

iWay

iWay Server Administration for UNIX, Windows NT,
OpenVMS, OS/400, OS/390, and z/OS
Version 5 Release 2.0

EDA, EDA/SQL, FIDEL, FOCCALC, FOCUS, FOCUS Fusion, FOCUS Vision, Hospital-Trac, Information Builders, the Information Builders logo, Parlay, PC/FOCUS, SmartMart, SmartMode, SNAPPack, TableTalk, WALDO, Web390, WebFOCUS and WorldMART are registered trademarks, and iWay and iWay Software are trademarks of Information Builders, Inc.

Due to the nature of this material, this document refers to numerous hardware and software products by their trademarks. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies. It is not this publisher's intent to use any of these names generically. The reader is therefore cautioned to investigate all claimed trademark rights before using any of these names other than to refer to the product described.

Copyright © 2003, by Information Builders, Inc. All rights reserved. This manual, or parts thereof, may not be reproduced in any form without the written permission of Information Builders, Inc.

Printed in the U.S.A.

Preface

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

How This Manual Is Organized

This manual includes the following chapters:

Chapter		Contents
1	Introduction	Describes how to use the console, provides an overview of server configuration, and introduces server security.
2	Configuring Data Adapters	Provides general information on configuring adapters and outlines configuration options.
3	Configuring a Remote Server	Provides general information on configuring remote servers.
4	Managing Metadata	Defines server application, discusses application paths, and provides general information on creating server metadata.
5	Editing and Running Procedures	Defines procedures and outlines procedure options.
6	Running and Monitoring Your Server	Introduces the Workspace Manager and describes how to use it to monitor all aspects of your server, including agents, sessions, connections, deferred procedures, and listeners.
7	Managing Listeners and Special Services	Provides general information about the communications configuration file and its component node blocks.
8	Troubleshooting	Lists diagnostic tools available in the console and describes how to use them to analyze and correct problems.

Documentation Conventions

The following conventions apply throughout this manual:

Convention	Description
THIS TYPEFACE or <i>this typeface</i>	Denotes syntax that you must enter exactly as shown.
<i>this typeface</i>	Represents a placeholder (or variable) in syntax for a value that you or the system must supply.
<u>underscore</u>	Indicates a default setting.
<i>this typeface</i>	Represents a placeholder (or variable) in a text paragraph, a cross-reference, or an important term. It may also indicate a button, menu item, or dialog box option you can click or select.
this typeface	Highlights a file name or command in a text paragraph that must be lowercase.
Key + Key	Indicates keys that you must press simultaneously.
{ }	Indicates two or three choices; type one of them, not the braces.
[]	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.
	Separates mutually exclusive choices in syntax. Type one of them, not the symbol.
...	Indicates that you can enter a parameter multiple times. Type only the parameter, not the ellipsis points (...).
.	Indicates that there are (or could be) intervening or additional commands.

Related Publications

To view a current listing of our publications and to place an order, visit our World Wide Web site, <http://www.iwaysoftware.com> . You can also contact the Publications Order Department at (800) 969-4636.

Customer Support

Do you have questions about iWay Server Administration for UNIX, Windows NT, OpenVMS, OS/400, OS/390, and z/OS?

Call Information Builders Customer Support Service (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 iWay Server Administration for UNIX, Windows NT, OpenVMS, OS/400, OS/390, and z/OS questions. Information Builders consultants can also give you general guidance regarding product capabilities and documentation. Please be ready to provide your six-digit site code (xxxx.xx) when you call.

You can also access support services electronically, 24 hours a day, with InfoResponse Online. InfoResponse Online is accessible through our World Wide Web site, <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 also provides usage techniques, diagnostic tips, and answers to frequently asked questions.

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 iWay Software configuration:
 - The iWay Software version and release.
 - 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?
- 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 Documentation Services staff welcomes your opinions regarding this manual. Please use the Reader Comments form at the end of this manual to relay suggestions for improving the publication or to alert us to corrections. You can also use the Documentation Feedback form on our Web site, <http://www.iwaysoftware.com>.

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 World Wide Web site (<http://www.iwaysoftware.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 World Wide Web site (<http://www.iwaysoftware.com>).

Contents

1. Introduction	1-1
Using the Web Console	1-2
Configuration Overview	1-3
Preparing for Communications Configuration	1-4
Communications Configuration Worksheets	1-5
Understanding Server Security	1-7
Security ON	1-8
Security WCPROTECT	1-9
LDAP Considerations	1-9
Security OFF	1-9
2. Configuring Data Adapters	2-1
Adapter Configuration Change	2-2
3. Configuring a Remote Server	3-1
4. Managing Metadata	4-1
Specifying the Path for an Application	4-2
Configuring Application Path	4-2
Working with Application Files	4-3
Editing Metadata	4-3
5. Editing and Running Procedures	5-1
Setting Optional Parameters	5-2
Procedure Options	5-2
6. Running and Monitoring Your Server	6-1
Configuring Workspace Manager	6-2
Agent Service	6-3
Modes of Deployment	6-3
Deferred Management Configuration	6-4
Monitoring Server Activity	6-4
Server Statistics	6-4
Monitoring Agents	6-7
Monitoring Sessions	6-10
Monitoring Connections	6-11
Deferred Statistics	6-13
Deferred List	6-13
Monitoring Listeners and Special Services	6-14
Migrating Your Server	6-16
Configuring Traces	6-16
Editing Configuration Files	6-17
Viewing and Editing Your License Number	6-17

7. Managing Listeners and Special Services	7-1
Communications Configuration File	7-2
8. Troubleshooting	8-1
Viewing Version Information	8-2
Analyzing Server Activity	8-2
Analyzing FOCUS Database Server Activity	8-3
Enabling and Viewing Trace Files	8-3
Viewing a Trace File	8-3
Recording and Reproducing User Actions	8-4
Playback Log Files	8-6
Troubleshooting the Workspace Manager Web Console	8-6
Workspace Manager Safe Mode	8-6

CHAPTER 1

Introduction

Topics:

- Using the Web Console
- Configuration Overview
- Preparing for Communications Configuration
- Understanding Server Security

Release 5 introduces an expanded Web Console that enables you to configure, operate, monitor, tune, and troubleshoot your server from a single, easy-to-use interface.

Using the Web Console

The HTTP 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
- 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

Procedure Accessing the Workspace Manager Web Console

1. Start the Workspace Manager.
2. Enter the following URL in the address space of your Web browser:

`http://ip_address:http_service`

where:

`ip_address`

Is the IP address of the machine on which the server is installed.

`http_service`

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

Note: See *Troubleshooting the Workspace Manager Web Console* in Chapter 8, *Troubleshooting* if you have trouble contacting the Server.

3. If you are running your server with security on, you will need to enter the user name and password used to access the operating system.

Logging on with the server administrator ID activates the management features and the diagnostic pages. Non-administrator IDs can only view statuses, statistics, and run the test tools. The non-administrator pages look very similar to the administrator pages, and are just missing the features to manage the server. The administrator versions of the pages are shown in this manual.

The Web Console opens. On the left of the page is a navigation pane giving access to the different features of the Web Console. The top of the navigation pane displays the last date and time of communication between the browser and the server.

4. Select an option from the navigation pane to access the corresponding console page. For tasks that display information or require no additional navigation, the console presents corresponding information in the right pane. For tasks that require additional, task-centered navigation, the console opens a new window. Use the new window's navigation pane to access the corresponding information in the new windows' right pane.

The console offers online help by providing two kinds of links to appropriate sections of this documentation.

- Clicking Help on the navigation pane provides general help in the context of the current page.
- Clicking on the ? icon, when available, provides contextual help specific to the item associated with the ? icon.

Configuration Overview

An individual server's characteristics are defined by a set of configuration files. These configuration files define the protocols, services, and data sources supported by the server. In the UNIX, OS/390 USS, Windows, OpenVMS and OS/400 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. Once you have successfully installed 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-based Administration Console to configure all necessary functionality.

To configure your 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 then edit configuration files. For sample files, see Configuration File Reference. Note that some configuration errors can make the server start in a limited mode called safe mode in which the Administration Console is still operational to allow fixing the mistakes.

Preparing for Communications Configuration

Depending on your environment and network configuration, inter-node communications may consist of TCP/IP, SNA (LU6.2), HTTP, or PIPE communication protocols. Inter-node communications are configured through the Listeners and Remote Servers links in the navigation panel of the Web Console.

Procedure How to Prepare to Configure TCP/IP or HTTP

Perform the following tasks to prepare to configure for TCP/IP or HTTP:

1. Verify that TCP/IP is installed, configured, and running on both the server and client platforms.
2. List any TCP service names/port numbers and IP addresses you will be using for inbound server and outbound client or subserver access. This list will be used during the server configuration.

Procedure How to Prepare to Configure SNA (LU6.2)

Perform the following tasks to configure for SNA (LU6.2):

1. Verify that System Network Architecture (SNA) is installed, configured, and running on both the server and client platforms.
2. Ensure that all installation prerequisites have been met. SNA (LU6.2) is not supported on all platforms. See the Server Installation manual for details.
3. List all SNA profiles and parameters you will be using for inbound server and outbound subserver access. This list will be used during the server configuration.
4. Create an SNA configuration for intra-node communications. Depending on your platform, you create some or all of the following SNA (LU6.2) definitions for use with the server:
 - Local LU name.
 - Partner LU and Partner LU Alias.
 - Partner LU and Partner LU Alias for local loop back.
 - Mode Name. The default is PARALLEL. Do not change this parameter unless you are instructed to do so by the site administrator.
 - TP Name. The default for use with an OS/390 or z/OS subserver is MVSSRVR. Do not change this parameter unless you are instructed to do so by the site administrator.

Procedure How to Configure PIPE Communications

No prerequisite is required for PIPE.

Note: The client and the server must reside on the same physical machine.

Communications Configuration Worksheets

Complete one or several of the remaining worksheets, which will depend on the following:

- Communications protocol.
- Inbound or outbound communications.
- MVS Remote Server (subserver) access.

In the following examples, inbound and outbound are used relative to the server; inbound refers to communications from the client, and outbound refers to communications to remote subservers.

Example Configuring for Inbound Communications Using TCP/IP

If you choose to configure for inbound communications using TCP/IP, complete this worksheet.

Prompt Description	Default	Supply Your Value Here
Inbound TCP/IP Port Number.	Will depend on server type. The Full-Function Server default is 8100.	

Note: This port should be the first of up to five consecutive ports that the server will use.

Example Configuring for Inbound Communications Using SNA (LU6.2)

If you choose to configure for inbound communications using SNA (LU6.2), complete this worksheet.

Prompt Description	Default	Supply Your Value Here
TP NAME for server.	EDATP	
LOCAL LU NAME for local test client test tool (RDAAPP).	None	
PARTNER LU NAME for local client test tool (RDAAPP).	None	
MODE NAME for local test client test tool (RDAAPP).	None	

Example Configuring for Outbound Communications Using TCP/IP

If you choose to configure for outbound communications using TCP/IP (Hub Server and Full-Function Server with Hub Services only), complete this worksheet.

Prompt Description	Default	Supply Your Subserver Values Here		
		Sub 1	Sub 2	Sub 3
Outbound host name or IP address.	Local host name.			
Outbound TCP/IP service name or port number.	8100			
User ID and password for connecting to the server on this port.	Leave blank for trusted node access.			
Is server located on MVS? If Yes, enter the MVS service name.	No			

Example Configuring for Outbound Communications Using SNA (LU6.2)

If you choose to configure for outbound communications using SNA (LU6.2) (Hub Server and Full-Function Server with Hub Services only), complete this worksheet.

Prompt Description	Default	Supply Your Value Here
LOCAL LU NAME used by the server.		
PARTNER LU NAME for the Remote Server.	None	
TP NAME for the Remote Server.	None	
PARTNER MODE NAME used by the client test tool (RDAAPP).	None	
User ID and password for connecting to the server on this port.	Leave blank for trusted node access.	
Located on MVS (Yes or No)? If Yes, enter the MVS service name.	No	

Understanding Server Security

The server allows flexible security configuration to satisfy a variety of installation needs. There are three security modes:

Security ON: Each connecting user is defined in the operating system on which the server is running: UNIX, NT, zOS, OS/400. The server uses operating system services to authenticate connecting users, impersonate them, and ensure access control to resources like files and DBMS objects. Access to the Web Console's administrative functions is protected via user authentication at the operating system level.

Security WCPROTECT: The users are not necessarily defined as operating system users. Instead they may be defined in the DBMS system, in the LDAP directory or not defined at all. Access to the Web Console's administrative functions is protected via user authentication at the configuration level.

Security OFF: All user information is ignored and there is no security restriction. Access to the Web Console is not protected.

Security ON

This mode provides the highest level of security since no user is allowed to connect to the server until his or her credentials have been checked against the operating system's native security system, such as RACF for zOS, UNIX security files, or Windows NT domain database. Once the connecting user is authenticated the server allocates a data access agent that fully impersonates that user (that is, the operating system will see it as if the user logged on via telnet).

The files in hierarchical directories on UNIX or Windows NT and in the native MVS datasets on zOS will be protected according to the system security rules.

DBMS connections can be controlled by the ENGINE SET CONNECTION command. If the connection is defined in edasprof.prf as

```
ENGINE SQLORA SET CONNECTION_ATTRIBUTES connection_name/,
```

the agent will connect to the DBMS carrying over its impersonation attributes.

Access to the console is protected. Only users matching a username listed in server_admin_id are allowed control operations on the console.

This security mode is enabled by granting sufficient privileges to the server process. Specifically:

- On UNIX, the startup tscom300 executable must have setuid of root
- On Windows NT, the server must be started as a service under SYSTEM account
- On z/OS, MVS load library must be APF authorized and hfs executables given +a option
- On OS/400, the ownership of libraries must be changed to QSECOFR

and by exporting the environment variable EDAEXTSEC=ON or leaving it unset (this is the default mode).

Note that on Windows NT the Server Administrator password is required for this security mode. If it is not provided in the configuration, the server will complain and start up in safe mode.

The client connection can be:

- Explicit. User ID and password are part of the connection header in both the native iWay protocol (HX50) and the HTTP protocol.
- IWA. For Windows NT only, the client and server will exchange security token, but not the password (this applies to both the HX50 and HTTP protocols).
- Trusted. The connection coming from a trusted client will contain only the user ID and the server will impersonate it without further authentication

Security WCPROTECT

This mode is applicable when the installation chooses not to create an operating system account for each connecting user. Instead the users may be defined on the DBMS server or on the iWay sub-server. This mode is called *passthru* as the user IDs and passwords are passed to the next "server" for action.

All the server processes run as a single user ID from the operating system point of view. There is no impersonation of data agents taking place.

This mode is useful in situations similar to the following:

- A Windows NT hub server connecting to a zOS subserver. The installation does not want to replicate RACF users on Windows NT.
- A UNIX server accessing ORACLE via Oracle/NET. The installation does not want to create UNIX accounts to duplicate Oracle accounts.
- A Windows NT AAS server connecting to CICS via ANYNET. The installation does not want to replicate CICS (RACF) users on Windows NT. Access to the Web Console is protected in this mode by authenticating the connecting user against the Server Administrator user ID and password. This authentication is done without the involvement of any system services (there is no privileged server process in this mode), just by comparison to encrypted configuration data. Note that the Server Administrator password must be configured BEFORE starting a server in this security mode, either by providing it at installation time or by running the command `edastart -change server_admin_id` from the EDACONF/bin directory.

To run the server in this mode, export the environment variable `EDAEXTSEC=WCPROTECT` before startup. If you never use Security ON mode, you can omit the authorization steps during installation.

LDAP Considerations

In Release 5 Version 2, the server supports LDAP via an exit that the installation has to write and install as a dll in the server directory. The connecting user ID and password are passed to the exit that authenticates the user. If the user is accepted then he or she is allowed access to data agents. No impersonation of data agents takes place. The DBMS access is performed according to connection definitions found in `edasprof.prf` and `user.prf`.

Security OFF

This mode is applicable when the installation does not need or want any security features.

To run the server in this mode, omit the authorization steps during install or export the environment variable `EDAEXTSEC=OFF` before startup.

CHAPTER 2

Configuring Data Adapters

Topic:

- Adapter Configuration Change

Clicking the **Adapters** menu item opens the Configuring Data Adapters window which presents a list of data adapters available for a given operating system and operating system release.

Most of the data 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, and EDASERVE.CFG contains database release and access method information.

For an experienced Server Administrator, there is the ability to edit global profile manually, but it is not recommended, and caution must be exercised as syntax may change from release to release.

Select **Release and Access Method** and click to configure.

All Database Configuration screens have same look and feel, with the exception of parameters keywords and number of parameter fields, which are different from database to database.

For details, see the documentation for a specific data adapter.

Adapter Configuration Change

The Data Adapters window displays a tree view of data adapters already configured for the current operational instance. Under 'Configured' subtree it lists each data adapter with all connections already configured.

Clicking on a data adapter allows you to:

Function	Description
Add Connection	Adds a connection for data adapters that have the functionality to support multiple connections.
Settings	Displays various settings in effect for the given adapter. This is for display only. Note: This only applies to adapters for relational DBMSs.
Remove	Removes adapter configurations and all connections setting from the list of configured adapters.

Any adapter definitions in user profiles have to be maintained manually.

Clicking on a connection allows you to:

Function	Description
Test	Runs select statement for name/owner against catalog table with limit up to 15 records.
Properties	Allows to view and change all of the connection parameters. Note: Duplicate entries will not be verified.
Delete	Deletes connection settings. Note: Entries will be deleted from the server global profile, EDASPROF.PRF, but not from the workspace configuration file.

CHAPTER 3

Configuring a Remote Server

Clicking the **Remote Servers** menu item opens the Configuring Remote Servers window which allows you to add remote server nodes to the communications configuration. The interface to input parameters for each protocol is similar to the Listeners window except that the CLASS parameter is fixed to CLIENT.

CHAPTER 4

Managing Metadata

Topics:

- Specifying the Path for an Application
- Editing Metadata

Application in the server refers to the location of metadata definitions, procedures and other files for development and deployment under a unique assigned name. That name can be a physical directory or a mapping name to a physical directory. Multiple application names can be configured and added to the Application Path.

Specifying the Path for an Application

An Application Directory is a logical name associated with physical location under the APPROOT directory tree. Maintaining logically organized application components provides ease of development, deployment, and maintenance.

Configuring Application Path

The Configure Application Path screen allows the maintenance of application directories and mappings, and the definition of the Application Path.

The following functions allow you to maintain applications:

Function	Description
APP ENABLED	Enables or disables application support.
New Directory	Creates New Application Directory. Enter the name you want to assign for the new application and click <i>OK</i> .
New Mapping	Adds a mapping from an application name to a physical directory name.
Delete Directory	Click on an Application directory name in the tree view to delete it.
Set APP PATH	Sets the Application Directory Path to the list in the box.
Add/Remove	To add a directory to the path, drag it to the box and click on Set APP PATH. To remove a directory from the path, select its name in the box, click on Remove, and then click on Set APP PATH.
Up/Down	Allows changes in the order of applications along the search path.

Working with Application Files

Application directories can contain metadata files and procedure files. In the metadata window, a tree view of the application directories can be accessed to work with the metadata files. In the procedures window, a similar tree view allows to work with the procedure files of each application.

The following functions allow you to work with application files:

Function	Description
Edit	Metadata files or procedures can be edited by clicking on the file and selecting the desired action. The contents of the file will be displayed in an editing mode. While in the editor screen, you can save the modified contents. For a procedure, you can also test/run the procedure.
Delete	You can delete a file by clicking on its name and selecting the desired action.
Copy/Move to:	Allows copying or moving of files from one Application Directory to another.

Editing Metadata

Clicking the **Metadata** menu item opens the Editing Metadata window which presents a list of existing metadata for editing and a list of data adapters already configured for which metadata can be added.

For details, see the documentation for a specific data adapter.

CHAPTER 5

Editing and Running Procedures

Topics:

- Setting Optional Parameters
- Procedure Options

Procedures are reusable logic components written in 4GL language. Using procedures allows application logic to be written once and executed many times. The Procedures window allows the creation and testing of stored procedures. It also allows the submission of stored procedures for execution at a later time, in deferred mode.

The Procedures window allows you to:

- Configure Application Path and manage application files.
- Set optional parameters for running procedures.
- Create, edit and run procedures.

Setting Optional Parameters

You can set the following optional parameters for running procedures:

Parameter	Description
Procedure Parameter	Passes parameters to a procedure. They can be positional or keyword.
Connect	Needed for the first query on the remote server. If Disconnect After Execution is selected, then it is needed for every execution.
Disconnect after execute	Terminates connection to remote server after query execution.
Server	Node name with communication definitions to the remote server.
Service name	Service name to connect to on the server.
User ID	User ID on the remote server.
Password	Password for the above user.

Procedure Options

You can create, edit and run procedures.

Function	Description
Create New Procedure	Click on a directory and enter the name of the new procedure without the extension.
Edit Procedure	Click on the procedure name and select Edit to open in an edit mode.
Run	Runs the procedure.
Run Deferred	Submits for deferred execution.
Run Stress	Allows to run a stress test of the procedure via generation of an HTI script.

CHAPTER 6

Running and Monitoring Your Server

Topics:

- Configuring Workspace Manager
- Monitoring Server Activity
- Migrating Your Server
- Configuring Traces
- Editing Configuration Files
- Viewing and Editing Your License Number

The Workspace Manager is a component of the server that is responsible for managing the interactions of all server processes. Server processes are listeners, data access agents, deferred execution agents, and so on.

The Workspace Manager Configuration screen allows the Server Administrator to manage resources, utilization, and other parameters through various settings stored in the `edaserve.cfg` configuration file. To change a value, type your modification in the appropriate input box. Click the Save and Restart button to save the new settings and restart the server instance with these settings in effect.

The following topics explain the main concepts involving these settings while the individual keywords are linked to a reference description for each parameter. Refer to one of the keyword links or click on the ? button next to the parameter on the Workspace Configuration page for a complete list with explanations.

Configuring Workspace Manager

Access to the administrative features of the Web Console can be restricted via a list of users defined in server admin id. Users defined in the list may have Server or Application administration level. A **Server Administrator** has the ability to perform all the administrative tasks available through Web Console operations. If there is more than one Server Administrator defined, the first valid member of the list will be used for impersonation of FDS and other special services. An **Application Administrator** is limited to the administrative tasks that do not require changing configuration or restarting the server. All other users (basic users) can only use the Web Console tasks indicated as such in the table below.

Any IDs (beyond the original ID used to set up the server) that are used for server or application administration also require r/w privileges to the respective locations that the IDs are expected to manage. This is usually accomplished by establishing group rights for the locations at the operating system level. To view and run Resource Governor procedures, IDs need to be at least an Application Administrator.

Web Console Task	Server Administrator	Application Administrator	Basic users
Home Page	Yes	Yes	Yes
Workspace in monitor mode only	Yes	Yes	Yes
Diagnostics page, display tracing only	Yes	Yes	Yes
Version, Log off, Preferences and Help Pages	Yes	Yes	Yes
Data Adapters Page, except Add/Change/Remove connections parameters and Edit configuration files	Yes	Yes	No
Remote Servers Page, except Add/Change/Remove connections parameters and Edit configuration files	Yes	Yes	No
Metadata and Procedures pages, except Configure Application Path	Yes	Yes	No
ETL page, except Configure Application Path	Yes	Yes	No
Start and stop the server	Yes	No	No

Web Console Task	Server Administrator	Application Administrator	Basic users
Create more Server or Application administrators	Yes	No	No

Agent Service

A server configuration needs at least one **agent service** with the name "DEFAULT", defined via a SERVICE block. An **agent service** is the 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 is running for a specific service, and each service may have different values for the settings defined at the service scope. Unless noted otherwise, Workspace Manager settings have global scope.

The settings on the Workspace Configuration page having service scope are as follows:

The maximum number of data access agents and the number of agents prestarted at server startup for a service are defined by maximum and number ready. The lifetime of a service's agents 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 can be put in a queue for the service (configured via queue size and queue time limit), and once connected their idle time can be limited via idle session limit.

Modes of Deployment

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. That is, 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 (see Security overview). With **security ON**, authentication is processed for every client logging on to the server. With **security OFF**, user identification and authentication is not required. Requests are processed as the server ID.

- In **pooled deployment**, a predetermined number of application agents can be used to support a large community of users, provided the application is designed to support the small LUW (Logical Unit of Work) concept. These application agents establish their application environments on startup and maintain their environments, including database connections between LUWs, for user connections. This option provides a way to reduce system resource usage and increase for the transaction processing type application. Pooled deployment executes the global server profile and the service profile only. Therefore, each application agent inherits the privileges of one user account. Determining the user account ID that all application agents will share depends on what operating system you are using and whether or not you have set external security on or off. On the server, each user in the pool shares the user ID of the pooled ID (configured via `pooled_user` and `pooled_password`).

The Workspace Configuration page can also be used to configure the following settings which have global scope: agent refresh, edaprint history, wc cookie expiration and `transaction_coordination_mode`.

Deferred Management Configuration

The `edaserve.cfg` settings corresponding to deferred features are managed separately via the Deferred Management Configuration screen. `dfm_int_min`, `dfm_int_max`, `dfm_maximum` and `dfm_maxuser` are about scheduling of deferred requests; `dfm_dir` and `dfm_maxage` are about deferred reports.

Monitoring Server Activity

Every server type can be monitored and operation parameters changed through the console. These changes can affect the behavior and the performance of the server. The following topics describe the screens used to perform such administrative tasks on a running server.

Clicking on **Workspace/Monitor** gives access to the monitoring screens by displaying the first screen in the right pane. Then the tabs at the top of the right pane are used to navigate between monitoring screens.

Server Statistics

The Statistics screen displays a list of statistics for the running server as collected by the Workspace Manager.

Note: Click the **Refresh Now** button to refresh the statistics. The information can be refreshed at pre-defined intervals by clicking on the checkbox and entering the number of seconds between each refresh.

Reference Server Statistics Parameters

This is a reference list of the parameters which can be displayed on the Server statistics page.

Parameter	Explanation
Workspace Manager Process ID	The operating system ID number for the current Workspace Manager process.
Started	Date and time when the current instance of the Workspace Manager was started.
Current Number of Agents	The number of agents that are currently running.
Peak Number of Agents	The maximum number of agents that have been running at any given time.
Current Number of Sessions	The number of sessions that are currently connected to agents.
Total Number of Sessions	The count of total sessions by all users since the server was started. Note that this is not necessarily the same as the total number of agents started since the server was started, because agents are often reused and can also be pre-started and not used.
Total Number of Connections	The count of total connections by all sessions since the server was started. Note that this is different from the total number of sessions since a persistent session can connect multiple times for different requests.
Average time in queue for above	Average number of seconds spent in queue for all connections, shown only when queuing has been turned on (maximum_q greater than zero).
Number of satisfied queued Connections	Total number of connections that were queued and were eventually successfully connected. Connections that were queued but then failed are not counted here.
Average time in queue for above	Average number of seconds waiting in queue before connecting for queued connections that eventually connected.
Number of queued Connections timed out	Total number of connections that went in the queue and timed out.

Parameter	Explanation
Number of Connections run	Total number of finished connections (corresponding session was suspended or disconnected), as opposed to the connections that might still be running at the time the statistics are sampled (corresponding session connected or resumed).
Average connection duration	See notes below.
Average agent processing time	See notes below.
Average running proportion	See notes below.
Peak number of queued connections	The maximum number of connections that have been queued at any given time.
EDATEMP available disk space	Number of kilobytes free on the disk used for EDATEMP directory, where the 'edatemp' subdirectory and EDAPRINT log are stored.
Number of security failures	Total number of connections that failed for security reasons.
Number of failures for no resources	Total number of connections rejected for lack of available agents. This includes timed out queued connections.

Notes:

1. Some of the variables above only appear if the corresponding total is not zero, grouped as follows:
 - total number of connections
 - avg time in queue for above (seconds)
 - number of satisfied queued connections
 - avg time in queue for above (seconds)
 - number of queued connections timed out
 - number of connections run
 - avg connection duration (seconds)
 - avg agent processing time (seconds)
 - avg running time proportion

2. Variables which are averages (avg) are fractional numbers of seconds rounded to the nearest millisecond for display purposes, but actually computed in higher precision (which is dependent on the operating system).

'connection duration' is a measure of waiting time + running (i.e. agent processing) time for a connection, which means it is really the time from the moment the user clicks to send his request (connect or resume) to the moment the answer is displayed back on the browser (suspend or disconnect)

'agent processing time' is the part of the connection duration that is only spent 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 3 corresponding averages is only limited by the precision of the operating system. In the rare case where a machine would be faster than its time-measuring precision, some accuracy side effects might occur.

For an individual connection which would have a duration shorter than the precision of the operating system, duration and running time cannot be measured and would be both 0, so the server would consider 100% running time. If there were a lot of these, the average proportion would tend to be overestimated.

On the other hand, 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 would be counted towards the average running time and in calculating the proportion so a 0% running time proportion would be recorded. If there were a lot of those, the average proportion would tend to be underestimated.

Monitoring Agents

The Agents screen displays the statistics for the current list of agents monitored by the Workspace Manager. From this screen the administrators can manage the existing agent processes (they can be monitored and stopped), and they can also pre-start new agents.

To stop an individual agent, click on the agent's row to access the contextual popup menu for that agent, and click on **Kill Agent**. The running agent will be terminated, which will invalidate any current connection to that agent. If a request is then issued from such a connection, an error message will be returned. Stopping an agent is therefore an emergency administrative measure as the application will be disrupted. Once an agent has been terminated, the Agents screen refreshes automatically. The corresponding row of the terminated agent remains, and the State is listed as 'stopping' until the row eventually disappears. For extreme situations, the **Kill All Agents** button at the top of the screen may be used to terminate all running agents.

Monitoring Server Activity

To pre-start new agents, type in the number of agents that you would like to start, and click **Start**. Additional agents can be started this way even when there are agents already running.

Note: Click the **Refresh Now** button to refresh the statistics displayed. The information can be refreshed at pre-defined intervals by clicking on the checkbox and entering the number of seconds between each refresh.

Reference Agent Statistics

This is a reference list of the parameters which can be displayed on the Agents page.

Note: You can click on an agent row to view additional statistics for that agent or to view the trace file for that agent if it is available.

Statistic	Explanation
Tscom ID	The identification number associated with the agent.
User	The user ID associated with the server connection.
State	<p>The current state of the agent. Possible values are starting, stopping, idle, in use, aborted or crashed.</p> <p><i>starting</i> and <i>stopping</i> are normal transitory states which are self-explanatory</p> <p><i>idle</i> is when the agent is not connected, i.e. it has no sessions at all, whether active or suspended</p> <p>an agent is <i>in use</i> as soon as a session connects and until it disconnects; this includes all time spent between session suspend and resume when the process is not using the CPU but still has resources allocated for at least one session</p> <p><i>aborted</i> and <i>crashed</i> 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 diagnostics purposes, the server administrator can clear (via kill) such agents once the problem has been investigated</p>
Session	The session ID uniquely identifying the currently active session.
Query Time	Indicates the last time that a request was made to the agent. This value is used to calculate the time an agent has been idle, in cases where idle agent limit has been set.
Last Command	Indicates the first 8 characters of the last instruction executed by the data access agent.
Foc/Ext IO	The first value is the number of FOCUS I/O operations performed by the agent. The second value is the number of External input operations performed by the agent.
CPU Time	Total CPU time used by the agent.
Memory Usage	Amount of memory in KB used by the agent.

Reference **Additional Agent Statistics**

The additional statistics displayed when clicking the View statistics option on an agent row are first the PID followed by system specific statistics for the agent process, then some additional portable statistics described below.

Statistic	Explanation
Number of Sessions	The current number of sessions connected to the agent.
Last Command	Indicates the last instruction executed by the agent against the Server.
Last masterfile name	Indicates the last masterfile used by the agent.
FOCUS I/O	Indicates the number of FOCUS database I/O operations performed by the agent.
External Database Input	Indicates the number of External Database rows retrieved for a TABLE command, or FIXFORM data captures for a MODIFY command performed by the agent.
Number of transactions or HLI commands	Indicates the number of transactions performed by the agent.

Monitoring Sessions

The Sessions screen displays the statistics for the current list of sessions assigned to data access agents, allowing administrators to monitor and if necessary kill individual sessions.

To terminate a session, click on the session's row to access the contextual popup menu for that session, and click on **Kill Session**. The session will be forcefully disconnected from its agent. Once a session has been terminated, the Sessions screen refreshes automatically. The corresponding row of the terminated session remains, and the State is listed as 'terminating' until the row eventually disappears.

Note: Click the **Refresh Now** button to refresh the statistics displayed. The information can be refreshed at pre-defined intervals by clicking on the checkbox and entering the number of seconds between each refresh.

Reference **Session Statistics**

This is a reference list of the parameters which can be displayed on the Sessions page.

Statistic	Explanation
Tscom ID	Identifies the agent to which the session is connected.
Session	The identification number associated with the session.
State	The current state of the session. Possible values are active, suspended or terminating. <i>active</i> is when the session is connected and active (not suspended) <i>suspended</i> is when the session is connected but suspended <i>terminating</i> is a transitory state when the session has been killed
User	The user ID who connected the session.
Last Query	Indicates the last time that a request was made by the session. This value is used to calculate the time a session has been idle, in cases where idle session limit has been set.
Last Command	Indicates the first 8 characters of the last instruction executed by the session within its agent.
Code Page	Indicates the character code page used by the client connected to the session.
Connected From	For some protocols, indicates the localization of the client who connected the session by displaying its network address (e.g. for TCP/IP the client's IP address will be displayed).
CPU Time	Total CPU time (seconds) used within the session.

Monitoring Connections

The Connections screen displays the statistics for the current list of connections, allowing 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: active and queued. An **active** connection is one that is assigned to a session in a data access agent. A **queued** connection is one for which there were 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.

To cancel a connection, click on the connection's row to access the contextual popup menu for that connection, and click on **Kill Connection**. For an active connection, its session will be forcefully disconnected from its agent. For a queued connection, it will simply be cancelled and the client will get the same error that it would get if queueing was off and there were no available agents (or if the queue was full).

Note: Click the **Refresh Now** button to refresh the statistics displayed. The information can be refreshed at pre-defined intervals by clicking on the checkbox and entering the number of seconds between each refresh.

Reference **Connection Statistics**

This is a reference list of the parameters which can be displayed on the Connections page.

Statistic	Explanation
Type	Identifies the connection type: connect or resume.
Status	The current status of the connection: active or queued. <i>active</i> is when there is a session associated with the connection <i>queued</i> is when there is no session yet because the connection is being queued (only happens if queueing is on)
Session	Identifies the session associated with the connection, if any.
User	The user ID who connected.
Security	Indicates the type of security used to connect: off (no security), trust, explicit or iwa.
Requester ID	Unique identifier for the network connection created by a listener.
Time In	Indicates the time at which the connection was activated or queued. This is the time value used to decide when a queued connection has timed out.
Connected From	Indicates the network address of the client who connected.

Deferred Statistics

The Deferred Statistics displays a list of statistics for deferred management.

Reference Deferred Management Statistics

The statistics that are listed are as follows:

- **DFM_Dir Available Disk space** is the amount of storage space available in the DFM_DIR directory. This allocation differs according to operating system. For Windows, it is the size of the drive where the server was configured.
- **Number of Requests Done Since Startup** is the total number of deferred requests that have been executed since the server was started.
- **Number of Response Ready** is the total number of deferred reports stored in the DFM_DIR directory.

Deferred List

The Deferred List screen is used to view the current status of all deferred reports, stop queuing or executing reports, or remove any report from the server.

Reference Deferred Focus Reports

The Summary of Deferred Status is as follows:

Status	Description
No Error	Done as Requested.
Ready	Response file is ready to be picked up.
Deleted	Response file has been deleted as requested.
Queuing	Request is waiting to be executed.
Bad Defer ID	Invalid ID or no request associated with that ID.
Bad User ID	Response File doesn't belong to that ID.
System Error	System failure, for example, out of memory, out of disk space.
Executing	Request is being executed.
Stopped	Request has been stopped as requested.
Agent Crashed	Agent crashed during execution, incomplete response file.
Connect Failed	Failed to connect to server, Communication error.
Unknown	Failed to determine request status, try again.

Reference Extension for Deferred Files

The summary of possible extension for the deferred files listed in the DFM_DIR Directory is as follows:

Extension	Description
RQD	Data file, contains user ID, optional flags, etc.
RQP	Request file, indicates request is being executed.
RQF	Completed Request file, ready to be executed.
RQI	Incomplete request file, request is being received.
RPF	Complete response file, ready to be retrieved.
RPI	Incomplete response file.
DEL	Request will be deleted.

Monitoring Listeners and Special Services

Clicking on **Listeners** opens the Listeners window which presents a tree view of listeners and special services in the left frame, and selected object statistics in the right frame. This allows administrators to view statistics of the listeners running in the Workspace Manager address space, and to quiesce and enable some listeners.

Note: Click the **Refresh Now** button to refresh the statistics displayed. The information can be refreshed at pre-defined intervals by clicking on the checkbox and entering the number of seconds between each refresh.

Reference Listeners Statistics

The statistics displayed for the Listeners list are:

Statistic	Description
Protocol	This identifies the type of the listener by displaying its network protocol (e.g. HTTP, TCP, SNA/LU6.2, ...). Note: OpenVMS as well as some UNIX platforms do not support SNA/LU62.
Status	This is the status of the listener. The possible values include: Active, Not Active, and Stopped.
PID/Job #	The process identification number, or Job # on OS/400, associated with each listener running in Workspace Manager address space. This job # was previously called PID on OS/400.
Port Number/Name	The port number or name associated with each listener.

Reference Special Services Statistics

The statistics displayed for the Special Services list are:

Statistic	Description
Type	This displays the type of the special service (e.g. FDS, DFM, ...).
Status	This is the status of the special service. The possible values include: Active, Not Active, and Stopped.
PID/Job #	The process identification number, or Job # on OS/400, associated with each special service running in Workspace Manager address space. This job # was previously called PID on OS/400.
Port Number	The port number associated with the special service, if applicable (for example, FDS).

Migrating Your Server

It is suggested that you migrate configuration information from previous releases after you have verified the proper basic installation of new release. To migrate from a previous release, enter the full path of the configuration instance directory (EDACONF) on the Migrate screen.

Configuring Traces

The Traces Configuration screen allows you to set the size limit of the trace files and select tracing options for various components of the server. Any selection made will be written into IBITRACE.FEX and will be in effect on the next server run.

The trace size limit specifies the maximum number of lines in the trace files. After the limit is reached, trace data will be dumped to an alternate file with the extension 'TRB'. Logging will continue into the trace file with extension 'TRC'.

There are an extensive number of components that can be traced and it is advisable to change from the default setting to custom at the suggestion of Customer Support.

Component	Description
Default Components	<ul style="list-style-type: none">• R1H• QOPSYS• PRH• NWH• NLS
All Components	All traceable server components.
Typical Components	<ul style="list-style-type: none">• CEH• NWH2• PRH• SQLAGGR• STMTRACE
Custom Components	Select components.

Traces can also be used to capture the server input and create a script file. To have this type of tracing, select custom components and choose the NWHSIM trace component only.

The IBITRACE settings will have

`SET TRACEON=NWHSIM`

Editing Configuration Files

It should be understood that manually editing configuration files requires extensive knowledge of the inner workings of the server. All files except VERSION.CFG are available for editing on the Web Console's Edit Configuration Related Files screen. VERSION.CFG is created by installation/configuration process and is available for viewing only from this screen.

Viewing and Editing Your License Number

The current license code can be viewed and changed via the License Management screen.

The license code is encoded to determine the configuration, additional products available in the configuration, the number of CPU's on the server and the number of user seats the configuration supports. Contact Customer Support or the local Information Builders sales office for more information on how to obtain a new license code.

Viewing and Editing Your License Number

CHAPTER 7

Managing Listeners and Special Services

Topic:

- Communications Configuration File

Clicking the **Listeners** menu item opens the Listeners and Special Services Configuration window which presents a list of configured Communication Nodes. You can modify communication parameters of existing nodes, remove existing nodes or add new nodes.

Note: You cannot delete the HTTP listener node, otherwise you would not be able to start the Administration Console after server restart.

Communications Configuration File

There are three major components that must be set to establish communication between a client and a server: the Client, the Protocol, and the Server.

A communication configuration file is broken down into blocks called NODEs. Each NODE is identified by name and represents one client, one server (i.e. a listener node), or one cluster and identified by the keyword CLASS. Each block also describes all parameters necessary for communication, security, etc.

Note: The client and agent must communicate using the same protocol.

See the following topics in the reference part of the documentation for details about the node syntax and for syntax specific to the different communication protocols supported in the server architecture:

- Syntax for the NODE Parameter
- Syntax for a Client Node Block
- Syntax for a Cluster Node Block
- Syntax for a Listener Node Block
- Syntax for a Special Service Client Node Block
- Syntax for a Special Service Listener Node Block
- TCP, HTTP, SOAP Protocol-specific Parameters
- SNA (LU6.2) Protocol-specific Parameters
- RFC Protocol-specific Parameters
- PIPE Protocol-specific Parameters
- MQXML Protocol-specific Parameters
- SMTP Protocol-specific Parameters

CHAPTER 8

Troubleshooting

Topics:

- Viewing Version Information
- Analyzing Server Activity
- Analyzing FOCUS Database Server Activity
- Enabling and Viewing Trace Files
- Recording and Reproducing User Actions
- Troubleshooting the Workspace Manager Web Console
- Workspace Manager Safe Mode

The Web Console allows the administrators to access several diagnostics tools which can be used to visualize different internal information. The following sections describe the screens used to access such information in order to perform problem analysis tasks.

Viewing Version Information

The Version information screen displays the main identification parameters of the server configuration that was in effect when the server was started. The parameters and their description are as follows:

Parameter	Explanation
Configuration date	Indicates the configuration date of the Server.
Build date, gen number, release, source date	Identify the release and build dates of a running instance of the Server.
Host Name	The name of the machine where the server was installed.
Server name	As defined in configuration file. Note: Used on Windows platforms as the system service name for the Server.

Analyzing Server Activity

The EDAPRINT screen of the diagnostics section of the Web Console allows you to view the current or prior server activity log (edaprint.log) from either a management perspective (Session and Connection activity), or a raw viewing of the log with or without filtering for certain components and IDs. The activity log records chronologically all server activity since the Workspace Manager was started: it not only contains basic activity information, but also server start up information and IBISNAP and shutdown information. IBISNAP is a snapshot of the server environment showing various usage statistics, listener, and agent statuses. If an abend has occurred, the snapshot will also contain additional debugger stack information that is useful in problem determination for Solution Programming staff.

Clicking the **View Using Selected Options** button from the EDAPRINT page, with the **Unfiltered Log** radio button selected, displays the raw EDAPRINT log file in a new window.

If the log display selection has filtering, then the output will contain only selected lines from the EDAPRINT log file.

Management reporting from the EDAPRINT page contains several selections that range from detailed, summary, or graph of session or connection activity.

You can also select a connection summary report, as well as a graphic representation.

A sample user-defined report is also available. To use this feature click the EDIT consusr.fex, make changes as needed, and click **Save**. Return to the EDAPRINT panel; click the **User Defined Report** selection, and then the **View Using Selected Options** button.

Analyzing FOCUS Database Server Activity

The HLIPRINT screen of the diagnostics section of the Web Console allows you to view the HLIPRINT log file that logs information from the FOCUS Database Server (FDS) Service.

Clicking on the **Show HLIPRINT** button will display the contents of the HLIPRINT log file in a new window.

Enabling and Viewing Trace Files

The Traces screen of the diagnostics section of the Web Console allows you to view traces and turn traces dynamically on or off for a running server. It is only available to the server administrators. It does not display for an end user ID.

If tracing is set to off and it has never been turned on, the screen will show that no traces are available and will allow you to turn traces on.

If you turned on tracing at server startup (e.g. on Windows systems by using Workspace Start with Traces from the Diagnostics menu), or you click the **Enable Traces** button, the screen will then display the available traces in drop-down boxes (which traces are available depend on what requests have been made against the server).

Clicking the **Enable Traces** button asks for confirmation before starting traces. This is in part to remind you that a dynamic trace is not the same as turning traces on at server startup. A dynamic trace is usually not sufficient for following a problem through with customer support, but it may suffice for other purposes, such as seeing how something is parsed.

To turn dynamic traces on or off for one user, SET TRACEUSER=ON or SET TRACEUSER=OFF should be present in the user profile.

SET TRACEUSER=tracename command can be used to turn dynamic traces on and set the trace name to tracename, where tracename includes the full path to the trace.

Note: The default for tracing is to trace all components when tracing is turned on, however, the trace settings file (ibitrace.fex) may have been altered. Therefore, components that you are expecting to be traced may not actually be traced in the first place. A trace setting may be viewed and set by clicking on the **Configuration** button to access the Traces Configuration screen.

Viewing a Trace File

With the radio button next to the Trace that you would like to view (Agent, WSM, Listener, or Installation Log), click the **Show the File** button. The trace file displays in a new browser window. If you had selected Filtering and nothing matches the requirements, the new window will contain the **No Trace for Given Component List** message.

Existing trace files can be filtered for errors before viewing the file by selecting the Errors radio button.

Recording and Reproducing User Actions

The Recording and Playback features allow the server to record the exact sequence of user actions applied through a browser, and then reproduce it (playback) as single or multiple users under the same or different conditions. Files generated by playback and record -- known as HTI script (http internal script) -- along with server traces are used for problem analyzing and testing.

Note: Recording and Playback are only available for Common Gateway Interface (CGI) connections.

Note: Click the **Refresh Now** button to refresh the statistics displayed. The information can be refreshed at pre-defined intervals by clicking the checkbox and entering the number of seconds between each refresh.

Once recording is started a script file gets created. This file is located in the catalog directory of the server. The file name can be edited before recording starts. By checking **Append to Existing**, any recording will be appended to the existing HTI script.

All commands issued through a CGI connection will be recorded. These commands can be run using the Procedures panel on the Web console.

Click the **Stop** button to stop the recording.

Note: Click the **Refresh Now** button to refresh the statistics displayed. The information can be refreshed at pre-defined intervals by clicking the checkbox and entering the number of seconds between each refresh.

Use the dropdown list to select the Script Name that was created. This Script can be edited by using Edit Script. Before starting the playback, click **Playback**, and select the parameters that will be used.

Reference **General Playback Parameters**

This section covers the general playback parameters that are available.

Parameters	Description
Number Of Threads	Is a positive number of threads to be used when playing the script. Each thread represents single client (user).
Interval Parameter	Used to specify timing in a multiple-client (multithreaded) playback. Possible formats of this value are m or m, n, k, where m is number of seconds between each client startup, and after each n started clients, an interval of k seconds will be used instead.
Compare Option	Determines if data received by every client (thread) is identical. Uses binary comparison mode and writes comparison result message to playback log file.
Immediate Processing	Ignores every SLEEP and WAIT statement in the HTI script. Issues HTTP requests without any delay between them.
Size Statistics	Displays general output files size statistics information for multiple-client playback in the log. This option can be useful when analyzing results of a playback with huge threads number.
Traces	Sets the Playback utility traces on or off. A trace file is then created for every thread.

Reference **Recording Hints**

When recording is on, the HTTP listener is recording every CGI request. Make sure nobody else is submitting requests to the same listener.

It is recommended to open a separate instance of a browser before recording and dealing with actual operations to be recorded, and switching recording on or off in two different windows.

Do not try to record script from the middle of a persistent session. Always try to use user ID and password, then recording the first request.

Playback Log Files

Playback log files are generated during script playback. Every file contains general information about playback processing, such as threads startup and termination, connect errors and comparison results.

Log file names are built using script file name and log extension. Two additional log files (*stdout* and *stdlog*), if not empty, contain a description of errors in case of playback failure caused by critical errors.

Troubleshooting the Workspace Manager Web Console

If the web browser has problems accessing the Web Console, you may see the following message:

Error Message	Troubleshooting Tips
Internet Explorer cannot open the Internet site http://address:http_service. A connection with the server could not be established.	Check to make sure the Workspace Manager is running or else contact the local system administrator.
There was no response. The server could be down or is not responding. If you are unable to connect again later, contact the server's administrator.	Check to make sure the Workspace Manager is running or else contact the local system administrator.

Workspace Manager Safe Mode

If the configuration files contain some non fatal errors that prevent the server from coming up in a consistent state, the Workspace Manager will start in *safe mode*. In this mode only the Web Console will be operational. This will permit the administrator to check for errors via Diagnostics EDAPRINT page of the Web Console (the errors that trigger the safe mode would be visible in the edaprint log), correct the problem via Workspace Configuration page(s) and then restart the server.

Index

A

active connections 6-11
administering servers 1-1 to 1-2, 6-1 to 6-2
agent monitoring 6-7, 6-9 to 6-10
agent services 6-3
application administrators 6-2
application directories 4-2
application paths 4-1 to 4-2

C

client node blocks 7-2
cluster node blocks 7-2
communications configuration 1-4
communications configuration files 7-1 to 7-2
communications configuration worksheets 1-5 to 1-7
configuration files 2-1
 editing 6-17
configuring communications 1-4
 worksheets 1-5 to 1-7
configuring data adapters 2-1 to 2-2
configuring server trace files 6-16
configuring servers 1-1 to 1-3, 6-1 to 6-2
connection monitoring 6-11 to 6-12
console security 1-7, 1-9

D

data adapters 2-1 to 2-2
 configuring 2-1 to 2-2

deferred file extensions 6-14
deferred FOCUS reports 6-13
Deferred List page 6-13
deferred management statistics 6-13
deferred procedure execution 5-2, 6-4
Deferred Statistics page 6-13
diagnostics for servers 8-1, 8-6
 EDAPRINT files 8-2
 HLIPRINT files 8-3
 record and playback 8-4 to 8-6
 safe mode 8-6
 trace files 8-3

E

EDAPRINT files 8-2
edaserve.cfg configuration files 2-1, 6-1
edasprof.prf profiles 2-1
editing server configuration files 6-17
extensions for deferred files 6-14

G

global server profiles 2-1

H

HLIPRINT files 8-3
HTTP communications 1-4

I

inbound communications 1-5 to 1-6
 configuration worksheets 1-5 to 1-6

L

LDAP support 1-9

Index

License Management page 6-17

listener node blocks 7-2

listener statistics 6-15

listeners 7-1 to 7-2
monitoring 6-14

LU6.2 communications 1-4
configuration worksheets 1-6

M

managing metadata 4-1, 4-3

managing servers 1-1 to 1-2, 6-1 to 6-2

metadata management 4-1, 4-3

migrating servers 6-16

modes of server deployment 6-3

monitoring listeners 6-14 to 6-15

monitoring server activity 6-4 to 6-5, 6-7, 6-9 to 6-16

monitoring server agents 6-7, 6-9 to 6-10

monitoring server connections 6-11 to 6-12

monitoring server sessions 6-10 to 6-11

monitoring special services 6-14 to 6-15

N

named pipes communications 1-4

NODE parameter 7-2

O

outbound communications 1-6 to 1-7
configuration worksheets 1-6 to 1-7

P

PIPE communications 1-4

playback log files 8-6

playback of user actions 8-4 to 8-6

pooled server deployment mode 6-3

private server deployment mode 6-3

procedures 5-1 to 5-2

Q

queued connections 6-11

R

recording user actions 8-4 to 8-6

remote servers 3-1
configuring 3-1

S

safe mode 8-6

security for servers 1-7 to 1-9

server administration 1-1 to 1-2, 6-1 to 6-2

server administrators 6-2

server configuration 1-1 to 1-3, 6-1 to 6-2

server configuration files 2-1, 6-1
editing 6-17

server deployment modes 6-3

server diagnostics 8-1, 8-6
EDAPRINT files 8-2
HLIPRINT files 8-3
record and playback 8-4 to 8-6
safe mode 8-6
trace files 8-3

server management 1-1 to 1-2, 6-1 to 6-2

server metadata 4-1, 4-3

server migration 6-16

server profiles 2-1

server security 1-7 to 1-9

- server statistics 6-4 to 6-5
- server trace files 6-16
- session monitoring 6-10 to 6-11
- SNA (LU6.2) communications 1-4
 - configuration worksheets 1-6
- special service node blocks 7-2
- special services 7-1
 - monitoring 6-14
 - statistics 6-15
- stdlog log files 8-6
- stdout log files 8-6

T

- TCP/IP communications 1-4
 - configuration worksheets 1-5 to 1-7
- trace files 6-16, 8-3
- troubleshooting servers 8-1, 8-6
 - EDAPRINT files 8-2
 - HLIPRINT files 8-3
 - record and playback 8-4 to 8-6
 - safe mode 8-6
 - trace files 8-3

V

- version information 8-2

W

- WCPROTECT security setting 1-7, 1-9
- Web Console 1-1 to 1-2, 6-1 to 6-2
 - troubleshooting 8-1 to 8-6
- worksheets 1-5 to 1-7
 - communications configuration 1-5 to 1-7
- Workspace Manager 1-2, 6-1
 - configuring 6-2
 - monitoring server activity 6-4 to 6-5, 6-7, 6-9 to 6-16

Reader Comments

In an ongoing effort to produce effective documentation, the Documentation Services staff at Information Builders welcomes any opinion you can offer regarding this manual.

Please use this form to relay suggestions for improving this publication or to alert us to corrections. Identify specific pages where applicable. You can contact us through the following methods:

Mail: Documentation Services - Customer Support
Information Builders, Inc.
Two Penn Plaza
New York, NY 10121-2898

Fax: (212) 967-0460

E-mail: books_info@ibi.com

Web form: <http://www.informationbuilders.com/bookstore/derf.html>

Name: _____

Company: _____

Address: _____

Telephone: _____ Date: _____

E-mail: _____

Comments:

Reader Comments

Information Builders, Two Penn Plaza, New York, NY 10121-2898

(212) 736-4433

iWay Server Administration for UNIX, Windows NT, OpenVMS, OS/400, OS/390, and z/OS

Version 5 Release 2.0

DN3501110.0103