one request</td>
</tr>
</tbody>
</table>
4. To filter the values that you want to display on the page, click the Choose Rows button. The pane that opens lists the values for the State statistic. Select the check box for each value that you want to reflect on the page, and deselect the check box for each value that you do not want to reflect. For example, if you select the check box for in use and the check box for crashed, only the agents whose State is in use or crashed will be displayed on the page.

Optionally, you can:

- Use the arrow buttons to the left of State to open (expand) the statistic or close it.
- Select the check box to the left of State to select all the values for that statistic.
The following image shows the pane from which you can filter the values for State on a Data Service Agents page. In this example, the agents whose State is in use or crashed will be displayed on the page.

5. Click OK when you have filtered the page as desired.

You are returned to the Data Service Agents page. The following image shows a sample customized report with selected statistics. In this example, the agents identified as Tscomid 1 through 6 were killed, as described in How to Kill One or More Data Service Agents on page 513.

6. At the upper-right of the report pane, optionally click Refresh Now to refresh the statistics, or click the Refresh interval check box and type the number of seconds between automatic refreshes.
In the following image, the cursor is pointing to the Refresh Now button.

![Refresh Now button](image)

**Procedure:** How to Display and Customize a Data Service Agents Page Associated With a Selected Service

Since agents are associated with services, you may wish to display current service statistics.

1. From the menu bar, select **Workspace**.
2. In the navigation pane, expand the **Data Services** folder.
3. Right-click the name of the service on which you want to report, for example, **WC_DEFAULT**.
4. From the menu, click **Agents**.

   The Data Service Agents page associated with the selected service is displayed on the right. The table in *Data Service Agents Performance Parameters* on page 496 describes all the statistics that are provided on the page.
5. You can customize and filter the report, as described in *How to Display and Customize the Data Services Agents Page* on page 491.

**Reference:** Data Service Agents Performance Parameters

The following statistics can appear on a Data Service Agents page. Each agent is represented as a separate row on the report.

- **General**
  - **Tscomid**
    - Identification number associated with the Data Service Agent.
  - **Service**
    - Name of the data service for the agent.
  - **State**
    - Current state of the agent. Possible values are in use, DBMS call, idle, aborted, crashed, stopping, or starting.
A session connects and is in use until the moment that it disconnects. This includes all time spent between a session suspension and resumption when the process is not using the CPU but still has resources allocated for at least one session.

*DBMS call* indicates that the agent is waiting for a database to return data.

Idle means that the agent is not connected. It has no sessions at all, whether active or suspended.

Aborted and crashed are abnormal states resulting from a fatal software error detected by the program (aborted) or by the operating system (crashed). The agent process is no longer running, and these states are provided for diagnostic purposes. The Server Administrator can clear (using the kill option) such agents after the problem is investigated.

Stopping and starting are normal transitory states, which are self-explanatory.

**Client Information**

*User*

User ID associated with the server connection.

*Group*

Group ID associated with the server connection.

*Client Session*

Session ID uniquely identifying the client session.

*Client Address*

For some protocols, the network address of the connected client.

*Code Page*

Character code page used by the client connected to the session.

*Defer ID*

Unique identifier assigned to the submitted deferred request.

*Scheduler Job ID*

Unique identifier assigned to the last submitted scheduled or CMASAP request.

**FOCUS Information**

*Query Time*

Last time that a request to the agent was made. This value is used to calculate the time that an agent is idle, in cases in which an *idle agent limit* was set.
**Command**
First eight characters of the last instruction executed by the data access agent.

**Procedure**
Displays the procedure currently being executed or completed by each agent. For example, when a procedure, which is a part of a job, executes another procedure, the name of this procedure is shown in a Procedure column.

**Top Level Procedure**
Displays calling procedures or calling flows executed or submitted by agents.

**Note:** This column is not shown by default on the Data Services Agents page. To display it, click *Choose Columns*, select its check box on the Select the columns that will appear on the Agents page, and click *OK*.

**Master File**
Name of the last Master File that was processed by the agent. The displayed name can be up to 64 characters.

**Executed Class**
Last Java class executed. This value includes explicitly called Java classes (such as CALLJAVA), and implicitly called classes (such as GRAPH FILE).

**Response Time**
Time from the moment that the server receives the request (regardless of the requesting tool, that is, Web Console, DataMigrator, or WebFOCUS) until the request completes and the response is sent to the requester.

**Server Time**
Response time minus DBMS processing time.

**Error Number**
Last &RETCODE that is set upon procedure (FOCEXEC) completion. Zero (0) is normal. Any other value indicates an abnormal completion.

**Focus I/O**
Number of FOCUS I/O operations performed by the agent.

**Foccache Ticket**
Unique identifier assigned to the last request that used the foccache directory.

**Number of Transactions**
Number of transactions or HLI commands performed by the agent.
**Adapter Information**

**DBMS I/O**
Number of external I/O operations performed by the agent.

**DBMS Time**
Amount of DBMS processing time in seconds.

**Change Data Capture Information**

**Source DBMS Adapter**
Suffix of the listening adapter.

**Source Table Name**
Data source that is listened on.

**Status**
Current status of the adapter.

**Processed Transactions**
Number of processed LUWs (files).

**Polling Interval**
Interval at which polling takes place.

**Timeout Interval**
Amount of time during which there is no activity, and after which a timeout occurs.

**Transactions Processing Limit**
Maximum number of LUWs (files) that are processed by the adapter in one request.

**File Listener Information**

**Source File Type**
Suffix of the listening adapter.

**Source Directory (File)**
Data source that is listened on.

**File Extension**
Extension of processed files.

**Status**
Current status of the adapter.
**Processed Files**
Number of processed LUWs (files).

**Processed Bytes**
Number of bytes processed by the file listener adapter.

**Files in wait queue**
Number of selected files waiting to be processed by the file listener adapter.

**Processing time**
Rounded number of seconds that the file listener adapter spent in processing files.

**Wait for work time**
Rounded number of seconds that the file listener adapter spent in waiting for files.

**Average files per second**
Average number of files per second that the file listener adapter processed.

**Average bytes per second**
Average number of bytes per second that the file listener adapter processed.

**Average file wait time**
Average time in seconds that the file listener adapter spent in waiting for files.

**Polling Interval**
Interval at which polling takes place.

**Timeout Interval**
Amount of time during which there is no activity, and after which a timeout occurs.

**Files Processing Limit**
Maximum number of LUWs (files) that are processed by the adapter in one request.

**System**

**CPU Time**
Total CPU time used by the process.

**Memory Usage (KB)**
Amount of memory, in kilobytes, used by the process.

**Disk Usage (KB)**
Disk space, in kilobytes, used by the process.
Process ID

Operating system specific process identification number that is associated with the agent.

Procedure: How to Display Statistics for an Individual Data Service Agent

1. Customize and display the Data Services Agents page, as described in How to Display and Customize the Data Services Agents Page on page 491.

2. On the page, right-click the row for the individual Data Service Agent whose statistics you want to display. For example, right-click the row for the agent identified as Tscomid 11.

3. From the menu, click Statistics.

   The Agent Statistics pane opens. On this pane, you will see the statistics described in Data Service Agents Performance Parameters on page 496, followed by system-extended statistics for the selected agent process.

Reference: System-Extended Statistics for an Individual Data Service Agent

The following table describes the system-extended statistics for an individual Data Service Agent.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PageFaultCount</td>
<td>Standard Windows memory management statistics</td>
</tr>
<tr>
<td>PeakWorkingSetSize (KB)</td>
<td>for the monitored process.</td>
</tr>
<tr>
<td>WorkingSetSize (KB)</td>
<td></td>
</tr>
<tr>
<td>QuotaPeakPagedPoolUsage</td>
<td></td>
</tr>
<tr>
<td>QuotaPagedPoolUsage</td>
<td></td>
</tr>
<tr>
<td>QuotaPeakNonPagedPoolUsage</td>
<td></td>
</tr>
<tr>
<td>QuotaNonPagedPoolUsage</td>
<td></td>
</tr>
<tr>
<td>PagefileUsage</td>
<td></td>
</tr>
<tr>
<td>PeakPagefileUsage</td>
<td></td>
</tr>
<tr>
<td>Total Execution Time</td>
<td>Cumulative execution time of transactions performed by</td>
</tr>
<tr>
<td></td>
<td>the agent.</td>
</tr>
</tbody>
</table>
Displaying Status Statistics and Aggregated Statistics for Data Services

How to:
Display and Customize a Data Services Status Page
Display Aggregated Statistics for All Data Services
Display Aggregated Statistics for a Selected Data Service

Reference:
Aggregated Statistics for Data Services
Calculating and Displaying Averages

You can display and customize a status report for all Data Services, and display aggregated statistics for all Data Services or for a selected service.

Procedure: How to Display and Customize a Data Services Status Page

1. From the menu bar, select Workspace.
2. In the navigation pane, right-click the Data Services folder, and select Services.

   The Data Services Status page is displayed on the right, as shown in the following image.

   ![Data Services Status Screenshot]

   The table in Aggregated Statistics for Data Services on page 505 describes all the statistics that you can display on the report.

3. To choose specific statistics that you want to display on the report, click Choose Columns, and proceed according to the instructions in How to Display and Customize the Data Services Agents Page on page 491.

4. At the upper-right of the report pane, optionally click Refresh Now to refresh the statistics, or click the Refresh interval check box and type the number of seconds between automatic refreshes.
Procedure: How to Display Aggregated Statistics for All Data Services

1. From the menu bar, select Workspace.

2. From the ribbon, click the Data Service Statistics icon, or right-click the Workspace folder in the navigation pane, and select Data Service Statistics.
The Data Service Statistics pane opens on the right. The following image shows a sample Data Service Statistics pane.

The table in *Aggregated Statistics for Data Services* on page 505 describes the statistics that are provided.
**Procedure:** How to Display Aggregated Statistics for a Selected Data Service

1. From the menu bar, select *Workspace*.
2. In the navigation pane, open the *Data Services* folder.
3. Right-click the name of the service on which you want to report, for example, *WC_DEFAULT*, and select *Statistics*.

   The aggregated statistics for the selected service are displayed on the right. The table in *Aggregated Statistics for Data Services* on page 505 describes the statistics that are provided.

**Reference:** Aggregated Statistics for Data Services

The following aggregated statistics are provided for Data Services:

**General**

*Service*

- If you are displaying aggregated statistics for all Data Services, this value is All Services.
- If you are displaying aggregated statistics for a selected service, this value is the name of the service configured for Workspace Manager in the edaserve.cfg file.

**Performance**

*Agents Now*

- Number of agents that are currently running.

*Agents Peak*

- Maximum number of agents that were running at any given time.

*Connections Total*

- Number of attempted connections to servers since they were started, or from the time that statistics were reset.
- This value is different from the total number of sessions, since a persistent session can connect multiple times for different requests.

*Connections Completed*

- Number of successfully completed connections to servers since they were started, or from the time that statistics were reset.

*Avg. Response Time*

- Average number of seconds for server response. This value does not include data transfer time. See *Calculating and Displaying Averages* on page 507, for more information.
Running Avg. Response Time

Response time, averaged over the time interval defined by the edaserve.cfg parameter stats_runningavg. The default value is 600 seconds.

Avg. DBMS Time

Average DBMS processing time in seconds.

Running Avg. DBMS Time

Average DBMS processing access time in seconds.

Avg. Server Time

Average response time minus DBMS processing time in seconds.

Running Avg. Server Time

Average response time minus DBMS processing access time in seconds.

Queued Now

Number of currently queued connections. Not applicable when queuing is off.

Currently running jobs are included in the connection total, but not in connections completed or in resource failures.

Queue Timeout

Number of connections that went into the queue and timed out (not available when queuing is off).

Queued Peak

Maximum number of connections that are queued at any given time (not available when queuing is off).

Queue Time

Average number of seconds spent in queue by all connections (not available when queuing is off).

Errors

Resource Fails

Number of connections rejected for lack of available agents. This value includes timed-out queued connections.

Security Fails

Number of connections that failed due to invalid credentials. For details about errors and failures, see the edaprint.log file, which is saved where the server is installed.
Focus Errors

Number of completed connections with WebFOCUS errors during request execution. For example, the adapter was not properly configured, or the data description or procedure was not found.

System

CPU Time

Total CPU time used by the server.

Memory Usage (KB)

Amount of memory, in kilobytes, used by the server.

Disk Usage (KB)

Total disk space, in kilobytes, used by the server.

Reference:  Calculating and Displaying Averages

Variables that are averages (avg) are fractional numbers of seconds rounded to the nearest millisecond for display purposes, but actually computed in higher precision, depending on the operating system:

- Avg Rsp Time is a measure of waiting time - idle time + running (that is, agent processing) time for all connections, divided by number of connections. It is actually the average time from the moment that the user clicks to send a request to connect or resume, until the moment that the answer appears in the browser, when the user suspends or disconnects the session.

- Agent processing time is the part of the connection duration spent only on running the request.

- Running time proportion of a connection is the percentage of its running time compared to its duration.

The accuracy of the three corresponding averages is limited only by the precision of the operating system. In the rare case in which a machine is faster than the precision of its time-measuring, accuracy side effects may occur:

- For an individual connection that has a duration shorter than the precision of the operating system, duration and running time cannot be measured and are both 0. The server considers it a 100% running time. A high occurrence of these instances produces an overestimated average proportion.
If the duration is longer than the precision because of waiting time, but the running time is still less than the precision, then a zero is counted toward the average running time and in calculating the proportion. A 0% running time proportion is recorded. A high occurrence of these instances produces an underestimated proportion.

Working With the Connection Queue

How to:
Display Statistics for All Connections
Kill a Connection

Reference:
Connection Statistics

The Connection Queue displays the statistics for the current list of connections, enabling administrators to monitor, and if necessary, cancel individual connections.

A connection refers to a physical connection between Client and Server. There are two types of connections:

- An active connection is one that is assigned to a session in a data access agent.
- A queued connection is one for which there are no available agents for the requested service, and the service is configured with a queue.

A queued connection waiting for an agent becomes active as soon as an agent is available. If the maximum time to wait in the queue is reached, the connection is automatically cancelled by the Workspace Manager.

Procedure: How to Display Statistics for All Connections

1. From the menu bar, select Workspace.
2. In the navigation pane, right-click the Data Services folder, and select Connection Queue, as shown in the following image.

![Connection Queue Image]

The Connection Queue report is displayed on the right.
The table in Connection Statistics on page 509 describes the statistics on the report. Each connection is represented as a separate row on the report.

**Reference: Connection Statistics**

The following statistics appear on the Connection Queue report.

- **Service**
  Name of the data service for the connection.

- **Type**
  Connection type, either connect or resume.

- **User**
  User ID that connected to the session.

- **Authentication**
  Type of authentication used to connect, either trusted, explicit, or IWA.

- **Requester ID**
  Unique identifier for the network connection created by a listener.
Time In

Time at which the connection was activated or queued. This value determines when a queued connection times out.

Client Address

Network address of the connecting client.

Foccache Ticket

Unique identifier assigned to the last request that used the foccache directory.

Procedure: How to Kill a Connection

To cancel a connection, click the row for the connection on the Connection Queue report, and from the menu, click Kill Connection, as shown in the following image.

Connection Queue

<table>
<thead>
<tr>
<th>Service</th>
<th>Type</th>
<th>User</th>
<th>Authentication</th>
<th>Requester Id</th>
<th>Time In</th>
<th>Client Address</th>
<th>Foccache Ticket</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>connect</td>
<td>pgmtst1</td>
<td>explicit</td>
<td>cmpip000081</td>
<td>Mar 17, 10:54:42</td>
<td>127.0.0.1:3878</td>
<td>--</td>
</tr>
</tbody>
</table>

- For an active connection, its session is forcefully disconnected from its agent.
- For a queued connection, it is simply cancelled and the client gets the same error that it would get if queuing was off and there were no available agents, or if the queue was full.
Performing Administrative Tasks for Data Services

**How to:**
- Reset Aggregated Statistics for Data Services
- Save the Last FOCUS Command
- Kill One or More Data Service Agents
- Kill Agents by Connected User ID
- Start One or More New Data Service Agents
- Display an Error Message for a Data Service Agent

**Example:**
Displaying an Error Message for a Data Service Agent

You can perform certain administrative tasks as you monitor Data Service activity.

- Reset aggregated statistics for Data Services.
- Save the last FOCUS command.
- Kill one or more Data Service Agents.
- Kill agents by connected userid
- Start one or more new Data Service Agents.
- Display an error message for a Data Service Agent.

**Procedure: How to Reset Aggregated Statistics for Data Services**

You can clear aggregated Workspace Manager statistics for Data Services and start collecting them from the beginning.

1. From the menu bar, select *Workspace*.
2. In the navigation pane, right-click the *Data Services* folder.
3. From the menu, click *Reset Statistics*.

**Procedure: How to Save the Last FOCUS Command**

You can save the last FOCUS command executed by an agent as a new procedure and run it separately from the Web Console. This provides a great tool for debugging server issues.

1. From the menu bar, select *Workspace*. 
2. Right-click an agent on the Data Services Agent page and select Save Last FOCUS Command.

The Create New Procedure as Text page opens, as shown in the following image.

![Create New Procedure as Text](image)

3. Click the Save button.

The Save Procedure page opens, as shown in the following image.

![Save Procedure](image)

4. Enter an application folder in the Application field, or click the ellipsis (…) and navigate to one.

5. Enter a name in the Name field.
6. Click Save.

**Procedure:** How to Kill One or More Data Service Agents

There are a number of ways to kill Data Service Agents:

- To stop one or a number of agents, select the check box next to each agent, and click *Kill Selected Agents*, as shown in the following image.

![Data Services Agents](image)

The running agent is terminated, invalidating any current connection to that agent. If a request is then issued from such a connection, an error message is returned. Stopping an agent is therefore an emergency administrative measure, as it disrupts the application. After an agent is terminated, the Data Services Agents pane refreshes automatically. The corresponding row of the terminated agent remains, and the State is listed as *stopping* until the row eventually disappears. You can also click *Refresh Now* to update the pane and remove the row.

- To stop an individual agent, you can also right-click the row for the agent, and click *Kill This Agent* from the menu. When asked if you want to continue to kill the agent, click *OK*.

- To stop an individual agent without permitting the DBMS to perform any cleanup tasks, choose *Hard Kill This Agent* from the menu. A message informs you that a hard kill may leave resources inaccessible and should be used only as a last resort. Click *OK* to continue the hard kill.

**Important:** Use this option only when *Kill This Agent* fails.
To stop all agents belonging to the same user ID, look for a row for the agent that is currently connected to the desired user ID. Right-click that row, and select *Kill Agents With The Same User ID.*

<table>
<thead>
<tr>
<th>Tscomid</th>
<th>Service</th>
<th>State</th>
<th>User</th>
<th>Group</th>
<th>Client Address</th>
<th>Scheduler Job ID</th>
<th>Query Time</th>
<th>Last Cmnd</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>DEFAULT</td>
<td>in use</td>
<td>edaga0</td>
<td>EDA</td>
<td>127.0.0.1:26140</td>
<td>--</td>
<td>Jul 30 12:19:49</td>
<td>SET</td>
</tr>
<tr>
<td>2</td>
<td>DEFAULT</td>
<td>in use</td>
<td>edaga6</td>
<td>EDA</td>
<td>127.0.0.1:25322</td>
<td>--</td>
<td>Jul 30 12:16:02</td>
<td>SET</td>
</tr>
<tr>
<td>7</td>
<td>DEFAULT</td>
<td>in use</td>
<td>edaga0</td>
<td>EDA</td>
<td>127.0.0.1:26228</td>
<td>--</td>
<td>Jul 30 12:19:38</td>
<td>SET</td>
</tr>
<tr>
<td>3</td>
<td>WC_DEFAULT</td>
<td>idle</td>
<td>--</td>
<td></td>
<td>Statistics</td>
<td>Jul 30 12:17:56</td>
<td>SET</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>WC_DEFAULT</td>
<td>idle</td>
<td>--</td>
<td></td>
<td>Save Last FOCUS Command</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
</tbody>
</table>

To stop all agents associated with a selected service, right-click the service beneath the Data Services folder, and select *Kill All Agents* from the menu, as shown in the following image. When asked to confirm your request, click *OK.*
For extreme situations in which you want to terminate all running agents, right-click the Data Services folder in the navigation pane. From the menu, select Kill All Agents. When asked to confirm your request, click OK.

Procedure: How to Kill Agents by Connected User ID

In the Web Console, look for a row for the agent in the Data Services Agents pane that is currently connected to the desired user ID, then right-click that row and select Kill Agents With The Same User ID, as shown in the following image.

To kill agents from the command line, the syntax is:

`edastart -killuser <userid>`

In addition, for the z/OS platform, a z/OS operator MODIFY command can also be used, as follows:

`/F <server_jobname/started task>, -killuser <userid>`

Procedure: How to Start One or More New Data Service Agents

Use this method to start additional agents, even when there are agents already running.

1. From the menu bar, select Workspace.
2. In the navigation pane, expand the Data Services folder.
3. Right-click the name of the service for which you want to start agents.
4. From the menu, select Start New Agents.
5. On the Start New Data Service Agents pane, type the number of new agents to start for the selected service, as shown in the following image. Then click Start.

![Start New Data Service Agents](image)

On the Data Services Agents pane, you will see that the new agents are listed, with the State of starting.

Procedure: How to Display an Error Message for a Data Service Agent

If a procedure generates an error, you can display the error message on the active agent.

1. From the menu bar, select Workspace.

   The Data Service Agents pane opens.

2. In the Tscomid column, right-click the number associated with an agent, and select View Error from the menu, as shown in the following image.

   ![Data Services Agents](image)

The latest error is displayed in a separate window.
Example: Displaying an Error Message for a Data Service Agent

The following error was generated on an agent when a procedure was run against a file that could not be found. Clicking the number of the agent that ran the procedure produced the following message:

(FOC205) THE DESCRIPTION CANNOT BE FOUND FOR FILE NAMED: XYZ
BYPASSING TO END OF COMMAND

Tip: The error message is also stored in the Session Log, which you can access by clicking the Show Session Log Window icon on the Web Console menu bar. In the Session Log, you can click the message to see expanded information, including troubleshooting suggestions. For example:

(FOC205) THE DESCRIPTION CANNOT BE FOUND FOR FILE NAMED:
No data description can be found for the file requested. Check the Master File Descriptions allocated or available, or the spelling of the file name.

For more information on the Session Log, see Showing the Session Log on page 591.

Monitoring Java Services

In this section:

Displaying and Customizing a Performance Report for Java Service Agents
Displaying Aggregated Statistics for Java Services
Performing Administrative Tasks for Java Services

From the Web Console, you can:

- Display a Performance Report for all Java Service Agents. The report displays statistics for the current list of agents monitored by the Workspace Manager. Multiple connections are supported, providing redundancy and load balancing capabilities. Also provided is the ability to refresh JSCOM3 instances after a specified number of connections, while ensuring that at least one connection is always available.

- Display statistics for an individual Java Service Agent.

- Display aggregated statistics for all Java Services.

As you monitor Java Service activity, you can also perform the following administrative tasks from the Web Console.

- Reset aggregated statistics for Java Services and start collecting them from the beginning.

- Stop or start one or more existing Java Service Agents.
Kill one or more Java Service Agents.

Start one or more new Java Service Agents.

**Displaying and Customizing a Performance Report for Java Service Agents**

**How to:**

Display a Performance Report for All Java Service Agents

Display Statistics for an Individual Java Service Agent

**Reference:**

Performance Report for Java Service Agents

Statistics for an Individual Java Service Agent

This topic describes how Server Administrators can display a Performance Report for the agents for all Java Services or statistics for an individual Java Service Agent.

**Procedure: How to Display a Performance Report for All Java Service Agents**

1. From the menu bar, select *Workspace*.

2. In the navigation pane, right-click the *Java Services* folder, and select *Agents*.

The Java Services Agents pane opens on the right.

The following image shows a sample report.

<table>
<thead>
<tr>
<th>Second</th>
<th>Port</th>
<th>Status</th>
<th>Process ID</th>
<th>Connections</th>
<th>Active Connections</th>
<th>Last User</th>
<th>Last Executed Class</th>
<th>Free Memory (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8103</td>
<td>active</td>
<td>2736</td>
<td>0</td>
<td>0</td>
<td>--</td>
<td>--</td>
<td>1361</td>
</tr>
<tr>
<td>2</td>
<td>starting</td>
<td>3180</td>
<td>0</td>
<td>0</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>3</td>
<td>starting</td>
<td>3744</td>
<td>0</td>
<td>0</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

The table in *Performance Report for Java Service Agents* on page 519 describes the statistics displayed on the report.

3. At the upper-right of the report pane, optionally click *Refresh Now* to refresh the statistics, or click the *Refresh interval* check box and type the number of seconds between automatic refreshes.
In the following image, the cursor is pointing to the Refresh Now button.

Reference: Performance Report for Java Service Agents

The following statistics appear on the Performance Report for Java Service Agents. Each agent is represented as a separate row on the report.

Jscomid
Unique identification number assigned to each Java Service Agent. You can start and kill JSCOM3 connections. Each started connection is issued a unique number. If you kill a connection, its number is retired. A new connection is assigned an entirely new Jscomid.

Port
Port number for each Java Service Agent. Numbering starts with a base number and increases by one for each active agent.

Status
Current status of the instance. Possible values are starting, active, stopping, or stopped.

Process ID
Operating system specific process identification number associated with each Java Service Agent.

Connections
Total number of clients connected to JSCOM3, both active and inactive.

Active Connections
Active client connections to JSCOM3.

Last User
Name of the user who executed the class.

Last Executed Class
Last executed Java class. This includes explicitly called Java classes (such as CALLJAVA), and implicitly called classes (such as GRAPH FILE).

Free Memory (KB)
Amount of memory, in kilobytes, available to the Java Virtual Machine (JVM).
Procedure: How to Display Statistics for an Individual Java Service Agent

1. Display the Performance Report for all Java Service Agents, as described in How to Display a Performance Report for All Java Service Agents on page 518.

2. Right-click the row for the individual Java Service Agent whose statistics you want to display, and select View Statistics.

The Statistics pane opens, as shown in the following image. On this pane, you will see the statistics described in Statistics for an Individual Java Service Agent on page 521.

3. At the upper-right of the report pane, optionally click Refresh Now to refresh the statistics, or click the Refresh interval check box and type the number of seconds between automatic refreshes.

<table>
<thead>
<tr>
<th>Statistics</th>
<th>JSCOM3</th>
<th>Refresh interval:</th>
<th>10</th>
<th>second(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>JSCOM3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remark</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>active</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process ID</td>
<td>1184</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Number</td>
<td>5103</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PageFaultCount</td>
<td>9129</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PeakWorkingSetSize (KB)</td>
<td>26216</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkingSetSize (KB)</td>
<td>25440</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QuotaPeakPagedPoolUsage</td>
<td>56198</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QuotaPagedPoolUsage</td>
<td>54572</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QuotaPeakNonPagedPoolUsage</td>
<td>14032</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QuotaNonPagedPoolUsage</td>
<td>13224</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PageFileUsage</td>
<td>25243648</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PeakPageFileUsage</td>
<td>26056752</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Execution Time</td>
<td>0:00:02.625</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connections</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jscomid</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Connections</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Active Connections</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last User</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Executed Class</td>
<td>ibi.jsgraph.B1RunJSCOMGraph</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Reference:** Statistics for an Individual Java Service Agent

The following statistics are for an individual Java Service Agent.

**General**

**Name**

Name of the Listener that is serving the Java Service.

**Remark**

Additional property of the Service or Listener, where available.

**State**

Current state of the connection. Possible values are starting, active, stopping, or stopped.

**Process ID**

Operating system specific process identification number associated with the Java Service.

**Port Number**

Port number for the Java Service. Numbering starts with a base number and increases by one.

**System**

**PageFaultCount**

**PeakWorkingSetSize (KB)**

**WorkingSetSize (KB)**

**QuotaPeakPagedPoolUsage**

**QuotaPagedPoolUsage**

**QuotaPeakNonPagedPoolUsage**

**QuotaNonPagedPoolUsage**

**PagefileUsage**

**PeakPagefileUsage**

Standard Windows memory management statistics for the monitored process.

**Total Execution Time**

Cumulative execution time of transactions performed by the agent.
Connections

Jscomid

Unique identification number assigned to the Java Service Agent. You can start and kill JSCOM3 connections. Each started connection is issued a unique number. If you kill a connection, its number is retired. A new connection is assigned an entirely new Jscomid.

Number of Connections

Total number of clients connected to JSCOM3, both active and inactive.

Number of Active Connections

Total number of active client connections to JSCOM3.

Last User

Name of the user who executed the class.

Last Executed Class

Last executed Java class. This includes explicitly called Java classes (such as CALLJAVA), and implicitly called classes (such as GRAPH FILE).

Displaying Aggregated Statistics for Java Services

How to:

Display Aggregated Statistics for All Java Services

Reference:

Aggregated Statistics for Java Services

You can display aggregated statistics for all Java Services.

Procedure:  How to Display Aggregated Statistics for All Java Services

1. From the menu bar, select Workspace.
2. In the navigation pane, right-click the Java Services folder, and select Statistics.

The Java Services Statistics pane opens on the right, as shown in the following image.
The table in *Aggregated Statistics for Java Services* on page 523 describes the statistics that are provided.

3. At the upper-right of the report pane, optionally click *Refresh Now* to refresh the statistics, or click the *Refresh interval* check box and type the number of seconds between automatic refreshes.

**Reference:**  *Aggregated Statistics for Java Services*

The following aggregated statistics are provided for Java Services.

**Total Connections**

Total number of clients connected to JSCOM3, both active and inactive.

**Total Active Connections**

Total number of active client connections to JSCOM3.

**Performing Administrative Tasks for Java Services**

**How to:**

- Reset Aggregated Statistics for Java Services
- Stop an Individual Java Service Agent
- Stop All Agents for a Selected Java Service
- Kill One or More Java Service Agents
- Start One or More New Java Service Agents

You can perform certain administrative tasks as you monitor Java Service activity.

- Reset aggregated statistics for Java Services.
- Stop or start one or more existing Java Service Agents.
- Stop or start all agents for a selected Java Service.
- Kill one or more Java Service Agents.
- Start one or more new Java Service Agents.
**Procedure:** How to Reset Aggregated Statistics for Java Services

You can clear aggregated Workspace Manager statistics for Java Services and start collecting them from the beginning.

1. From the menu bar, select **Workspace**.
2. In the navigation pane, right-click the **Java Services** folder, and select **Reset Statistics**.

**Procedure:** How to Stop an Individual Java Service Agent

1. Display the Performance Report for all Java Service Agents, as described in *How to Display a Performance Report for All Java Service Agents* on page 518.
2. Right-click the row for the individual Java Service Agent that you want to stop, and select **Stop**, as shown in the following image.

![Java Services Agents](image)

3. When asked if you want to continue to stop this JSCOM3 instance, click **OK**.

   On the Performance Report, you will see the status *stopping*. If you click **Refresh Now**, you will see the status *stopped*.

   **Tip:** You can restart the agent by right-clicking the applicable row on the Performance Report and clicking **Start** from the menu.

**Procedure:** How to Stop All Agents for a Selected Java Service

1. From the menu bar, select **Workspace**.
2. In the navigation pane, expand the **Java Services** folder.
3. Right-click the service whose agents you want to stop, for example, **DEFAULT**, and select **Stop All**.
4. When asked if you want to continue to stop all Java Service Agents, click **OK**.

   **Tip:** You can restart the agents by right-clicking the service in the navigation pane, and clicking **Start All** from the menu.
Procedure: How to Kill One or More Java Service Agents

1. From the menu bar, select Workspace.
2. In the navigation pane, expand the Java Services folder.
3. Right-click the name of the service for which you want to kill agents, and select Kill Agents.
4. On the Kill Java Service Agents pane, type the number of agents that you want to kill, and click Kill.

On the Performance Report for all Java Service Agents, you will see that the number of agents that you specified is removed from the list.

Procedure: How to Start One or More New Java Service Agents

Use this method to start one or more additional agents, even when there are agents already running.

1. From the menu bar, select Workspace.
2. In the navigation pane, expand the Java Services folder.
3. Right-click the name of the service for which you want to start agents, and select Start New Agents.
4. On the Start New Java Service Agents pane, type the number of new agents to start for the selected service, and click Start.

On the Performance Report for all Java Service Agents, you will see that the new agents are listed, with the Status of starting, as shown in the following image.
Monitoring Special Services and Listeners

In this section:
Deferred Lists
Web Sessions
Performing Administrative Tasks for Special Services and Listeners

How to:
Display a Performance Report for All Special Services and Listeners
Display Statistics for an Individual Special Service or Listener

Reference:
Performance Report for All Special Services and Listeners
Statistics for an Individual Special Service
Statistics for an Individual Listener

From the Web Console, you can:

- Display a Performance Report for all Special Services and Listeners. The Performance Report displays statistics for the current list of Special Service processes and Listener processes monitored by the Workspace Manager.

- Display statistics for an individual Special Service or Listener.

- Display the Deferred List, which includes statistics and status for deferred requests.

- Display a Performance Report for all web sessions, or display statistics for an individual web session associated with an HTTP Listener.

As you monitor Special Service and Listener activity, you can also perform the following administrative tasks from the Web Console.

- Enable or quiesce certain Special Services or Listeners.

- Start or stop certain Special Services or Listeners.

- Kill all web sessions.

- View the log for a web session.
**Procedure:** How to Display a Performance Report for All Special Services and Listeners

1. From the menu bar, select *Workspace*.

2. In the navigation pane, right-click the *Special Services and Listeners* folder, and select *Processes*.

The Performance Report for all Special Services and Listeners opens on the right, as shown in the following image.

![Performance Report for All Special Services and Listeners](image)

The table in *Performance Report for All Special Services and Listeners* on page 527 describes the statistics displayed on the report.

3. At the upper-right of the report pane, optionally click *Refresh Now* to refresh the statistics, or click the *Refresh interval* check box and type the number of seconds between automatic refreshes.

**Reference:** Performance Report for All Special Services and Listeners

The following statistics appear on the Performance Report for all Special Services and Listeners.

**Name**

Type of Special Service (for example, FDS, DFM, or SCHEDULER), or type of Listener (for example, HTTP or TCP).

**Status**

Status of the Special Service or Listener. Possible values include active, not active, or stopped.

**Process ID**

Operating system specific process identification number associated with each Special Service or Listener running in a Workspace Manager address space.
Port Number/Directory
Port number or directory associated with the Special Service if applicable (for example, FDS port or DFM directory), or the port number associated with the Listener.

Number of Requests
Total number of requests processed by the Special Service or Listener.

CPU Time
Total CPU time used by the process, displayed as hours:minutes:seconds.milliseconds (for example, 0:00:05.625).

Memory Usage (KB)
Amount of memory, in kilobytes, used by the process.

**Procedure:** How to Display Statistics for an Individual Special Service or Listener

1. Display the Performance Report for all Special Services and Listeners, as described in How to Display a Performance Report for All Special Services and Listeners on page 527.

2. Right-click the row for the individual Special Service or Listener whose statistics you want to display, and select Statistics, as shown in the following image.

![Special Services and Listeners](image)

The Statistics pane opens. On this pane, you will see the statistics described in Statistics for an Individual Special Service on page 529 or Statistics for an Individual Listener on page 531.

**Tip:** You can also display the Statistics pane for FDS, HTTP, TCP or SOAP by expanding the Special Services and Listeners folder, right-clicking one of these Special Services or Listeners, and clicking Statistics from the menu.
**Reference:** Statistics for an Individual Special Service

The following statistics appear for an individual Special Service.

**General**

Name

Type of Special Service (for example, FDS, DFM, or SCHEDULER).

Remark

Additional property of the Special Service, where available.

**State**

Current state of the Special Service connection. Possible values are starting, active, stopping, or stopped.

**Process ID**

Operating system specific process identification number associated with the Special Service.

**Port Number**

Applies to the Special Service FDS.

Port number for the FDS. Numbering starts with a base number and increases by one.

**System (Applies to the Special Services FDS and SCHEDULER)**

PageFaultCount

PeakWorkingSetSize (KB)

WorkingSetSize (KB)

QuotaPeakPagedPoolUsage

QuotaPagedPoolUsage

QuotaPeakNonPagedPoolUsage

QuotaNonPagedPoolUsage

PagefileUsage

PeakPagefileUsage

Standard Windows memory management statistics for the monitored process.

**Total Execution Time**

Cumulative execution time of transactions performed by the agent.
**Connections for FDS**

**Number of Connections**

Total number of active connections.

**Maximum Number of Connections**

Hard-coded limit for the number of connections (512).

**Number of FCB Blocks**

Total number of opened File Control Blocks (FCB) by all users.

**Maximum Number of FCB Blocks**

Hard-coded limit for the number of opened FCBs at the sink side (4096).

**Last User**

User ID of the last connection to the FDS Service.

**Last Executed HLI Commands**

Last command executed by the FDS Service.

**Connections for SCHEDULER**

**Status**

Current status of the Scheduler. For example, *scanning* means that the Scheduler is in the process of scanning the application path for scheduled jobs, and *ready* means that the Scheduler is ready to process a job.

**Last Full Scan**

Timestamp for the last full scan of the application path. A full scan is performed on the Scheduler *Start* and *Force Rescan* options, which are available on the Scheduler menu.

**Last Incremental Scan**

Timestamp for the last incremental scan. An incremental scan looks for files that have changed since the last scan. The last scan can be full or incremental, depending on which one happened last.

**Next Incremental Scan**

Timestamp for the next incremental scan. An incremental scan is based on the value specified by the Scheduler property sched_interval, which is in seconds.

**Number of Scheduled Events**

Number of jobs currently scheduled to run.
Number of Scheduled Runs

Number of all runs since the startup of the Scheduler.

Number of CMASAP Runs

Number of all jobs submitted through CMASAP since the startup of the Scheduler.

DFM for SCHEDULER

DFM_DIR Available Disk Space (KB)

Disk space, in kilobytes, in the directory dfm_dir that is available for the DFM Service write results of deferred requests.

Number of Requests Done Since Startup

Number of requests processed by the DFM Service since server startup.

Number of Responses Ready

Number of responses in the directory dfm_dir that are ready for a user to view (get).

Reference: Statistics for an Individual Listener

The following statistics appear for an individual Listener.

General

Name

Type of Listener, based on its network protocol (for example, HTTP or TCP).

Remark

Additional property of the Listener, where available. For example, an HTTP Listener can be CLM-enabled.

State

Current state of the Listener. Possible values include active, not active, and stopped.

Process ID

Operating system specific process identification number associated with the Listener.

Port Number

Port number for the Listener. Numbering starts with a base number and increases by one.

Total number of requests

Total number of requests processed by the Listener.
**System**

- `PageFaultCount`
- `PeakWorkingSetSize (KB)`
- `WorkingSetSize (KB)`
- `QuotaPeakPagedPoolUsage`
- `QuotaPagedPoolUsage`
- `QuotaPeakNonPagedPoolUsage`
- `QuotaNonPagedPoolUsage`
- `PagefileUsage`
- `PeakPagefileUsage`

  Standard Windows memory management statistics for the monitored process.

**Total Execution Time**

Cumulative execution time of transactions performed by the agent.

**Deferred Lists**

**How to:**

- Display the Deferred List
- Retrieve the Answer Set for a Deferred Request
- Delete a Deferred Request From the Queue

**Reference:**

Deferred List Statistics

The Deferred List displays the current status of all deferred requests. You can stop the queuing or execution of deferred requests, and remove requests from the queue.

**Procedure:** How to Display the Deferred List

1. From the menu bar, select *Workspace*.
2. In the navigation pane, expand the *Special Services and Listeners* folder.
3. Right-click *SCHEDULER*, and select *Deferred List*.
The Deferred List is displayed on the right, as shown in the following image. In the image, the Get and Delete menu options for an individual row are shown.

Each row displays statistics for a procedure that has been submitted for deferred execution. For details about these statistics, see Deferred List Statistics on page 533.

4. All deferred requests are displayed by default. However, you can select the check box next to one or more deferred requests, then click Delete Selected, to remove those requests from the report.

  Optionally, you can:

  - Click Select All to select the check boxes for all deferred requests.
  - Click Refresh Selected to refresh the status of the deferred request or requests whose check boxes are selected.

Reference: Deferred List Statistics

The following statistics appear on the Deferred List.

Defer ID

Unique identifier that the server assigns to each deferred request submitted.

User ID

ID of the user who requested deferred execution of the named procedure.

Status

Can be one of the following: Ready, Queuing, Executing, Agent crashed, Connect failed, Exceed limit, or Unknown.
### How to Retrieve the Answer Set for a Deferred Request

1. On the Deferred List, right-click a row for a deferred request whose status is Ready.
2. From the menu, click Get to retrieve the answer set for the deferred request in that row. The output is displayed on the right.

### How to Delete a Deferred Request From the Queue

Click anywhere in a row for a deferred request, and from the menu, click Delete.

**Tip:** To delete multiple rows, click the check box next to the rows that you wish to delete. Then click the Delete Selected button.

### Web Sessions

**How to:**
- Display a Performance Report for All Web Sessions
- Display Statistics for an Individual Web Session

**Reference:**
- Performance Report for All Web Sessions
- Statistics for an Individual Web Session

You can display a Performance Report for all web sessions and statistics for a single web session.
**Procedure:** How to Display a Performance Report for All Web Sessions

1. From the menu bar, select *Workspace*.

2. In the navigation pane, right-click the *Workspace* folder, and select *Web Sessions*.

   or

   In the navigation pane, expand the *Special Services and Listeners* folder, right-click *HTTP*, and select *Web Sessions*, as shown in the following image.

   ![Special Services and Listeners](image)

The Performance Report for all web sessions opens on the right.

The table in *Performance Report for All Web Sessions* on page 535 describes the statistics displayed on the report.

3. At the upper-right of the report pane, optionally click *Refresh Now* to refresh the statistics, or click the *Refresh interval* check box and type the number of seconds between automatic refreshes.

**Reference:** Performance Report for All Web Sessions

The following statistics appear on a Performance Report for all web sessions.

**Web Session Number**

Unique number assigned to a web session at logon to the server until the end of the session. The session ends by logging off the server or by closing the browser.

**Web Session ID**

A unique number that the server assigns to a specific user for the duration of the user session. Every time you connect to the Web Console, a new session number is assigned.

**User**

ID of the connected user.
Remote Address

IP address or machine on which the web browser running the Web Console resides.

Login Time

Time at which the web session originated.

Last Access Time

Last time at which the user was active in this web session.

Authentication

Mechanism that performs user authentication at the time the web session is created.

Console Message Count

Number of messages that a user received in this session.

Procedure: How to Display Statistics for an Individual Web Session

1. Display the Performance Report for all web sessions, as described in How to Display a Performance Report for All Web Sessions on page 535.

2. Right-click the row for the individual web session whose statistics you want to display, and select View Statistics.

   The Web Session Statistics pane opens.

   The table in Statistics for an Individual Web Session on page 536 describes the statistics displayed on the pane.

Reference: Statistics for an Individual Web Session

The following statistics appear for an individual web session.

Web Session Number

Unique number assigned to a web session at logon to the server until the end of the session. The session ends by logging off the server or by closing the browser.

User ID

ID of the connected user.

Number of Requests

Number of HTTP requests processed during the current web session.

User Login Time

Time at which the web session originated.
Last Access Time
Last time at which the user was active in this web session.

Login Type
Type of user logon, for example, explicit or cookie.

HTTP User Agent
Standard HTTP client that is used for connection to the HTTP Listener.

URI
Uniform Resource Identifier (URI) of the last Web Console page that was processed by the current web session.

Remote Address
IP address or machine on which the web browser running the Web Console resides.

Web Session ID
A unique number that the server assigns to a specific user for the duration of the user session. Every time that you connect to the Web Console, a new session number is assigned.

Performing Administrative Tasks for Special Services and Listeners

How to:
Enable/Quiesce or Start/Stop a Special Service or Listener
Kill All Web Sessions
View the Log for a Web Session

You can perform several administrative tasks for Special Services and Listeners.

- Enable or quiesce certain Special Services or Listeners.
- Start or stop certain Special Services or Listeners.
- Kill all web sessions.
- View the log for the web session.

Procedure: How to Enable/Quiesce or Start/Stop a Special Service or Listener
1. Expand the Special Services and Listeners folder in the navigation tree.
2. Right-click a Special Service or Listener.
3. Select one of the following options from the menu if the option is available for the selected Special Service or Listener:

- Quiesce/Enable
- Start/Stop

In the following image, the Quiesce menu option is selected for the TCP listener.

![Quiesce/Enable Option Selected](image)

The Performance Report or statistics pane reflects the changed status:

- For Enable or Quiesce: *active* or *not active*.
- For Start or Stop: *started* or *stopped*.

**Procedure: How to Kill All Web Sessions**

1. Display the Performance Report for all web sessions, as described in *How to Display a Performance Report for All Web Sessions* on page 535.

2. Near the top-left of the report, click *Kill All Web Sessions*, as shown in the following image.
Procedure: How to View the Log for a Web Session

1. Display the Performance Report for all web sessions, as described in How to Display a Performance Report for All Web Sessions on page 535.

2. Right-click the row for the web session whose log you want to view.

3. From the menu, click View Session Log.

For more information, see Showing the Session Log on page 591.

Custom Pages

How to:
Create Custom Pages

Custom Pages let you create pages that monitor the various services available from the Workspace folder, as well as run procedures. These pages are represented by icons on the navigation pane of the Applications page.

Custom Pages allow you to include multiple monitoring pages on a single page, creating a combination of Data Agents, Java Services, Listener and Special Services, Cluster Manager, and Resource Management pages. They also allow you to include procedures that generate reports. These pages and reports can be arranged horizontally, vertically, or in a cascade. Refresh and autorefresh will update all sections of a Custom Page. Custom Pages can be saved in a server application for future use.

Note: Custom Pages are only supported when the appearance of the Web Console is set to an RIA option.

Procedure: How to Create Custom Pages

Custom Pages are created in Application directory folders.
1. From the Application page, select New and Custom Page, as shown in the following image.

![Custom Page workspace](image)

The Custom Page workspace opens, as shown in the following image.

![Custom Page workspace](image)

2. To add a monitor page, click Add Workspace.

   The Select Page(s) to Add dialog box opens, showing the Monitor Pages folders.

3. Open the Monitor Pages folders and select an item to add.
The monitor page is added to the Selected Page(s) field, as shown in the following image.

4. Click **OK**.
   The monitor page is added to the workspace.

5. To add a procedure, click **Add Procedure**.
   The Select Page(s) to Add dialog box opens, showing the application folders.

6. Open an application folder and click a procedure.
The procedure is added to the Selected Page(s) field, as shown in the following image.

7. Click OK.

The procedure is added to the workspace.
8. You can continue adding monitor pages and procedures. When you are finished, use the *Arrange Windows* button to position the pages. The windows can be arranged *Horizontally*, *Vertically*, *In a Cascade*, or *Automatically*, as shown in the following image.
9. Click the Save As button.
   The Save Custom Page opens.

10. Enter an Application folder and a name in the corresponding fields, and click Save.

   Optionally, you can replace an existing page by selecting the Overwrite existing file check box.
You can add other pages at any time using the Add new windows (+) button next to the Arrange Windows drop-down menu.

The Custom Page is added to the Application folder. Right-click and select Open to open the page.
The following section describes how to manage listeners and special services.

**Topics:**
- Using the Listeners and Special Services Configuration Panes
- Special Services
- Listeners
Using the Listeners and Special Services Configuration Panes

The server provides special services and listeners, which are available from the Special Services and Listeners folder of the Workspace navigation pane.

In most instances, there is no need to alter the default configurations for these features.

Special Services

In this section:

The Scheduler and Deferred Service

The special services are:

- **FDS.** FOCUS Database Server.
- **SCHEDULER.** The Scheduler is used to schedule flows and stored procedures, and to manage deferred requests and reports.
The Scheduler and Deferred Service

How to:
Display and Customize the Scheduler Agents Page
Set Scheduler and Deferred Management Properties
Start or Stop Scheduler Scanning Manually
View Deferred Process Statistics

Reference:
Scheduler Agent Columns
Scheduler Agent States
Scheduler Scanning Properties
Scheduler Execution Properties
Scheduler Logging and Output Properties
Scheduler E-Mail Notification Properties
Deferred Management Properties
Extensions for Deferred Files

You can configure the settings that are used to manage the Scheduler and deferred requests and reports from the Web Console Scheduler Configuration pane. The parameters are stored in the edaserve.cfg file. You can also view and configure the Scheduler Agents page.

Procedure:  How to Display and Customize the Scheduler Agents Page

1. From the menu bar, select Workspace.

2. From the ribbon, click the Scheduler Agents icon, or expand the Special Services and Listeners folder in the navigation pane, right-click SCHEDULER, and select Scheduler Agents.
   The Scheduler Agents page opens.

3. To customize the columns that appear on the page, click Choose Columns.
Select the check boxes for the columns you want to appear, as shown in the following image.

4. Click **OK**.

5. To customize the states that appear on the page, click **Choose States**.

---

Special Services
All states appear by default. Deselect the check boxes for the states you want to remove, as shown in the following image.

6. Click OK.

7. To activate or deactivate a Scheduler agent, select the check box and click Activate Selected or Deactivate Selected.

**Reference:** **Scheduler Agent Columns**

You can add the following columns to the Scheduler Agents page.
General

<table>
<thead>
<tr>
<th></th>
<th>Category/Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>General</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ID</td>
<td>Identification number associated with the scheduler agent.</td>
</tr>
<tr>
<td></td>
<td>State</td>
<td>The current state of the scheduler agent (Starting, Scheduled, Running, Failed, Killed, Killing, Quiesced, Quiescing, Inactive, Reloading, or Done).</td>
</tr>
<tr>
<td></td>
<td>Application</td>
<td>Application name of the scheduled procedure.</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
<td>Name of the scheduled procedure.</td>
</tr>
<tr>
<td></td>
<td>User ID</td>
<td>User credentials used to run the scheduled procedure.</td>
</tr>
</tbody>
</table>

Schedule

<table>
<thead>
<tr>
<th></th>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Status</td>
<td>The current status for this procedure (Active or Inactive).</td>
</tr>
<tr>
<td></td>
<td>Schedule Type</td>
<td>The schedule type for this procedure (Run Once, Recurring, Multi-Day, Run when server starts, CMASAP, CMASAP Iterator, or CMASAP Iterator Group).</td>
</tr>
<tr>
<td></td>
<td>Start Date/Time</td>
<td>The initial start date and time for the schedule.</td>
</tr>
<tr>
<td></td>
<td>End Date/Time</td>
<td>The date and time on which this schedule expires.</td>
</tr>
<tr>
<td></td>
<td>Intraday Start</td>
<td>The start time of the intraday restriction interval.</td>
</tr>
<tr>
<td></td>
<td>Intraday End</td>
<td>The end time of the intraday restriction interval.</td>
</tr>
<tr>
<td></td>
<td>Interval</td>
<td>For recurring schedules, the number of minutes, hours, days, weeks, months or years between runs</td>
</tr>
<tr>
<td></td>
<td>Days of week</td>
<td>The days of the week on which the schedule will run.</td>
</tr>
<tr>
<td></td>
<td>Days of month</td>
<td>The days of the month on which the schedule will run.</td>
</tr>
</tbody>
</table>

Status

The current status for this procedure (Active or Inactive).

Schedule Type

The schedule type for this procedure (Run Once, Recurring, Multi-Day, Run when server starts, CMASAP, CMASAP Iterator, or CMASAP Iterator Group).
Start Date/Time
The initial start date and time for the schedule.

End Date/Time
The date and time on which this schedule expires.

Intraday Start
The start time of the intraday restriction interval.

Intraday End
The end time of the intraday restriction interval.

Interval
For recurring schedules, the number of minutes, hours, days, weeks, months, or years between runs.

Days of week
The days of the week on which the schedule will run.

Days of month
The days of the month on which the schedule will run.

E-Mail

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>E-Mail</td>
</tr>
<tr>
<td>[ ]</td>
<td>E-Mail on Failure</td>
</tr>
<tr>
<td>[ ]</td>
<td>E-Mail on start</td>
</tr>
<tr>
<td>[ ]</td>
<td>E-Mail on completion</td>
</tr>
</tbody>
</table>

E-Mail on Failure
The email address where confirmation will be sent on failure of each scheduled run.

E-Mail on start
The email address where confirmation will be sent on start of each scheduled run.

E-Mail on completion
The email address where confirmation will be sent on completion of each scheduled run.
### Statistics

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Run Time</td>
<td>The time of the last scheduled run.</td>
</tr>
<tr>
<td>Next Run Time</td>
<td>The time of the next scheduled run.</td>
</tr>
<tr>
<td>Tscomid</td>
<td>The identification number for the data service agent running the scheduled procedure.</td>
</tr>
<tr>
<td>Job ID</td>
<td>The job ID.</td>
</tr>
<tr>
<td>Parent Job ID</td>
<td>The parent job ID.</td>
</tr>
</tbody>
</table>

**Reference:** **Scheduler Agent States**

By default, the Scheduler Agents includes all states. You can removes the following states to limit what is displayed on the page.

**Main states**

**SCHEDULED**

The agent is waiting for its next scheduled run time. When it arrives, the agent attempts to establish a connection with a tscom3 agent to execute the scheduled procedure. When a connection is established, the agent enters the RUNNING state. The agent may transition into the FAILED state if a problem occurs. The administrator may set the agent to transition into the QUIESCED state by issuing a 'Quiesce Agent' request.

**INACTIVE**

An idle state. The procedure has been marked inactive. No action is required.

**DONE**

An idle state. The agent will not run because the scheduled end time has passed. The operation is complete and no further action will be initiated by the agent.
RUNNING
A connection has been established with a tscom3 agent to execute the procedure, which has begun to execute. Attempting to kill this agent will kill the underlying tscom3 agent process and cause a transition to the KILLED state. A critical error, such as a lost or broken connection, will move the agent into the FAILED state.

FAILED
A critical error occurred while the agent was trying to connect to a tscom3 agent or while executing the procedure. Administrator action is required to move the agent out of this state. Removing a FAILED agent forces a re-scan and creates a new agent for the procedure.

QUIESCED
The agent has been placed in this state by an administrator request to stop a SCHEDULED agent. No connection exists between this agent and a tscom3 agent. Without administrator action, the agent will remain in this state permanently. To transition from this state, the administrator must remove the agent. This forces a re-scan and creates a new agent for the procedure.

KILLED
The agent has been placed in this state by an administrator request to kill a RUNNING agent. The underlying tscom3 process has been killed. No active connection exists between this agent and tscom3. Without administrator action, the agent will remain in this state permanently. To transition from this state, the administrator must remove the agent. This forces a re-scan and creates a new agent for the procedure.

Transitional states

STARTING
The agent should successfully pass through this state into a SCHEDULED, DONE, INACTIVE, or FAILED state, with no intervention.

QUIESCING
The agent will transition from this state into a QUIESCED state, with no intervention.

KILLING
The agent should successfully pass through this state into a KILLED state, with no intervention.

RELOADING
A RELOAD AGENT request was received to reload a QUIESCED, DONE, FAILED, KILLED, or INACTIVE agent. The agent should successfully pass through this state into a SCHEDULED, DONE, INACTIVE, or FAILED state, with no intervention.
The scheduled agent has failed, but is automatically restarting because of the sched_restart_failed option. The agent transitions into a RUNNING state after sched_restart_interval seconds.

**Procedure: How to Set Scheduler and Deferred Management Properties**

1. From the menu bar, select *Workspace*.
2. In the navigation pane, expand the *Special Services and Listeners* folder.
3. Right-click SCHEDULER, and select *Properties*.
   The Scheduler Configuration page opens. The page has *Scanning*, *Execution*, *Logging and Output*, *Notification*, and *DFM* sections.
4. To set properties for the Scheduler or for deferred execution of requests, enter values in the corresponding fields.
5. Click *Save and Restart Scheduler*.

**Reference: Scheduler Scanning Properties**

The Scheduler Scanning properties are shown in the following image.

```
<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sched_scan_id</td>
<td>IBI\js02109</td>
</tr>
<tr>
<td>sched_interval</td>
<td>9999</td>
</tr>
<tr>
<td>sched_autostart</td>
<td>y</td>
</tr>
</tbody>
</table>
```

**sched_scan_id**

Determines what user ID the Scheduler uses to scan the application path for scheduled flows. It can be used to restrict the set of application directories scanned by the Scheduler to a subset of the APP PATH of the effective administrator. The default value is the effective administrator ID of the server.

**sched_interval**

Specifies the time interval in seconds used by the Scheduler. The Scheduler will wake-up and search for scheduled flows to run at this interval. The default value is 9999.
**sched_autostart**

If set to `y`, scanning for scheduled events is started when the DFM listener or a Scheduler service starts. If a service is not running, turning on `sched_autostart` will not make scanning available.

If set to `n`, a user may still start the scanning manually.

Depending on the number of files in the application path, `sched_autostart` may affect server performance.

The default value is `n`.

**Reference: Scheduler Execution Properties**

The Scheduler Execution properties are shown in the following image.

![Scheduler Execution Properties](image)

**sched_run_id**

Determines the user ID the a flow uses to run scheduled flows, either `server_admin_id` or `user`. The default value is `server_admin_id`.

**Note:** Flows submitted from the Data Management Console, the Web Console, or CMRUN are run under the userid that submits the specific flow.

**sched_service**

Defines the agent service that the Scheduler will use when running flows. If not set, the DEFAULT service will be used.

**sched_restart_interval**

Specifies the time interval in seconds between restart attempts for all restartable flows. The default value is 60 seconds.

**sched_restart_failed**

Determines whether scheduled agents will be restarted after they fail. The valid values are:
n - Failed agents will be restarted at most n times.
0 - Failed agents will not be restarted.
-1 - Failed agents will be restarted infinitely.
The default value is -1.

CMASAP_clear_interval

Specifies how often (in seconds) CMASAP agents are removed from the agents list. The default value is -1, meaning never.

Reference: Scheduler Logging and Output Properties

The Scheduler Logging and Output properties are shown in the following image.

sched_log_lines

Defines the maximum number of lines per request that the Scheduler will write to the log. When this number of lines is reached, logging stops. Exceeding this limit for one request does not affect logging for other requests.

When set to -1, the number of lines is unlimited. When set to 0, logging is disabled. The default value is -1.

sched_log_commit_interval

Specifies the maximum time interval in seconds that can elapse before log data is committed to the log. Used in conjunction with sched_log_commit_maxlines, these settings can fine-tune Scheduler logging behavior. The logging subsystem will commit data to the log whenever one of these maximums has been reached. Finding the best commit interval is a compromise among latency (the delay between the time a log message is received and when it is committed to the log database), reliability, and performance. Longer intervals enable greater I/O efficiency, but increase the potential amount of log information lost in a crash. The default value is 10.
sched_log_commit_maxlines

Specifies the maximum number of log lines to collect before committing them to the log. Used in conjunction with sched_log_commit_interval, these settings can fine-tune Scheduler logging behavior. The logging subsystem will commit data to the log whenever one of these maximums has been reached. Larger numbers enable greater I/O efficiency, but increase the potential amount of log information lost in a crash. The default value is 1000.

Merge Log and Formatted Output

Changes value of sched_log_output_destination keyword.

When checked, it specifies that only the job Log is stored in the Scheduler log (sched_log_output_destination=Log). The output is stored in dfm_dir location.

When unchecked, it specifies that the job Log and Output are stored in the Scheduler log (sched_log_output_destination=LogAndOutput).

Reference: Scheduler E-Mail Notification Properties

The Scheduler E-Mail Notification properties are shown in the following image.

<table>
<thead>
<tr>
<th>E-Mail Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Start</td>
</tr>
<tr>
<td>On Completion</td>
</tr>
<tr>
<td>On Failure</td>
</tr>
<tr>
<td>sched_email_address</td>
</tr>
</tbody>
</table>

Place each email address (id@domain.com), a user ID (myid) or a procedure name (%myfex) on a new line with no separators.

On Start
Sends email when the procedure starts.

On Completion
Sends email when the procedure completes.

On Failure
Sends email if the procedure fails.
sched_email_address

Defines the list of email recipients. The list can contain one or multiple email addresses and/or user IDs. Multiple entries should be on separate lines.

Procedure: How to Start or Stop Scheduler Scanning Manually

If the Scheduler is active, you can start or stop scanning manually.

1. Select Workspace from the menu bar.
2. Open the Special Services and Listeners folder in the navigation pane.
3. Right-click SCHEDULER and select Start Scanning or Stop Scanning.

Reference: Deferred Management Properties

The Scheduler Deferred Management (DFM) properties are shown in the following image.

![Deferred Management Properties Image]

dfm_dir

Defines the location where deferred requests and responses are stored. For related information, see Extensions for Deferred Files on page 561.

dfm_int_min

Defines the minimum time interval that the DFM listener sleeps between handling two requests.

dfm_int_max

Defines the maximum time interval that the DFM listener sleeps between handling two requests.

dfm_maxage

Defines the maximum number of days that deferred reports are kept in the server after they are created.
**dfm_maxoutput**

Defines the maximum size of a deferred report expressed as the number of kilobytes [K] or megabytes [M] between 0 and 65535, where 0 means unlimited. Kilobytes is the default.

Reports that are over this limit are removed.

**dfm_autostart**

When set to y, the DFM listener is started when the server starts.

**Procedure: How to View Deferred Process Statistics**

1. From the menu bar, select Workspace.
2. In the navigation pane, expand the Special Services and Listeners folder.
3. Right-click SCHEDULER, and select Statistics.

The Statistics SCHEDULER page displays the following information in the DFM section:

- DFM_DIR Available Disk Space (KB)
- Number of Requests Done Since Startup
- Number of Response Ready

For more information, see *Statistics for an Individual Special Service* on page 529.

**Reference: Extensions for Deferred Files**

The following table lists possible extensions for the deferred files listed in the dfm_dir directory.

<table>
<thead>
<tr>
<th>Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REQ</td>
<td>Request file.</td>
</tr>
<tr>
<td>RQD</td>
<td>Data file. Contains user ID, optional flags, and so on.</td>
</tr>
<tr>
<td>RQP</td>
<td>Request is being executed.</td>
</tr>
<tr>
<td>RQF</td>
<td>Request is waiting to be executed.</td>
</tr>
<tr>
<td>DEL</td>
<td>Request is deleted.</td>
</tr>
<tr>
<td>RSP</td>
<td>Response file. Contains the whole report for one request.</td>
</tr>
<tr>
<td>Extension</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>RPF</td>
<td>Response is ready.</td>
</tr>
<tr>
<td>RPE</td>
<td>Response exceeds maximum limit.</td>
</tr>
</tbody>
</table>

### Listeners

#### In this section:
- Configuring Listeners
- Other Listener Options

#### How to:
- Configure a SOAP Listener

The listeners are:
- HTTP
- TCP
- SOAP

These listen for activity on their respective ports.

**Note:** To include a SOAP listener, you need to configure one. For more information, see *How to Configure a SOAP Listener* on page 567

### Configuring Listeners

#### How to:
- Configure a Listener

**Reference:**
- Listener Basic Parameters
- Additional Listener Parameters

All listeners have the same type of basic parameters. They differ in the additional parameters that are available. All three types have Security parameters. HTTP also includes Sessions Control, Aliases and Miscellaneous Settings.
**Procedure:** How to Configure a Listener

1. From the menu bar, select *Workspace*.
2. Open the *Special Services and Listeners* folder in the navigation pane.
3. Right-click a listener and select *Properties*.
   The Listener Configuration page opens.
4. In the *Basic* section, you can enter a value for the *HOST* parameter.
5. If you need to set additional parameters, expand the corresponding section and enter values in the parameter fields.
6. Click *Save and Restart Server*.

**Reference:** Listener Basic Parameters

The HTTP, TCP, and SOAP listeners have the same type of basic parameters.

**NODE**

Defines the logical name of a node block. The settings are:

- For HTTP - LST_HTTP.
- For TCP - LST_TCP.
- For SOAP - LST_SOAP.

**PORT**

Defines the port number that a listener is listening on. The default value for the HTTP listener is 8117. The default value for the TCP listener is 8116.

**HOST**

Defines an IP address that a listener is listening on. If blank, the listener will listen on all IP addresses.

**Reference:** Additional Listener Parameters

The HTTP, TCP, and SOAP listeners have the following security parameter:

**RESTRICT_TO_IP**

Defines the name of a host or IP address(es) that will be accepted by the listener. The syntax is

```
hostname, xxx.xxx.xxx.xxx, yyy.yyy.yyy, ...
```
The address must be in base 256 standard dot notation. For platforms that support IPv6, IPv6 notation can be used if it is enabled (for example, 2001:1b1:719:1b1:203:baff:fe0a:fe23)

The internal default is *.*.*.*, which allows all IP addresses.

**Note:** You can use a wildcard to mask an entire section of the address, as in the following examples:

```
172.204.201.*
172.*.*.*
172.204.*.*
2001:1b1:719:1b1:203:baff::*:fe23
```

Partial masking is not supported, for example:

```
172.204.201.1*
172.204.201.*23
```

The HTTP listener has the following additional parameters:

**Security**

```
SECURITY
```

Defines the authentication protocol used by a secured listener. The valid values are:

- IWA - for NTLM protocol.
- KERBEROS - for Kerberos protocol.

```
LOGIN_FAILURE
```

Defines the type of message shown for a login error. The valid values are:

- 0 - Shows a general error message.
- 1 - Shows a precise error message.

The default value is 0.

```
LOGIN_HIDE_PROVIDERS
```

Defines whether available security providers or domains should be shown in the login screen. The valid values are:

- 0 - shows all available security providers or domains.
- 1 - hides all available security providers or domains.

```
CSRF_TOKEN
```

Defines whether a secret token should be used in all form submissions. This is used to prevent cross-site request forgery attacks. The valid values are:
- 0 - disable CSRF token.
- 1 - enable CSRF token.

**Enable HTTPS**

Enables HTTPS support, either for OpenSSL or Microsoft Windows SSL.

Both types have the following additional parameters:

**SSL_CERTIFICATE**

Defines the SSL certificate. The default certificate name for Microsoft SSL is iwaycert.p12.

**SSL_PASSPHRASE_E**

If the private key of the certificate is encrypted, an encrypted passphrase must be provided to decrypt the private key.

The following additional parameters are specific to OpenSSL:

**SSL_PRIVATE_KEY**

Defines the file that contains the private key for the listener. It must correspond to the public key embedded in the PEM certificate and must be in PEM format.

**SSL_CA_CERTIFICATE**

Defines the file containing the trusted CA certificate in PEM format. It is used to verify the client certificate. If the client fails to send the certificate or if verification fails, connections will be rejected. More than one CA certificate may be present in the file.

The following additional parameter is specific to Microsoft SSL:

**SSL_FRIENDLY_NAME**

Indicates a name used to identify the certificate in the PKCS#12 file, if the file contains more than one certificate.

**Sessions Control**

**PERSISTENT_GLOBAL**

Defines whether global FOCUS variables will be persistent within a browser session. The valid values are:

- 0 - Global variables are not persistent within a browser session.
- 1 - Global variables are persistent within a browser session.

The default value is 0.
PASS_EXPIRE_NOTIFICATION

Determines whether users receive a password expiration notification by defining the number of days before expiration at which a notification will occur. The default value is 0, meaning no notification.

MAX_WEBSESSION

Defines the maximum number of active sessions. The HTTP listener will reject connections to the Web Console if this number is reached. The default value is 0, meaning no limit.

LOG_LAST_REQUESTS

Defines the maximum number of last requests in a session that will be collected as statistics. The default value is 10.

Alias

IBI_HTML

Defines a URL alias for the primary file lookup directory. Lookup is performed first in the directory described by this alias. The default value is $EDAHOME/etc.

HTML_HOME

Defines a comma-delimited list of directories for file lookup. Directories are searched in the order in which they appear in this list.

SESSION_EXPIRATION

This parameter has been deprecated and has been combined with the foccache_maxage parameter, in order to make sure that no foccache files remain when the session has expired. For more information about the foccache_maxage parameter, see Application Settings on page 462.

Miscellaneous Settings

DEFAULT_HOST

Defines the preferred hostname or IP address for the listener when a listener has multiple IP addresses or hostnames.

PROXY_SERVER

Runs the HTTP Listener as a proxy server. The valid values are:

0 - Proxy server for the HTTP protocol is off.
1 - Proxy server for the HTTP protocol is on.

The default value is 0.
**Procedure: How to Configure a SOAP Listener**

A SOAP listener needs to be configured before it will appear in the Special Services and Listeners folder.

1. From the menu bar, select *Workspace*.
2. Right-click the *Special Services and Listeners* folder, and select *New*, then *SOAP*.

![Listener Configuration page](image)

The Listener Configuration page opens.

3. Enter values in the *PORT* and *HOST* fields.
4. Optionally, enter a host or IP address that will be accepted by listener in the *RESTRICT_TO_IP* field.
5. Click Save and Restart Listener. The SOAP listener is added to the Special Services and Listeners folder.

**Other Listener Options**

<table>
<thead>
<tr>
<th>How to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the Servlet</td>
</tr>
<tr>
<td>Refresh the WebFOCUS Jar Files</td>
</tr>
</tbody>
</table>

The Listener right-click menu also enables you to configure the servlet and refresh the WebFOCUS jar files.

**Procedure: How to Configure the Servlet**

1. From the menu bar, select **Workspace**.
2. Open the **Special Services and Listeners** folder in the navigation pane.
3. Right-click **TCP/HTTP** and select **Configure Servlet**. The Configure Servlet page opens.
4. Enter the path to your Java Development Kit in the **JDK_HOME** field or click or click the selector button (…) and navigate to it.
5. Optionally, you can elect to register the JDK by selecting y from the **Register JDK_HOME** drop-down menu.
6. Enter the string that uniquely identifies the servlet and is a part of the URL allowing access to the servlet in the **Context PATH** field. The default value is ibi_apps.
7. Click **Configure**.

**Procedure: How to Refresh the WebFOCUS Jar Files**

1. From the menu bar, select **Workspace**.
2. Open the **Special Services and Listeners** folder in the navigation pane.
3. Right-click **TCP/HTTP** and select **Refresh WF jar files**. The Copy server related java components into WF installation directory page opens.
4. Enter the path to the jar files in the **IBI_Repository_Root_Directory** field or click the selector button (…) and navigate to it.
5. Click **Refresh WF jar files**.
Note: After copying the files, the application server will need to be restarted.
Listeners
The Web Console enables administrators to access several diagnostics tools that can be used to visualize different internal information. The following section describes the pages used to access such information to perform problem analysis tasks.

**Topics:**
- Viewing Version Information
- Analyzing Server Activity
- Analyzing FOCUS Database Server Activity
- Tracing Server Activity
- z/OS-Specific Troubleshooting for the Unified Server
- z/OS-Specific Troubleshooting for z/OS HFS Deployment
- Recording and Reproducing User Actions
- Troubleshooting the Console
- Server Processes
- Gathering Diagnostic Information for Customer Support Services
Viewing Version Information

**How to:**
Access Version Information on the Web Console

The Version information page displays the main identification parameters of the Server configuration that was in effect when the Server was started.

**Procedure: How to Access Version Information on the Web Console**

On the Web Console menu bar, click Help, then select Version. The Version pane opens.

The following information is displayed:

**General**

- **Configuration Date**
  Indicates the configuration date of the Server.

- **Build date**
  Identifies the build.

- **Gen number**
  Identifies the gen.

**Release**

- **Source date**
  Identifies the source date.

**Extended**

- **WF jar seq number**
- **WF jar release**
  Provides jar-related information.

- **Build system**

- **Support System**
  Build-related and system-related information.
C Compiler
C Version
Identifies the C compiler and version.

Ajax Framework
identifies the Windows version.

Host Name
Name of the machine where the Server is installed.

Server Name
As defined in the configuration file.

Note: Used on Windows platforms as the system service name for the Server.

Analyzing Server Activity

How to:
Access the Server Log Files
Display the Live EDAPRINT Log File
Open a Copy of the EDAPRINT Log File
Set Workspace Log Properties to Control the Edaprint Log
Filter the Server Log

Reference:
Controlling EDAPRINT History

You can use the Server Log pane in the diagnostics section of the Web Console to view the current or prior server activity log (edaprint.log) from either a management perspective (Session and Connection activity) or a raw version of the log with or without filtering for certain components and IDs. By default, the Server Log chronologically records all server activity from the time the Workspace Manager was started. It contains basic activity information, as well as server start up information and IBISNAP and shutdown information. IBISNAP is a snapshot of the server environment showing various usage statistics, CPU and server times for each data agent connection, and listener and agent status. If an abend occurs, the snapshot contains additional debugger stack information that aids the Customer Support Services staff in determining the problem.

You can view the first 50,000 lines of the log file from the Web Console. If you wish to view lines beyond 50,000, you can open or save the file in a text editor.
Procedure: How to Access the Server Log Files

1. From the menu bar, select Workspace.
2. Expand the Logs and Traces folder in the navigation pane.
3. Right-click Workspace Logs and select View.
   The Workspace Logs page opens.

4. Right-click hliprint.log and select View
or
Right-click edaprint.log and select a report type:

- Full Report has View and Open or Save options.
- Connection Report has Detail, Summary and Graph options.
- Page Hit Report has Detail and Summary options.

The log opens in the right pane.

Procedure: How to Display the Live EDAPRINT Log File

To display the live EDAPRINT log file:
1. From the main menu, select *Workspace*.

2. Right-click the *Workspace* folder and select *Live Console*, as shown in the following image.

![Image showing the selection process](image)

The EDAPRINT log opens in a separate browser tab, as shown in the following image.
You can also access the live EDAPRINT log by selecting Live Console from the Monitor section of the ribbon, as shown in the following image.

![Live Console Monitor](image)

**Note:** This option is only available when using a Firefox or Chrome browser.

**Procedure: How to Open a Copy of the EDAPRINT Log File**

To open a copy of the EDAPRINT log:

1. From the Web Console, click **Workspace**.

2. From the ribbon, click the **Current Workspace Log** icon, or right-click the **Workspace** folder in the navigation pane, and select **Current Workspace Log**.

Your browser will ask whether you want to open or save the file. If you choose open, the file will open in your default text editor.

**Procedure: How to Set Workspace Log Properties to Control the Edaprint Log**

The Workspace Log Properties page controls both the edaprint log and event routing email. For information on event routing email, see **Setting Workspace Log Properties for Event Routing** on page 436.

1. From the menu bar, select **Workspace**.
2. Open the *Logs and Traces* folder.

3. Right-click *Workspace Logs* and select *Properties*.

   The Workspace Logs Properties page opens, as shown in the following image.

![Workspace Logs Properties](image)

4. Enter or select values for the EDAPRINT parameters.

   The EDAPRINT parameters are:

   - **edaprint_history**
     
     Defines the number of saved edaprint.log files to keep. Valid values are 0-99. The default value is 5.

   - **edaprint_max_lines**
     
     Defines the maximum number of lines in an edaprint.log before it is archived, and a new edaprint.log is started. The default value is 0, which means unlimited.

   - **edaprint_max_days**
     
     Defines the maximum number of days from the time the server is started before an edaprint.log is archived and a new edaprint.log is started. The default value is 0, which means unlimited.
**Note:** A new edaprint.log file will only be created after the edaprint_max_days value has been exceeded, and a connection event has occurred. For example, if the server is idle, the new edaprint.log file will not be created until a connection request is received.

**edaprint_ipname**

Defines whether the server should convert IP host addresses to names. It requires DNS lookups. The default value is \( n \).

5. Click **Save and Restart Server**.

**Procedure: How to Filter the Server Log**

1. From the menu bar, select **Workspace**.
2. Expand the **Logs and Traces** folder in the navigation pane.
3. Right-click **Workspace Logs** and select **Filter**.
   
The EDAPRINT Log Filter page opens.
   
   Select an option from the Select Filtering drop-down menu.

4. Click **Set Filter**.
5. If you choose Filter by Category, the following page opens. Set your filtering parameters and click Set Filter. For any item, clicking the check box without an entry in the input box filters on all items of that type. If you also enter a specific value in the input box, that filter will be executed. (For example, you can request filtering on all users, which defaults to *, or an individual user.) You can combine items from the list, mixing all items of a type with specific items, as needed.

![EDAPRINT Log Filter](image-url)

- Any Error
- Any Warning
- Warning (Unauthorized Access or Rejected)

Use the asterisk character (*) as a wildcard

- User ID (user)
- Group (group)
- Role (role)
- Process ID (pid)
- TSCOM ID (tscomid)
- Session ID (sesid)
- Client Session ID (session)
- JSOCOM ID (jscomid)
- Service name (svc)
- HTTP connection ID (cmrphc)
- TCP connection ID (cmripip)
- Deferred connection ID (cmrpdf)
- Deferred file ID (did)
- Search for a string (grep)
6. If you choose *Filter by Timestamps*, the following page opens. Enter From timestamp and To timestamp information and click *Set Filter*.

![EDAPRINT Log Filter](image)

7. Right-click *Workspace Logs* and select View.
   
The Workspace Logs page opens.

8. Right-click *edapring.log* and select a report type.

**Reference: Controlling EDAPRINT History**

The size of the server activity log, the number of files archived in the EDAPRINT history, and the maximum number of days each edaprint.log is maintained before it is archived and a new edaprint log is started are controlled by *edaprint_max_lines*, *edaprint_history*, and *edaprint_max_days*, respectively.

Limit the size of each log file by setting the maximum number of lines to a value other than zero. There is no minimum, but the recommended value is at least 1000 lines. If the limit is too low and the system is too fast (such that two archived files can have the same file system time stamp to the same second), whichever of the archived files is deleted first is undefined.
The first log file for each server start always contains more lines than the maximum because the count begins only after the edaplog process is created, thus it is larger by the size of the startup information. Each time the limit is reached, the current log file is archived and the new file starts with an additional identification line. This line indicates the rank of the file in the series of continuation files, and a reference to the archived name of the first file in the series (the one with the startup information), in a format similar to the following:

`continuation #n of edapiNN`

The number of files kept archived is determined by setting the edaprint_history parameter to the maximum number of edapiNN.log files. Each time the server is restarted or the current log reaches maximum size, the previous edaprint file is moved to edapiNN.log, and the maximum number of files is enforced by deleting the oldest files. The effective minimum number of files kept may be as high as 2 in addition to the current edaprint.log, even if edaprint_history was set to 0 or 1 because when files are split to respect edaprint_max_lines, the most recent file and the most recent file containing startup information are always preserved.

### Analyzing FOCUS Database Server Activity

**In this section:**

- Controlling the HLIPRINT Transaction Log
- Controlling HLIPRINT Output

FOCUS Database Server (FDS) is a listener that enables multiple users (or multiple agents) to update central a FOCUS database simultaneously. Database transaction events are logged to the HLIPRINT log file (hliprint.log), which is created in the server directory.

You can view the first 50,000 lines of the log file from the Web Console. If you wish to view lines beyond 50,000, you can open or save the file in a text editor.

### Controlling the HLIPRINT Transaction Log

**How to:**

Control the Size of the HLIPRINT Log From the Web Console

You can control the size of the HLIPRINT transaction log by using the hliprint_max_lines parameter in the configuration file, edaserve.cfg. The parameter defines the maximum number of lines to be included in hliprint.log before it is archived and a new hliprint log is started.
Each time the line limit is reached, the current HLIPRINT log file is archived to HLIPRI01 and the new file starts with an additional identification line. This line indicates that the file was truncated and looks like the following:

continued from hlipri01

Archiving also takes place the first time the FDS listener is activated and the HLIPRINT log from the previous run is found in the server directory.

**Procedure: How to Control the Size of the HLIPRINT Log From the Web Console**

1. From the menu bar, select *Workspace*.
2. Expand the *Special Service and Listeners* folder in the navigation pane.
3. Right-click *FDS*, and select *Properties*.
   
   The Special Services Configuration page opens.

4. Expand the *Advanced* section by clicking the arrow.

5. Enter a value for:

   *hliprint_max_lines*

   Is the maximum number of lines to include in the hliprint.log before it is archived and a new hliprint log is started. You can limit the size of the log file by setting the maximum number of lines to a value other than zero. (0 means an unlimited number of lines can be included in the file.)
There is no minimum, but the recommended value is at least 1000 lines. If the limit is too low, the FDS listener may experience performance problems due to excessive archiving.

6. To register this setting, click Save.

**Controlling HLIPRINT Output**

The Server Administrator can control hlprint.log output by manually adding the EDAHLIP variable, with a value, to the edaserv.cfg file, in the form edahlip=value where valid values are:

- **none**
  
  No hlprint.log is created. Turning logging off will increase performance, however, this is not recommended, because it makes it harder to diagnose problems.

- **echo**
  
  The hlprint.log is created and contains basic transaction information (one line per transaction; line length 80 characters).

- **stat**
  
  The hlprint.log is created and contains basic transaction plus timing information (one line per transaction; line length is 133-characters).

The default value is stat.
Tracing Server Activity

In this section:
Configuring Traces
Filtering Traces
Showing the Session Log

How to:
Access the Last Agent Trace

Reference:
SET TRACEUSER Commands

You can activate traces at server startup or while the server is running. Information Builders recommends starting the server with traces active so that a full set of traces can be sent to Customer Support Services to help diagnose issues that arise. If you need to contact Customer Support Services for assistance, you can use a facility called savediag to expedite the transmission of server information. For details about using savediag, see Gathering Diagnostic Information for Customer Support Services on page 616. Refer to the Installation manual for your platform for more information on starting the server with traces active.

To activate traces for a running server, a server administrator can quickly enable or disable traces at any point in a work process by clicking Workspace, Enable (or Disable) Traces from the Web Console menu bar.

The server administrator can use the Web Console to initiate and control a wide range of traces, and dynamically turn traces on or off for a running server. To see a list of traces, select Workspace from the menu bar. Open the Logs and Traces folder on the navigation pane, right-click Traces, and select View.
The Web Console displays the following list of traces: Workspace Manager, Data Services, Java Services, Special Services, Listeners. (The traces that are active varies depending on the types of requests that have been made against the server.)

### Traces

<table>
<thead>
<tr>
<th>Type</th>
<th>File Name</th>
<th>Size (KB)</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace Manager</td>
<td>edaph.trc</td>
<td>58</td>
<td>2010/05/18 12:47:32</td>
</tr>
<tr>
<td>Workspace Manager</td>
<td>edarqmon.trc</td>
<td>5</td>
<td>2010/05/18 12:47:32</td>
</tr>
<tr>
<td>Workspace Manager</td>
<td>edaplog.trc</td>
<td>83</td>
<td>2010/05/18 12:47:37</td>
</tr>
<tr>
<td>Workspace Manager</td>
<td>edaplogw.trc</td>
<td>89</td>
<td>2010/05/18 12:47:37</td>
</tr>
<tr>
<td>Workspace Manager</td>
<td>edaphcp.trc</td>
<td>15</td>
<td>2010/05/18 12:47:30</td>
</tr>
<tr>
<td>Workspace Manager</td>
<td>edapdfm.trc</td>
<td>9</td>
<td>2010/05/18 12:47:08</td>
</tr>
<tr>
<td>Data Services</td>
<td>ts000011.trc</td>
<td>6155</td>
<td>2010/05/18 12:47:30</td>
</tr>
<tr>
<td>Java Services</td>
<td>jscom3_1.trc</td>
<td>3</td>
<td>2010/05/18 12:47:32</td>
</tr>
<tr>
<td>Java Services</td>
<td>jscom3_1_l.trc</td>
<td>0.133</td>
<td>2010/05/18 12:47:08</td>
</tr>
<tr>
<td>Listeners</td>
<td>ht000115.trc</td>
<td>1046</td>
<td>2010/05/18 12:46:50</td>
</tr>
<tr>
<td>Listeners</td>
<td>ht000117.trc</td>
<td>65</td>
<td>2010/05/18 12:46:50</td>
</tr>
<tr>
<td>Listeners</td>
<td>ht000118.trc</td>
<td>22</td>
<td>2010/05/18 12:47:02</td>
</tr>
<tr>
<td>Listeners</td>
<td>ht000119.trc</td>
<td>1539</td>
<td>2010/05/18 12:47:06</td>
</tr>
<tr>
<td>Listeners</td>
<td>ht000120.trc</td>
<td>925</td>
<td>2010/05/18 12:47:13</td>
</tr>
<tr>
<td>Listeners</td>
<td>ht000121.trc</td>
<td>324</td>
<td>2010/05/18 12:47:16</td>
</tr>
</tbody>
</table>

Right-clicking a trace displays the follow options:

- **View.** Displays the trace in the right pane.
- **Open or Save.** Enables you to open the trace in a local editor or to save it to a local disk.
- **Delete.** Enables you to delete the selected trace file. On Windows, a trace file cannot be deleted if it is still in use by a process.

Note that the selected trace file is displayed with any active filtering applied.

Once traces have been configured and turned on by a server administrator, they can be viewed by application administrators and server operators.

**Procedure:** How to Access the Last Agent Trace

To access the last agent trace:

1. From the menu bar, select **Workspace**.
2. From the ribbon, click Last Agent Trace icon, or the right-click the Workspace folder in the navigation pane, and select Last Agent Trace.

The last agent trace opens.

Reference: **SET TRACEUSER Commands**

If you want to turn dynamic traces on or off for one user, you can include the command SET TRACEUSER={ON|OFF} in a user profile or in an individual procedure.

You can also use the SET TRACEUSER=tracename command turn dynamic traces on and send the trace to a named file. The file must specify a .trc extension and use a full path name for server traces so the traces are retained after server execution.

**Configuring Traces**

**How to:**

Configure Traces

**Reference:**

Limiting the Size of a Trace File
Displaying Microseconds in Trace Timestamps

You can configure traces to limit their size and select the components to activate.

**Procedure:** **How to Configure Traces**

1. From the menu bar, select Workspace.

2. Open the Logs and Traces folder on the navigation pane, right-click Traces, and select Configure.
The Traces Configuration page opens.

3. Optionally, set the trace size limit to a specific number of lines. After the limit is reached, trace data is dumped to an alternate file with the extension TRB. Logging continues into the trace file with extension TRC. For related information, see Limiting the Size of a Trace File on page 589.

A blank entry indicates no trace size limit.

4. Select an option from the Choose the trace components to activate drop-down menu. The selections you make here are written into a file called ibitrace.fex. The settings take effect on the next server start/restart.

Note that Customer Support Services may request that you change from the default trace setting to a custom setting to facilitate their research.

**Default Components**

- R1H
- QOPSYS
- PRH
- NWH
- NLS

**All Components**

- All traceable server components.
**Typical Components**

- CEH
- NWH2
- PRH
- SQLAGGR
- STMTRACE

**Custom Components**

This option allows you to select the specific components to activate.

The components are categorized as follows (each category has a list of trace options within it):

- COMMAND PROCESSING
- COMMUNICATIONS and SYSTEMS
- COMMON ADAPTER LAYERS AND SERVICES
- SQL TRANSLATOR
- SQL DATA ADAPTERS
- OLAP DATA ADAPTERS
- NON-SQL DATA ADAPTERS
- LEGACY DATA ADAPTERS
- REPORT SERVICES
- NLS SERVICES
- ODIN INFORMATION
- SMART MODE
- MAINTAIN PROGRAMMER TRACES
- MAINTAIN INTERNAL SERVICES
- MISCELLANEOUS SERVICES
- TRANSACTION COORDINATOR
- XFOCUS
- USE-WHERE
5. Click the Save or Save and Restart Server.

**Tip:** If you wish to restore default settings or choose typical settings, select these options, then click Save Settings. The selected group will be checked when you reopen the Custom Components list.

**Reference:** Limiting the Size of a Trace File

You can use set the size limit of the trace files. The trace size limit specifies the maximum number of lines in the trace files. The value is written into the IBITRACE.FEX file as SET TRACESIZE = value and requires a server restart to activate. After the size limit is reached for a particular trace, the trace data is redirected to an alternate file with an extension of .TRB. When the size limit is reached in the .TRB version of the file, then writing resumes with the .TRC version of the file.

A trace cycles between the two matched sets of files to alleviate maxing out a disk drive with large individual traces. Each cycle starts a fresh file (versus an append). If there are intermediate traces that need to be saved, it is up to the site to monitor and implement specific methods to save traces based on their needs and capabilities. For example, copying to an archive disk or secondary machine and possibly using compression.

The SET TRACESIZE=# setting must be used in conjunction with a SET TRACEON= value. If the IBITRACE.FEX file is changed or created using an editor, ensure that there is also a SET TRACEON=value setting. The existence of the IBITRACE.FEX file only sets what is traced when tracing is active, but does not control if tracing itself is active.

**Reference:** Displaying Microseconds in Trace Timestamps

Displaying microseconds may be useful if trying to match very precise event times between traces or study the performance of specific events when multiple events occur within a given second on a normal trace.

The setting syntax is SET TRACESTAMP=TLEFT and may be used in a focexec to activate in a specific trace or in the IBITRACE.FEX file to activate at server start.

There is no Web Console feature on the Trace Configure page to activate TRACESTAMP in IBITRACE.FEX, but the line can be added by opening the Configuration Files folder in the Web Console and using the edit against the Trace Profile object.

The SET TRACESTAMP=TLEFT setting must be used in conjunction with a SET TRACEON= value. Always ensure that there is also a SET TRACEON=value setting in the IBITRACE.FEX file when editing. The existence of the IBITRACE.FEX file only sets what is traced when tracing is active, but does not control if tracing itself is active. The SET TRACESTAMP=TLEFT feature also negates the ability to properly use Web Console Trace Filtering for specific events, do not using filtering with this feature active.
Filtering Traces

**How to:**

- Filter Traces
- Capture Traces in a Script File

Filter allows you to limit the types of errors or components that are included in the traces.

**Procedure: How to Filter Traces**

1. From the menu bar, select **Workspace**.
2. Open the *Logs and Traces* folder on the navigation pane, right-click **Traces**, and select **Filter**.
   
The Traces Filter page opens.
3. Select an option from the **Trace components to filter** drop-down menu:
   - **No Filtering** (the default) displays all trace information.
   - **Errors** displays only errors, crashes, errno, abort, or fail conditions.
   - **Typical Components** displays trace information from typical components.
   - **Custom Components** displays trace information from components which you select.

4. Click **Set Filter**. The filters take affect when you enable and run traces.
Procedure: How to Capture Traces in a Script File

Capturing traces in a script file enables you to isolate server problems. Specifically, you can enable this type of custom trace, then reproduce the problem and capture the input commands issued from a front-end tool (such as WebFOCUS Developer Studio) to the server. Customer Support Services can then isolate debugging for the server only, instead of having to recreate a whole complex environment.

1. From the menu bar, select *Workspace*.
2. Open the *Logs and Traces* folder on the navigation pane, right-click *Traces*, and select *Configure*.
3. Select *Custom Components* from the *Trace components to filter* drop-down menu.
4. Click the *Unselect All* button.
5. Choose *AJ - NWHSIM/1* under Communications and Systems.
6. Click *Set Filter*.

The trace setting will be active the next time the server is started.

Showing the Session Log

In this section:
- Changing the Size of the Session Log Buffer

How to:
- Change the Size of the Session Log Buffer
- Show the Session Log
- Show the Log for a Web Session

The Session Log records the activity that takes place between the current Web Console session and the server. For example, when a procedure or DataMigrator job is run, the Session Log records the WebFOCUS code and SQL statements that are sent from the console to the server for execution on the server.

The log also records the response that the server returns, in addition to the answer set, such as error messages and informational messages.

Changing the Size of the Session Log Buffer

By default, the Session Log holds 500 lines. You can increase or decrease the number of lines.
**Procedure:** How to Change the Size of the Session Log Buffer

1. From the menu bar, select *Workspace*.
2. In the navigation pane, right-click the *Workspace* folder, and select *Miscellaneous Settings*.
3. On the Miscellaneous Settings page, locate the `seslog_max_lines` field, and type the number of lines to assign to the buffer for the Session Log.
In the following image, the value for seslog_max_lines is set to 750.

4. Click Save. You do not need to restart the server for the new setting to take effect.
Procedure: How to Show the Session Log

1. On the Web Console menu bar, click the Show Session Log Window icon, as shown in the following image.

Tip: After you open the Session Log, the Show Session Log Window icon disappears from the menu bar. When you hide the Session Log, as described in step 6, the icon reappears.

A small pane opens near the bottom of the window, similar to the one shown in the following image.

2. Click the Maximize button at the upper-right of the pane to enlarge it.

3. Click the Refresh button on the left of the Session Log menu bar to display the current contents of the log.

4. Optionally, click the Filter drop-down list to select only those commands or data that you want to include in the Session Log. You can select:

- Focus, to display WebFOCUS commands sent to the server for execution.
- Sql/mdx, to display SQL or MDX code that is generated by an adapter and sent to a relational database or OLAP database, respectively.
- Transform, to display the result of transforming the user-supplied code in a procedure, into WebFOCUS code that is supported on the server. This option is useful for DataMigrator jobs that require transformation.
- Errors, to display error messages returned from the server.
- Messages, to display informational messages returned from the server, for example, NUMBER OF RECORDS IN TABLE, SVG FILE SAVED, and others.
Timestamp, to display the date and time at which a command or message was exchanged. For example, if you select Errors and Timestamp, the Session Log displays the time at which an error message was returned from the server.

No Delay, to display the Session Log while a request is still running, not after it has finished running. This option is recommended for long-running requests.

In the following image, the check boxes for Focus, Messages, and Timestamp are selected to include the display of WebFOCUS commands and messages, and to include the date and time of each entry in the log.

When you filter the Session Log, its contents automatically refresh to reflect the last criterion that you specified.

5. Optionally, you can do one of the following:

- Click the Clear Messages button on the left of the Session Log menu bar to remove the current contents of the log.

- Click the Refresh button on the left of the Session Log menu bar to update the log.

- Use standard editing functions, such as:
  - Ctrl+A, Ctrl+C, and Ctrl+V to select all the contents of the log, copy it, and paste it into another file.
  - Ctrl-click to highlight a line.
  - Shift at the beginning of a block of lines, and Shift-click at the end of the block of lines, to highlight the lines.

6. When you have finished reviewing the messages in the Session Log and want to close it, click Hide on the right of the Session Log menu bar.
How to Show the Log for a Web Session

Procedure: You can display a log of the activity that takes place in an individual Web Session.

1. From the menu bar, select Workspace.
2. From the ribbon, click the Web Sessions icon, or expand the Special Services and Listeners folder in the navigation pane, right-click HTTP, and select Web Sessions.

The Performance Report for all Web Sessions is displayed.

3. On the report, right-click a row for an individual Web Session, and from the menu, click View Session Log.

The log for the selected Web Session opens, as shown in the following image.

### Session Log
Log for Web Session 3

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/21/2010 10:26:32</td>
<td>Focus</td>
<td>? FOCUTL</td>
</tr>
<tr>
<td>03/21/2010 10:26:32</td>
<td>Focus</td>
<td>END</td>
</tr>
<tr>
<td>03/21/2010 10:26:32</td>
<td>Focus</td>
<td>TABLEF FILE _EDAHOME/CATALOG/SYSAPPS</td>
</tr>
<tr>
<td>03/21/2010 10:26:32</td>
<td>Focus</td>
<td>PRINT APPNAME APPFULL DIRPAR APPNLMAP APPACCMA APPEXEC APPDESC APPLOC ALTLOC</td>
</tr>
<tr>
<td>03/21/2010 10:26:32</td>
<td>Focus</td>
<td>WHERE (ALIST NE 0) AND (APPNLMP NE 0) ;</td>
</tr>
<tr>
<td>03/21/2010 10:26:32</td>
<td>Focus</td>
<td>ON TABLE PCHOLD FORMAT COMT FORMATTED</td>
</tr>
<tr>
<td>03/21/2010 10:26:32</td>
<td>Focus</td>
<td>END</td>
</tr>
</tbody>
</table>

z/OS-Specific Troubleshooting for the Unified Server

### In this section:
- Server Traces and Saved Diagnostics on the Unified Server
- U4039 Abends on the Unified Server
- System Dumps on the Unified Server
- Freeing Data Sets Allocated to the Server on the Unified Server

If you are working in the z/OS environment, you should be aware of several diagnostic techniques that are described in this topic.

### Server Traces and Saved Diagnostics on the Unified Server

To generate a server trace:
1. Turn tracing on from the Web Console or by issuing the MODIFY operator command:

   F <iway_server_jobname/started task>, -traceon

2. Alternatively, on HFS you can run the ITRCON JCL member.

3. Reproduce the problem.

4. Submit the ISAVEDIA member to produce the diagnostic information.

For PDS deployment, diagnostic information is generated at the JES log output of the server.

For HFS deployment, a directory called $dnnnnnnn is created under your configuration directory (for example, /ibi/server53/ffs/sd123456). Diagnostic information is placed in this directory. Verify that you have access to this directory.

Do not change anything in the EDAENV DD statement, as changes could prevent the correct information from being copied to your directory.

**U4039 Abends on the Unified Server**

In some instances, the server may abend with a U4039 code. This is a generic abend.

**Solution:** Determine what caused the abend by checking the file, SYSOUT DDname and the MVS system log. If you suspect this is a bug, follow the instructions in *z/OS-Specific Troubleshooting for the Unified Server* on page 596 and *System Dumps on the Unified Server* on page 597 in order to collect information to send to Information Builders support.

**System Dumps on the Unified Server**

To generate a system dump:

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 abendaid from intercepting the dump, add:

   //ABNLINCR DD DUMMY
5. To prevent 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).

Freeing Data Sets Allocated to the Server on the Unified Server

**How to:**
Free a Data Set From the MVS System Console

**Example:**
Freeing the Allocated Data Set

A z/OS operator can issue modify commands 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.

**Syntax:**  How to 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 dsname (all occurrences in the server):

\[ F <iway_server_jobname/started task>,DYNAM FREE DA <dsname> \]

To free multiple DDNAMES, passing a pattern (free all ddnames staring with AB):

\[ F <iway_server_jobname/started task>,DYNAM FREE FI AB* \]

To free a multiple dsname (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 JESMSGLG indicating if the command was processed successfully or not.

success:

\[ @DYNAM COMMAND SUCCESSFULLY PROCESSED Rc=0 \]

failure:

\[ @DYNAM ERROR: IKJ56225I DATA SET IWAY.TEST ALREADY IN USE, TRY LATER \]
Once the data set is freed and the batch utility runs, the operator can reallocate the data set to the server, using the same modify command, but this time issuing DYNAM ALLOC, instead of DYNAM FREE.

**Example:**  **Freeing the Allocated Data Set**
Suppose ISTART JCL (jobname IWAYP) has the following allocation:

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

The operator can free this file using the command (from MVS console):
```
F IWAYP,DYNAM FREE VSAMFILE
```

Later, after the batch utility runs, the operator can re-allocate the file to the server by issuing the command:
```
F IWAYP,DYNAM ALLOC F VSAMFILE DA VSAM.FILEA.CLUSTER SHR REU
```

All valid DYNAM ALLOC and DYNAM FREE syntaxes are supported. For more information on DYNAM command, please refer to the appropriate WebFOCUS manual.

**z/OS-Specific Troubleshooting for z/OS HFS Deployment**

**In this section:**
- Recovering Orphaned Shared Memory Segments on z/OS
- INSUFFICIENT AUTHORITY TO GETPSEND Messages on z/OS

The troubleshooting techniques described in this sections are available for a z/OS HFS deployment.

**Recovering Orphaned Shared Memory Segments on z/OS**

When the server is restarted after an abend, an orphaned shared memory segment is often found. A server start will try to clear the memory segment so that it may continue the start process. The accompanying error message (which also displays even if the server self-recovers) is:

```
Shared memory remains but WSM process is gone
```
Self-recovery is often successful and the message may be ignored. However, if the server still fails to actually start, you can use manual commands to find and remove the shared memory. The associated directory location that is used as the shared memory key will not actually be available until a machine IPL. To avoid waiting for a machine IPL, you can set EDASHARE manually in ISSTART EDAENV DD and the ISTOP JCL to point at a new directory location.

1. To display the orphaned memory objects, issue the command:
   
   IPCS M -X

2. To remove the orphaned memory objects, issue the command:
   
   IPCRM M

   IPL will eliminate the orphaned shared memory segment.

3. If you cannot IPL the machine, temporarily add the following EDASHARE setting (with the client directory path) to the ISTART EDAENV DD.

   000050 //EDAENV DD *
   000051 TZ=EST5EDT
   000053 EDASHARE=/ibi/srv77/ffs/web

   where:

   web

   Is a newly created directory. It can be any name.

   This will point the server to a new directory to be used as the shared memory segment key.

   This syntax should also be added to the ISTOP JCL, but should be removed from both JCLs after IPL.

***INSUFFICIENT AUTHORITY TO GETPSEN T Messages on z/OS***

INSUFFICIENT AUTHORITY TO GETPSEN T messages may appear in JESLOG. For more information about what causes these messages, see the IBM APAR II11813.

The APAR recommends issuing one of the following RACF commands to work around this problem:

```plaintext
SETOPTS 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:

```plaintext
ICH408I USER(default) GROUP(dgltgprp) NAME(bpxdefaultuser) 060 CL(PROCACT ) INSUFFICIENT AUTHORITY TO GETPSEN T
```
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.

Recording and Reproducing User Actions

**How to:**
- Configure Your Browser to Use the Reporting Server as a Proxy Server
- Stress Test Server Performance
- Refresh or Remove Script Directories
- Display Percentile Statistics in Results

**Reference:**
- Parameters for Playback of HTI Script Files
- Additional Recording Hints
- Playback Files

You can use the Web Console Record and Playback tools to record an exact sequence of user actions applied through a browser, and then reproduce it (play it back) to evaluate server response times in an environment that simulates single or multiple users under the same or different conditions. Files generated by record and playback, known as HTI scripts (HTTP internal scripts), are stored in the scale directory of the server (parallel to APPROOT). The file name can be edited before recording starts. These scripts, along with server traces, are used for testing and analysis of problems.

Record/Playback is an iterative process in which you can repeat your tests under varying conditions until you achieve the throughput and response time you require.

**Tip:** It is often useful to employ two browser windows for stress testing using the Record/Playback tool, one to turn the recording on and off and enter playback parameters, the second to capture the actions you wish to record. (Note that if you do not use two sessions, you will have to edit the request being stressed to remove the record/setup actions.)

In order to be able to capture these actions, you must properly configure your LAN setting. Here is an overview of the steps:

1. Set your browser to use the Reporting Server as a proxy server. This will allow you to capture user actions in a web browser. For details, see *How to Configure Your Browser to Use the Reporting Server as a Proxy Server* on page 602.
2. Start the script recording.
3. Run the request you want to test.
4. Stop the recording. You will be able to reuse this script with varying test conditions.
5. Play back the script you recorded, setting stress parameters, such as the number of threads (simulated users) and the intervals at which the request will be run.
6. Evaluate server performance using the Playback log, the output (.hto) files generated by the test, and stress test performance reports.
7. Repeat steps 2-7 as many times as necessary to simulate and evaluate the conditions you want to test.

**Note:** The Report/Playback feature is not currently supported on the PDS Deployment Server. Therefore, options are disabled on the Web Console.

**Procedure: How to Configure Your Browser to Use the Reporting Server as a Proxy Server**

When using an Reporting Server as a proxy, you can record user actions that are directed to any web site. In order to be able to record the sequence of actions that a user will complete using the browser, you must first enter the proper LAN settings.

1. From the Internet Explorer toolbar, select **Tools** and then **Internet Options** from the browser menu bar.
2. Select the Connections tab, then click the **LAN Settings** button. The Local Area Network (LAN) Setting window opens.
   **Tip:** Before you make the required changes, note your standard settings. You will want to revert to them later.
3. Click the **Use a proxy server for your LAN** check box.
4. Enter the host name in the Address box. (This identifies the machine on which the client software is installed.)
5. Enter the port number for which the client is configured.
6. Click **OK** to return to the Internet Options window.
7. Click **OK** again to complete the task.

Leave the browser open since you will use it to display the Web Console.
**Procedure: How to Stress Test Server Performance**

The simplest way to record an HTI script is by running a stress test on a procedure. For information, see *How to Run a Stress Test* on page 407.

1. From the menu bar, select the $W$ icon, then *Scalability*.

   ![Scalability tree](image)

   The Scalability tree opens in the navigation pane.

2. Right-click the *Scalability* folder and select *New*, and then *Recording*.

   ![Recording](image)

   The Playback of HTI Script files pane opens.
3. Click **New**, then **Recording** on the expanded menu bar to open the Recording of HTI Script File pane, where you can specify a script name and the directory in which you want to store it.

![Recording of HTI Script File](image)

A default directory name appears in the Script Directory drop-down list. You can use the default name, edit it, or choose an existing directory from the list.

4. Enter a script name or use the default name. This is the name of the file that will contain the script.

5. By default, a new HTI script is generated when you start a recording session. Click the **Append to Existing** check box if you prefer to append a recording to the existing HTI script.

6. By default, the recording captures all user actions. Click the **Do not record requests to get css, js, gif, bmp, jpg, class, jar, or png files** if you wish to exclude requests for these operations from the recording.

7. Before you start the recording, you must get into position to execute the set of actions you want to test. Open a second browser and ensure that the correct LAN setting are in effect. (For details, see *How to Configure Your Browser to Use the Reporting Server as a Proxy Server* on page 602.)

8. Return to the first browser window, where the Recording of HTI Script pane is still open, and click **Start** to begin recording.

9. Return to the second browser window and perform the actions you wish to record.

10. When you have captured all of the required actions, return to the first browser window, where the first the Recording of HTI Script pane is still open. Click **Stop** to end the recording.
11. Click the Refresh icon on the navigation pane to display the new directory and script.

12. Since you have completed the recording task in the second browser window, it is a good idea to remove the LAN setting you entered expressly for this purpose. (For more information, see How to Configure Your Browser to Use the Reporting Server as a Proxy Server on page 602.) You can now close this window.

13. You are now ready to perform your stress tests. From the Playback folder in the navigation pane, expand the Individual Tests folder, expand the script directory you named in step 3, and click the script name you entered in step 4.

14. Choose Start from the menu. The Playback of HTI Script Files pane lists the available test parameters.

You can choose basic and advanced test options from the Playback of HTI Script Files pane. For details about these options, see Parameters for Playback of HTI Script Files on page 609.

For example, you might wish to perform a stress test twice with the following conditions:

Test 1: Use the default Number of Threads (1) to simulate one user and the default Interval Parameters (.5) second to indicate how often you want the request to run. Enter a Test Description, such as Baseline with one user, to be able to distinguish among the tests. Click the Advanced tab and accept the default format of one file per thread. (In this case, you are only testing one thread.)

Click Start to run the test.

Test 2: Set Number of Threads to 30 to see how performance would be affected if 30 users ran the request simultaneously (with a given number of agents that may or may not be less that 30). This setting is key to stress testing. Adjusting the number of threads allows you to assess how many requests the server will be able to handle at a given point in time. Increasing the number of threads puts more load on the server(s). In practice, users may want to start out with a smaller or larger number depending on their installations. Keep the Interval Parameters as .5 seconds. Enter Sample 30 Users as the Test description.

Click the Advanced tab. This time select one file per request (rather than per thread) in the Results field and set the Keep alive parameter to 30 to indicate how long, in seconds, you want the script to run. This option enables enough statistics to be generated to make a comparison among server response times. (You may need to try different settings to find the optimal length of time to run the script.)

Click Start to run the test.
In each case, two files are stored in the ibi/scale/performance directory:

- A summary log is displayed in a separate window. The log provides information about the number of threads that ran (indicated by thread=), the number of requests serviced (indicated by request=), how long it took to service each request (indicated by resp=), and the time that the processing began (indicated by start=). It also reiterates your input and summarizes the test processing.

- An .hto output file is displayed in the Playback, Individual Tests folder, under the specified script directory and script name. This file indicates whether the client/server communication worked properly.

**15.** You can perform the following additional functions from the Individual Tests folder. Click a script name and choose:

- **Show requests.** Lists all submitted hti requests.

- **Edit script.** Opens the hti script file in a text editor. You can save the script or refresh from the disk.

- **Start.** Opens the Playback of HTI Script Files pane, where you can revise parameters and rerun the script.

- **View Log file.** Reopens the log file.

- **View Graph.** Produces the same output as the log file in graph format. The graph is particularly useful for comparing the average response time of the server with your specified Maximum Response time to determine if you have met your performance goals.

- **Delete Result.** Deletes the generated output but retains the script for reuse.

- **Delete Script and Result.** Deletes the generated output but retains the script for reuse.

**16.** Once the script is run, you may also want to open the Performance Reports folder and choose:

- **Basic Report** to see basic stress test statistics.

- **Extended Report** to see an expanded group of stress test statistics.
Custom Report to specify which statistics to include in the reports.

17. Typically, you would run additional tests with different input parameters in order to compare statistics under different simulated loads conditions. Based on these comparisons, you could determine the best server scenario for your needs.
**Procedure: How to Refresh or Remove Script Directories**

You can expand the Individual Tests folder and click a specific directory. A pop-up menu enables you to remove the selected directory or refresh it without having to refresh all of the other test directories.

1. From the menu bar, select the \( C \) icon, then *Scalability*.
2. From the navigation pane, expand the *Individual Tests* folder (if not already expanded).
3. Right-click a directory and choose either *Refresh* or *Delete Script Directory* from the menu.

**Procedure: How to Display Percentile Statistics in Results**

A percentile is the point in a distribution of scores below which a given percentage of scores is found. When you perform a stress test you can calculate percentile statistics for processing time by specifying the percentage against which the percentile value will be derived.

You request percentile statistics from the Playback HTI Script Files pane, which you can access in either of the following ways:

**As a diagnostics option:**

1. From the menu bar, select the \( W \) icon, then *Scalability*.
2. In the navigation pane, expand a directory folder, click a script name, and select *Start* from the menu. The Playback of HTI Script files pane lists Basic and Advanced test parameters. Enter basic test conditions: *Number of Threads* and *Interval Parameter*.
3. Click the *Advanced* tab. A variety of additional test options are displayed.
4. In the *Show percentile statistics* field, enter a number \( N \), between 1 and 99, to calculate the processing time in your stress test distribution against which \( N\% \) of the other processing times are lower. For example, if the distribution of 6 processing times in a stress test includes the following values: 1-1-3-3-4-5, and the percentage value for *Show Percentile Statistics* is set to 50 (%), then the 50th percentile processing time will be 3 because that is the lowest value in the distribution against which 50% of the processing times are lower.
5. Click *Start* to run the test with the specified condition(s).

The Percentile result, along with other test results, appears in a separate window.

**When stress testing a particular procedure:**

1. From the Web Console menu bar, select *Applications*.
2. Expand an application directory, right-click a procedure, and select *Run Advanced*, then *Run Stress*. The Playback of HTI Script Files opens. This pane lists the available test parameters.
3. Enter basic test conditions: Number of Threads and Interval Parameter.

4. Click the Advanced tab, and proceed as described in steps 4 and 5 above.

**Reference:** Parameters for Playback of HTI Script Files

Following is a list of general playback parameters that are available.

**Basic:**

- **Number of Threads**
  
  A positive number of threads to be used when playing the script. Each thread represents a single client (user).

- **Interval Parameter**
  
  Specifies timing in a multiple-client (multi-threaded) playback. Possible formats of this value are \( m \) or \( m, n, k \), where \( m \) is the number of seconds between each client startup, and after each \( n \) started clients, an interval of \( k \) seconds is used instead.

- **Test Description**
  
  Enables you to create notes at playback time that will be displayed in the Extended Report.

  If you reset statistics, all information about previous runs is deleted, including any Test descriptions.

  **Tip:** This description provides a useful way to distinguish results as you test different combinations of options.

**Advanced:**

- **Compare option**
  
  Determines whether the response data received by all clients (threads) are identical. It uses a binary comparison mode and writes the comparison results to a playback log file.

- **Immediate processing**
  
  Ignores every SLEEP and WAIT statement in the HTI script. Issues HTTP requests without any delay between them.

- **Show percentile statistics**
  
  A percentile is the point in a distribution of scores below which a given percentage of scores is found. When you perform a stress test you can calculate percentile statistics for processing time by specifying the percentage against which the percentile value will be derived.
Enter a number $N$, between 1 and 99, to calculate the processing time in your stress test distribution against which $N\%$ of the other processing times are lower. For example, if the distribution of 6 processing times in a stress test includes the following values: 1-1-3-3-4-5, and the percentage value for Show Percentile Statistics is set to 50 (%), then the 50th percentile processing time will be 3 because that is the lowest value in the distribution against which 50\% of the processing times are lower.

For related information, see How to Display Percentile Statistics in Results on page 608.

**Size statistics**

Displays general output file size statistics for multiple-client playback in the log.

These are useful for analyzing Playback results with a large number of threads. Size should be consistent between similar runs. A size change would generally indicate an execution failure.

**Simulate browser caching**

Enables browser-style simulated caching of static pages (currently, css, js, gif, bmp, jpg, class and jar files). Each thread (simulated user) maintains its own cache of requests. When a cached static URL is requested again by the same user, the Stress tool skips the request instead of downloading the URL again.

**Submit as deferred**

Executes a request using deferred, rather than immediate, logic.

**Save playback statistics**

Choose this option to make statistics for the current run available on reports.

The statistics are saved internally in the $EDACONF/catalog directory as rec0001hti, rec0001log, and rec0001_0001hto.

For example, if the script generated in a recording session has the name rec0001hti, then the run log and statistics are stored in the rec0001log file and the output generated by each of three threads is rec0001_0001hto, rec0001_0002hto, rec0001_0003hto.

**Traces**

Sets the Playback utility traces on or off. A trace file (TRC) is then created for each thread.

**Keep alive for**

Causes every thread to repeat a request for a specified time, in seconds. This option enables the server to generate enough statistics to make a comparison among response times.
Result

The HTTPTST module that records and plays back Web Console sessions can simulate multiple client access to the Web Console on playback (that is, a multi-threaded application).

Each thread does what is recorded in the .hti file. The server reply is recorded in the .hto file. However, you can control the output provided by selecting one of the following options:

- **One file per thread (default).** Displays output in .hto files. The server generates a summary .hto file that reports on the success or failure of the server/client communication in the format: For example:

  Number of successfully run threads : 5

  You can access this file by selecting Playback, Individual Tests, and then the script_directory folder in the format

  `scriptname--nnnn`

  where:

  `nnnn`

  Is a number that is appended to the file name. It indicates the size of the generated file.

  This option also generates a separate .hto file for each thread being tested; these files contain the code that renders the report. You can access these files by selecting Playback, Individual Tests, and then the script_directory folder in the format

  `scriptname_thread#_filesize`

  and view the contents in a text editor.

- **One file per request.** Displays a single .hto file in the Playback>Individual Tests folder. This is the summary file that reports on the success or failure of the server/client communication. For example:

  Number of successfully run threads : 5

  You can access this file by selecting Playback, Individual Tests, and then the script_directory folder in the format

  `scriptname--nnnn`

  where:

  `nnnn`

  Is a number that is appended to the file name. It indicates the size of the generated file.
In addition to the summary file, the output for each request is written to the 
ibi/scale/performance directory in the format 

```
scriptname_thread#_request#.ext
```

where:

- **ext**
  
  Is determined by the nature of the request (for example, HTML), and by its success or failure (failure is often represented as a .txt file). For example:

  - **rec0001_0002_0041.html**

  where:

  - **rec0001**
    - Is the script name.
  
  - **0002**
    - Is the thread number.

  - **0041**
    - Is the request number.

  Additional requests in the thread would be represented as:

  - **rec0001_0002_0042.html**
  - **rec0001_0002_0043.html**

**Server**

Sends request to a server defined in the odin.cfg file.

**Use HTTP proxy**

Send all requests through an HTTP proxy server. For example, www.myproxy.com:3192.

**Save output to another directory**

Saves output files, including traces, to a specified location (for example, c:\myfiles).

**Reference: Additional Recording Hints**

- When recording is on, the HTTP listener records every CGI request. It is important to ensure that no one else is submitting requests to the same listener.

- Do not try to record a script from the middle of a persistent session. Always try using user ID and password, then recording the first request.
Reference: Playback Files

Playback log files are generated during script playback. Each file contains general information about playback processing, such as thread startup and termination, connection errors, and comparison results.

- Log file names are composed by appending .log to the base file name of the HTI script used to generate the log. Two additional log files, stdout and stdlog, may be generated to report critical playback failures.

- Playback HTO files are generated when the script playback is complete. Every file contains data received by a thread.

HTO file names are composed of the script file name, followed by the thread number and the .hto extension.

Troubleshooting the Console

If the web browser has problems accessing the Web Console, you may see the following messages.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Troubleshooting Tips</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer cannot open the Internet site <a href="http://address:http_service">http://address:http_service</a>. A connection with the server could not be established.</td>
<td>Ensure that the Workspace Manager is running or else contact the local system administrator.</td>
</tr>
<tr>
<td>There was no response. The server could be down or is not responding. If you are unable to connect again later, contact the administrator of the server.</td>
<td>Ensure that the Workspace Manager is running or else contact the local system administrator.</td>
</tr>
</tbody>
</table>
Server Processes

The server uses a series of processes to accomplish various tasks. Some processes have specialized administrative functions, such as workspace management and logging, while others do end-user tasks. System administrators may want to know what processes the server creates and how many of each. The administrator may want this information for machine sizing or simply to know what processes to consider or ignore when a problem occurs.

Note that each operating environment uses operating system-specific commands to view processes. The processes are described generically, not how they would appear in a system listing.

Server Work Space Manager Daemon

The server workspace is control by a daemon process known as PTH. There is one process per server.

Deferred Requests Special Services Daemon

The server has several types of special services. The DFM daemon is used for deferred (DFM) and Scheduler requests. There is one process per server.
Server Log Daemon

The server log (edaprint.log) is now written using a single daemon process. Previous versions wrote to the log independently from the various processes that might write to the log. In very rare and specific cases, the prior methods were problematic, hence, the change to the use of a daemon. As a result, starting a server brings up this additional server log daemon (edaplog).

Server Check Up Daemon

The server has always had a process that wakes up and checks various states and takes actions. An example of this is stopping agents that are inactive past the idle limit. In the past this process has been part of the Workspace Manager function, but is now a separate daemon that runs independently. As a result, starting a server brings up this additional server check up daemon (edachkup).

HTTP Listener Daemon

The server has several types of listeners. The HTTP daemon is used for requests using the HTTP protocol. There is one process per server.

TCP Listener Daemon

The server has several types of listeners. The TCP daemon is used for requests using the TCP protocol. There is one process per server.

FDS Special Services Daemon

The server has several types of special services. The FDS daemon (HLISNK) is used for FOCUS Database requests from agent processes. There is one process per server.

Java Services Daemon

The JSCOM daemon is used for requests using Java. There can be more than one process per server.

Agent Daemons

The actual worker processes for requests are known as agents or tscom3 processes (tscom3 is the actual program name). There is one process per configured agent that is active. Agent processes normally are reused until a recycle point or until they become inactive for a set period. Thus, for a given server, the number of processes associated with agents will change over time.
Gathering Diagnostic Information for Customer Support Services

**How to:**
Create a Savediag From the Web Console
Report Server Related Problems From the Command Line
Report edastart -t, -x, or -f Problems Outside the Server Environment

**Example:**
Sample edastart -savediag Processing With Variations

**Reference:**
Files Gathered by the edastart -savediag Command

Diagnostic Service Accelerator (DSA) automates the gathering, packaging, and shipping (using FTP) of trace files and other diagnostic information for Customer Support Services using the edastart -savediag facility. A prompt mode is available for ease-of-use, as well as archiving and FTP posting capabilities. Automatic triggers are available for customer email confirmation. DSA also triggers the logging of the upload to the support case and flags the case as requiring attention, thereby accelerating diagnostics services by automating and closing the communication gap between customer and customer services.

In one step a customer can run a repro, then describe, archive (for example, as a ZIP file), and ship (using FTP) all the required information to Information Builders Customer Support Services.

Automatic triggers are available for customer email confirmation. DSA also triggers the logging of the upload to the support case and flags the case as requiring attention, thereby accelerating diagnostics services by automating and closing the communication gap between customer and customer services.

Note the following platform-specific information:

- **On Windows,** users must have a command line version of ZIP installed and on the system path for the archive and send feature to work properly.

- **On OpenVMS,** this feature optionally uses ZIP if it is installed and a symbol is declared. (Any commercial or open source version of ZIP may used.) Otherwise, the -savediag process uses BACKUP to create the archive.

- **All other platforms** use system supplied tools such as tar and pax, and require no additional steps to use the feature.
On IBM i (formerly known as i5/OS), z/OS, and Open/VMS, batch/command files—CMD/CL, JCL, and DCL files, respectively—are available for users who prefer to use this method to control tracing and save diagnostics.

On Windows, the Start menu has equivalent options under the Diagnostics folder.

The files and their equivalent edastart commands are:

<table>
<thead>
<tr>
<th>File</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITRCON</td>
<td>edastart -traceon</td>
</tr>
<tr>
<td>ITRCOFF</td>
<td>edastart -traceon</td>
</tr>
<tr>
<td>ISAVERDIA</td>
<td>edastart -savediag</td>
</tr>
</tbody>
</table>

The physical execution of these batch files varies by platform. For information about location and use of supplied batch/command files, see the chapter for your platform in the Server Installation manual.

Note:

- The diagnostic process suggests a local location in which to save your files. However, you can supply a custom location if you prefer, as long as you avoid reserved system locations including the following: EDAHOME; APPROOT; EDAPRFU; SCAROOT; EDACONF bin; EDACONF etc; EDACONF edatemp; EDACONF dfm_dir; EDACONF img_dir; EDACONF catalog; EDACONF web; EDACONF user; any location that is a direct parent in the paths listed above; an ID’s HOME; the root of a device (that is, \ or /); c:\windows; c:\\Program Files; c:\Documents and Settings; /usr and /usr/bin.

- In the case of PDS deployment on z/OS, tracing and the edastart -savediag function must be done using the ISAVERDIA JCL method described in the z/OS PDS section of the Server Installation manual (where the diagnostic files go directly to the JES log output of the server) rather than the method described in the remainder of this section.

Procedure: How to Create a Savediag From the Web Console

To run a Savediag, you must be a Server Admin or have administrator privileges.

1. Click the Console icon and select Savediag - Report a Bug.
From the menu bar, select Workspace. From the navigation pane, open the Logs and Traces folder, right-click Workspace Logs, and select Savediag - Report a Bug.

The Savediag page opens, as shown in the following image.

2. Select from the Diagnostic Options drop-down menu.

The options are:

- **Save Diagnostics (savediag) and Post.** This is the default.
- **Save Diagnostics (savediag).**
- **Post existing diagnostics.**
- **Delete existing diagnostics.**

The available fields will vary, depending on the Diagnostic Option selected.
3. Choose whether to save files from the catalog by selecting the corresponding radio button.

4. For Save options, you can change the part of the **Savediag Directory** field that follows the underscore, which is the time.

5. For Post options, you can enter information in the **Comments** field.

6. For Save options, enter applications in the **List of Applications** field.

7. For Post options, enter the case number you received from Customer Support Services in the **Case Number** field.

8. For Post options, enter the information you received from Customer Support Services in the **Post ID** and **Post Password** fields. This information is required to access the Customer Support Services FTP site.

9. Click **Submit**.

If you selected a Post option, your information is posted on the Customer Support Services FTP site. If not, the information is saved to the Savediag Directory folder.

**Note:** If you choose the **Delete existing Diagnostics** option, select a folder from the **Delete Savediag Directory** drop-down menu and click **Submit**.

---

**Procedure:** **How to Report Server Related Problems From the Command Line**

In order to provide Information Builders Customer Support Services with a proper reproduction of your problem, follow these steps:

**Note:** The use of edastart in this procedure assumes that the directory for the edastart script has been added to the system search path for your platform (or that another method for locating and using edastart has been used). If this is not the case, you must preface edastart with its path when you enter it here.

1. Turn traces on with the command `edastart -traceon`. Initially starting the server with traces is strongly recommended.
2. Reproduce the problem while traces are on.

3. If the application abends, write the core dump information to the edaprint.log file using one of the following techniques:
   - To create the log from the Web Console menu bar, select Workspace, Diagnostics, Server Log, then click WRITE IBISNAP Information To Current Log.
   - To create the log manually, issue the edastart -ibisnap command.

4. Use the edastart -savediag command to gather and send files to the support FTP site as an archive (using the archive method required on your platform). The edastart -savediag command includes options for saving and FTPing, saving locally, and FTPing a prior local save. The system prompts as follows:

   Select an option (type Q to quit for most prompts):
   1. Save diagnostic to a directory and FTP post
   2. Save diagnostic to a directory
   3. FTP post prior diagnostic from a directory

   Enter a selection (Default=1) : 1

   For related information, see Files Gathered by the edastart -savediag Command on page 621.

   **Note:** Typically, users save and post in one operation (the default), however, you may wish to consider the following reasons for saving and posting as separate steps:
   - If you have multiple reproduction variations, you may wish to confirm them all first, then ship them to Customer Support Services.
   - If you wish to reproduce multiple separate problems, the two-part option enables you to save each one separately, then ship.
   - If the server cannot be shut down (and edastart -cleardir cannot be used), the two part option may enable you to delete unneeded items before shipping.
   - For security/privacy reasons, items need to be reviewed and possibly cleansed before shipping.

**Procedure:** How to Report edastart -t, -x, or -f Problems Outside the Server Environment

If a problem occurs on the Server environment, attempting to reproduce it in a free-standing environment may facilitate troubleshooting. If you wish to try this strategy, follow these steps.

1. Create a reproduction application directory (preferably called repro or repro_case#).

2. Place the required files (*.fex, *.mas, and so on) that are not already in APP PATH in the reproduction application directory.
3. Physically switch to the reproduction application directory so that traces and other files go to this known location.

4. Run the desired request with the command:

   ```
   edastart -traceon { -t | -x | -f }
   ```

   where:

   `-t`, `-x`, `-f`

   Are three separate trace modes.

5. If the server edatemp directory is not needed to reproduce the problem, shut the server down and issue the `edastart -cleardir` command so that edatemp is not captured during `-savediag` processing.

   **Note:** If the server must be kept running 24x7, skip this shutdown step and proceed to step 6.

6. Issue the `edastart -savediag` command, specifying the repro application directory (and any other needed directories) in order to gather and send files to the support FTP site as an archive (using the archive method required on your platform). The `edastart -savediag` command includes options for saving locally, saving and FTPing, and FTPing a prior local save. Choose:

   1. Save diagnostic in a new directory and post
   2. Save diagnostic in a new directory
   3. Post diagnostic from an existing directory

   Enter a selection (Default=1) : 2

   For related information, see *Files Gathered by the edastart -savediag Command* on page 621.

7. Restart the server to resume normal operation.

   In the case of an abend (core dump), Information Builders may ask that debuggables be installed (as described in the software installation manual) and that the repro/savediag steps be repeated with `IBI_DBGLIB=ON` to gather more detailed information. Do not install debuggables or perform these steps unless requested by Information Builders.

**Reference:** *Files Gathered by the edastart -savediag Command*

- Server log ($EDACONF/edaprint.log)
- Traces and other contents from the $EDACONF/edatemp/... directory, including the following:
<table>
<thead>
<tr>
<th><strong>File</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>edachkup.trc</td>
<td>Daemon check up facility trace</td>
</tr>
<tr>
<td>edapdfm.trc</td>
<td>Deferred Listener trace</td>
</tr>
<tr>
<td>edaplog.trc</td>
<td>EDAPRINT log daemon trace</td>
</tr>
<tr>
<td>fds.trc</td>
<td>FDS trace</td>
</tr>
<tr>
<td>jscom*.trc</td>
<td>Java traces</td>
</tr>
<tr>
<td>edapth.trc</td>
<td>Main workspace manager trace</td>
</tr>
<tr>
<td>edaphtp.trc</td>
<td>HTTP communication traces (listener)</td>
</tr>
<tr>
<td>ht000nnn.trc</td>
<td>HTTP communication traces (threads)</td>
</tr>
<tr>
<td>edaptcp.trc</td>
<td>TCP/IP communication traces (listener)</td>
</tr>
<tr>
<td>ip000nnn.trc</td>
<td>TCP/IP communication traces (threads)</td>
</tr>
<tr>
<td>lu000nnn.trc</td>
<td>SNA communication traces</td>
</tr>
<tr>
<td>ts000nnn.trc</td>
<td>Agent traces</td>
</tr>
</tbody>
</table>

- Server configuration ($EDACONFIG/bin/edaserve.cfg).
- Profiles from $EDACONFIG/etc/edasprof.prf and ibi/profiles/*.
- Complete content of application directories, as specified during -savediag processing.

**Example:** Sample edastart -savediag Processing With Variations

The following sample includes annotations that indicate what is happening as the process runs.

```
$ bin/edastart -savediag
```
A log of environment information is displayed.

Select an option (type Q to quit for most prompts):
1. Save diagnostic to a directory and FTP post
2. Save diagnostic to a directory
3. FTP post prior diagnostic from a directory

Enter a selection (Default=1) : 1

Enter directory path for diagnostic information
(Default=/u1/prod/iadmin/ibi/srv71/ffs/sd122905_110820)

Please supply location or <Enter>:
/u1/prod/iadmin/ibi/srv71/ffs/myrepro

Enter space separated non mapped application names to save in the diagnostic or ALL for all non mapped application names Default= baseapp): repro

12/29/2005 11:08:49


- Repro is the application directory for the saved application. myrepro is the directory in which the information generated by -savediag will be saved.

- A log of file copies is displayed. Note that some copy errors are normal since the process is trying to catch files (like those used for NLS set up), which users may or may not have.

12/29/2005 11:08:50 Diagnostic Information has been saved in /u1/prod/iadmin/ibi/srv71/ffs/myrepro

- If you selected Option 2, Save diagnostic to a directory, -savediag processing stops here.

- If you selected Option 3, FTP post prior diagnostic from a directory, -savediag processing provides the next prompt.

Enter existing directory path with diagnostic information to post (Default=/u1/prod/iadmin/ibi/srv71/ffs/sd122905_111616)
Please supply location or <Enter>: /u1/prod/iadmin/ibi/srv71/ffs/myrepro
It then continues as Option 1 would have.

Please enter Hottrack Case number to post (8 digits or more): 9999999999

Please enter user id on cssftp.ibi.com (Default=incmgr):

Please enter comments for the Hottrack Case 9999999999.

Enter as many lines as needed, blank line indicates end of comments.

My reproduction for error

12/29/2005 11:09:37 Creating myrepro.tar to post savediag information

Please supply confirmation to proceed with posting (Y/N/Q Default=Y): Y

Note:

- An FTP log of posting activities is displayed.
- As a final step, an HTTP message is sent silently to Customer Support Services. This triggers a confirmation email to the customer and alerts Customer Support Services systems that a –savediag has arrived.
Unicode is a universal character encoding standard that assigns a code to every character and symbol in every language in the world. Since no other encoding standard supports all languages, Unicode is the only encoding standard that ensures that you can retrieve or combine data using any combination of languages.

Topics:
- Unicode and the WebFOCUS Reporting Server
- Accessing Unicode Data
- Selecting, Reformatting, and Manipulating Characters
- Sort Order Under Unicode
- Added Unicode Support for Master Files, Data Files, and Application Directory Names
- Unicode PDF Output
Unicode and the WebFOCUS Reporting Server

How to: Configure the Server for Unicode

The WebFOCUS Reporting Server supports a Unicode Transformation Format (UTF) called UTF-8 in ASCII environments, and UTF-EBCDIC in EBCDIC environments:

- **For ASCII**, the UTF-8 encoding standard assigns each character of each language a code that can be from 1-3 bytes long. The codes assigned to European characters are 1 or 2 bytes long, Middle Eastern characters are 2 bytes long, and those assigned to Asian characters are 3 bytes long. This standard is compatible with ASCII format because the first 128 UTF-8 codes have the same 1-byte representation as the corresponding ASCII codes.

- **For EBCDIC**, the UTF-EBCDIC encoding standard assigns each character a code that can be from 1-4 bytes long. EBCDIC characters, including C1 control characters, have the same 1-byte representation in UTF-EBCDIC.

In non-Unicode single-byte encoding standards, such as ASCII, each character is assigned a code that is 1 byte long, limiting the number of characters that can be represented by the standard. When using those standards, it became common to equate a character with a byte of storage. If you had a string of 10 characters, the amount of storage needed was 10 bytes, and many character manipulation routines expected character string lengths to be specified as a number of bytes.

With Unicode encoding, bytes and characters are no longer equated: characters are represented internally by a varying number of bytes, depending on the character. If you configure the server for Unicode, you define the length of strings and alphanumeric fields in terms of characters, not bytes. This simplifies specifying string and field lengths. Each character is represented internally by up to 3 bytes, and the server automatically adjusts for the actual storage length. In reports, each character displays in a report column using one space, regardless of how many bytes it takes up in memory. This character-based processing mode employed for Unicode environments is called **character semantics**. The non-Unicode mode is called **byte semantics**.

Procedures that had been developed using byte semantics will continue to work when deployed in a Unicode environment, without adjustment, in most cases.

To compress trailing blanks and display columns as the width of the largest actual data value, issue the SET SQUEEZE=ON command. For more information on the SQUEEZE parameter, see the chapter on Formatting Report Data in the Creating Reports With WebFOCUS Language manual.
The main benefit of the new system is the ability to have multiple languages (both European and Asian) in the following WebFOCUS and Dialogue Manager objects:

- Titles, descriptions, and names in synonyms.
- Headings and prompts in procedures.
- Data for all supported adapters (for example, SAP BW, SAP R/3-ECC, Oracle, DB2, Sybase ASE, Sybase IQ, Teradata, MySQL, Web Services, Fixed files). For more information, see Accessing Unicode Data on page 628.

**Procedure: How to Configure the Server for Unicode**

To configure the server for UTF-8 or UTF-EBCDIC character encoding:

1. From the menu bar, select **Workspace**.
2. From the navigation pane, right-click the **Workspace** folder, and select **NLS**.
   The NLS Configuration Wizard pane opens.
3. Select **65001 - Unicode (UTF-8)** or **65002 - Unicode (UTF-EBCDIC)** from the **CODE_PAGE** drop-down list.
   The server will be configured for Unicode once you save this configuration.
Accessing Unicode Data

Reference:
- Unicode Considerations for Oracle
- Unicode Considerations for DB2
- Unicode Considerations for Sybase ASE
- Unicode Considerations for Sybase IQ
- Unicode Considerations for Microsoft SQL Server
- Unicode Considerations for Teradata (CLI)
- Unicode Considerations for MySQL
- Relational Adapter Data Type Support for Unicode
- Unicode Considerations for SAP BW and SAP R/3-ECC
- Unicode Considerations for Fixed-Format Sequential Files

Adapters for the following types of data sources support Unicode:
- DB2
- Fixed-format sequential files
- Microsoft SQL Server
- MySQL
- Oracle
- SAP BW
- SAP R/3-ECC
- Sybase ASE
- Sybase IQ
- Teradata (CLI)
- Web Services
- XBRL
- XML

Relational adapters in a Unicode environment assume that the DBMS returns character data to the server already converted to Unicode. The relational adapters convert data to the correct DBMS API when writing to a relational data source (for example, Oracle to UTF-8, Microsoft SQL Server to UTF-16, and DB2 on MVS to UTF-EBCDIC).

XML-based adapters (the Adapter for XML, and the Adapter for XBRL) obtain the code page from the XML declaration of the processed XML document. For more information, see http://www.w3.org/TR/REC-xml#sec-prolog-dtd.

The Adapter for Web Services generates SOAP requests using the UTF-8 code page.
Reference: Unicode Considerations for Oracle

The adapter supports Unicode data in Oracle release 10g or higher databases that have been configured with the NLS_CHARACTERSET parameter set to UTF8. You must set the NLS_LANG environment variable in the edastart file, in a separate shell file, in a database profile, or in a user profile.

Set NLS_LANG using the following syntax

NLS_LANG = language_territory.characterset

where:

language
  Is the selected language.

territory
  Is the name of the country associated with the selected language.

characterset
  Is the value of the NLS_CHARACTERSET variable that is set in the Oracle database. For Unicode, this is always UTF8.

For example, for American English UTF-8, you would use the following setting:

NLS_LANG=American_America.UTF8

For information about data type support, see Relational Adapter Data Type Support for Unicode on page 632.

Reference: Unicode Considerations for DB2

Information Builders supports DB2 databases, version 8 and higher. To prepare the DB2 environment for Unicode on:

- **Windows**, the database must have been created with the option CODESET UTF-8, and you must add the following variable to the environment using Windows or in the edastart file:
  
  DB2CODEPAGE=1208

- **UNIX**, the database must have been created with the option CODESET UTF-8, and you must set the LANG and NLS_LANG environment variables in the edastart file or in a separate shell file.

For example, for American English, you would export the following variables:

  export LANG=EN_US.UTF-8
  export NLS_LANG=American_America.UTF8
- **z/OS**, the database must have been created with the CCSID UNICIDE option, and you must ensure that the DSNAOINI environment variable points to a configuration file containing the following specification:

  CURRENTAPPENSCH=UNICODE

  The adapter supports Unicode only with the CLI interface.

  In a Unicode environment, the Adapter for DB2 requires a BIND command for PREPARE/EXECUTE logic using parameter markers.

  For information about data type support, see *Relational Adapter Data Type Support for Unicode* on page 632.

- **IBM i**, Unicode is only supported in DB2 CLI mode. DB2 allows column-by-column specification of CCSID information at CREATE TABLE time and the columns may or may not be explicitly Unicode 1208 and 1200, however, all CCSIDs are transcoded to the server as CSID 1208 UTF8. Thus, any existing table may be used in a Unicode configuration regardless of its underlying CCSID specifications.

**Reference:**  **Unicode Considerations for Sybase ASE**

The adapter supports Unicode data in Sybase ASE version 15.0 and higher databases that have been created with the CHARACTER SET option set to UTF-8. You must set the LANG and NLS_LANG environment variables in the edastart file or in a separate shell file before starting the server.

For example, for American English, you would export the following variables:

  export LANG=EN_US.UTF-8
  export NLS_LANG=American_America.UTF8

  For information about data type support, see *Relational Adapter Data Type Support for Unicode* on page 632.

**Reference:**  **Unicode Considerations for Sybase IQ**

Beginning with Sybase IQ version 12.7, the adapter supports Unicode data in Sybase IQ databases that have been created with the UTF-8 character set. You must set the LANG and NLS_LANG environment variables in the edastart file or in a separate shell file before starting the server.

For example, for American English, you would export the following variables:

  export LANG=EN_US.UTF-8
  export NLS_LANG=American_America.UTF8

  For information about data type support, see *Relational Adapter Data Type Support for Unicode* on page 632.
**Reference:** Unicode Considerations for Microsoft SQL Server

The adapter, using the OLE DB interface, supports Unicode data stored in NCHAR and NVARCHAR fields (where N stands for national). N columns can support data of any language or combination of languages.

For information about data type support, see *Relational Adapter Data Type Support for Unicode* on page 632.

**Reference:** Unicode Considerations for Teradata (CLI)

The Adapter for Teradata (CLI) supports Unicode UTF-8 format if:

- The Teradata CLI client components are part of release TTU8.0 or higher.
- The Teradata database is release V2R6.0 or higher and appropriate language support was enabled during the sysinit process.

Contact your database administrator (DBA) to determine whether international language support has been enabled in your Teradata system and/or consult the Teradata documentation for details about International Character Set support.

Note that, at the present time, when Unicode is enabled the length of a Teradata Column Name and/or TITLE cannot exceed 21 characters (bytes).

For information about data type support, see *Relational Adapter Data Type Support for Unicode* on page 632.

**Reference:** Unicode Considerations for MySQL

The Adapter for MySQL is implemented using JDBC. This implementation supports Unicode data stored in character fields with CHARACTER SET set to UTF-8.

You must set the LANG environment variable in the edastart file or in a separate shell file before you start the server. For example, for American English you would export the following variable:

```
export LANG=EN_US.UTF-8
```

For information about data type support, see *Relational Adapter Data Type Support for Unicode* on page 632.
Reference: Relational Adapter Data Type Support for Unicode

In Unicode databases the information in CHAR(n) columns is stored in a UTF-8 encoding scheme. Most RDBMS Unicode columns of CHAR type specify length in bytes, not characters. The B-modifier in the Actual format denotes that a character column with a fixed byte length might contain a varying number of UTF-8 characters. This is reflected in the AnV Usage format.

<table>
<thead>
<tr>
<th>DBMS</th>
<th>Column Type</th>
<th>Usage</th>
<th>Actual *</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2</td>
<td>CHAR(n)</td>
<td>AnV</td>
<td>AnB</td>
</tr>
<tr>
<td></td>
<td>GRAPHIC(n)</td>
<td>An</td>
<td>An</td>
</tr>
<tr>
<td></td>
<td>VARCHAR(n)</td>
<td>AnV</td>
<td>AnVB</td>
</tr>
<tr>
<td></td>
<td>VARGRAPHIC(n)</td>
<td>AnV</td>
<td>AnV</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>CHAR(n) single byte code page</td>
<td>An</td>
<td>An</td>
</tr>
<tr>
<td></td>
<td>CHAR(n) double byte code page</td>
<td>AnV</td>
<td>AnV</td>
</tr>
<tr>
<td></td>
<td>NCHAR(n)</td>
<td>An</td>
<td>An</td>
</tr>
<tr>
<td></td>
<td>VARCHAR(n)</td>
<td>AnV</td>
<td>AnV</td>
</tr>
<tr>
<td></td>
<td>NVARCHAR(n)</td>
<td>AnV</td>
<td>AnV</td>
</tr>
<tr>
<td>MySQL</td>
<td>CHAR(n)</td>
<td>An</td>
<td>An</td>
</tr>
<tr>
<td></td>
<td>VARCHAR(n)</td>
<td>AnV</td>
<td>AnV</td>
</tr>
<tr>
<td>Oracle</td>
<td>CHAR(n CHAR)</td>
<td>An</td>
<td>An</td>
</tr>
<tr>
<td></td>
<td>CHAR(n BYTE)</td>
<td>AnV</td>
<td>AnB</td>
</tr>
<tr>
<td></td>
<td>NCHAR(n)</td>
<td>An</td>
<td>An</td>
</tr>
<tr>
<td></td>
<td>VARCHAR(n CHAR)</td>
<td>AnV</td>
<td>AnV</td>
</tr>
<tr>
<td></td>
<td>VARCHAR(n BYTE)</td>
<td>AnV</td>
<td>AnVB</td>
</tr>
<tr>
<td></td>
<td>NVARCHAR(n)</td>
<td>AnV</td>
<td>AnV</td>
</tr>
</tbody>
</table>
### DBMS

<table>
<thead>
<tr>
<th>DBMS</th>
<th>Column Type</th>
<th>Usage</th>
<th>Actual *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybase ASE</td>
<td>CHAR(n)</td>
<td>A{n}</td>
<td>A{nB}</td>
</tr>
<tr>
<td></td>
<td>UNICHAR(n)</td>
<td>A{n}</td>
<td>A{n}</td>
</tr>
<tr>
<td></td>
<td>VARCHAR(n)</td>
<td>A{nV}</td>
<td>A{nVB}</td>
</tr>
<tr>
<td></td>
<td>UNIVARCHAR(n)</td>
<td>A{nV}</td>
<td>A{nV}</td>
</tr>
<tr>
<td>Sybase IQ **</td>
<td>CHAR(n)</td>
<td>A{n}</td>
<td>A{nB}</td>
</tr>
<tr>
<td></td>
<td>VARCHAR(n)</td>
<td>A{nV}</td>
<td>A{nVB}</td>
</tr>
<tr>
<td>Teradata</td>
<td>CHAR(n)</td>
<td>A{n}</td>
<td>A{n}</td>
</tr>
<tr>
<td></td>
<td>VARCHAR(n)</td>
<td>A{nV}</td>
<td>A{nV}</td>
</tr>
</tbody>
</table>

* Note that on EBCDIC platform(s) the ACTUAL size for a B-suffixed format is increased 1.5 times to accommodate the expansion when converting from UTF-8 to UTF-EBCDIC. For example, on MVS the synonym created for a DB2 CHAR(10) column contains the following: USAGE=A10, ACTUAL=A15B.

**Note the following limitation for Sybase IQ:** You cannot use the HOLD FORMAT SYBASE command with the Unicode implementation of Sybase IQ since this command depends on the availability of UNICHAR and UNIVARCHAR data types, which are not supported by Sybase IQ.

### Reference: Unicode Considerations for SAP BW and SAP R/3-ECC

SAP uses UTF-16 encoding in its Unicode system. The server uses UTF-8 and handles all conversions between the two encoding schemes. The server may not need to be configured for Unicode when accessing the SAP Unicode system.

NLS settings for the server must be configured in such a way that the server code page can handle the list of chosen languages. For example, ISO 8859-1 can accommodate most Western European languages. The 8859 family can handle character specifics with the lower set almost being mapped to US ASCII. Therefore, with 8859-1 one could request English, German, French, and Spanish. When a character set requires a code page that takes more than one byte per character (for example, many Asian languages), the only choice for the server is 65001 (UTF-8).
The adapters provide access to Unicode SAP BW and SAP ECC systems, respectively. This extends support of data and metadata in multiple languages to the server, consistent with support by the SAP server. A synonym can be created using one or more languages. Those languages will be used to create titles and descriptions.

- For SAP BW, the userid and password in the sapserv.cfg file must be able to connect to SAP BW using the enumeration of desired languages.
- For SAP R/3-ECC, the server logon language is used to retrieve all languages.

**Reference: Unicode Considerations for Fixed-Format Sequential Files**

When retrieving a fixed-format sequential file, the server attempts to determine the code page the file was meant to be retrieved with by checking the Master File CODEPAGE attribute. If the Master File does not contain the CODEPAGE attribute, the server code page is used to read the file.

If you use the Data Management Console to generate a data flow that creates a fixed-format sequential file, you can specify a code page in the Data Management Console. DataMigrator will then create the fixed-format file in a way that can be read by the server when that server has been configured for the specified code page.

In a Unicode configuration, HOLD files in BINARY and ALPHA formats are created using UTF-8 conversion, which assigns each character three bytes of storage in ASCII environments or four bytes in EBCDIC environments. Fields defined in the Master File using the data type A in both the USAGE and ACTUAL attributes are described in terms of characters. Fields defined using any other combination of USAGE and ACTUAL attribute values are described in terms of bytes.

To force a field in a fixed-format sequential file to be described in terms of bytes, add B to the end of the ACTUAL attribute. For example, to specify that a field is stored in 10 bytes, you would specify:

```
ACTUAL=A10B
```

The adapter will then read the specified number of bytes from the record and convert their contents to the number of characters specified by the file code page.

Regardless of how much storage a character occupies, it occupies only one space on a report, as always.
Selecting, Reformatting, and Manipulating Characters

Example: Defining a Virtual Field

Consider the following DEFINE in the Master File for the EMPLOYEE data source:

```
DEFINE FIRST_ABBREV/A5 WITH FIRST_NAME = EDIT(FIRST_NAME, '99999$');$
```

In character semantics mode, format A5 is interpreted as five characters (up to 15 bytes on ASCII platforms, up to 20 bytes on EBCDIC platforms), and the comparison is performed based on this number of bytes. In byte semantics mode, format A5 is interpreted as five bytes, and the comparison is performed based on five bytes. In either case, the correct characters are compared and extracted.

Example: Reformatting a Field

Consider the following PRINT command:

```
PRINT FIELD1/A10
```

In character semantics mode, format A10 is interpreted as 10 characters (up to 30 bytes), meaning that up to 30 bytes must be retrieved when this field is referenced. In byte semantics mode, format A10 means that 10 bytes will be retrieved. In either case, the field displays as 10 characters that take up 10 spaces on the report output.
Reference: Character Functions That Support Character Semantics

In character semantics mode, all character manipulation functions interpret lengths in terms of characters. The following functions operate on alphanumeric strings in character semantics mode when Unicode is configured:

- **String manipulation and extraction functions.**
  - GETTOK, OVRLAY, PARAG, REVERSE, SQUEEZ, STRIP, SUBSTR, SUBSTV, TRIM, TRIMV

- **Justification functions.**
  - CTRFLD, LJUST, RJUST

- **Length and position functions.**
  - ARGLEN, LENV, POSIT, POSITV

- **Format conversion functions.**
  - EDIT

- **Decoding, comparison, and editing functions.**
  - CHKFMT, EDIT, DECODE, SOUNDEX

- **String replacement functions.**
  - CTRAN, HEXBYT, BYTVAL (see notes below), STRREP

- **Case translation functions.**
  - LCWORD, LOCASE, LOCASV, UPCASE, UPCASV

**Note:** The HEXBYT, BYTVAL, and CTRAN functions have been extended to handle multibyte characters in Unicode configurations. These functions use or produce numeric values to represent characters. In Unicode configurations, they use or produce values in the range:

- 0 to 255 for 1-byte characters
- 256 to 65535 for 2-byte characters
- 65536 to 16777215 for 3-byte characters
- 16777216 to 4294967295 for 4-byte characters (primarily for EBCDIC)

To find the numeric value corresponding to a given character, find its hexadecimal code and convert to decimal with a hex calculator such as the Windows XP Calculator program. (Make sure to use the UTF-8 or UTF-EBCDIC code, not the Unicode code point, which would be the UTF-16 value.)
For example, assume you would like to create a variable of format A1 containing the euro sign. The euro sign in UTF-8 is, in hex, E282AC. Converting this to decimal gives 14849492. Thus, the proper DEFINE or COMPUTE would be:

\[
\text{EUROSIGN/A1} = \text{HEXBYT}(14849492, \ 'A1');
\]

If you are creating a FOCEXEC with a UTF-8 compliant editor, you can also get the value of the euro sign in this way:

\[
\text{EUROVAL/I8} = \text{BYTVAL}(\ '€', \ 'I8');
\]

The CTRAN function replaces all occurrences of a character in a string with another character, given the decimal values that represent the hexadecimal codes for the two characters. Traditionally, this technique was used to replace characters that were difficult to input directly. Decimal values of characters can be complicated to determine. Therefore, if you want to replace characters or character strings that you can input directly using a UTF-compliant text editor, Information Builders recommends that you use the STRREP string replacement function.

The following translates all of the euro signs in a 40-character UTF-8 field to pound sterling signs (£ = C2A3 or 49827):

\[
\text{NEWFLD/A40} = \text{CTRAN}(40, \text{OLDFLD}, \text{EUROVAL}, 49827, \ 'A40');
\]

**Sort Order Under Unicode**

Sort order is based on the binary values assigned to the characters. When the server is configured for Unicode, the sort order is based on the Unicode encoding standard. If ascending values of the codes correspond to the alphabetical order of the letters in the language being used, a report can be sorted in alphabetical order. This is entirely dependent on the encoding standard and its mapping of codes to letters. In many, but not all cases, the encoding standard assigns codes in the alphabetical order of each language.

For example, Ukrainian added a new letter (Cyrillic capital letter ghe with upturn) to its alphabet after the UTF-8 coding specification had already been set. This letter was not assigned a code that sorts it alphabetically, either in Unicode or in code page 1251 (used for Ukrainian). It sorts differently and incorrectly using either encoding scheme.

- With code page 1251, this letter sorts as the first letter on the report output.
- With UTF-8, this letter sorts as the last letter on the report output.

To determine whether a language sorts alphabetically, you can examine the hexadecimal codes assigned to its letters on the code page you are using and check whether ascending hexadecimal codes match the alphabetical order.
Added Unicode Support for Master Files, Data Files, and Application Directory Names

Support for UTF-8 file names is now available for Master Files, Data Files, and Application Directory names.

Unicode PDF Output

Reporting from a Unicode data source with PDF output format is available when using the following two fonts which support Unicode characters:

- Lucida Sans Unicode, which is used to display single-byte characters only. This font is available on Windows version 2000 and higher.
- Arial Unicode MS, which is used to display both single-byte and double-byte characters. This font can be installed as an option from the Microsoft Office CD, version 2000 and higher.

The Lucida Sans Unicode font is the default font if the WebFOCUS Reporting Server is configured for UTF-8 (code page 65001) or UTF-EBCDIC (code page 65002).

If the server is configured for Unicode, and you want to use the Arial Unicode MS font instead, you must specify the Arial Unicode MS font in the stylesheet. Alternatively, if the WebFOCUS PDF font mapping file (for example, EDAHOME NLS pdf.fmp) has DEFAULT-FONT=YES specified for Arial Unicode MS, then it becomes the default font. For example:

```plaintext
font=Arial Unicode MS, style=normal, metricsfile=PDARUM AFM *, DEFAULT-FONT=YES, $
```

For more information about how to use the PDF font mapping file, see the *Creating Reports With WebFOCUS Language* manual.
Environment variable EDAEXTSEC is only used to override the security provider setting that is stored in edaserve.cfg file in order to start the server with security OFF.

Topics:
- Platform-Specific Methods for Setting EDAEXTSEC
## Platform-Specific Methods for Setting EDAEXTSEC

<table>
<thead>
<tr>
<th>Platform</th>
<th>Start Method</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Start Menu</td>
<td>Under the main software folder for the server, select <strong>Start Security ON</strong> or <strong>Start Security OFF</strong>.</td>
</tr>
<tr>
<td></td>
<td>As a Service under a local system account</td>
<td>Set the system environment variable EDAEXTSEC, under <em>My Computer, Properties, Advanced</em> tab, to OFF. Restart Windows to initialize.</td>
</tr>
<tr>
<td></td>
<td>As a Service under the current account</td>
<td>Set the system environment variable EDAEXTSEC, under <em>My Computer, Properties, Advanced</em> tab, to OFF. Restart Windows to initialize.</td>
</tr>
<tr>
<td>UNIX</td>
<td>Command prompt or Script that calls edastart</td>
<td>Export the variable setting in the edastart shell script, or before any calls to the shell script, as follows: <code>export EDAEXTSEC=OFF</code></td>
</tr>
<tr>
<td>z/OS Unified Server</td>
<td>JCL</td>
<td>Place the variable in the EDAENV allocation of the IRUNJCL member of the configuration library <code>EDAEXTSEC=OFF</code></td>
</tr>
<tr>
<td>IBM i</td>
<td>QSH command prompt or QSH script that calls edastart</td>
<td>Export the variable in the edastart shell script, or before any calls to the shell script, as follows: <code>export EDAEXTSEC=OFF</code></td>
</tr>
<tr>
<td></td>
<td>CALL {lib}/TSCOM300 or CL that calls TSCOM300 or CL that calls QSH, which, in turn, calls the edastart shell script</td>
<td>Before the call to TSCOM300, add the following: <code>ADDENVVAR ENVVAR(EDAEXTSEC) VALUE(OF)</code></td>
</tr>
</tbody>
</table>
**B. Platform-Specific Methods for Specifying EDAEXTSEC**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Start Method</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenVMS</td>
<td>Command prompt or DCL script that calls edastart</td>
<td>Before calling edastart.com or in edastart.com, add the following: \n\n<strong>DEFINE EDAEXTSEC OFF</strong> \nYou can also define the logical EDAEXTSEC in the EDAENV.COM file.</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Use the Web Console (Workspace, Configuration Files folder, Miscellaneous folder, Environment - edaenv.cfg) to edit the edaenv.cfg file and add the following: \n\n<strong>EDAEXTSEC=OFF</strong> \n<strong>Note:</strong> After a change, a hard restart of the server must be done.</td>
</tr>
</tbody>
</table>
Index

-? command 343
-* command 343
-CLOSE command 344
-DEFAULTS command 344, 359
-EXIT command 344
-GOTO command 344, 361
-IF command 344, 362, 363, 364
-INCLUDE command 344, 365
-label command 344
-PASS command 344
-PROMPT command 344
-QUIT command 344
-READ command 344
-REMOTE BEGIN command 344
-REMOTE END command 345
-REPEAT command 345
-RUN command 345
-SET command 345, 360
-TYPE command 345
-WRITE command 345
-&name variable 349
-APPROOT variable 352
-&DATE variable 352, 355
-&DATEfmt variable 352
-&DMY variable 353
-&DMYY variable 353
-&ECHO variable 353, 358, 359
-&EXITRC variable 354
-&FOCFOCEXEC variable 353
-&FOCINCLUDE variable 353
-&FOCMODE variable 353
-&FOCPRINT variable 353
-&FOCREL variable 353
-&IORETURN variable 353
-&MDY variable 352
-&MDYY variable 353
-&name variable 349, 350
-&RETCODE variable 354
-&TOD variable 354
-&YMD variable 353
-&YYMD variable 353

A
accessing APP directories on Windows 227
accessing pop-up menus from Web Console
navigation panes 19
accessing Sun LDAP libraries 80
accessing WebFOCUS components with single
sign-on 69, 70
active connections 508
active reports license code 470
adapter configuration 280
    changing 280
adapter connections 281
adapters 278
    configuring 278
administering servers 17, 18, 418
administration levels 114
administrative tasks for Data Services 511
administrative tasks for Java Services 523
administrative tasks for Special Services and Listeners 537
agent monitoring 490, 501, 520, 528
agent services 421
    configuring 421
agents 496, 513, 515, 516, 525
    error messages 516
    starting 515, 525
    statistics 496
    stopping 513, 515
aggregated statistics for Data Services 502
aggregated statistics for Java Services 522
ALLOCATE subcommand 376, 379
allocating data files 262
allocating data sets 379
allocating files 397
allocating temporary files 265
alphanumeric expressions 368, 369, 371
AND keyword 370
answer sets
    returning 373, 374, 375
APP ? METALLOCATIONSAME command 228
APP APPENDPATH command 224
APP application management commands 220
APP commands 219, 220, 222, 223, 224, 225, 228, 232, 233, 234, 235, 236, 237, 238, 239, 240, 244, 246, 247, 248, 251, 252, 257
APP APPENDPATH 222, 224
APP COPY 232
APP COPYF 233
APP CREATE 220
APP DELETE 220, 236
APP DELETETH 236, 237
APP FI 248
APP HELP 257
APP HOLD 246
APP LIST 251
APP MAP 225
APP MOVE 234
APP MOVEF 235
APP PATH 222, 223
APP PREPENDPATH 222, 224
APP PROPERTY CODEPAGE 238
APP QUERY 252
APP RENAME 220, 238
APP RENAMETH 239
APP SHOWPATH 228
FI 244
file types 240
HOLD 244
HOLDDATA 244, 247
HOLDMETA 244, 248
APP COMMANDS
    APP ? METALLOCATIONSAME 228
    APP SET METALLOCATIONSAME 227
APP COPY command 232
APP COPYF command 233, 240
APP DELETE command 236
APP DELETETH command 236, 237, 240
APP FI command 244, 248
APP HELP command 221, 257
APP HOLD command 244, 246
APP HOLDDATA command 244, 247
APP HOLDMETA command 244, 248
APP LIST command 221, 251
APP MAP command 225
APP MOVE command 234
APP MOVEF command 235, 240
APP PATH command 201, 202, 223
configuring 223
search paths 223
APP PREPENDPATH command 224
APP PROPERTY CODEPAGE command 238
APP QUERY command 221, 252
APP RENAME command 238
APP RENAMEF command 239, 240
APP reporting and help commands 221
APP SET METALOCATIONSAME command 227
APP SHOWPATH command 228
appearance of Web Console 25
Appearance option 25
appending applications to search path 224
application (APP) 162
physical location of 162
application components 162, 252
listing 252
application directories 183, 201, 202, 206, 225, 226, 230
creating 230
filtering in Web Console 206
mapping from Web Console 183, 202
mapping manually 225
application paths 201, 202, 222, 223
APP PATH 201, 202
APP PATH command 223
configuring 222
application repositories 161, 162
applications 236
deleting 236
APPROOT hierarchy 109
approot parameter 162
arithmetic expressions 367, 368
authenticating an LDAP server with SSL 72
averages 507
B
baseapp directory 163
branching 361, 362
C
Caching files for WebFOCUS Active Technologies 462
calling procedures 365
case translation functions 636
changing adapter configurations 280
changing passwords 94
changing the password delimiter 93
character semantics and functions 635, 636
CLOSE subcommand 376, 389
Cluster Manager 479
Cluster Manager properties 485
code page values 445, 447
for IBM i 447
for UNIX 445
for Windows 445
codepage, application 238
Column Management options 23
command lines 359
commands 343
communications configuration 282
compound expressions 372
COMPRESS subcommand 376, 397
CONCAT subcommand 376, 387
concatenating files 398
concatenation 369
conditional branching 362
configuration files 162
configuring 421
    agent services 421
    deployment modes 421
configuring adapters 278
configuring application paths 222
configuring DBMS security 66
configuring OPSYS security 56
configuring remote servers 282
configuring server trace files 590
configuring servers 17, 18, 29, 418
connection monitoring 508, 509
Connection Queue 508, 509
connection statistics 509
connections 509, 510
    monitoring 509
    stopping 509, 510
CONTAINS operator 370
controlling HLIPRINT output 583
controlling output 583
cookie, retrieving the value of 146
COPY subcommand 376, 390
COPYDD subcommand 392
Core Engine settings 456
creating data files 262
creating data sets 398
creating expressions 366
creating procedure files 261
creating synonyms 290
custom message from quiesced server 420
customer support using trace files 616

D
data access agents 421
data files 262
data set names 264
data sets 376, 378, 379, 398
    allocating 379
    creating 398
    locking 378
DBMS security 66, 68
    configuring 66
    password passthru 68
ddnames (logical names) 399
decoding, comparison and editing functions 636
defferred files 561
    valid extensions 561
Deferred List 532
defferred list statistics 533
defferred management 556
    setting properties in 556
defferred procedure execution 549, 556, 561
defferred process 561
    monitoring 561
    statistics 561
deferred requests 532, 533
deleting 533
monitoring 533
retrieving answer sets 533
DELETE subcommand 376, 393
deployment modes 426
designating a network drive on Windows 227
diagnostics for servers 571, 573, 584, 601, 609, 612, 613
EDAPRINT files 573
record and playback 601, 609, 612, 613
trace files 584
Dialogue Manager commands 343, 344, 345, 359, 360, 361, 362, 363, 364, 365, 375
-? command 343
-* command 343
-CLOSE 344
-DEFAULTS 344, 359
-EXIT 344
-GOTO 344, 361
-IF 344, 362, 363, 364
-INCLUDE 344, 365
-label 344
-PASS 344
-PROMPT 344
-QUIT 344
-READ 344
-REMOTE BEGIN 344
-REMOTE END 345
-REPEAT 345
-RUN 345
-SET 345, 360
-TYPE 345
-WRITE 345
Dialogue Manager procedures 343, 345, 346, 348, 349, 350, 375
calling 346
platform-specific commands 375
running 345
variables and 348, 349, 350
Dimension View Display option 24
DYNAM command 263, 376, 378, 379, 388, 397
DYNAM SET LONSGNYM 267
DYNAM subcommands 376, 379, 387, 389, 390, 392, 393, 394, 396, 397
ALLOCATE 376, 379
CLOSE 376, 389
COMPRESS 376, 397
CONCAT 376, 387
COPY 376, 390
COPYDD 392
DELETE 376, 393
FREE 376
RENAME 376, 394
SUBMIT 376, 396
DYNAM SUBMIT command 469

E

EDACONF 108, 109
EDAHLIP variable 583
EDAHOME 108, 109
EDAPRINT files 573
EDASERVE.CFG 279
edaserve.cfg configuration file 162
EDASPROF.PRF 279
EDATEMP 108, 109
editing 473
server files 473
user.prf file 473
editing procedures 321
enabling Cluster Manager 479
encrypting passwords 139
encrypting passwords for configuration files 139
EQ operator 370
error messages 516, 517
  agents 516, 517
EX procedures 271
EXEC command 357, 365, 366
executing profiles 455
execution flow 358, 359, 361
  debugging 358, 359
expressions 366, 367, 368, 369, 370, 371, 372

F

FDS (FOCUS Database Server) 581
file attributes
  specifying 399
FILEDEF command 262, 263, 264, 399, 401, 402
files 397, 398
  concatenating 398
  freeing 398
filtering application directories in Web Console 206
filtering traces 590
fine-tuning the server 476
  JVM memory usage 476
Fixed files 634
Fixed files configuration for Unicode 634
flow of execution 358, 359, 361
  debugging 358, 359
foccache directory 163, 462
FOCUS Database Server (FDS) 581
fonts 638
  Unicode in PDFs 638
Force Finalization 477
format conversion functions 636
FREE command 388
FREE subcommand 376
freeing files 398

G

GE operator 370
General Privileges 111
General Workspace Configuration Settings 469
  calling exit for DYNAM SUBMIT on z/OS 469
GETCOOKI function 146
global server profiles 34
global variables 348, 349, 351, 352
  naming 349
group profiles 35, 455
GT operator 370

H

header variable, retrieving the value of 146
heap size 476
HLIPRINT log 581, 582, 583
  controlling 581
  controlling number of lines 582
HTI script (HTTP internal script) 601
hto files 613
HTTP header variable, retrieving the value of 146
HTTP internal script (HTI script) 601

I

ibisamp directory 163
IBISNAP 573
IBM i language and code page values 447

J

Java Services 517, 519
Java Virtual Machine (JVM) 477
JCL commands 397
JSCOM3 connections 517
justification functions 636
JVM 476
JVM (Java Virtual Machine) 476, 477
memory usage 476
memory tuning options 476

K
keyword parameters
passing 357
killing agents 513, 515
by user id 515

L
language values 445, 447
for IBM i 447
for Windows and UNIX 445
languages and code pages 445, 447
for IBM i 447
for Windows and UNIX 445
LDAP security 70
LDAP security settings 70
LDAP security with SSL 72
LDAP support 70
LDAP vendor libraries 77
LE operator 370
left-click menus 19
length and position functions 636
license codes 470
active reports 470
server 470
site code 470
License Management pane 470
listener statistics 531
listeners 526
Listeners and Special Services Configuration page 548
local variables 348, 349, 350
naming 349
locking data sets 378
logical expressions 370, 371
logical names 399
logical operators 370
Login Info option 21
login information 21
login password expiration 94
LONGSYNM 267

M
managing deferred requests 556, 561
managing servers 17, 18, 418
mapping application directories 183, 202, 225
manually 225
Master Files 264
max_connections_per_user 425
max_connections_per_user property 425
metadata 260
accessing 260
Microsoft SQL Server configuration for Unicode 631
migrating servers 472
modes of server deployment 426
monitoring 561
deferred 561
monitoring connections 509
monitoring Data Service Agents 490
monitoring deferred requests 533
monitoring Java Services 517
monitoring JSCOM3 connections 517, 519
monitoring listeners 526
monitoring server activity 488, 496, 501, 508, 509, 520, 527, 528, 590
monitoring server agents 490, 501, 520, 528
monitoring server connections 508, 509
monitoring special services 526, 527
monitoring the WebFOCUS Reporting Server 417
MVS commands 376
My Console options 26

N
naming variables 349
NE operator 370
nesting 365
non-data files 261
NOT operator 370
notifying about password expiration 94

O
OFFLINE command 402
OMITS operator 370
ON TABLE HOLD 373
ON TABLE PCHOLD 373, 374, 375
opening the Web Console 18
operators 370
CONTAINS 370
EQ 370
GE 370
LE 370
NOT 370
OMIT 370
OR 370
OPSYS security 53, 56, 108, 109
APPROOT 109
configuring 56
EDACONF 109
EDAHOME 109
EDATEMP 109
file areas 108
temporary files (EDATEMP) 109
OR operator 370
Oracle character semantics 629
Oracle configuration for Unicode 629
output files 246, 247, 248
creating 246, 247, 248

P
parameters
passing 357, 358
passing parameters 357, 358
password delimiter 93
password encryption for configuration files 139
password expiration notification 94
password passthru and DBMS 68
passwords
changing 94
encrypting 139
PDF report output 638
Unicode fonts 638
Performance Report for Data Service Agents 491, 496
Performance Report for Java Service Agents 518
Performance Report for Special Services and Listeners 526, 527
Performance Report for Web Sessions 534
physical file location 225, 248
mapping to 225
platform-specific commands 375
playback hto files 613
playback log files 613
playback of user actions 601, 609, 612, 613
Playback tool features 608
percentile processing in stress tests 608
refreshing directories 608
pooled server deployment mode 426
positional parameters 358
passing 358
preference settings for Web Console 26
Preferences option 22
prepending applications to search path 224
private server deployment mode 426
procedures 261, 321, 358, 359, 365
calling 365
testing 358, 359
profile levels 33
profiles 222
applications and 222
PTH security 60

Q
queue_max_user_conns 425
queue_max_user_conns property 425
queued connections 508
Queuing property 425
queuing user connections 425
quiesced server 420

R
recording user actions 601, 609, 612, 613
releasing unused memory 477
remote servers 282, 479
RENAME subcommand 376, 394
Reporting Options 25
right-click menus 19
role profiles 35
Run Options 23
running procedures 321
running the WebFOCUS Reporting Server 417

S
SAP BW configuration for Unicode 633
SAP portal logon 69, 70
SAP R/3-ECC configuration for Unicode 633
Save Last Report option 28
savediag facility 584, 616
saving last report 28
Scheduler agents 549
script file 591
capturing traces 591
search paths 219, 223, 224
adding names to 224
appending applications manually 224
search paths (continued)
commands 219
prepending applications manually 224
Secure Sockets Layer (SSL) with LDAP security 72
security DBMS 66
security features 114, 127, 139, 143, 144
controlling Web Console access on OPSYS 114
password encryption 139
setting privileges 127
SSL encryption 143, 144
security LDAP 70
security modes
  LDAP security 70
  security DBMS 66
  security OPSYS 53
  security PTH 60
security OPSYS 53
security PTH 60
selecting client code pages 445
server activity 488, 496, 501, 508, 520, 528, 584, 590
server administration 17, 18, 418
server agents 490, 501, 520, 528
server configuration 17, 18, 29, 418
server connections 508
server deployment modes 426
server deployment parameters 427
  server profiles 427
  setting 427
server diagnostics 571, 573, 584, 601, 609, 612, 613
  EDAPRINT files 573
  record and playback 601, 609, 612, 613
  trace files 584
server error messages 440
server fine-tuning 476
  JVM memory usage 476
server management 17, 18, 418
server migration 472
server profiles
  commands 37
server security 41
server trace files 590
service profiles 34
service properties 496
  agents 496
Session Log 591
SET TRACEUSER commands 586
setting edahlip variable for HLIPRINT output 583
setting properties 556
  deferred management, and 556
setting server security 41
setting user privileges 127
setting Web Console preferences 26
Show General Privileges option 26
showing Session Log 591
single sign-on 69, 70
sink machine 264
site code 470
social media adapters 288
sort order with Unicode 637
special service statistics 526
special services statistics 527
SSL 143, 144
SSL (Secure Sockets Layer) with LDAP security 72
SSL API calls 72
SSL/TLS connections 72
SSO prerequisites 69, 70
SSO verification 69, 70
stack size 477
stacked commands 345
starting agents 515, 525
statistical variables 348, 349
statistics 488, 490, 496, 501, 509, 519, 520, 526, 527, 528, 533
agent 496
agents 490, 501, 520, 528
connection 509
defered requests 533
for individual agents 501, 528
for individual Java Service Agents 520
Performance Report for Java Service Agents 519
special services (FDS, SCHEDULER, DFM) 526, 527
system-specific 501, 520, 528
statistics for Java Service Agents 518
statistics for listener 531
statistics for special services and listeners 526
statistics for Web Session 534
status statistics for Data Services 502
stdlog log files 613
stdout log files 613
stopping agents 513, 515
by user id 515
stopping connections 510
string manipulation and extraction functions 636
string replacement functions 636
SUBMIT subcommand 376, 396
Sun LDAP libraries 80
supplying variable values 356, 357, 359, 360
Sybase ASE Adapter 630
  Unicode support 630
Synonym Editor options 24
synonym locations 227, 228
synonyms 267, 290
  long names on z/OS 267
system variables 348, 349, 352, 355
system-extended statistics 501
T
temporary files 109, 265
testing for variable values 363, 364
trace files 584, 589, 590
  limiting size 589
trace files for customer support 616, 619, 620
  reporting problems outside server environment 620
  reporting server problems 619
traces 590, 591
  filtering 590
  in script file 591
troubleshooting servers 571, 573, 584, 601, 609, 612, 613
  EDAPRINT files 573
  record and playback 601, 609, 612, 613
  trace files 584
TSO commands 397
tuning server performance 476
  JVM memory usage 476
U
unconditional branching 361
Unicode 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 637, 638
  access non-FOCUS data sources 628
  Asian characters and 626
  configuring WebFOCUS for UTF-8 627
  data type support for Relational adapters 632
  DB2 data types 632
Unicode (continued)
  European characters and 626
  Fixed files configuration 634
  fonts for PDFs 638
  manipulating characters 635
  Microsoft SQL data types 632
  Microsoft SQL Server configuration 631
  Oracle configuration 629
  Oracle data types 632
  PDF output 638
  reformatting characters 635
  SAP BW configuration 633
  SAP R/3-ECC configuration 633
  sort order and 637
  Sybase ASE Adapter 630
  Sybase ASE data types 632
universal character encoding standard 625, 626
Universal Naming Convention (UNC) 227
UNIX language and code page values 445
USE command 262, 264
user actions 601, 612
user connections 425
user exit routines 379
UTF (Unicode Transformation Format) 626

V
variable values 356, 357, 359, 360, 363, 364
  setting 359, 360
  testing 363, 364
variables 348, 349, 350, 351, 352
  naming 349
vendor libraries for LDAP 77
version information 572

W
Web Console 17, 18, 201, 202, 206, 223, 418, 571, 573, 584, 601, 609, 612, 613
  application path 201
  application paths 202, 223
  troubleshooting 571, 573, 584, 601, 609, 612, 613
Web Console access control 114
  DBMS security mode 114
  LDAP security mode 114
  OPSYS 114
  PTH security mode 114
web console appearance 454
Web Console navigation pane menus 19
WebFOCUS Reporting Server 417
  running and monitoring 417
Windows 227, 445
  accessing a network drive 227
  language and code page values 445
Workspace configuration settings 428, 430, 442, 454, 456, 463, 466, 469, 471
  Core Engine 456
  e-mail settings 430
  foccache settings 463, 466
  General 469
  general options 430, 442, 456, 463, 466, 471
  license settings 471
  NLS (National Language Support) settings 442
  profile settings 456
  web console appearance 454
Workspace Manager 18, 418, 488, 496, 501, 508, 509, 520, 526, 527, 528, 590
  configuration privileges 418
  configuring 418
  monitoring connections 509
  monitoring server activity 488, 496, 501, 508, 520, 526, 527, 528, 590
Z

z/OS commands 376
Reader Comments

In an ongoing effort to produce effective documentation, the Technical Content Management staff at Information Builders welcomes any opinion you can offer regarding this manual.

Please share your suggestions for improving this publication or alert us to corrections. Identify specific pages where applicable. You can contact us through the following methods:

Mail: 
Technical Content Management
Information Builders, Inc.
Two Penn Plaza
New York, NY 10121-2898

Fax: 
(212) 967-0460

Email: 
books_info@ibi.com

Website: 
http://documentation.informationbuilders.com/connections.asp

Name: ________________________________________________________________

Company: ________________________________________________________________

Address: __________________________________________________________________

Telephone: ___________________________ Date: ___________________________

Email: ______________________________________________________________________

Comments: ______________________________________________________________
WebFOCUS

Server Administration

DataMigrator Server Release 7 Version 7.06
WebFOCUS Reporting Server Release 8.1M