Appeon Server Configuration Guide for J2EE

Appeon® 6.2 for PowerBuilder®

Contents

1 About This Book

1.1 Audience

This book is intended for users and system administrators that are responsible for the configuration of servers used in the Appeon for PowerBuilder architecture.

1.2 How to use this book

There are five chapters in this book.

Chapter 1: About This Book

        A general description of this book

Chapter 2: Server Configuration Tasks

        Describes configuration stages and tasks related to Appeon Server.

Chapter 3: Appeon Server Status Monitor

        Describes how to configure and use Appeon Server Status Monitor.

Chapter 4: Database Connection Setup

        Describes how to set up connection between Appeon Server and Database Server.

Chapter 5: AEM User Guide

        Describes how to configure Appeon Enterprise Manager.

1.3 Related documents

Appeon provides the following user documents to assist you in understanding Appeon for PowerBuilder and its capabilities:

- *Appeon Demo Applications Tutorial*:

Introduces Appeon's demo applications, including the Appeon Sales Application Demo, Appeon Code Examples, Appeon ACF Demo, and Appeon Pet World, which illustrate Appeon's capability in converting PowerBuilder applications to the Web.

- *Appeon Developer User Guide* (or *Working with Appeon Developer Toolbar*)

Provides instructions on how to use the Appeon Developer toolbar in Appeon 6.2.

Working with Appeon Developer Toolbar is an HTML version of the *Appeon Developer User Guide*.

- *Appeon Server Configuration Guide*

Provides instructions on how to configure Appeon Server Status Monitor, establish connections between Appeon Server and Database Server and configure AEM for maintaining Appeon Server and Appeon deployed Web applications.

- *Appeon Supported Features Guide* (or *Appeon Features Help*):

Provides a detailed list of PowerBuilder features that are supported and can be converted to the Web with Appeon, and features that are unsupported.

Appeon Features Help is an HTML version of the *Appeon Supported Features Guide*.

- *Appeon Installation Guide*:

Provides instructions on how to install Appeon for PowerBuilder successfully.

- *Appeon Migration Guide*:

A process-oriented guide that illustrates the complete diagram of the Appeon Web migration procedure and various topics related to steps in the procedure, and includes a tutorial that walks the user through the entire process of deploying a small PowerBuilder application to the Web.

- *Appeon Performance Tuning Guide*:

Provides instructions on how to modify a PowerBuilder application to achieve better performance with its corresponding Web application.

- *Appeon Troubleshooting Guide*:

Provides information about troubleshooting issues, covering topics such as product installation, Web deployment, AEM, Web application runtime, etc.

- *Introduction to Appeon*:

Guides you through all the documents included in Appeon 6.2 for PowerBuilder.

- *New Features Guide* (or *What's New in Appeon*):

Introduces new features and changes in Appeon 6.2 for PowerBuilder.

What's New in Appeon is an HTML version of the *New Features Guide*.

1.4 If you need help

Each Sybase installation that has purchased a support contract has one or more designated people who are authorized to contact Sybase Technical Support or an Authorized Sybase Support Partner. If you have any questions about this product, or if you need assistance during the installation process, ask the designated person to contact Sybase Technical Support, or an Authorized Sybase Support Partner based on your support contract. You may access the Technical Support Web site at http://www.sybase.com/support.

2 Server Configuration Tasks

2.1 Overview

Server configuration for Web architecture is usually a daunting task that requires a wide range of server knowledge. The same rule applies to Appeon architecture. Appeon architecture resides in at least three types of servers: Web server, application server, and database server. Each server involves a third-party server product: for example, Appeon Server can be installed to EAServer, WebLogic, and WebSphere. A number of configuration tasks must be performed before an Appeon application can work on the Web, and still there is more involved in the maintenance and management of the server.

This chapter will help you understand the configurations in this guide and will assist you to quickly locate the correct configuration information.

2.2 Scope of configurations discussed in this book

Appeon architecture is a typical Web architecture that can provide development and runtime environments for both Appeon and non-Appeon applications. This book focuses on the configurations for supporting Appeon applications in the architecture, and does not provide: (1) configurations for setting up the architecture, (2) configurations specific to the functioning and performance of third-party servers within the architecture.

The configurations needed for setting up the architecture are discussed in the other documents, and therefore, will not be addressed in this guide. The following configuration instructions can be found in the *Web Server Configuration Guide* in Appeon Help. :

- Third-party Web server configuration: configuring Apache or IIS Web server to work with Appeon Server.

- Appeon Server load-balancing configuration: configuring the Appeon Server load-balancing feature.

- The following configuration instructions can be found in the *Appeon Installation Guide*:

- Configuration for supporting dynamic DataWindows: this one-time configuration at the database server enables dynamic DataWindows for all Appeon applications.

- Configuration for patching the ASE chained mode issue: this one-time configuration at the database server can patch the ASE chained mode issue for all Appeon applications.

Configurations specific to the functioning and performance of third-party servers in Appeon architecture may still impact the architecture. For example, indexing database tables has nothing to do with Appeon knowledge but can greatly improve the performance of an Appeon application. Although such configurations are not provided in this book, it is strongly recommended that you refer to the configuration documents of any third-party servers used and perform necessary configurations to achieve the best possible performance of Appeon architecture.

2.3 Configuration stages and tasks

Server configuration is divided into several stages as shown in Table 2-1. Understanding which stage of the configuration, allows one to simply focus on the configurations recommended for that particular stage. This helps save time and effort of searching through the complete document for information.

Table 2-1: Sever configuration stages

Configuration During…	For the Purpose of …
Application Deployment	Ensuring that the application data displays correctly and that all functions in the application work correctly.
Debugging Process	Efficient debugging.
Security Management	Managing the security of applications and servers within the architecture.
Performance Management	Improving server performance.
Server Information Management	Managing server-related information.
Emergency Control	Restarting Appeon Server automatically when it shuts down.

After reading the introduction in this section, you will find that most of the configurations can be performed in Appeon Enterprise Manager (AEM). AEM is a Web tool designed for managing Appeon Server and deployed Web applications over the Internet or an intranet and can greatly simplify configuration.

2.3.1 Configuration during application deployment

Table 2-2 lists the server configuration tasks for ensuring that application data displays correctly and that all functions within the application work. Tasks marked as "in AEM" are performed in AEM.

Table 2-2: Configuration tasks during application deployment

Task	Description	See section
Database Connection	Establish the database connection between the application server and the database server by configuring connection caches (also called data sources).	4
(In AEM) Connection Cache		5.3.11
(In AEM) Basic Information	Display PowerBuilder version, application size, and the DLL/OCX file size.	5.4.2
(In AEM) Transaction Object	Set up static mapping between application transaction objects and connection caches (or data sources).	5.4.3
(In AEM) Charset	Specify the input charset and database charset to ensure characters in applications display correctly.	5.4.4
(In AEM) DLL/OCX Files Download	Configure the mode for installing and downloading DLL and OCX files used in an application.	5.4.8

(In AEM) Registry Mode	Enable Web applications to directly access the client machine Windows registry or use Appeon registry emulation, so that PowerBuilder registry functions will work properly.	5.4.9
(In AEM) INI File Mode	Make Web applications manipulate the INI files at the client or by Appeon emulation, so that INI file function will work properly.	5.4.11
(In AEM) Error Message Mode	Specify the display mode for errors in different levels. They can be displayed in the status bar or in popup messages.	5.4.12
(In AEM) Decimal Precision	Select a proper decimal precision for the Web application.	5.4.15

2.3.2 Configuration during debugging

Table 2-3 lists the server configuration tasks for efficient debugging in case of abnormal behavior of Appeon applications.

Table 2-3: Configuration tasks during debugging process

Task	Description	See section
(In AEM) Log Files	Set the log file generation mode.	5.3.5
(In AEM) Log Viewer	View the log files generated by Appeon Server or the application server.	5.3.6
(In AEM) Run Mode	Set the run mode for Web applications.	5.4.13

2.3.3 Configuration during security management

Table 2-4 lists the server configuration tasks for managing the security of applications and servers in Appeon architecture.

Table 2-4: Configuration tasks during security management

Task	Description	See section
Database security	Implement script-coded and database security for applications	4.5
(In AEM) AEM Login	Modify the AEM user name and password.	5.5.2
(In AEM) System Settings	Set the system security mode and type.	5.5.3
(In AEM) Application Security	Limit the accessibility of an Appeon application to selected groups.	5.5.4
(In AEM) Group Management	Create groups and grant access rights.	5.5.5
(In AEM) User Management	Create user profiles and grant access rights.	5.5.6

(In AEM) Deployment Security	Limit the number of users permitted to deploy applications to Appeon Server.	5.5.7

2.3.4 Configuration during performance management

Table 2-5 lists the server configuration tasks for improving server performance.

Note: In order to maximize the performance of Appeon architecture, besides the tasks in the table, you must also follow instructions from the documents of all the related third-party servers.

Table 2-5: Configuration tasks during performance management

Task	Description	See section
(In AEM) Active Sessions	Monitor all active sessions in the system. Some sessions can be killed if necessary.	5.3.2
(In AEM) Active Transactions	Monitor all active transactions in the system. Some active transactions can be killed if necessary.	5.3.3
(In AEM) Temporary Files Cleanup	Set the schedule for automatically clearing temporary files, or manually deleting temporary files.	5.3.7
(In AEM) Deployment Sessions	Monitor all active deployment sessions in the system. Some active deployment sessions can be killed if necessary.	5.3.8
(In AEM) Application Server Cache	Allocate server cache between deployed applications. Ensures that important applications are cached.	5.4.6
(In AEM) DataWindow Data Cache	Cache DataWindow data on the Web server to improve data-reading performance.	5.4.7
(In AEM) Multi-Thread Download	Download static resources with multi-threads to boost performance.	5.4.10
(In AEM) Transfer Encoding	Choose the proper encoding mode to reduce network traffic.	5.4.14

2.3.5 Configuration during server information management

Table 2-6 lists the server configuration tasks for managing server-related information.

Table 2-6: Configuration tasks during server information management

Task	Description	See section
(In AEM) Web	Set the temporary files path, PDF printer name, session timeout, transaction timeout, download timeout and receive timeout.	5.3.4
(In AEM) Cluster	Specify connection information for all Appeon Servers used within the architecture.	5.3.9

(In AEM) Licensing	View license information.	5.3.10

2.3.6 Configuration for emergency control

Table 2-7 lists the server configuration task with which Appeon Server can be started automatically when it shuts down.

Table 2-7: Configuration tasks for emergency control

Task	Description	See section
Status Monitor	Configure the Appeon Server Status Monitor so it can be used for restarting Appeon Server automatically.	3

3 Appeon Server Status Monitor

3.1 Overview

IMPORTANT NOTE: Appeon Server Status Monitor works with WebLogic, WebSphere, and EAServer 5.x, but does not work with EAServer 6.x.

Appeon Server Status Monitor (hereinafter referred to as "Status Monitor") is a small program installed along with Appeon Server. It backs up Appeon Server session information, monitors if Appeon Server is in "started" status, and in the event that the Server shuts down it automatically restarts Appeon Server and recovers the runtime information.

3.2 Configuring Status Monitor

Verify the presence of the following files according to the Appeon Server type. Each will need to be configured, with the exception of appeonserver.jar, before Status Monitor can be run successfully.

Appeon Server	Windows	Unix\Linux
EAServer	<Appeon Home>\bin\appeonmonitor.bat <Appeon Home>\bin\appeonserver.bat <Appeon Home>\config\monitor.props	<Appeon Home>/bin/appeonmonitor.sh <Appeon Home>/bin/appeonserver.sh <Appeon Home>/config/monitor.props
WebLogic	<Appeon Home>\bin\appeonmonitor.bat <Appeon Home>\lib\appeonserver.jar <Appeon Home>\bin\appeonserver.bat <Appeon Home>\config\monitor.props	<Appeon Home>/bin/appeonmonitor.sh <Appeon Home>/lib/appeonserver.jar <Appeon Home>/bin/appeonserver.sh <Appeon Home>/config/monitor.props
WebSphere	<Appeon Home>\lib\appeonserver.jar <Appeon Home>\bin\appeonmonitor.bat <Appeon Home>\bin\appeonserver.bat <Appeon Home>\config\monitor.props	<Appeon Home>/lib/appeonserver.jar <Appeon Home>/bin/appeonmonitor.sh <Appeon Home>/bin/appeonserver.sh <Appeon Home>/config/monitor.props

Notes:

1) <Appeon Home> indicates the installation path of Appeon Server.

2) Changes to the files will take effect after the Status Monitor is restarted.

3.2.1 Configuring appeonmonitor.bat

The *appeonmonitor.bat* file (Windows) or *appeonmonitor.sh* file (Unix\Linux) is the batch program run by Status Monitor.

Make the following changes to the settings in *appeonmonitor.bat* file (Windows) or *appeonmonitor.sh* file (Unix\Linux).

For appeonmonitor.bat and appeonmonitor.sh files, the settings and modification are almost the same. The only difference is that forward slash ("/") is used as the path separator in Unix\Linux while back slash ("\") is used in Windows.

Table 3-1: Settings in appeonmonitor.bat

Settings	Description
JAVA_HOME	Specifies the JDK location, which must be the same one used by Appeon Server.
	For example, for EAServer running on Windows, the value of JAVA_HOME is:
	JAVA_HOME=C:\Program Files\Sybase\Shared\jdk1.4.1_03.
	Note: 1) If Appeon Server works on WebLogic, verify that the WLS_USER and WLS_PW variables in the startWebLogic.cmd (Windows) or startWebLogic.sh (Unix\Linux) file contain the correct login credentials.
	2) If Appeon Server works on WebSphere, only when the IBM JDK is used can Status Monitor function properly.
APPEON_HOME	Specifies the Appeon Server home directory.
	EAServer: <JAGUAR>\appeon
	WebSphere: <WAS_HOME>\appeon
	WebLogic: <WL_DOMAIN>\appeon
	Note: <JAGUAR> indicates the EAServer installation directory; <WAS_HOME> indicates the home directory of WebSphere server; and <WL_DOMAIN> indicates the domain path of WebLogic.
	For example, if Appeon Server works on EAServer, the Appeon Server home directory is: APPEON_HOME= C:\Program Files\Sybase\EAServer\appeon.
J2EE_JAR	Changes the default setting according to the Appeon Server in use:
	EAServer: <JAGUAR>\java\lib\eas-server-15.jar
	WebLogic: <WL_HOME>\server\lib\weblogic.jar
	WebSphere: <WAS_HOME>\lib\j2ee.jar
	For example, if Appeon Server works on EAServer, the home directory is: J2EE_JAR=C:\Program Files\Sybase\EAServer\java\lib\eas-server-15.jar.
CLASS_PATH	Default setting:
	CLASS_PATH=%APPEON_HOME%\..\java\lib\appeon_server.jar;%J2EE_JAR%
	You do not need to make any changes to the default setting.

3.2.2 Configuring appeonserver.bat

The *appeonserver.bat* file (Windows) or *appeonserver.sh* file (Unix\Linux) is the batch program run by Status Monitor when it detects that Appeon Server has shut down.

3.2.2.a Configuring appeonserver.bat (Windows)

The *appeonserver.bat* file contains the following code:

```
REM if use EAServer, please uncomment the line below.
REM start cmd /c "<EAServer>\bin\run-server.bat" -jvmtype server
```

```
REM if use WebLogic, please uncomment the line below.
REM start cmd /c "<Domain>\startWebLogic.cmd"

REM if use WebSphere, please uncomment the line below.
REM start cmd /c "<WebSphere>\AppServer\bin\startServer.bat"
server1
```

Make the following changes to the file:

1. Remove the notation "REM" before the command line that starts the application server/Appeon Server.

2. Replace the wildcard character string, which stands for the application server, with the home directory of the application server.

For example, if Appeon Server works on EAServer, the following script should be modified.

Original script:

```
REM start cmd /c "<EAServer>\bin\run-server.bat" -jvmtype server
```

Modified script:

```
start cmd /c "C:\Program Files\Sybase\EAServer\bin\run-server.bat"
-jvmtype server
```

3.2.2.b Configuring appeonserver.sh (Unix\Linux)

The *appeonserver.sh* file contains the following script:

```
#If use EAServer, please uncomment the line below.
#"<EAServer>/bin/serverstart.sh" -jvmtype server

#If use WebLogic, please uncomment the line below.
#"<Domain>/startWebLogic.sh"

#If use WebSphere, please uncomment the line below.
#"<WebSphere>/AppServer/bin/startServer.sh" server1
```

Make the following changes to the file:

- Remove the notation "#" before the command line that starts the application server/Appeon Server.

- Replace the wildcard character string that stands for the application server, with the home directory of the application server.

For example, if Appeon Server is installed to EAServer, the following script should be modified.

Original script:

```
#"<EAServer>/bin/serverstart.sh" -jvmtype server
```

Modified script:

```
"/export/home/user/Sybase/EAServer/bin/serverstart.sh" -jvmtype
server
```

3.2.3 Configuring monitor.pros

The *monitor.pros* file contains the property settings of Status Monitor.

Make the following changes to the property settings in *monitor.pros*, as shown in Table 3-2.

Table 3-2: Settings in monitor.pros

Setting	Description
com.appeon.server.monitor.instance.names	The names of server instances that need to be monitored. Separate multiple instance names with comma (",").
com.appeon.server.monitor.instance.cpus	The information for CPU(s) of the server instances. The value ranges from CPU0 to CPU31. The value can also be an asterisk ("*"), which stands for all CPUs of the local machine. If there are more than one server, their names should be separated by comma (",") and ranked in the same order with com.appeon.server.monitor.instance.names. If one server has multiple CPUs, they can be connected by the plus sign ("+").
com.appeon.server.monitor.instance.ports	The port via which Status Monitor monitors Appeon Server. Separate multiple server instances with comma (",") and range them in the same order with com.appeon.server.monitor.instance.names. Make sure the port number you specify is not occupied. Note that changes to this setting will not take effect until Appeon Server is restarted.
com.appeon.server.monitor.instance.files	The files that Status Monitor will check when the server shuts down. If there are more than one server instance, separate them with comma (",") and range them in the same order with com.appeon.server.monitor.instance.names.
com.appeon.server.monitor.instance.commandlines	The command line for starting Appeon Server. Default setting: com.appeon.server.monitor.instance.commandlines=appeonserver.bat If there are more than one server instance, separate them with comma (",") and range them in the same order with com.appeon.server.monitor.instance.names.
com.appeon.server.monitor.mail.smtp.server	The mail server that Status Monitor uses for sending notification emails. Contact your network administrator to get the valid mail server that can be accessed from the machine.

com.appeon.server.monitor.mail.smtp.recievers	The email address(es) of the recipient(s) to who Status Monitor will send the notification emails. It can contain one or multiple email addresses.
	Use the comma (",") as the email address separator if you want to specify multiple email receivers.
	The auto-mail functionality will not work unless being specified.
com.appeon.server.monitor.mail.smtp.port	The port number that is specified for the mail server.
	Contact your network administrator to get the valid port number of the mail server specified. The default port number is "25".
com.appeon.server.monitor.mail.smtp.sender.account	The account for sending mails.
	If the mail server uses SMTP to validate, an account for sending mails must be specified. Otherwise anonymous mails will be sent.
com.appeon.server.monitor.mail.smtp.sender.password	The password for sending mails.
	If the mail server uses SMTP to validate, a password must be specified.
com.appeon.server.monitor.session.checkcycle	The cycle for automatic backup.
	The unit is second.
com.appeon.server.monitor.session.backup	The switch for turning on/off session auto-backup.
	Specify the value to true or false.
com.appeon.server.monitor.memory.checkcycle	The cycle for checking memory information.
	The unit is second.
com.appeon.server.monitor.memory.maxvalue	The maximum value for memory usage.
	The value ranges from 0 to 100.
	If the memory usage reaches the peak, the Status Monitor will check the existence of active sessions. If there is none, the monitor will immediately restart the server instance(s). If there is one or more active sessions, the monitor will determine whether to restart the server instance(s) according to the restart flag. Before the restart, the monitor will determine whether the sessions will be backed up according the backup settings.
com.appeon.server.monitor.memory.minvalue	The minimum value for memory usage.
	The value ranges from 0 to 100.
	If the memory usage reaches the bottom, the Status Monitor will check the existence of active sessions. If there is none, the monitor will immediately restart the server instance(s). If there is one or more, the monitor will continue checking until the memory usage reaches the peak.
com.appeons.erver.monitor.memory.restart	The switch to restart serve instance by force when the memory usage reaches the peak.
	The value can be true or false.

com.appeon.server.monitor.scheduled.task. cycle	The cycle for scheduled tasks. The value can be daily, weekly or monthly, among which only the daily mode is supported at present.
com.appeon.server.monitor.scheduled.task. when	The moment to start carrying out scheduled tasks. The value ranges from 00:00:00 to 23:59:59.
com.appeon.server.monitor.scheduled.task. restart	The switch to restart server instance(s) if active sessions still exist when starting to carry out scheduled tasks. The value can be true or false.

3.2.4 Additional configuration required for Status Monitor in Appeon Server cluster

If an Appeon Server works in a cluster, the Appeon Server will not only back up the "active" sessions but also the "passive" sessions. The "passive" sessions are remote sessions created by another Appeon Server in the cluster and backed up in the current Appeon Server.

The "active" sessions for an Appeon Server will always be restored if that Appeon Server shuts down abnormally and then is restarted by its Status Monitor, while the "passive" sessions will be restored only if you select the "Enable Logical Restore with Status Monitor" option in the AEM Cluster tool. If this option is not selected, Status Monitor will only restore the "active" sessions and will not restore the "passive" sessions on an Appeon Server.

3.3 Information backed up by Status Monitor

Status Monitor detects Appeon Server status, backs up and restores session information, and automatically restarts Appeon Server every time Appeon Server is detected "shut-down". This is very helpful, because Status Monitor detects if Appeon Server shuts down abnormally, and will automatically restart Appeon Server while restoring the most recent state of Appeon Server based on the last backup.

3.3.1 What is backed up?

Status Monitor periodically backs up Appeon Server session information that includes:

- User authentication information

- References to Appeon Server transaction components

- References to NVO components (for EAServer only)

Status Monitor does not back up:

- Information being processed in active transactions

- States of stateful NVOs.

3.4 Using Status Monitor

3.4.1 Starting Status Monitor

Step 1 – Locate the *bin* subdirectory under <Appeon Home>/bin where *appeonmonitor.bat* (Windows) or *appeonmonitor.sh* (Unix\Linux) is stored. For example: C:\Program Files\Sybase\EAServer\appeon\bin.

Step 2 – Run the *appeonmonitor.bat* file (Windows) or *appeonmonitor.sh* (Unix\Linux) to start Status Monitor.

Note: In Unix\Linux, be sure to run Status Monitor in the background by executing the command "nohup statusmonitor.sh &". If Status Monitor runs in the foreground, executing a ctrl-c command for Status Monitor will stop both the Status Monitor and the Appeon Server process started by Status Monitor.

Once Status Monitor is successfully started, the Status Monitor window displays, indicating that Status Monitor is functioning. To keep the Status Monitor running you must keep the window open or minimized. If you close the Status Monitor window, Status Monitor stops working, and loses the information that has been backed up.

3.4.2 Understanding the information in Status Monitor Window

Once Status Monitor and Appeon Server are simultaneously running, the Status Monitor window as well as the configuration information will display as illustrated in Figure 3-1.

Figure 3-1: Status Monitor window
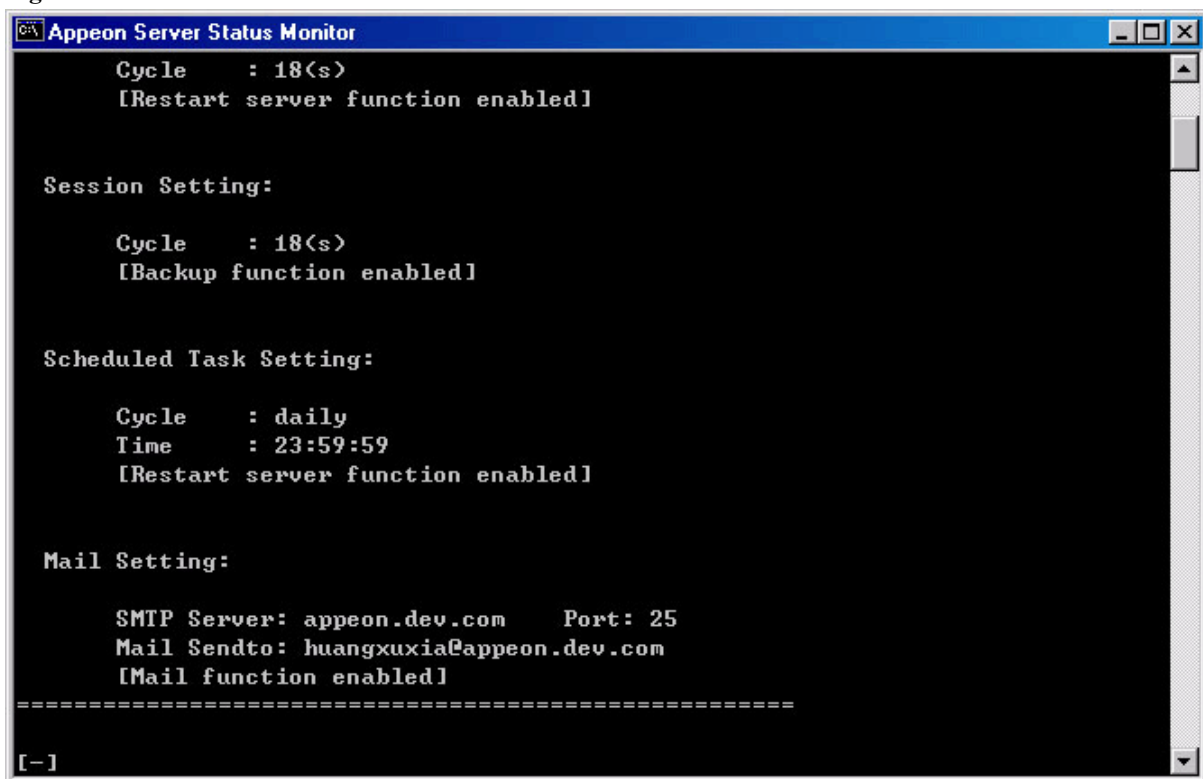
Appeon Server Status Monitor can monitor one or multiple server instances at the same time. You can tell how many server instances are configured for being monitored from the signs at the bottom left of the window. As shown in the above figure, there is only one server instance configured for being monitored. If the sign is shown as "[S]", the server instance is shut down.

4 Database Connection Setup

4.1 Overview

The steps for configuring the database for an Appeon-deployed application are the same as the steps for configuring the database for a PowerBuilder application. However, the way the database server is accessed is different: a PowerBuilder application directly accesses the database server via transaction object(s), while an Appeon-deployed application accesses the database server via Appeon Server connection caches (or data source).

This chapter describes how to enable a deployed application to access its database. Two key tasks are involved:

- Setting up communication between the database server and Appeon Server. This refers to setting up Appeon Server connection caches (or data sources).

- Setting up communication between the deployed application and Appeon Server. This refers to setting up the mapping between the application transaction objects and Appeon Server connection caches (or data sources).

Some advanced configurations are also related to database connection setup (for example, database auditing). This chapter outlines common techniques for handling such configurations in the Appeon environment.

4.2 What is Appeon Server connection cache\data source?

Appeon Server connection cache is also called **Appeon Server data source** which is actually the same terminology as **connection cache** in EAServer 5.x and **data source** in EAServer 6.x, WebLogic, and WebSphere. The only difference between them is the configuration tool:

- Appeon Server connection cache (**for EAServer 5.x**) can be configured in either Appeon Server AEM or EAServer Manager. The connection cache tool in EAServer Manager is made accessible from AEM for convenience, and changes you made in either AEM or EAServer Manager will be synchronized to the other.

  Refer to the following section for instructions on setting up connection caches for various database types in AEM. If you have problems creating connection caches, refer to the documentations from the database/JDBC driver vendor or Sybase EAServer.

- Appeon Server data source (**for EAServer 6.x**, WebLogic, and WebSphere) can only be configured in their corresponding application server management console.

  For detailed instructions, please refer to the corresponding documents of EAServer, WebLogic or WebSphere.

4.2.1 Why Appeon Server connection cache\data source?

The connection cache (or data source) for a Web application is the counterpart to the transaction object in the target PowerBuilder application. The transaction properties in the target PowerBuilder application contain database connection parameters, which should be correspondingly configured in connection caches.

Appeon Web applications rely on Appeon Server connection caches to interact with the database servers. When creating a connection cache, you can use different JDBC drivers. However, Appeon has some recommendations on which JDBC driver is to be used for certain types of databases.

4.2.2 Why JDBC driver only?

In Appeon Web applications, data-related operations are managed by Appeon Server. The data related operations are built with J2EE technology and they require the JDBC interface. Regardless of the interface (ODBC, JDBC, or native driver) target PowerBuilder application uses for its database connection, the Web application must use JDBC.

One issue with the JDBC interface is that most PowerBuilder applications use a native database driver, and there may be differences between the behavior of the native/ODBC database interface and the JDBC interface. Before you configure a JDBC connection cache, you should test your PowerBuilder applications with the JDBC driver to make sure it does not cause any issues.

4.2.3 Supported JDBC driver type

The JDBC connection caches can use any of the four types of JDBC drivers:

Type 1: JDBC-ODBC Bridge

Type 2: Native-API/partly Java driver

Type 3: Net-protocol/all-Java driver

Type 4: Native-protocol/all-Java driver

Each type has advantages and disadvantages. You should run tests to decide which type of JDBC driver works the best for the specific application and database. Generally, Type 3 and Type 4 drivers show better performance than Type 2 drivers. Therefore, it is recommended that you evaluate Type 3 or Type 4 for both intranet and Internet Web deployments. Because of performance considerations, Type 2 drivers should only be used in an intranet environment where response times are generally faster.

4.2.4 JDBC driver preparation

4.2.4.a Preparing PowerBuilder component support files (for EAServer only)

If Appeon Server is installed to EAServer, whichever database and JDBC driver you use for the deployed application, you must add the following PowerBuilder component support files to the *%JAGUAR%\lib\ext* directory (*%JAGUAR%\java\lib* for EAServer 5.x) in the Appeon Server computer. *%JAGUAR%* indicates the installation path of the EAServer that hosts Appeon Server:

Table 4-1: PowerBuilder component support files

PB Version	File Name
8	pbjdbc12.jar
9	pbjdbc1290.jar
10	pbjdbc12100.jar
10.5	pbjdbc12105.jar
11.1	pbjdbc12110.jar

11.5	pbjdbc12115.jar

Retrieve the file from the *%Sybase%\Shared\PowerBuilder* folder. Make sure the version of the file is the same as the version of PowerBuilder that Appeon supports.

4.2.4.b Checklist for JDBC driver preparation

Before you configure a JDBC connection cache for your application database, the following JDBC driver file(s) must be copied to the Appeon Server computer. Table 4-2 is the checklist of the JDBC driver file(s) that should be copied to the directory.

Table 4-2: Checklist for JDBC driver preparation

Database	Driver Type	Driver Files	Availability of the Driver Files
ASA 7.0.4, 8.0.2, 9.0, 10.0, or 11.5	iAnywhere JDBC-ODBC driver (Recommended)	For Appeon Servers on Windows: dbjodbc8.dll, dbjodbc9.dll, or dbjodbc10.dll jodbc.jar For Appeon Servers on Unix\Linux: dbjodbc8.so jodbc.jar	Available in Sybase ASA 8.0.2 Build 4361 or above. For earlier versions, you can obtain the files from http://www.sybase.com/downloads. Note: dbjodbc8.dll or dbjodbc9.dll must be copied to %Sybase%\Shared*jdkversion*\ire\bin\. *Jdkversion* indicates which version of JDK is used, for example, jdk1.4.1_03.
	Sun JDBC-ODBC driver	-	Bundled with the Java 2 SDK, Standard Edition, so there is no need to download it separately.
	jConnect JDBC driver	jconn2.jar for jConnect 5.5, or jconn3.jar for jConnect 6.	Available at *%Sybase%\Shared\jConnect-5_5\classes* or at *%Sybase%\Shared\jConnect-6_0\classes*. Note: Install *sql_asa.sql* provided at *%Sybase%\Shared\jConnect-5_5\sp* for jConnect to function properly.
ASE 12.5.x or 15.x	jConnect JDBC driver	jconn2.jar for jConnect 5.5, or jconn3.jar for jConnect 6. Note: ASE 15 supports jConnect 6.0 only.	Available at *%Sybase%\Shared\jConnect-5_5\classes* or at *%Sybase%\Shared\jConnect-6_0\classes*. Note: Install *sql_server12.5.sql* for ASE 12.5 or *sql_server15.0.sql* for ASE 15 for jConnect to function properly.
Sybase IQ 12.7.x	jConnect JDBC driver	jconn2.jar for jConnect 5.5, or jconn3.jar for jConnect 6	Available at *%Sybase%\Shared\jConnect-5_5\classes* or *%Sybase%\Shared\jConnect-6_0\classes*.
	Sun JDBC-ODBC driver	-	Bundled with the Java 2 SDK, Standard Edition, so there is no need to download it separately.
Oracle 8i	Oracle JDBC driver	classes12.zip Oracle8i 8.1.7.1 Patch nls_charset12.zip	Available at the Oracle Web site (http://otn.oracle.com/software/tech/java/sqlj_jdbc/index.html).

Oracle 9i	Oracle JDBC driver	For use with JDK 1.3: classes12.zip nls_charset12.zip For use with JDK 1.4: Ojdbc14.jar	Available at the Oracle Web site (http://otn.oracle.com/software/tech/java/sqlj_jdbc/index.html). Note: *Classes12.zip* and *ojdbc14.jar* cannot be placed in the same location and used at the same time.
Oracle 10g or 11g	Oracle JDBC driver	For use with JDK 1.4: Ojdbc14.jar For use with JDK 1.5: Ojdbc15.jar	Available at the Oracle Web site (http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html). Note: *Ojdbc14.jar* and *ojdbc15.jar* cannot be placed in the same location and used at the same time.
SQL Server 2000	jTDS JDBC driver (Recommended)	jtds-1.2.jar	Available at SourceForge Web site (http://sourceforge.net/project). Note: You need to download the jtds-1.2-dist.zip file, which contains the jtds-1.2.jar file. According to our tests, jTDS JDBC driver is better than Microsoft SQL Server JDBC driver in the way that it can prevent memory leak and boost performance.
	Microsoft SQL Server JDBC driver	msbase.jar mssqlserver.jar msutil.jar	Available at the Microsoft Web site (http://www.microsoft.com/sql/downloads). Note: The files have different versions. Make sure the file sizes are equal or close to the following. msbase.jar: 281KB mssqlserver.jar: 66KB msutil.jar: 58KB
SQL Server 2005 or 2008	jTDS JDBC driver (Recommended)	jtds-1.2.jar	Available at SourceForge Web site (http://sourceforge.net/project). Note: You need to download the jtds-1.2-dist.zip file, which contains the jtds-1.2.jar file.
	Microsoft SQL Server JDBC driver	sqljdbc.jar	Available at the Microsoft Web site (http://www.microsoft.com/sql/downloads).
DB2 UDB 8.1, 8.2, or 9.5	IBM JDBC driver	db2java.zip and/or db2jcc.jar	Available in the *java* or *java12* folder of the DB2 Server installation directory. The JDBC driver must be exactly the same version as DB2.
Informix 7.x, 8.x, 9.x, or 10.x	Informix JDBC driver	ifxjdbc.jar and/or ifxjdbcx.jar	Available the IBM Web site (http://www-306.ibm.com/software/data/informix/tools/jdbc/).

Copy the above JDBC driver files to the proper directory in Appeon Server. The directory varies with the type of application server that Appeon Server is installed to, as shown in Table 4-3.

Table 4-3: Appeon Server directory for JDBC files

Server Type	Directory for Storing JDBC Files
EAServer	For Windows: %JAGUAR%\lib\ext directory (%JAGUAR%\java\lib for EAServer 5.x)
	For Unix\Linux: $JAGUAR/lib/ext
WebLogic	It can be any directory, but the directory path and name must be added in the ClassPath variable of the startWebLogic.cmd (Windows) or startWebLogic.sh (Unix\Linux) file.
	If the directory is %WL_HOME%\server\lib folder (Windows) or $WL_HOME/server/lib (Unix\Linux), where %WL_HOME% is the installation folder of the WebLogic server (for example, C:\bea\weblogic81\), it is unnecessary to update the ClassPath variable.
WebSphere	For Windows: %WAS_HOME%\lib (%WAS_HOME% is the installation folder of the WebSphere server)
	For Unix\Linux: $WAS_HOME/lib

Important Note: Remember to restart Appeon Server after copying files.

If EAServer is running as service, you need to re-install EAServer service, or stop the EAServer service and start EAServer from the Windows start menu, otherwise, you will encounter the "Exception was:javax.management.MBeanException" error when creating the data source. For details, refer to the "Failed to create new data source" section in *Appeon Troubleshooting Guide*.

4.3 Setting up Appeon Server data sources\connection caches

This section describes how to configure connection caches for EAServer 5.x using AEM, since the configurations can be performed in AEM more easily, and also gives detailed instructions on configuring data sources in EAServer 6.x, WebLogic, and WebSphere.

4.3.1 Setting up data sources for EAServer 6.x

The following section will take one database type (ASA database with jConnect JDBC driver) as an example to show you how to create a data source for EAServer, you can later create data sources for other database types by taking the same steps below but specifying different parameters according to EAServer 6.x data source settings.

Detailed steps are as below:

1. Start EAServer.

2. Log on to the Web Console and go to Services | JDBC | Data Sources..

3. Create a Data Source. Click Add button. Specify the new Data Source Name and
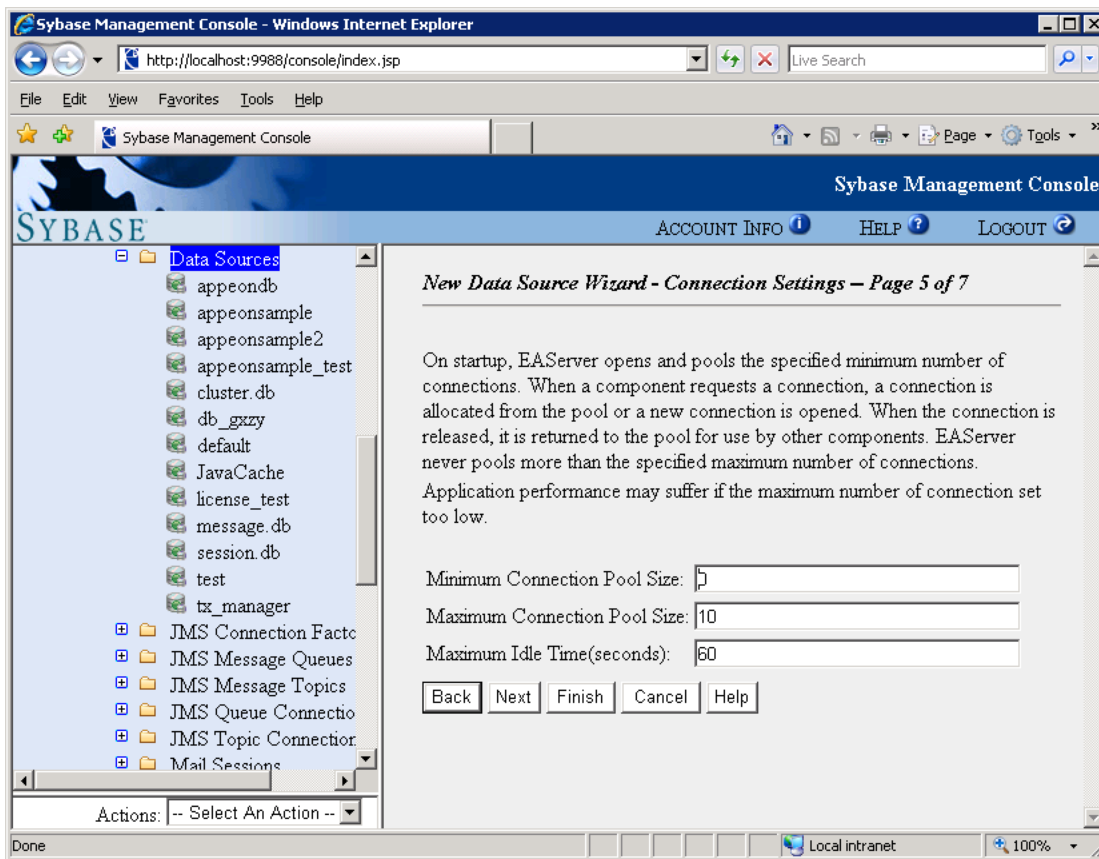
Click Next button.
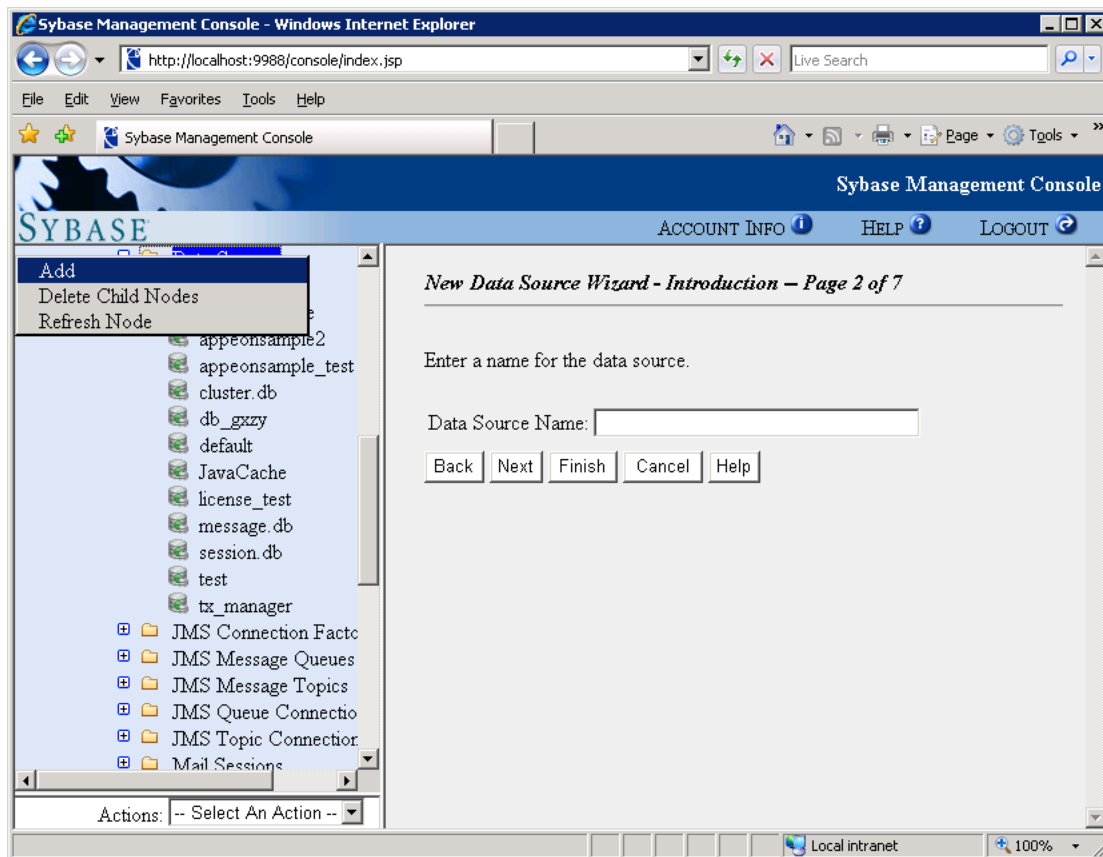
4. Specify the database type, the database driver/class settings, and the database server settings for the new Data Source. In this example, Sybase ASA database type is selected, and the default values for the other settings are used, as shown below.
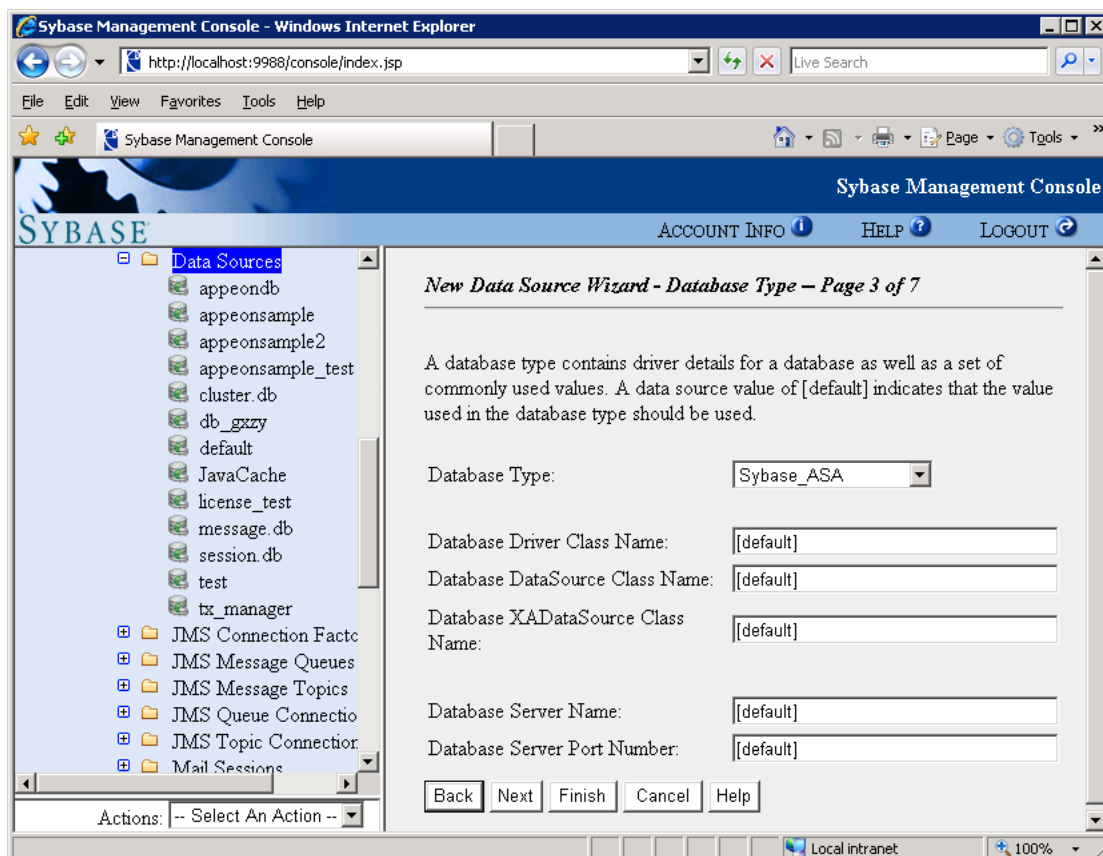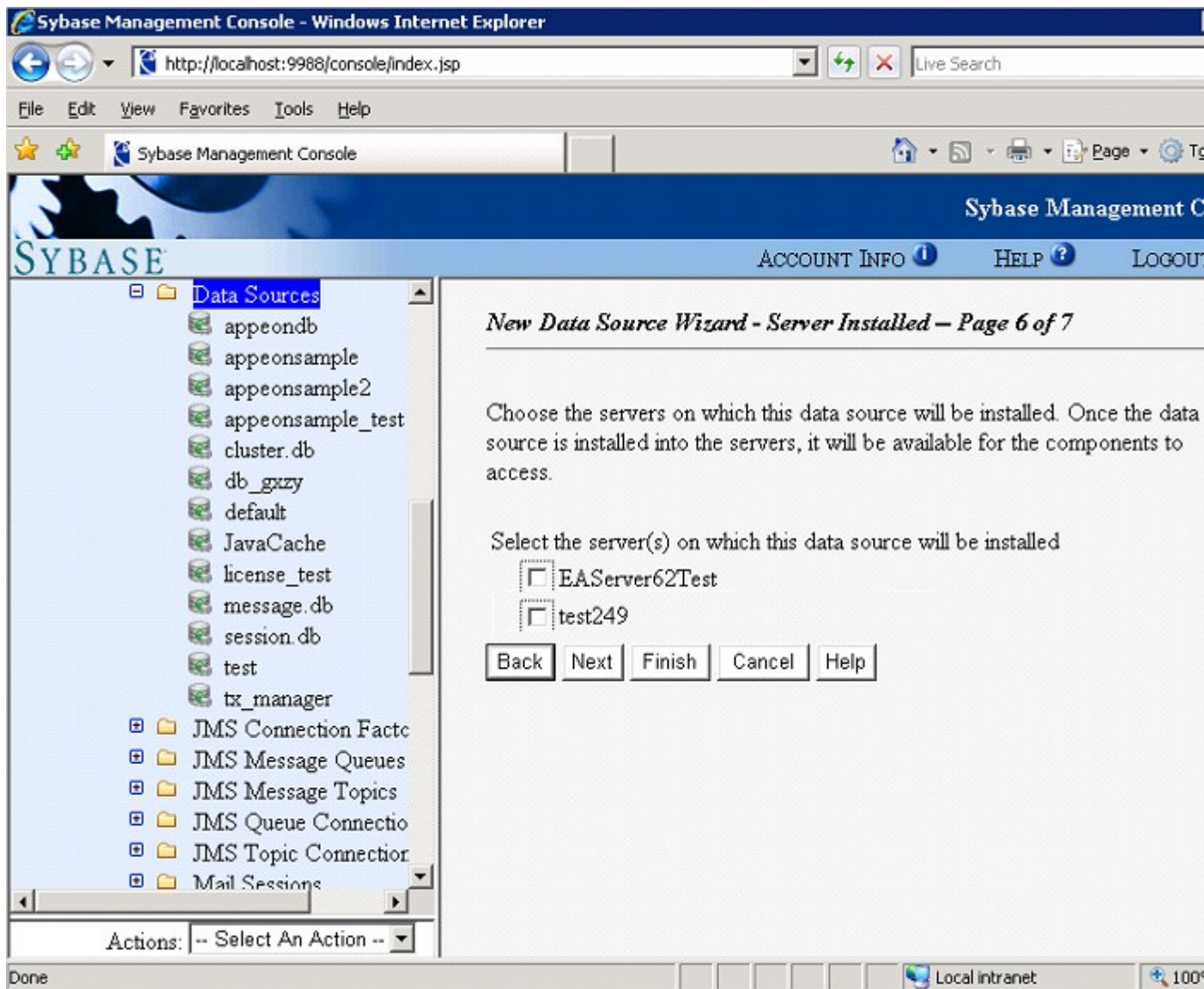
5. Click the Next button. Specify the User Name and Password.
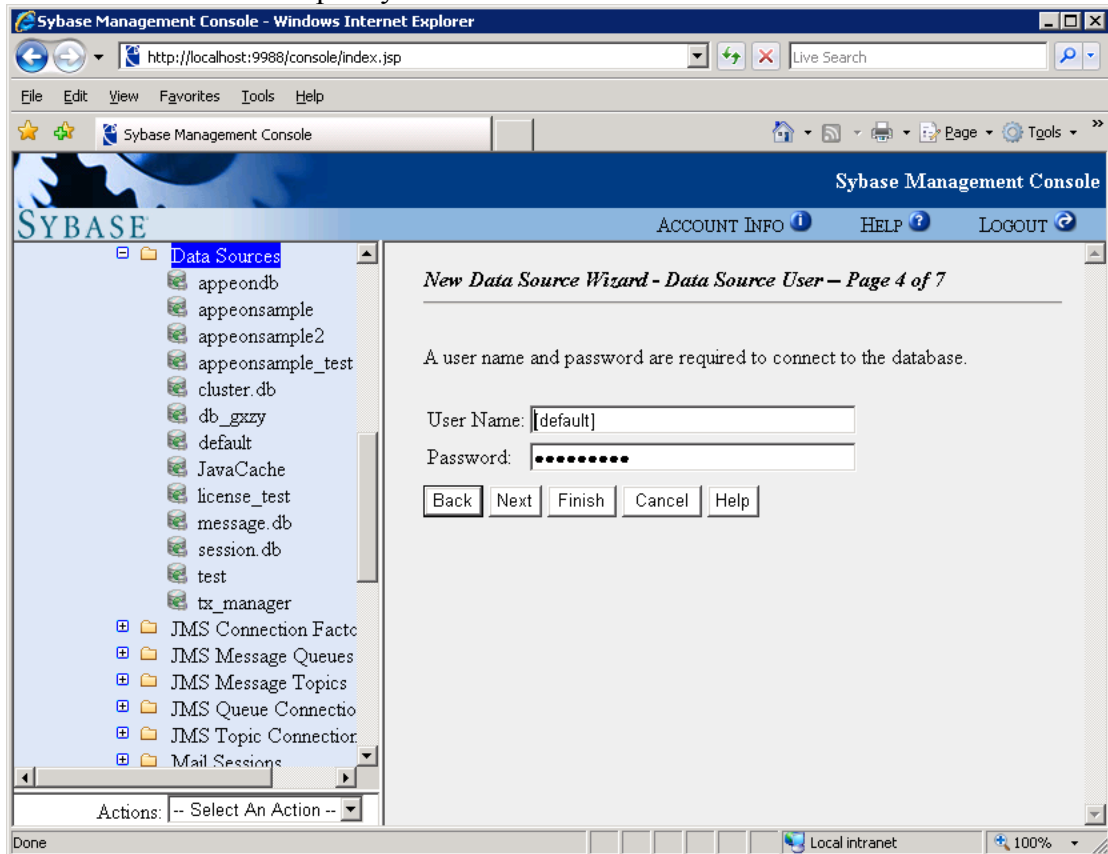
6. Click the Next button. Input the values in corresponding text box. You can use default values for the options.

7. Clear all check boxes, and then click the Next button.

Note: If any server instance is selected, the Appeon user sessions running on that server instance will be caused to expire and the following error will display to the user right after the data source is installed.
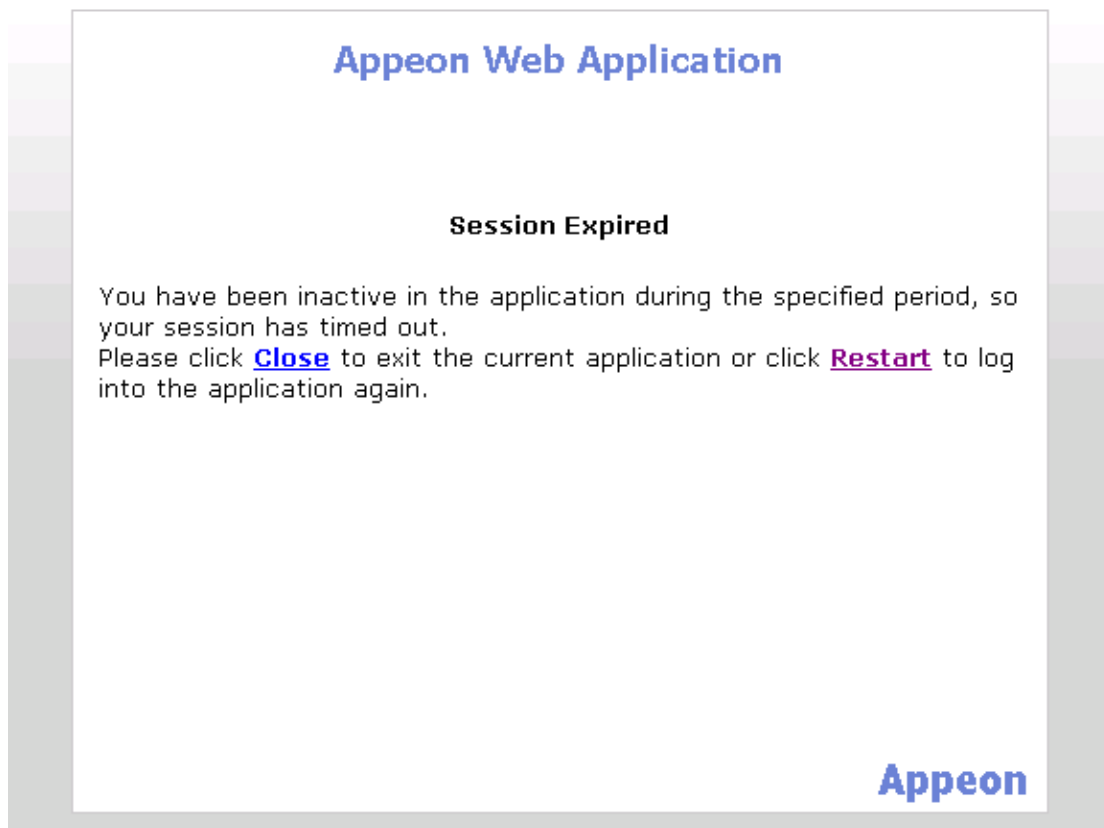
8. Click the Finish button.

Note that you should change the Database URL and input a new one. For different Database

URL, please refer to EAServer 6.x data source settings.
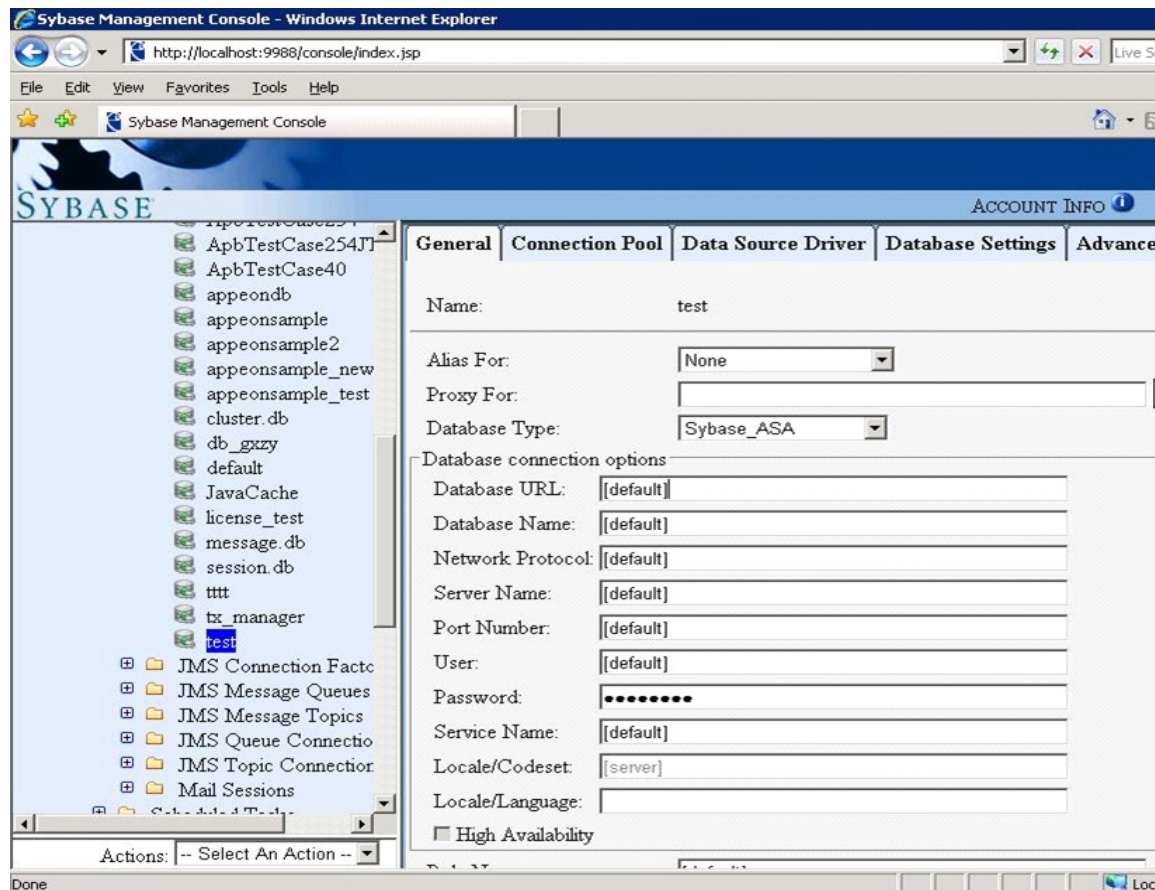
4.3.2 EAServer 6.x data sources settings

You can only go to EAServer Management Console to set up an EAServer\Appeon Server data sources for EAServer 6.x. For detailed instructions, please refer to the "Configuring Data Source" section in EAServer System Administration Guide.

The only point that is worth mentioning here is the **Database URL** setting in the Data Source tool in EAServer Management Console. Based on the test result Appeon gets, if the input **Database URL** is incorrect, you may still have a chance to receive a successful "Ping" result, but you will get unexpected errors when the Web application is actually run. Therefore, please make sure that you use the recommended **Database URL** setting in the following sections.

Note that the Database URL is case sensitive.

4.3.2.a Data source parameters for ASA

ASA databases support iAnywhere JDBC-ODBC (recommended), jConnect and Sun JDBC-ODBC bridge driver.

Note:

1) To use jConnect to connect with ASA, you must start ASA as service before configuration.

2) JConnect 6.0 is preferable to JConnect 5.5.

Table 4-4: Data source parameters for ASA

Setting	Value		Note
Database URL	iAnywhere JDBC-ODBC driver (Recommended)	jdbc:odbc:dsn=DSNname	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. The default ASA port is 2638. *ServiceName* stands for the name of the ASA database service specified during configuration. *DSNname* refers to the name of the ODBC DSN that is created for the database.
	jConnect JDBC driver	jdbc:sybase:Tds:*Hostname:Port/ServiceName*	
	Sun JDBC-ODBC driver	jdbc:odbc:*DSNname*	
User Name	(Type the database login username. The username is set on the database server.)		
Password	(Type the database login password. The password is set on the database server.)		

4.3.2.b Data source parameters for ASE

ASE databases support jConnect JDBC driver only. ASE 15 supports JConnect 6.0 only.

Table 4-5: Data source parameters for ASE

Setting	Value	Note
Database URL	jdbc:sybase:Tds:*Hostname:Port/DBName*	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. The default ASE port is 2048. *DBName* stands for the name of the database.
User Name	(Type the database login username. The username is set on the database server.)	
Password	(Type the database login password. The password is set on the database server.)	

4.3.2.c Data source parameters for Oracle

Oracle databases support the Oracle JDBC driver only.

Table 4-6: Data source parameters for Oracle

Setting	Value	Note
Database URL	jdbc:oracle:thin:@*Hostname:Port:DBName*	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. The default Oracle port is 1521. *DBName* stands for the name of the database to which the cache connects.
User Name	(Type the database login username. The username is set on the database server.)	
Password	(Type the database login password. The password is set on the database server.)	

4.3.2.d Data source parameters for IBM DB2

IBM DB2 databases support the IBM JDBC driver only.

Table 4-7: Data source parameters for IBM DB2

Setting	Value	Note
Database URL	jdbc:db2://*Hostname*:*Port*/*DBName*	*Hostname* stands for the database server name or IP address.
		Port stands for the database server port. The port used by JDBC will be different than the one used by db2 client. The default JDBC port is 6789 while the port used by db2 client is 50000.
		DBName stands for the name of the database to which the cache connects.
User Name	(Type the database login username. The username is set on the database server.)	
Password	(Type the database login password. The password is set on the database server.)	

4.3.2.e Data source parameters for Microsoft SQL Server

Appeon recommends using jTDS JDBC driver rather than the Microsoft SQL Server JDBC driver, because it can eliminate memory leak and boost performance.

Table 4-8: Data source parameters for Microsoft SQL Server

Setting	Value		Note
Database URL	jTDS JDBC driver (Recommended)	jdbc:jtds:sqlserver://*Hostname*:*port*/*DBName*; SelectMethod=cursor	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. The default SQL Server port is 1433.
	Microsoft SQL Server JDBC driver	jdbc:sqlserver://*Hostname*:*Port*; DatabaseName= *DBName*; SelectMethod=cursor	*DBName* stands for the name of the database to which the cache connects. "SelectMethod=cursor" must be specified, otherwise errors will occur when inserting data.
User Name	(Type the database login username. The username is set on the database server.)		
Password	(Type the database login password. The password is set on the database server.)		

4.3.2.f Data source parameters for Sybase IQ

Sybase IQ databases support JConnect JDBC driver or Sun JDBC-ODBC driver.

Table 4-9: Data source parameters for Sybase IQ

Setting	Value		Note
Database URL	JConnect JDBC driver (Recommended)	jdbc:sybase:Tds:*Hostname*:*Port*/*ServiceName*	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. *ServiceName* stands for the name of the database service specified during configuration.
	Sun JDBC-ODBC driver	jdbc:odbc:*DSNname*	*DSNname* refers to the name of the ODBC DSN that is created for the database.
User Name	(Type the database login username. The username is set on the database server.)		
Password	(Type the database login password. The password is set on the database server.)		

4.3.2.g Data source parameters for Informix

Informix databases support the IBM Informix JDBC driver only.

Table 4-10: Data source parameters for Informix

Setting	Value	Note
Database URL	jdbc:informix-sqli://*Hostname*:*Port*/*DBName*:informixserver=*DBServerName* For example: jdbc:informix-sqli://192.0.2.117:1527/mytestdb:informixserver=ol_s_122005_144417	*Hostname* stands for the name or IP address of the machine hosting the database server. One machine can host several database servers. *Port* stands for the database server port. *DBName* stands for the name of the database to which the cache connects. *DBServerName* stands for the name of the database server.
User Name	(Type the database login username. The username is set on the database server.)	
Password	(Type the database login password. The password is set on the database server.)	

4.3.3 Setting up connection caches for EAServer 5.x

The following sections walk you though how to set up connection caches for various database types in AEM. If you have problems creating connection caches, refer to the documentations from the database/JDBC driver vendor or Sybase EAServer.

4.3.3.a Setting up connection cache for ASA or ASE

Connection cache with jConnect JDBC driver

To set up an Appeon Server connection cache that connects to ASA/ASE with jConnect:

STEP 1 – Start EAServer and log in with AEM.

STEP 2 – Click *Connection Cache* in the tree view. Specify user name and password to log on. The default user name is "jagadmin" (Figure 4-1).

Figure 4-1: AEM Connection Cache
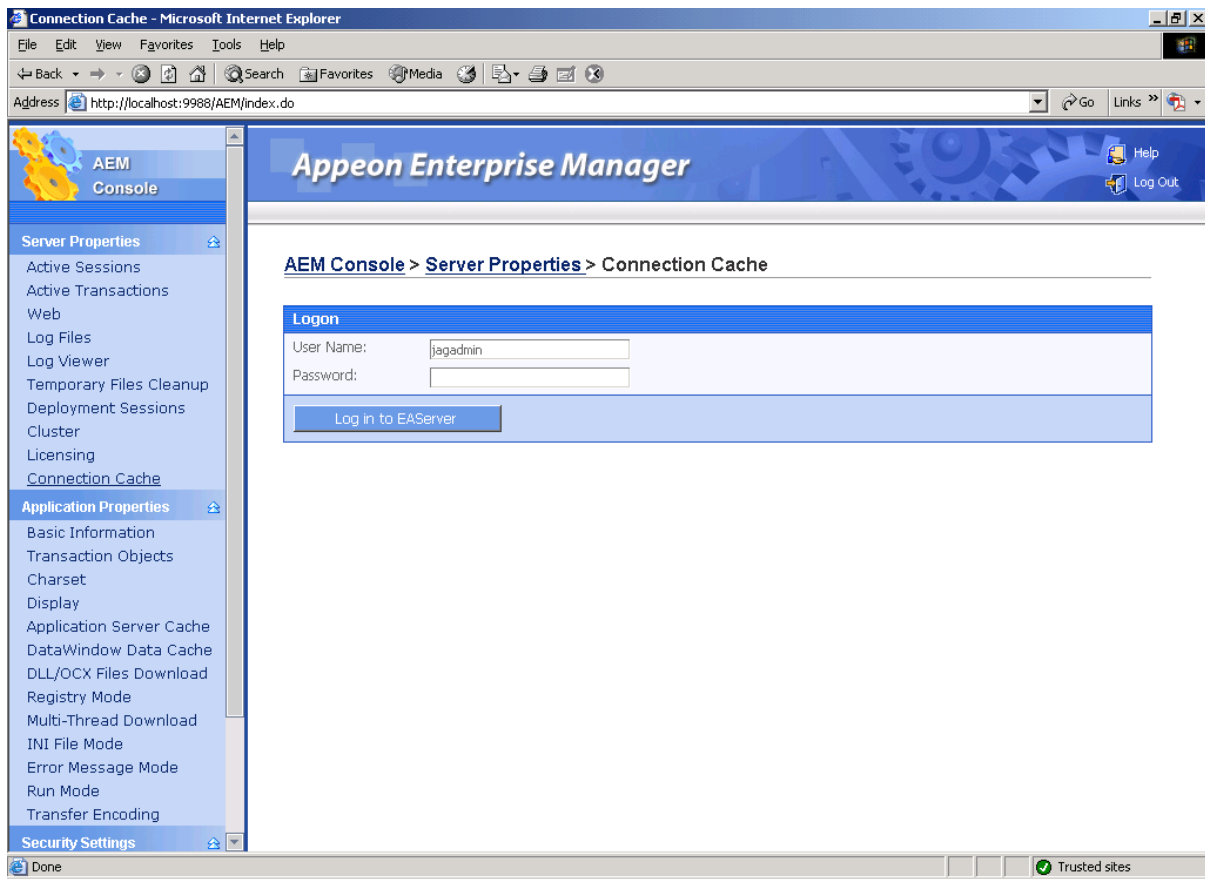
STEP 3 – Click *Add Connection Cache* below the list (Figure 4-2).

Figure 4-2: Connection cache list
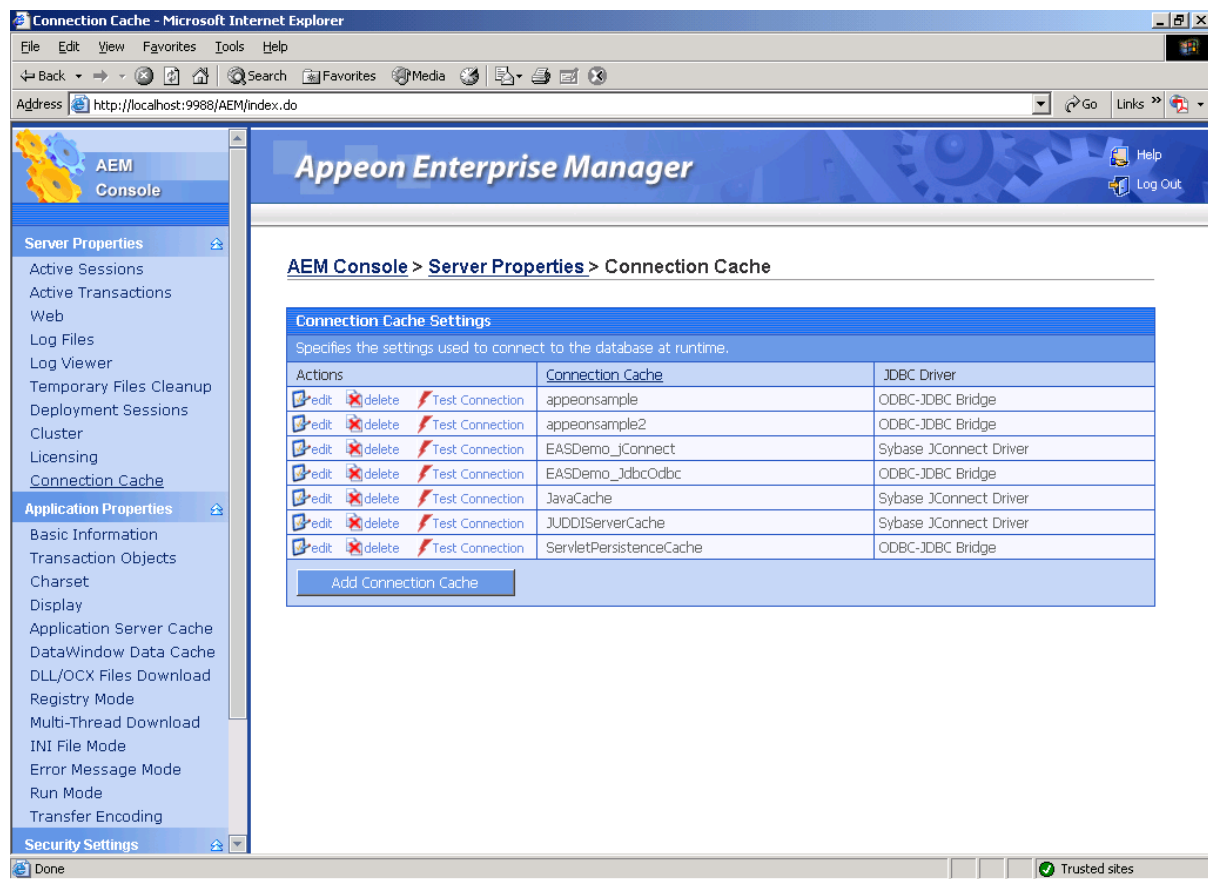
STEP 4 – Type the following settings into the Add Connection Cache page, as shown in Table 4-11 and Figure 4-3.

Table 4-11: Connection Cache Properties

Connection Cache Name	Input any text as the connection cache name.
Driver Type	Select "Sybase jConnect Driver" as the driver type for the connection cache.
Class Name	Type the driver string: "com.sybase.jdbc2.jdbc.SybDriver" (It is case-sensitive).
Database Host	Type the database host.
Database Port	Type the database port.
Database/Service Name	Type the database/service name.
User Name	Type the database login username. The username is set on the Database Server.
Password	Type the database login password. The password is set on the database server.
URL	Syntax: jdbc:sybase:Tds:*hostname:port/dbname*

Figure 4-3: Add connection cache
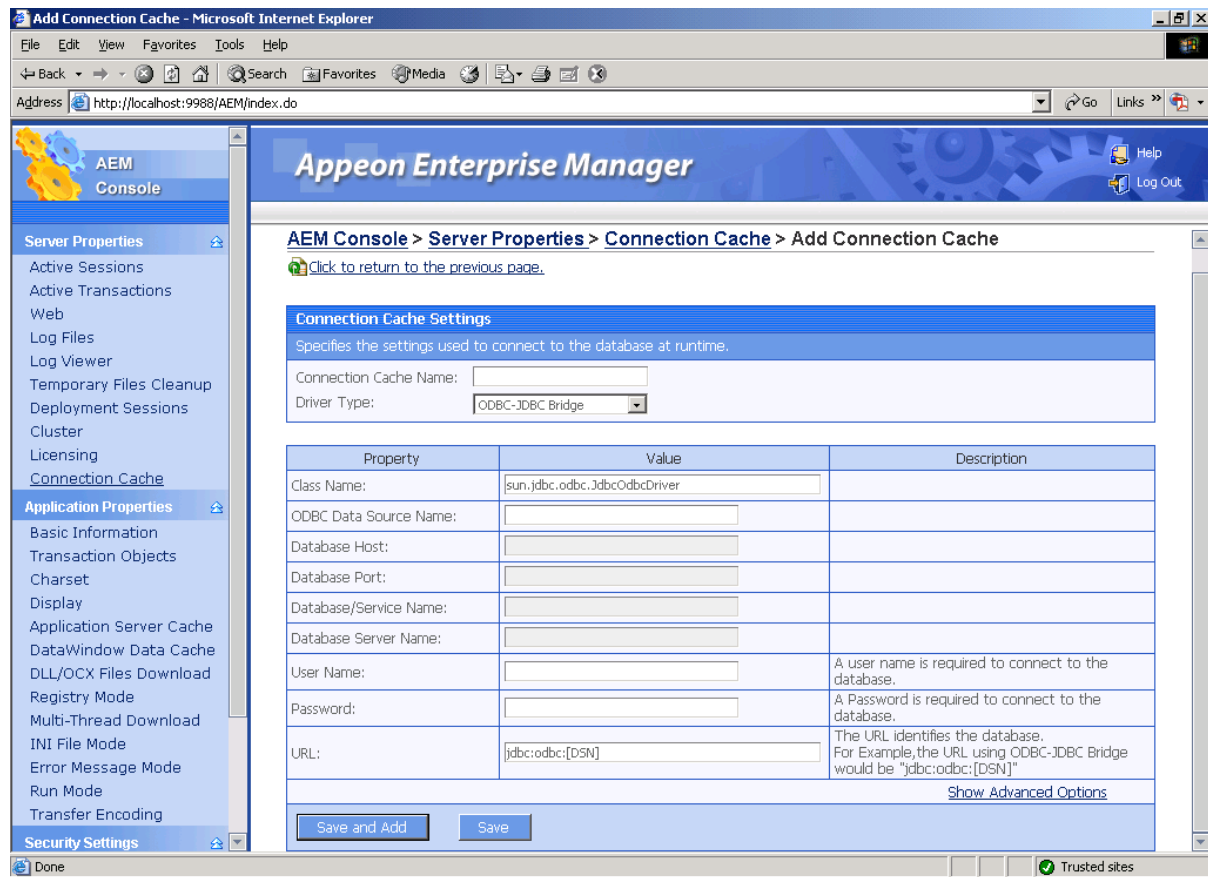
STEP 5 – Click *Save and Add*. If you have input all the required settings, a message will display saying "The connection cache has been added".

STEP 6 – Once the connection cache has been added into the list, click Test Connection. A message will display saying if testing connection cache succeeded.

Connection cache with Sun JDBC driver

Steps 1-3 for setting up a connection with Sun JDBC driver are the same as those in Section *Connection cache with jConnect JDBC driver*.

STEP 1 – Start EAServer and log in with AEM.

STEP 2 – Click *Connection Cache* in the tree view. Specify user name and password to log on. The default user name is "jagadmin".

STEP 3 – Click *Add Connection Cache* below the list.

STEP 4 – Type the following settings into the Add Connection Cache page, as shown in Table 4-12.

Table 4-12: Connection Cache Properties

Connection Cache Name	Input any text as the connection cache name.
Driver Type	Select "ODBC-JDBC Bridge" as the driver type for the connection cache.
Class Name	Type the driver string: "sun.jdbc.odbc.JdbcOdbcDriver" (It is case-sensitive).
ODBC Data Source Name	Type the ODBC data source name. For example, "appeonsample".

User Name	Type the database login username. The username is set on the Database Server.
Password	Type the database login password. The password is set on the database server.
URL	Syntax: jdbc:odbc:*DSNname* DSNname refers to the name of the ODBC DSN that is created for the database. e.g. jdbc:odbc:SybaseASE

STEP 5 – Click *Save and Add*. If you have input all the required settings, a message will display saying "The connection cache has been added".

STEP 6 – Once the connection cache has been added into the list, click Test Connection. A message will display saying if testing connection cache succeeded.

Connection cache with iAnywhere JDBC driver

Steps 1-3 for setting up a connection with iAnywhere JDBC driver are the same as those in Section *Connection cache with jConnect JDBC driver*.

STEP 1 – Start EAServer and log in with AEM.

STEP 2 – Click *Connection Cache* in the tree view. Specify user name and password to log on. The default user name is "jagadmin".

STEP 3 – Click *Add Connection Cache* below the list.

STEP 4 – Type the following settings into the Add Connection Cache page, as shown in Table 4-13:

Table 4-13: Connection Cache Properties

Connection Cache Name	Input any text as the connection cache name.
Driver Type	Select "Other" as the driver type for the connection cache.
Class Name	Type the driver string: "ianywhere.ml.jdbcodbc.IDriver" for JDBC 2.0 or "ianywhere.ml.jdbcodbc.jdbc3.IDriver" for JDBC 3.0" (They are case-sensitive).
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.
URL	Syntax: jdbc:odbc:dsn=DSNname

STEP 5 – Click *Save and Add*. If you have input all the required settings, a message will display saying "The connection cache has been added".

STEP 6 – Once the connection cache has been added into the list, click Test Connection. A message will display saying if testing connection cache succeeded.

Note: When using the iAnywhere driver, Merant, or other ODBC drivers to connect to Enterprise databases like Sybase ASE or Oracle, the following message or similar message may pop up on Appeon Server each time a Web DataWindow retrieval is executed. The Web browser will remain blank until you click the *OK* button in the message on Appeon Server, as shown in Figure 4-4. This is because the database driver has not been licensed for use with your database. To resolve this issue and continue using the iAnywhere driver, contact Sybase to get the appropriate license. For all other database drivers, contact the driver vendor.

Figure 4-4: License Warning

4.3.3.b Setting up connection cache for Oracle

Appeon recommends using the Oracle JDBC driver rather than the JDBC-ODBC bridge driver for Oracle databases. The following instructions refer to setting up connection caches that use the Oracle JDBC driver.

STEP 1 – Start EAServer and log in with AEM.

STEP 2 – Click *Connection Cache* in the tree view. Specify user name and password to log on. The default user name is "jagadmin".

STEP 3 – Click *Add Connection Cache* below the list.

STEP 4 – Type the following settings into the Add Connection Cache page, as shown in Table 4-14.

Table 4-14: Connection Cache Properties

Connection Cache Name	Input any text as the connection cache name.
Driver Type	Select "Oracle JDBC Driver" as the driver type for the connection cache.
Class Name	Type the driver string: "oracle.jdbc.driver.OracleDriver" (It is case-sensitive).
Database Host	Type the database host.
Database Port	Type the database port.
Database/Service Name	Type the database/service name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.
URL	Establish a connection to the database by specifying the DB URL. Syntax: jdbc:oracle:thin:@*hostname*:*port*:*DBName* e.g. jdbc:oracle:thin:@192.0.0.91:1512:oracletest01

STEP 5 – Click *Save and Add*. If you have input all the required settings, a message will display saying "The connection cache has been added".

STEP 6 – Once the connection cache has been added into the list, click Test Connection. A message will display saying if testing connection cache succeeded.

4.3.3.c Setting up connection cache for IBM DB2

Appeon recommends using the IBM JDBC driver rather than the JDBC-ODBC bridge driver for IBM DB2 databases. The following instructions refer to setting up connection caches that use the IBM JDBC driver.

STEP 1 – Start EAServer and log in with AEM.

STEP 2 – Click *Connection Cache* in the tree view. Specify user name and password to log on. The default user name is "jagadmin".

STEP 3 – Click *Add Connection Cache* below the list.

STEP 4 – Type the following settings into the Add Connection Cache page, as shown in Table 4-15.

Table 4-15: Connection Cache Properties

Connection Cache Name	Input any text as the connection cache name.
Driver Type	Select "IBM JDBC Driver" as the driver type for the connection cache.
Class Name	Type the driver string: "COM.ibm.db2.jdbc.net.DB2Driver" (It is case-sensitive).
Database Host	Type the database host.
Database Port	Type the database port.
Database/Service Name	Type the database/service name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.
URL	Establish a connection to the database by specifying the DB URL. Syntax:jdbc:db2://*hostname*:*port*/*DBName* e.g. jdbc:db2://192.0.0.71:6789/SAMPLE Note: The port used by JDBC will be different than the one used by db2 client. The default JDBC port is 6789 while the port used by db2 client is 50000.

STEP 5 – Click *Save and Add*. If you have input all the required settings, a message will display saying "The connection cache has been added".

STEP 6 – Once the connection cache has been added into the list, click Test Connection. A message will display saying if testing connection cache succeeded.

4.3.3.d Setting up connection cache for Microsoft SQL Server

Connection cache with jTDS

Appeon recommends using jTDS JDBC driver rather than the Microsoft SQL Server JDBC driver, because jTDS reduces memory leak and boosts performance. The following instructions refer to setting up connection caches using jTDS.

STEP 1 – Start EAServer and log in with AEM.

STEP 2 – Click *Connection Cache* in the tree view. Specify user name and password to log on. The default user name is "jagadmin".

STEP 3 – Click *Add Connection Cache* below the list.

STEP 4 – Type the following settings into the Add Connection Cache page, as shown in Table 4-16.

Table 4-16: Connection Cache Properties

Connection Cache Name	Input any text as the connection cache name.

Driver Type	Select "Other" as the driver type for the connection cache.
Class Name	Type the driver string: "net.sourceforge.jtds.jdbc.Driver" (It is case-sensitive).
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.
URL	Syntax: jdbc:jtds:sqlserver://*Hostname*:*port*/*DBName*

STEP 5 – Click *Save and Add*. If you have input all the required settings, a message will display saying "The connection cache has been added".

STEP 6 – Once the connection cache has been added into the list, click Test Connection. A message will display saying if testing connection cache succeeded.

Connection cache with Microsoft SQL Server JDBC driver

The following instructions refer to setting up connection caches that use the Microsoft SQL Server JDBC driver.

STEP 1 – Start EAServer and log in with AEM.

STEP 2 – Click *Connection Cache* in the tree view. Specify user name and password to log on. The default user name is "jagadmin".

STEP 3 – Click *Add Connection Cache* below the list.

STEP 4 – Type the following settings into the Add Connection Cache page, as shown in Table 4-17.

Table 4-17: Connection Cache Properties

|	
Connection Cache Name	Input any text as the connection cache name.
Driver Type	Select "Microsoft JDBC Driver" as the driver type for the connection cache.
Class Name	Type the driver string: "com.microsoft.jdbc.sqlserver.SQLServerDriver" (It is case-sensitive).
Database Host	Type the database host.
Database Port	Type the database port.
Database/Service Name	Type the database/service name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.
URL	Syntax: jdbc:microsoft:sqlserver://*hostname*:*port*;DatabaseName=*DBName*;SelectMethod=cursor e.g. jdbc:microsoft:sqlserver://192.0.0.94:1433;DatabaseName=sqltest; SelectMethod=cursor

STEP 5 – Click *Save and Add*. If you have input all the required settings, a message will display saying "The connection cache has been added".

STEP 6 – Once the connection cache has been added into the list, click Test Connection. A message will display saying if testing connection cache succeeded.

4.3.3.e Setting up connection cache for Sybase IQ

The following instructions refer to setting up connection caches that use the Sybase IQ JDBC driver.

STEP 1 – Start EAServer and log in with AEM.

STEP 2 – Click *Connection Cache* in the tree view. Specify user name and password to log on. The default user name is "jagadmin".

STEP 3 – Click *Add Connection Cache* below the list.

STEP 4 – Type the following settings into the Add Connection Cache page, as shown in Table 4-18.

Table 4-18: Connection Cache Properties

Connection Cache Name	Input any text as the connection cache name.
Driver Type	Select "ODBC-JDBC Bridge" or "Sybase JConnect Driver" as the driver type for the connection cache.
Class Name	Type the driver string: "sun.jdbc.odbc.JdbcOdbcDriver" for ODBC-JDBC Bridge, "com.sybase.jdbc2.jdbc.SybDriver" for Sybase JConnect 5.5 Driver, or "com.sybase.jdbc3.jdbc.SybDriver" for Sybase JConnect 6 Driver (They are case-sensitive).
Database Host	Type the database host.
Database Port	Type the database port.
Database/Service Name	Type the database/service name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.
URL	Syntax: For ODBC-JDBC Bridge: jdbc:odbc:ODBCNAME For Sybase JConnect Driver: jdbc:sybase:Tds:MachineAddress:Port/ServiceName

STEP 5 – Click *Save and Add*. If you have input all the required settings, a message will display saying "The connection cache has been added".

STEP 6 – Once the connection cache has been added into the list, click Test Connection. A message will display saying if testing connection cache succeeded.

4.3.3.f Setting up connection cache for Informix

The following instructions refer to setting up connection caches that use the Informix JDBC driver.

STEP 1 – Start EAServer and log in with AEM.

STEP 2 – Click *Connection Cache* in the tree view. Specify user name and password to log on. The default user name is "jagadmin".

STEP 3 – Click *Add Connection Cache* below the list.

STEP 4 – Type the following settings into the Add Connection Cache page, as shown in Table 4-19.

Table 4-19: Connection Cache Properties

Connection Cache Name	Input any text as the connection cache name.
Driver Type	Select "Informix JDBC Driver" as the driver type for the connection cache.
Class Name	Type the driver string: "com.informix.jdbc.IfxDriver" (It is case-sensitive).
Database Host	Type the database host.
Database Port	Type the database port.
Database/Service Name	Type the database/service name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.
URL	Syntax: jdbc:informix-sqli://MachineAddress:Port/DatabaseName: informixserver=dbServerName e.g. jdbc:informix-sqli://[Host]:1527/[DatabaseName]:informixserver=[DatabaseServerName]

STEP 5 – Click *Save and Add*. If you have input all the required settings, a message will display saying "The connection cache has been added".

STEP 6 – Once the connection cache has been added into the list, click Test Connection. A message will display saying if testing connection cache succeeded.

4.3.4 Setting up data sources for WebLogic

The following section will take one database type (ASA database with jConnect JDBC driver) as an example to show you how to create a data source for WebLogic, you can later create data sources for other database types by taking the same steps below but specifying different parameters according to Section 4.3.6: *WebLogic\WebSphere Data source settings*.

You can create a connection pool and a data source using either the WebLogic server console or the configuration wizard.

Note: the JNDI name specified for the data source will be regarded as the connection cache name by Appeon Server and AEM.

4.3.4.a Creating a JDBC connection pool

1. Start the WebLogic Server for your domain.

2. Log on to the WebLogic Server Console.

3. Go to Services | JDBC | Connection Pools.

Figure 4-5: Configure a JDBC connection pool
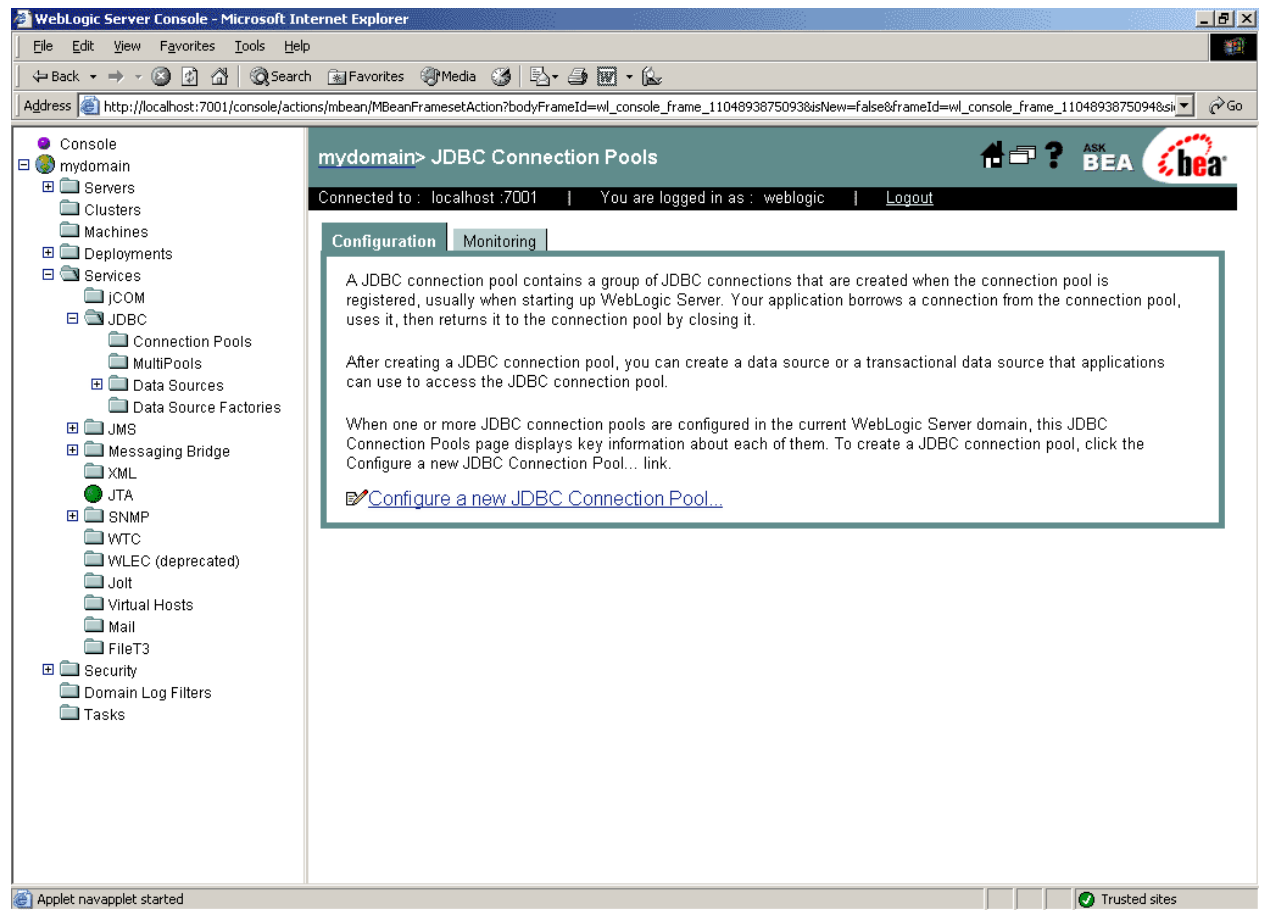
4. Click the *Configure a new JDBC Connection Pool* link.

5. Select the database type and driver from the dropdown list boxes and click *Continue*.

Figure 4-6: Choose database
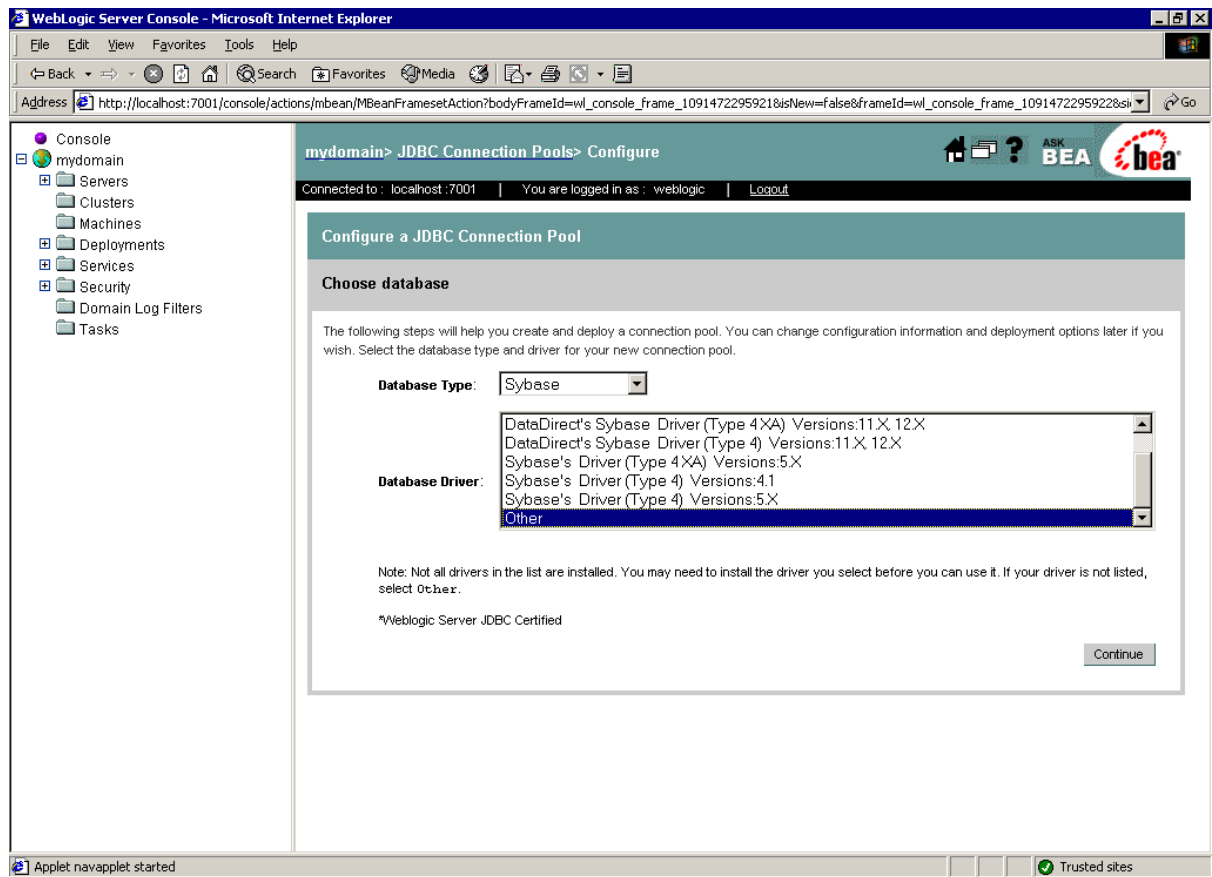
6. Choose a name for the new data source (for example, appeontutor) and fill in the blanks for the ASA database. Click *Continue*.

Table 4-20: data source properties

Name	Input the name of the new data source
Driver classname	com.sybase.jdbc2.jdbc.SybDriver
URL	jdbc:sybase:Tds:*hostname*:2638/*dbname* (The default port of ASA database is 2638)
Database User name	Type the database login username. The username is set at the database server.
Password	Type the database login password. The password is set at the database server.

Figure 4-7: data source properties
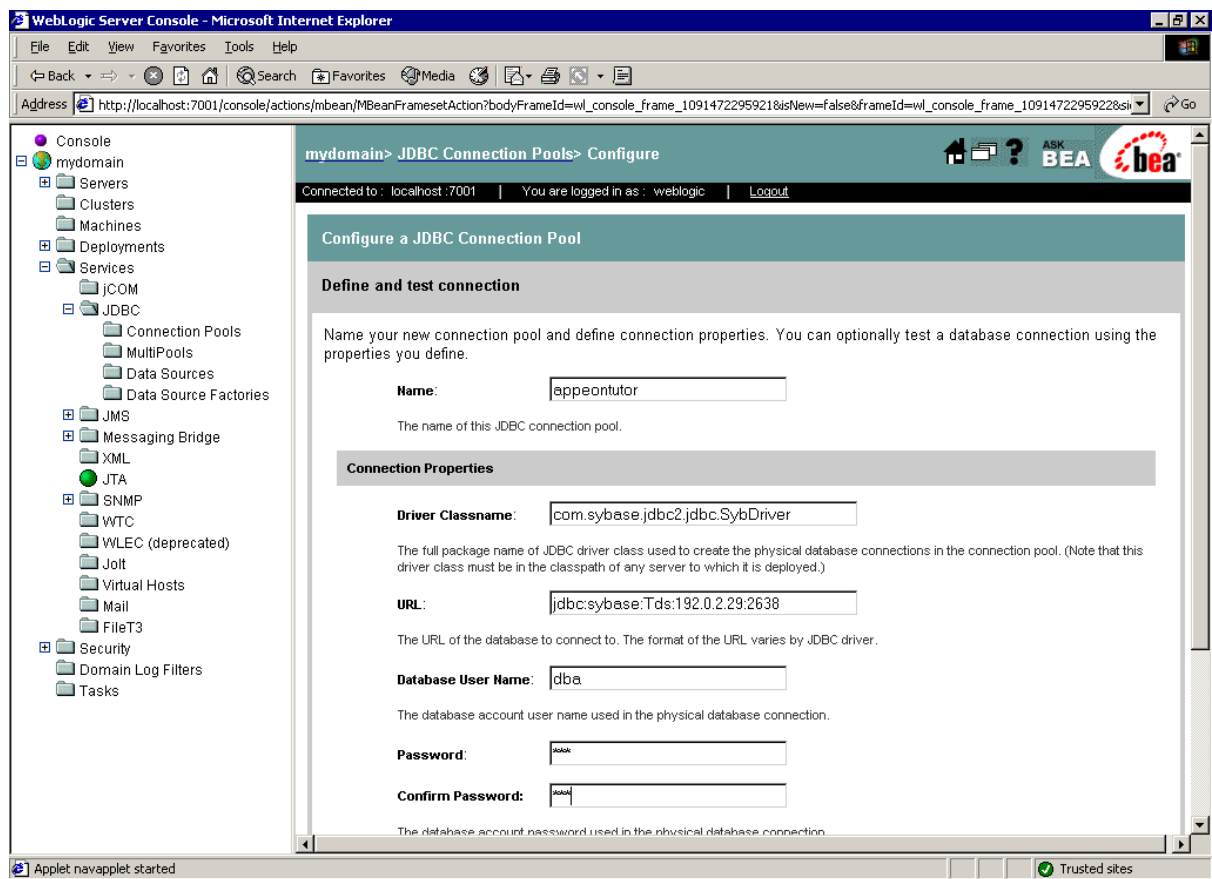
7. Test your connection to verify that you can connect to your database.

8. Create and deploy the new connection pool.

4.3.4.b Configuring a JDBC data source

1. Go to Services | JDBC | Data Sources.

Figure 4-8: Configure a JDBC data source
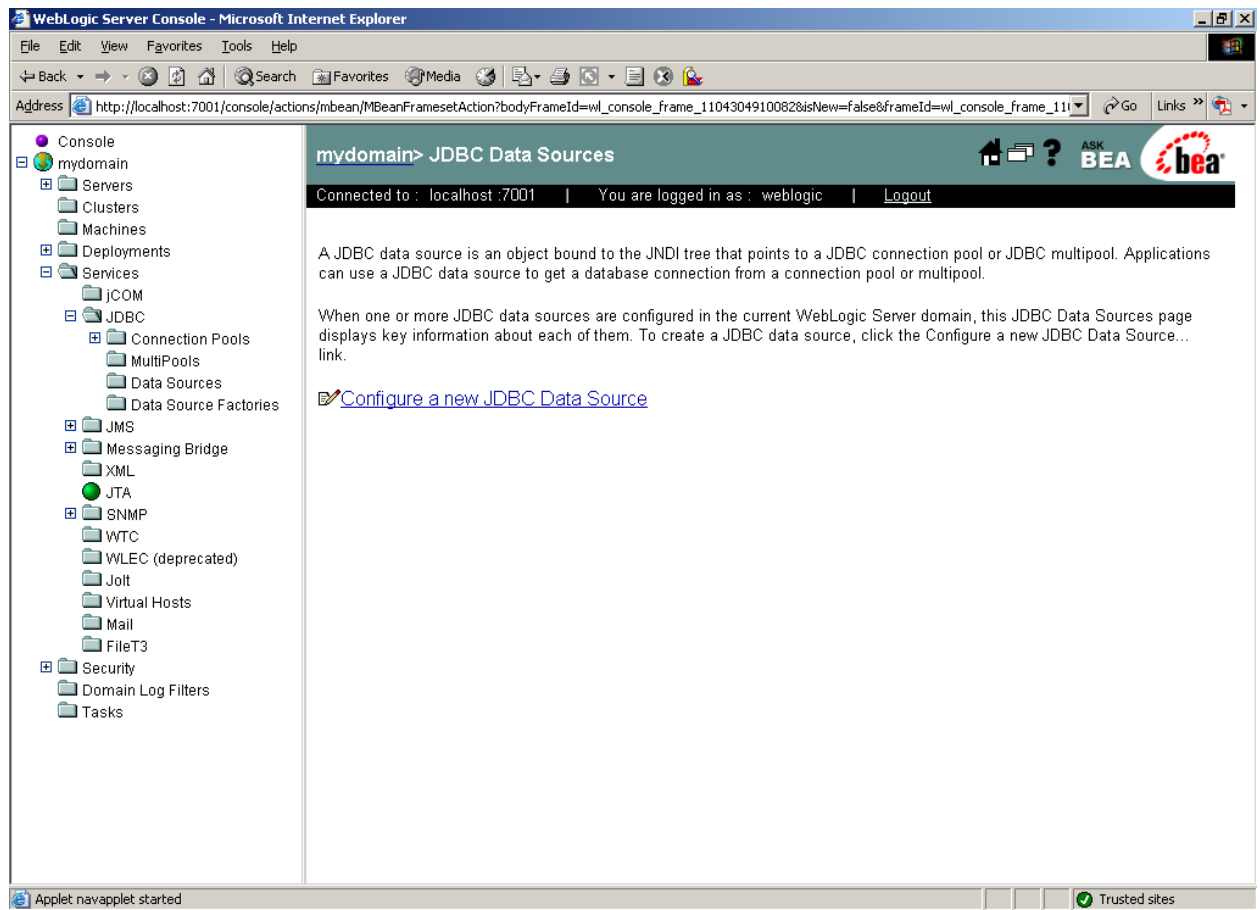
2. Click the *Configure a new JDBC Data Source* link.

3. Specify the new data source name and JNDI name and click *Continue*. You can use default values for the other options.

Figure 4-9: Data source properties
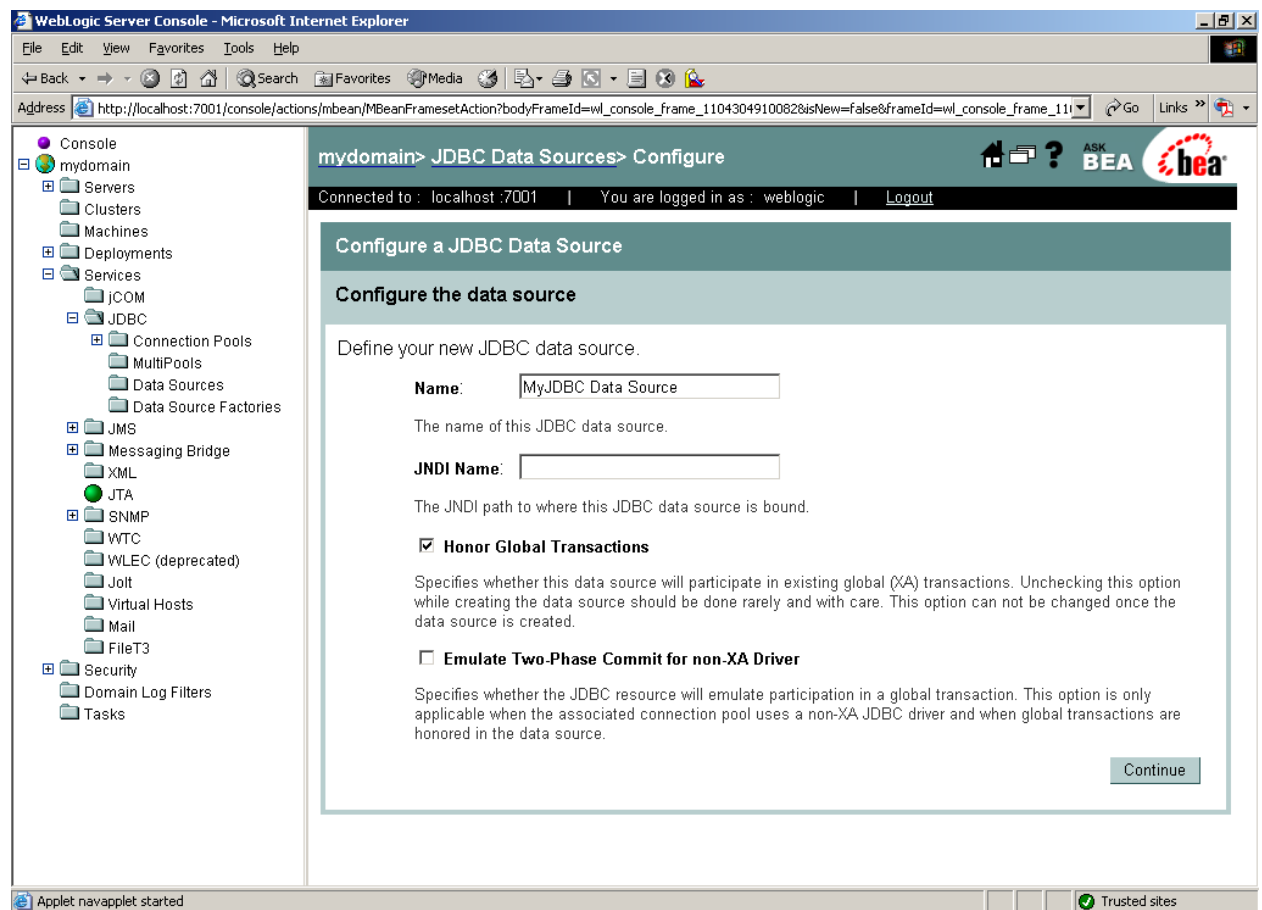
4. Select the newly created connection pool in the dropdown list box and click *Continue*.

Figure 4-10: Select the connection pool
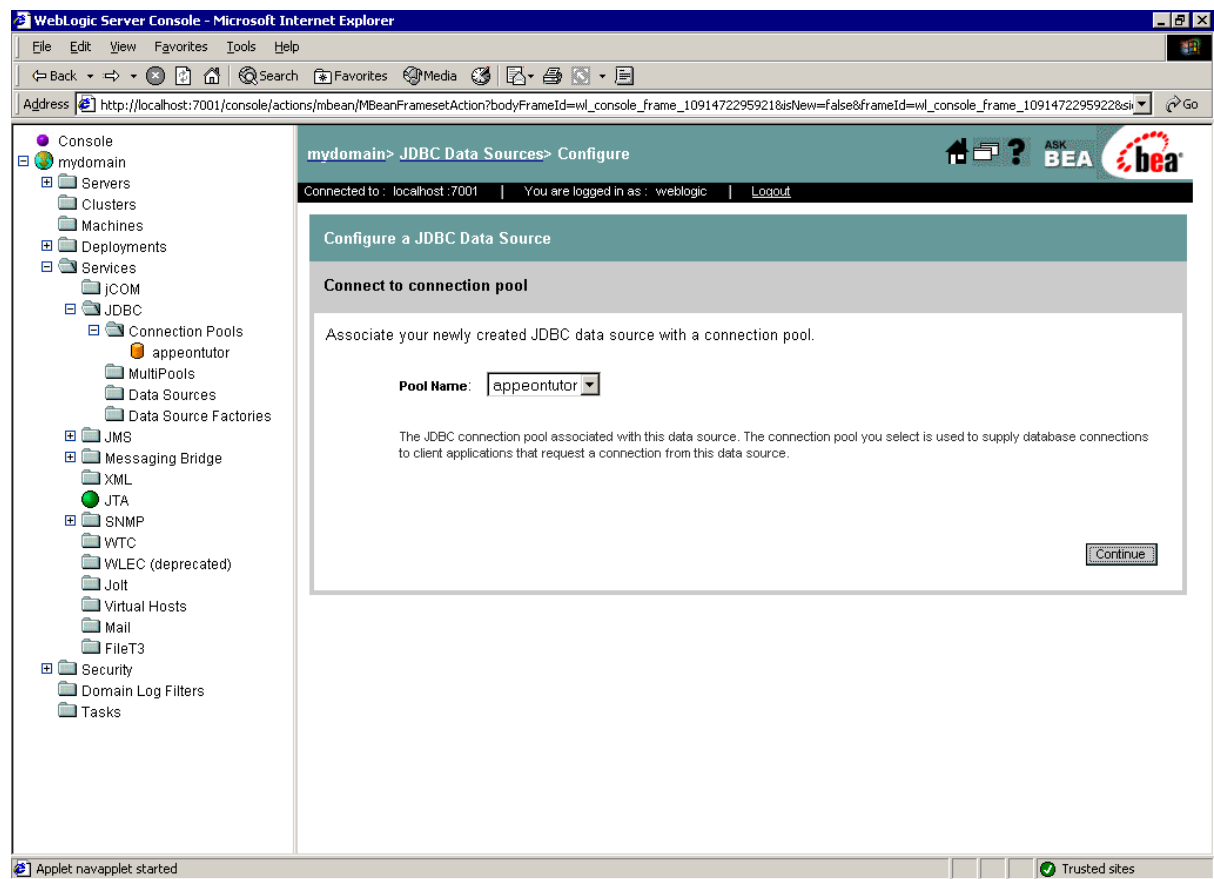
5. Select the server to which you want to deploy the JDBC data source, and click *Create*.

Figure 4-11: Target the data source
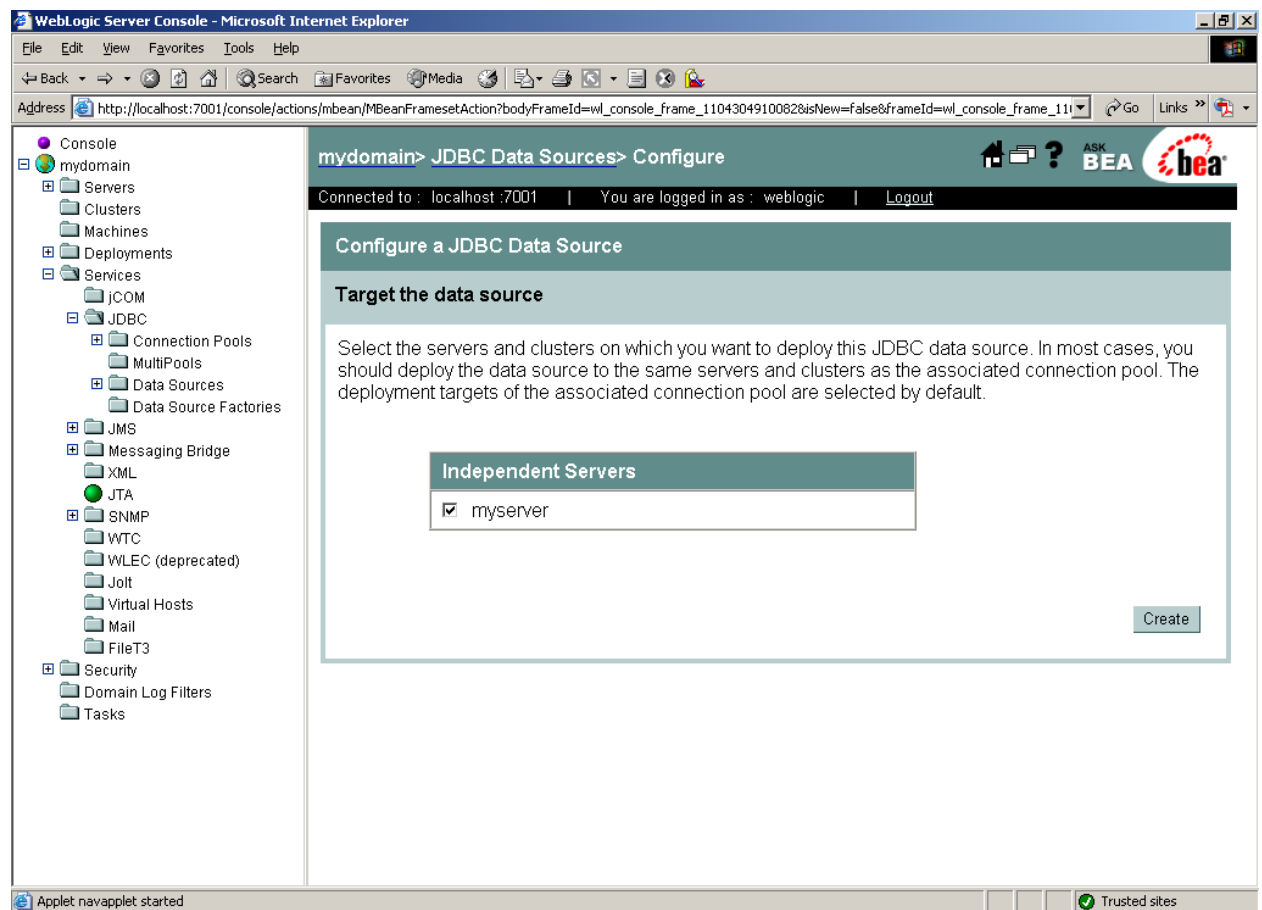
6. Confirm the Deployed status of the data source is "true" in the JDBC Data Sources window.

Figure 4-12: Deployed status

4.3.5 Setting up data sources for WebSphere

The following section will take one database type (Oracle database with Oracle JDBC driver) as an example to show you how to create a data source for WebSphere, you can later create data sources for other database types by taking the same steps below but specifying different parameters according to Section 4.3.6: *WebLogic\WebSphere Data source settings*.

Note: the JNDI name specified for the data source will be regarded as the connection cache name by Appeon Server and AEM.

4.3.5.a Updating JDBC driver path in master configuration

1. Start the WebSphere Server and log on to the WebSphere Server Console.

2. Click Environment | Manage WebSphere Variable in the console.

3. Set the path of the Oracle JDBC driver to the value of the ORACLE_JDBC_DRIVER_PATH variable.

    As required in Section 4.2.4: JDBC driver preparation, the path of the Oracle JDBC driver is %WAS_HOME%\lib\ (Windows) or $WAS_HOME/lib/ (Unix\Linux). WAS_HOME is the installation folder of the WebSphere platform.

4. Save changes to the ORACLE_JDBC_DRIVER_PATH variable in the master configuration.

4.3.5.b Creating a new J2C authentication data entry

1. Click Security | JAAS Configuration in the WebSphere administrative console, then click J2C Authentication Data.

2. Click *New* to create a new J2C authentication data entry.

Figure 4-13: New J2C authentication data entry

Fill in details as required in Table 4-21.

Table 4-21: Details for the new authentication data entry

Alias	Enter a suitable (short) name, such as "UDDIAlias"
Userid	Enter the database user ID used to read and write to the UDDI registry database.
Password	Enter the password associated with the user ID specified above.
Description	Enter a suitable description of the chosen user ID or leave it blank.

3. Click *Apply* and save changes to the master configuration.

4.3.5.c Creating and configuring a JDBC provider

1. Click Resources | JDBC Providers in the WebSphere administrative console.

2. Click *New*. The JDBC Providers configuration window opens.

Figure 4-14: JDBC Providers configuration window
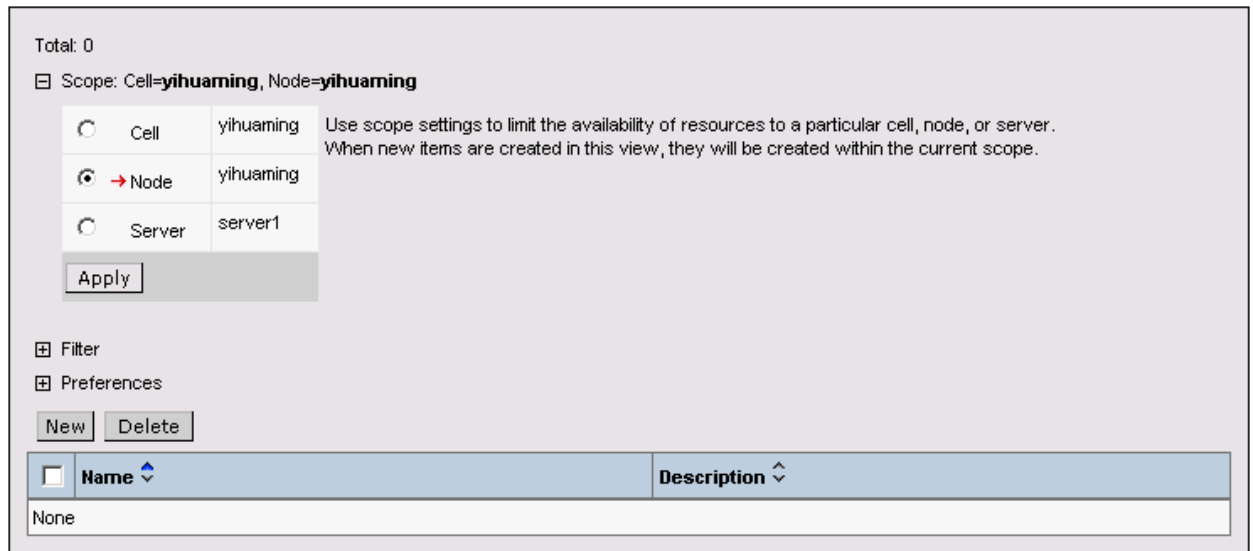
3. Select the correct JDBC provider type. For example, Oracle JDBC Driver.

Figure 4-15: Select JDBC Provider type
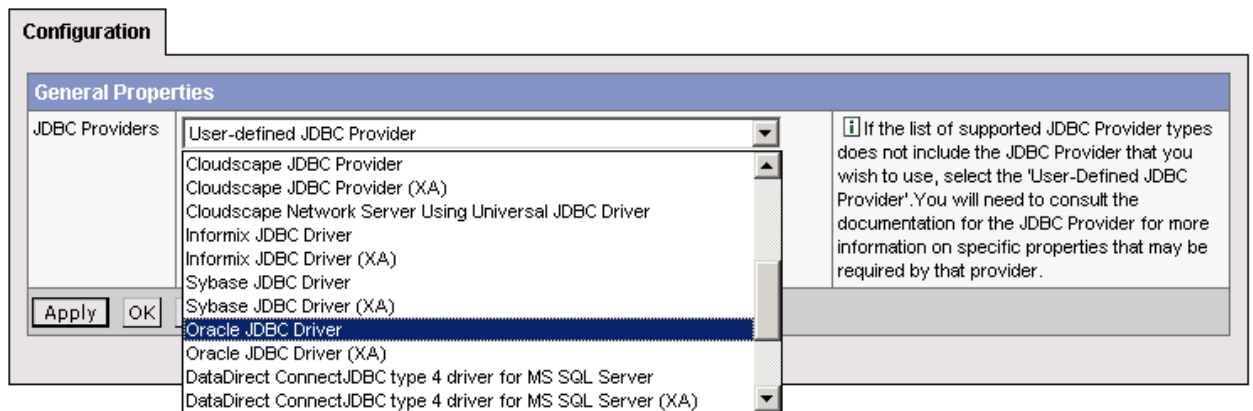
4. Select the driver provider and driver file.

Figure 4-16: JDBC driver provider and driver file

The Classpath field displays the path to the JDBC file that is configured in the WebSphere variable, for example, the ORACLE_JDBC_DRIVER_PATH driver.

5. Click *OK* to return to the JDBC providers page, where the new JDBC driver appears in the list.

6. Save the settings.

4.3.5.d Creating a data source

1. Click Resources | JDBC Providers in the administrative console.

2. Choose the JDBC resource provider under which you want to create the data source.

3. Click the *Data Sources* link under Additional Properties. The Data sources page is displayed.

Figure 4-17: Data source page

4. Click *New* to display the Data source settings page.

5. Specify the data source name and JNDI name of the data source.

Figure 4-18: Data source properties

6. Select the J2C authentication data entry configured in the *Creating a new J2C authentication data entry* section in the Container-managed Authentication Alias list box.

7. Click *Apply* and *OK* to return to the Data Sources window. The name of the new data source displays in the window.

8. Click the name of the new data source in the Data Sources window.

9. Click the link to Custom Properties in the Additional Properties of the data source configuration window.

Figure 4-19: Additional properties

10. Configure all the required fields according to the instructions in the window. For example, se the URL property to jdbc:oracle:thin:@192.0.0.51:1521:testing.

Figure 4-20: Data source URL property

11. Click *OK* to return to the data source configuration window.

12. Click the Test Connection for the new data source. Make sure the connection is successful before continuing.

13. Save the master configuration.

4.3.6 WebLogic\WebSphere Data source settings

The main two requirements for data source configuration are: (1) the driver must be JDBC type; (2) the data source must connect to the database used by the application. The settings discussed in this section focus on meeting these two requirements. Configure the other data source parameters that are not mentioned here based on your own knowledge about data source configuration or simply use the default settings.

Unless specified, the settings given in this chapter apply to the following application servers that Appeon supports: WebLogic, and WebSphere.

Note that the driver name and server name are case sensitive.

4.3.6.a Data source parameters for ASA

ASA databases support iAnywhere JDBC-ODBC (recommended), jConnect and Sun JDBC-ODBC bridge driver.

Note:

1) WebSphere server does not support JDBC-ODBC bridge driver, and supports only jConnect driver.

2) To use jConnect to connect with ASA, you must start ASA as service before configuration.

3) JConnect 6.0 is preferable to JConnect 5.5.

Table 4-22: Data source parameters for ASA

Parameter		Value	Note
jConnect JDBC driver (Recommended)	Driver name	For JConnect 5.5: com.sybase.jdbc2.jdbc.SybDriver For JConnect 6.0: com.sybase.jdbc3.jdbc.SybDriver	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. The default ASA port is 2638. *ServiceName* stands for the name of the ASA database service specified during configuration. *DSNname* refers to the name of the ODBC DSN that is created for the database.
	Server name	jdbc:sybase:Tds:*Hostname:Port/ServiceName*	
iAnywhere JDBC-ODBC driver	Driver name	For JDBC 2.0: ianywhere.ml.jdbcodbc.IDriver For JDBC 3.0: ianywhere.ml.jdbcodbc.jdbc3.IDriver	
	Server name	jdbc:odbc:dsn=DSNname	
Sun JDBC-ODBC driver	Driver name	sun.jdbc.odbc.JdbcOdbcDriver	
	Server name	jdbc:odbc:*DSNname*	
User Name		(Type the database login username. The username is set on the database server.)	
Password		(Type the database login password. The password is set on the database server.)	

4.3.6.b Data source parameters for ASE

ASE databases support jConnect JDBC driver only. ASE 15 supports JConnect 6.0 only.

Table 4-23: Data source parameters for ASE

Parameter	Value	Note
Driver name	For JConnect 5.5: com.sybase.jdbc2.jdbc.SybDriver For JConnect 6.0: com.sybase.jdbc3.jdbc.SybDriver	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. The default ASE port is 2048.
Server name	jdbc:sybase:Tds:*Hostname*:*Port*/*DBName*	*DBName* stands for the name of the database.
User Name	(Type the database login username. The username is set on the database server.)	
Password	(Type the database login password. The password is set on the database server.)	

4.3.6.c Data source parameters for Oracle

Oracle databases support the Oracle JDBC driver only.

Table 4-24: Data source parameters for Oracle

Parameter	Value	Note
Driver Name	oracle.jdbc.driver.OracleDriver	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. The default Oracle port is 1521. *DBName* stands for the name of the database to which the data source connects.
Server Name	jdbc:oracle:thin:@*Hostname*:*Port*:*DBName*	
User Name	(Type the database login username. The username is set on the database server.)	
Password	(Type the database login password. The password is set on the database server.)	

4.3.6.d Data source parameters for IBM DB2

IBM DB2 databases support the IBM JDBC driver only.

Table 4-25: Data source parameters for IBM DB2

Parameter	Value	Note
Driver Name	COM.ibm.db2.jdbc.net.DB2Driver	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. The port used by JDBC will be different than the one used by db2 client. The default JDBC port is 6789 while the port used by db2 client is 50000. *DBName* stands for the name of the database to which the data source connects.
Server Name	jdbc:db2://*Hostname*:*Port*/*DBName*	
User Name	(Type the database login username. The username is set on the database server.)	
Password	(Type the database login password. The password is set on the database server.)	

4.3.6.e Data source parameters for Microsoft SQL Server

Appeon recommends using jTDS JDBC driver (or WebLogic JDBC driver for WebLogic hosting Appeon Server) rather than the Microsoft SQL Server JDBC driver, because it can eliminate memory leak and boost performance.

Table 4-26: Data source parameters for Microsoft SQL Server

Parameter		Value	Note
jTDS JDBC driver (Recommended)	Driver Name	net.sourceforge.jtds.jdbc.Driver	*Hostname* stands for the database server name or IP address.
	Server Name	jdbc:jtds:sqlserver://*Hostname*:*port*/*DBName*; SelectMethod=cursor	*Port* stands for the database server port. The default SQL Server port is 1433.
WebLogic SQL Server JDBC driver (for WebLogic server only)	Driver Name	weblogic.jdbc.sqlserver.SQLServerDriver	*DBName* stands for the name of the database to which the data source connects.
	Server Name	jdbc:bea:sqlserver://*Hostname*:*Port*	"SelectMethod=cursor" must be specified, otherwise errors will occur when inserting data.
Microsoft SQL Server JDBC driver	Driver Name	For Microsoft SQL 2000: com.microsoft.jdbc.sqlserver.SQLServerDriver For Microsoft SQL 2005: com.microsoft.sqlserver.jdbc.SQLServerDriver	
	Server Name	jdbc:sqlserver://*Hostname*:*Port*; DatabaseName= *DBName*; SelectMethod=cursor	
User Name		(Type the database login username. The username is set on the database server.)	
Password		(Type the database login password. The password is set on the database server.)	

4.3.6.f Data source parameters for Sybase IQ

Sybase IQ databases support JConnect JDBC driver or Sun JDBC-ODBC driver.

Table 4-27: Data source parameters for Sybase IQ

Parameter		Value	Note
JConnect JDBC driver (Recommended)	Driver Name	For JConnect 5.5: com.sybase.jdbc2.jdbc.SybDriver For JConnect 6: com.sybase.jdbc3.jdbc.SybDriver	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. *ServiceName* stands for the name of the database service specified during configuration. *DSNname* refers to the name of the ODBC DSN that is created for the database.
	Server Name	jdbc:sybase:Tds:*Hostname*:*Port*/*ServiceName*	
Sun JDBC-ODBC driver	Driver Name	sun.jdbc.odbc.JdbcOdbcDriver	
	Server Name	jdbc:odbc:*DSNname*	
User Name		(Type the database login username. The username is set on the database server.)	
Password		(Type the database login password. The password is set on the database server.)	

4.3.6.g Data source parameters for Informix

Informix databases support the IBM Informix JDBC driver only.

Table 4-28: Data source parameters for Informix

Parameter	Value	Note
Driver Name	com.informix.jdbc.IfxDriver	*Hostname* stands for the name or IP address of the machine hosting the database server. One machine can host several database servers. *Port* stands for the database server port. *DBName* stands for the name of the database to which the data source connects. *DBServerName* stands for the name of the database server.
Server Name	jdbc:informix-sqli://*Hostname*:*Port*/*DBName*:informixserver=*DBServerName* For example: jdbc:informix-sqli://192.0.2.117:1527/mytestdb:informixserver=ol_s_122005_144417	
User Name	(Type the database login username. The username is set on the database server.)	
Password	(Type the database login password. The password is set on the database server.)	

4.4 Setting up transaction object to connection cache mapping

The purpose of setting up the mapping is to make sure the configured connection cache\data source can access the database server for the Appeon Web application as the replacement of the transaction object in the PowerBuilder application, as shown in Figure 4-21.

Figure 4-21: Map transaction to connection cache

Map Transaction to connection cache

```
Target PB app

    ...
    dw_1.SetTransObject(SQLCA)
    dw_1.Retrieve()
    ...
    ...
    dw_2.SetTransObject(SQLCA1)
    dw_2.Retrieve()
    ...
```

```
Web application
    Get mapping  ◄──────────
    ...
    Web dw_1 retrieve via ConnectionCacheA
    ...
    Web dw_2 retrieve via ConnectionCache B
    ...
```

```
Mapping:
SQLCA →  ConnectionCacheA
SQLCA1 →  ConnectionCacheB
```
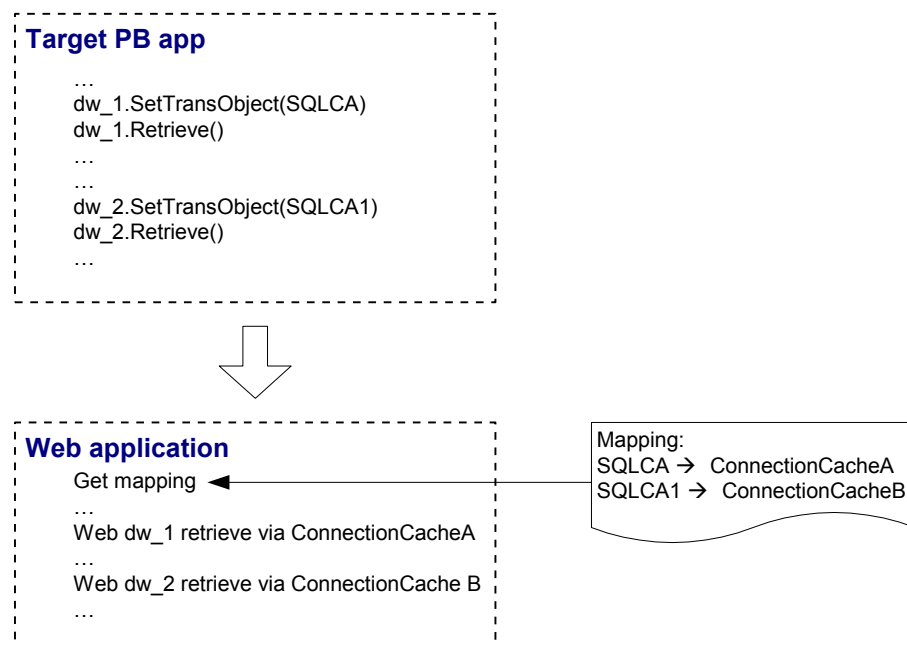
Once Appeon Server connection caches are configured, you can set up the transaction object to connection cache mapping in two different ways:

- Higher priority: Dynamic transaction object to connection cache mapping via PowerScript.

- Lower priority: Static transaction object to connection cache mapping in AEM. The mapping in PowerScript has priority over the static mapping in AEM.

Dynamic mapping is of higher priority, meaning that if a transaction object named "SQLCA" is both mapped to connection cache A via PowerScript and mapped to connection cache B in AEM, the transaction in effect is mapped to connection cache A.

Note that if Appeon Server is installed to WebLogic or WebSphere, Appeon Server and AEM reads data source JNDI names as connection cache names.

4.4.1 Dynamic transaction object to connection cache mapping

Transaction object to connection cache mapping can be dynamically set up or changed by setting or changing the DBMS and DBParm properties of the Transaction object in the application source code.

To set or change the connection cache dynamically, code the DBParm property of the Transaction object in this format:

```
SQLCA.DBParm="CacheName='ASEConnectionCache1'"
```

"ASEConnectionCache1" can be replaced by the name of the connection cache you want to use for the Transaction object.

To set or change the database type dynamically, code the DBMS property of the Transaction object using this format:

```
SQLCA.DBMS = "ODB-SYC"
```

The value of the DBMS property should be set based on the database type; refer to Table 4-29.

Table 4-29: Setting the DBMS property based on the database type

Database Type	ODBC Interface	JDBC Interface	OLE Interface	Native Interface
MS SQL Server 2000/2005/2008	ODB-MSS	JDB-MSS	OLE-MSS	MSS
Oracle8i	ODB-O84	JDB-O84	OLE-O84	O84
Oracle9i	ODB-O90	JDB-O90	OLE-O90	O90
Oracle10g	ODB-O10	JDB-O10	OLE-O10	O10
Oracle11g	ODB-ORA	JDB-ORA	OLE-ORA	ORA
Sybase ASE12.X/15.x	ODB-SYC	JDB-SYC	OLE-SYC	SYC
Sybase ASA7/8/9/10	ODB-ASA	JDB-ASA	OLE-ASA	
Sybase IQ	ODB-SYI	JDB-SYI	OLE-SYI	
IBM DB2 UDB	ODB-DB2	JDB-DB2	OLE-DB2	DIR
Informix V9	ODB-IN9	JDB-IN9	OLE-IN9	IN9
Informix V10	ODB-I10	JDB-IN7	OLE-IN7	IN7
Other	ODB-Oth	JDB-Oth	OLE-Oth	Oth

In Table 4-29:

The names are not case-sensitive (for example: ODBC is the same as odbc).

If ODB or ODBC is set as the DBMS property, Appeon will regard the database type as Sybase ASA. The "odb-asa" and "odb-db2" are Appeon defined values. They can be recognized by Appeon without affecting the running of the PowerBuilder application, because only the first three letters of the DBMS setting are valid in PowerScript syntax.

4.4.2 Static transaction object to connection cache mapping

For an Appeon Web application, you can set up transaction object to connection cache mapping in the Application Properties settings in AEM. This is a static way for mapping the Transaction object to the connection cache.

For detailed instructions on how to set up database configuration in AEM, please refer to Section 5.3.12 Connection Cache.

4.5 Advanced configurations related with database connection

4.5.1 Application security

For typical PowerBuilder applications, security is implemented at two levels: script coded security and database security. After Web conversion, the Appeon system provides an

additional built-in layer of Web application security on top of PowerBuilder application security. Appeon security is "either-or": the user either has or does not have access to the Web application.

You can implement security for deployed Appeon Web applications in many ways. PowerBuilder script-coded security can convert direct to the Web, and it provides security for the Web applications. There are also ways to implement database security in Appeon Web applications. Finally, you can use the Appeon user/group management system to restrict access to Appeon Web applications.

In addition, a way to incorporate the Appeon user/group management for use with the coded security in PowerBuilder applications is discussed in Section 4.5.2.a. You can also implement your own Web security using other Web technologies.

4.5.1.a Database security

Depending which user logs into an application, a PowerBuilder application can dynamically change the Transaction properties (user ID and password etc.) and connect to the database with different identities that determine the user privileges to access, read or modify the database tables.

Appeon Web applications rely on the JDBC connection caches to interact with the Database Servers. In the Web application, transaction object to connection cache mapping can be dynamically set up or changed by setting or changing the DBMS and DBParm properties of the Transaction object in the application source code, or it can be statically set up in AEM database configuration. There is a limitation with connection cache configuration: the user ID and password of a connection must be pre-configured in application server. Due to this limitation, you may want to consider the workarounds introduced in this section to improve the migration of database security in the original application.

Workaround one: Predefined connection caches

To work around this unsupported feature, you can pre-define in the application a certain number of connection caches that correspond to different security access levels in the database with different user IDs and passwords. When the user logs in, the application decides which transaction object to connection cache mapping to use for establishing the database connection.

You should set up an equal number of connection caches in the application server that connect to the database with different privileges, and map the connection caches dynamically using the Transaction DBParm property to the PowerBuilder Transaction objects. Transaction object to connection cache mapping can be dynamically set up or changed by setting or changing the DBMS and DBParm properties of the Transaction object in the application source code. See Section 4.4.1: *Dynamic transaction object to connection cache mapping* for the details.

Workaround two: The distributed application technique

The distributed application technique is supported by Appeon to work around the database security features in a PowerBuilder application. The methodology is to encapsulate the PowerBuilder source code that implements the database securities into NVOs and run them on EAServer. The NVOs may perform actions like creating database connections (manipulation of Transaction object properties), manipulating DataStore objects or executing SQL statements, and transferring the returned information to the Client.

For example, you can encapsulate the user authentication logic into an NVO, and then deploy the NVO to EAServer. In the application source code, you only need to pass the username and the password from the login window to the NVO.

STEP 1 – Create an NVO and declare a method in the NVO for user authentication. The method compares the user information entered in the application login window with that retrieved from the system table.

The method declared in the NVO:

```
public function boolean of_checkuser (string as_userid, string
as_password);
String  ls_DBPass
SELECT fpassword
     INTO :ls_DBPass
     FROM t_user
     WHERE t_user.fuserno = :as_userid;
If sqlca.SQLCode <> 0 Then
     Return false
End If
If ls_DBPass <> as_password Then
     Return false
End If
Return true
End function
```

STEP 2 – Deploy the NVO to EAServer and create a proxy object for the NVO in the Client application.

STEP 3 – Modify the user authentication logic in the Client application to get the user information from the login window and pass it to the NVO.

The modified script in the Client application:

```
String  ls_User,ls_Pass,ls_DBPass,ls_Err
Long  ll_ID
String ls_Mess = 'Please enter a valid user ID/password.'

If Trim(sle_name.Text) = '' Then
     sle_name.SetFocus()
     MessageBox('Login Not Valid',ls_Mess,exclamation!)
     Return
End if
ls_User = Trim(sle_name.Text)
ls_Pass  = Trim(sle_Pass.Text)
If i_logsec.of_checkuser(ls_User,ls_Pass) then
     MessageBox("Infomation","Login successful!")
Else
     MessageBox("Infomation","Login failure!")
End if
```

4.5.1.b Using INI files for connection security

You can set connection properties for a PowerBuilder application either by assigning values to the properties in the application script or using PowerScript Profile functions to read from an initialization (INI) file. It is recommended by Appeon that you set connection properties by reading from INI files only if your environment meets the following requirements:

- The browser for accessing the application must be cookie-enabled.

  Reason: Appeon Developer deploys the INI files as XML to Appeon Server. When a Client accesses the deployed application that uses the INI file profiles, a copy of the original XML file is specially created and carries all the profile information of the Client. The cookie on the Client browser enables the Client to read the correct copy of its XML file located on Appeon Server.

- Make sure the Windows user account profile on the Client is only used by one user for accessing the application.

  Reason: As the Cookie will reside in the Windows user profile cookie directory (for example, *C:\Documents and Settings\Administrator\Cookies*) any user with full access rights who also uses the Client computer will be able to gain access to another user's Web application identity.

If the same Windows user account profile will be used by multiple users on the Client, consider using another security method, Database security, as introduced in Section 4.5.1.a. *Database security*.

The initialization file should at least consist of the *Database* section:

```
[Database]
variables and their values
...
```

The following script example assigns connection properties to SQLCA. The database connection information is stored on the Web Server after application deployment; on some network configurations this can leave the database server unsecured:

```
SQLCA.DBMS = "MSS Microsoft SQL Server"
SQLCA.Database = "appeon_test"
SQLCA.ServerName = "192.0.0.246"
SQLCA.LogId = "sa"
SQLCA.AutoCommit = False
...
```

To set the Transaction object to connect to a database, the following script example reads values from App.INI, an initialization file. This method is much more secure in comparison to the preceding script.

```
sqlca.DBMS = ProfileString(App.INI, "database",&
    "dbms", "")
sqlca.database = ProfileString(App.INI,&
    "database", "database", "")
sqlca.userid = ProfileString(App.INI, "database",&
    "userid", "")
sqlca.dbpass = ProfileString(App.INI, "database",&
    "dbpass", "")
...
```

4.5.2 Appeon security

Appeon security features are set in Appeon Enterprise Manager (AEM), the Web application that manages the Appeon system and deployed Web applications. Appeon security is at the Web application level and is "either or": the user either has or does not have access to the Web application. By default, Appeon security is turned off for each deployed Web application.

When the security for a Web application is turned on, the Appeon Login Web dialog box pops up at the beginning of the Web application startup and prompts the user to enter the user name and password. The user name and password is verified by Appeon Server against the authentication schema that can be set in an LDAP server or in Appeon system database. If the user name or password is not correct, the user is not allowed to access the Appeon Web application.

For more information on using Appeon security features for Appeon Web applications, please refer to Section 5.5: *Security*.

4.5.2.a Incorporate Appeon security in PowerBuilder code

If your PowerBuilder application has not coded user name/password verification at application startup that restricts access to the application, you can utilize Appeon's built-in user group management. When the Web application runs, the user is prompted to enter the Appeon Web user name and password in the Appeon Login Web dialog box.

The Appeon Web user name can be passed to the Web application so that it can be utilized to implement script coded security features for the Web application. You can use the of_getappeonusername function in the Appeon Workarounds PBL to get the Appeon Web user name. For detailed information, refer to the *Appeon Workarounds PBL Reference | AppeonExtFuncs object* section in the *Appeon Workarounds Guide*.

4.5.2.b Database auditing

In Client/Server architecture, the database can easily keep track of every logged-in user if you enable the AUDITING option in the database.

Appeon deployed Web applications run in a three-tier architecture. Each time the Client wants to connect with the database, the call reaches Appeon Server first. Appeon Server will validate the user ID and password of the call. If the validation passes, Appeon Server connects with the Database Server using a unified user ID and password. The user ID and password that the database keeps track of is not the user ID and password that makes the call at the Client.

Passing user ID/password to database from EAServer connection cache

If you are using a Sybase ASE database, you can use the SSA connection cache property. This property changes the ID at the database to whatever user ID/Password is used by end users for accessing the server. If you are using a Sybase database, you can set this property in your connection cache props file. This cannot be used if you are using a different database type.

The following information is taken from the EAServer Administrator Guide Appendix B - Connection Cache Properties; please refer to the EAServer documentation for more detailed instructions.

The connection cache property, *com.sybase.jaguar.conncache.ssa,* enables set-proxy support for connections to databases that support this feature. By default, the property is set to false, which disables set-proxy support.

This feature can be used with any database that recognizes this command:

```
set session authorization "login-name"
```

When proxy support is enabled, connections retrieved from the cache are set to act as a proxy for the user name associated with the EAServer client. To set the proxy to another user name, use the Java JCMCache.getProxyConnection() method or the C JagCmGetProxyConnection() routine in your component.

The user name specified in the cache properties (com.sybase.jaguar.conncache.username) must have set-proxy privileges in the database and/or server used by the cache.

In EAServer Manager, set this property using the All Properties tab in the Connection Cache Properties dialog box.

Re-configuring database auditing functionality

To work around the database auditing functionality, you can also re-configure the auditing information that is saved on the database by adding a new field to it: user ID.

With the Client/Server application, make sure that a combination of user ID and password cannot hold multiple connections with the database at one time.

Add in the necessary code in the Client Server application so that every time the user wants to connect with the database, the call sent to the Database Server includes user ID information. For example, when sending the user ID as a column in the DataWindow or to the Stored Procedure, the user ID information in the call from the client-side will be saved in the user ID field on the Database Server.

5 AEM User Guide

5.1 Introduction

5.1.1 Overview

Appeon Enterprise Manager (AEM) is a Web-based application that is automatically installed with Appeon Server to manage the Appeon Server and Appeon deployed Web applications.

AEM is designed to manage both single-server installations and multiple-server installations with the same ease and power, and it provides an additional layer of security to the existing security already coded into your PowerBuilder application. It also allows the administrator to use the built-in Appeon security management system or LDAP security (recommended) to control the access rights at the application level.

All settings configured in AEM are saved to several XML files in the <Appeon Home>\repository\<instancename>\config folder. For example, if Appeon Server runs on EAServer, the XML files are saved in the %JAGUAR%\appeon\repository\<instancename>\config folder, where %JAGUAR% stands for the installation path of the EAServer on the computer.

5.1.2 AEM tools

AEM contains three sets of tools: Server Properties, Application Properties, and Security Settings. After login, you can access each tool either from the treeview window on the left or from the Welcome window on the right. Refer to Figure 5-1.

Figure 5-1: AEM Console

5.2 Getting started

5.2.1 Overview

Appeon Server must be running before you start AEM. If using an Appeon Server cluster, AEM should only be used in one server to manage all the servers in the cluster.

5.2.2 Running Appeon Server

Start Appeon Server, which means starting the application server (EAServer, WebLogic, or WebSphere) that Appeon Server is installed to.

For example, if Appeon Server is installed to EAServer, you can start Appeon Server with the following method:

In Windows: choose Programs | Appeon 6.2 for PowerBuilder | Appeon Server | %InstaceName% from the Windows Start menu.

In Unix\Linux: change to the $JAGUAR/appeon/bin/ folder and run the appeonserverstart.sh file.

When the command line window displays "Accepting connections", Appeon Server is ready for use.

5.2.3 Starting AEM

5.2.3.a AEM URL

The URL for launching AEM for a given Appeon Server is HTTP://*HOST_NAME*:*PORT*/AEM/ or HTTPS://HOST_NAME:*PORT/AEM/*, where *HOST_NAME* is the machine name or IP address of the server, and *PORT* is the HTTP or HTTPs port for the server.

The Appeon installation program creates an HTTP listener (localhost: 9988) for Appeon Server when installed to EAServer on Windows. If you want to start AEM from the computer that hosts the Appeon Server, the following URL should work: http://localhost:9988/AEM. However, you should not use a "localhost" listener in a production environment.

The default ports for EAServer, WebLogic, and WebSphere are:

- EAServer: 8080

- WebLogic: 7001

- WebSphere: 9080

5.2.3.b Three ways to launch AEM

There are three ways to launch AEM:

- Type the AEM URL in any Web browser that is able to connect via HTTP or HTTPS to the Web port of the Appeon Server.

- In the computer where Appeon Server is installed, select *Programs | Appeon 6.2 for PowerBuilder | Appeon Server | Appeon Enterprise Manager* from the Windows Start menu.

- In the computer where Appeon Developer is installed, click the *AEM* button (🦅) in the Appeon Developer toolbar. Before doing this, ensure that the AEM URL has been configured correctly for the server in Appeon Developer.

5.2.3.c AEM username and password

Enter a valid username and password for AEM. The username and password are those you specified when installing Appeon Server. If you did not specify the username and password during the installation, you can use the default user name and password (both "admin") to log into AEM. For security purposes, Appeon recommends that you change the username and password after the initial login.

5.2.4 AEM Help

On the index of Appeon Enterprise Manager, the *Help* button provides easy access to AEM Help, as shown in Figure 5-2:

Figure 5-2: Help button

Click the Help button, find the topic on the left pane, and view the content on the right pane, as shown in Figure 5-3:

Figure 5-3: Appeon Help
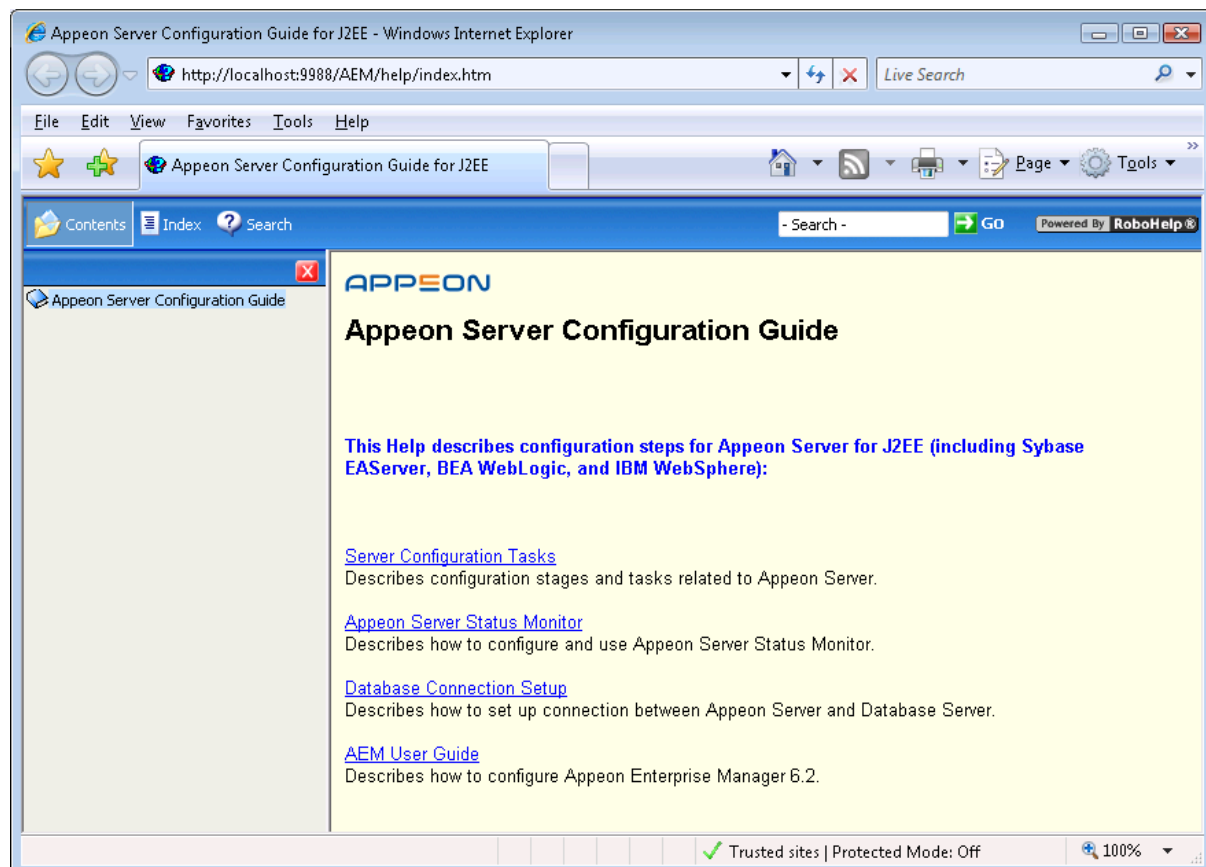
5.3 Server Properties

5.3.1 Overview

Server Properties is a set of tools for viewing and modifying all configurable system settings. There are eleven tools: Active Sessions, Active Transactions, Web, Log Files, Log Viewer, Temporary Files Cleanup, Deployment Sessions, Cluster, Licensing, Support, and Connection Cache. Refer to Figure 5-4.

Figure 5-4: Server Properties

5.3.2 Active Sessions

The AEM Active Sessions tool helps you manage and monitor all sessions on the system. Refer to Figure 5-5.

Figure 5-5: Active Sessions
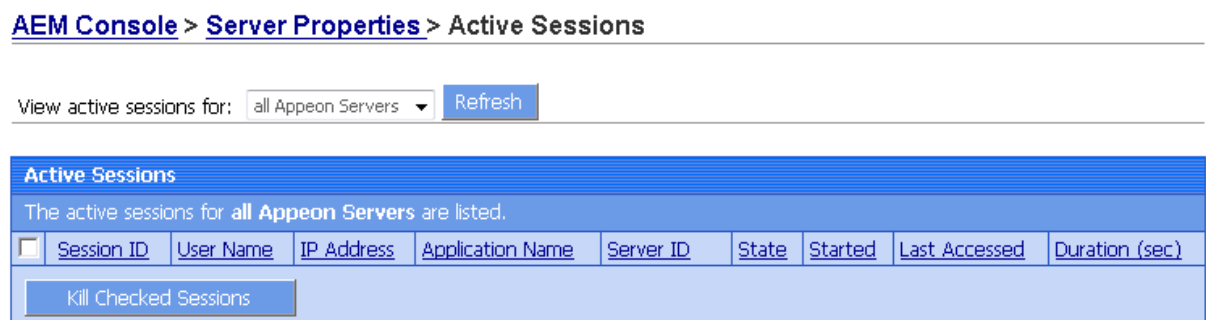
5.3.2.a Viewing sessions on an Appeon Server

By default, the Active Sessions table lists the current active and passive sessions on all Appeon Servers. If you want to view sessions on an Appeon Server, select the Appeon Server from the "Viewing active sessions for" dropdown list, and click the Refresh button. The dropdown list displays all the servers configured in the Cluster tool.

You can sort the Active Sessions table by clicking any heading of the columns.

Each session will have the following two states:

- Active sessions: if the session is created by an Appeon Server, the session will be recognized as an active session for that Appeon Server.

- Passive sessions: if the session is backed up in another Appeon Server (randomly picked according to the load balancing algorithm), the session will be recognized as a passive session for that Appeon Server. The passive sessions only exist when you enable session backup in the Cluster tool.

5.3.2.b Killing session(s)

You can kill a single or multiple sessions in the Active Sessions table to release Appeon Server resources or if you want to perform database maintenance. Each session may include several transactions. When you kill an active session, the active transactions that belong to the session will be rolled back.

Step 1 – Check the sessions that you want to kill.

Proceed with caution when checking sessions that you want to kill.

Step 2 – Click the *Kill Checked Sessions* button.

A message box displays for you to confirm the action. Once you confirm the action, the selected sessions are immediately killed and the Active Sessions table is refreshed.

5.3.3 Active Transactions

The AEM Active Transactions tool helps you manage and monitor all active transactions on the system. Refer to Figure 5-6.

Figure 5-6: Active Transactions
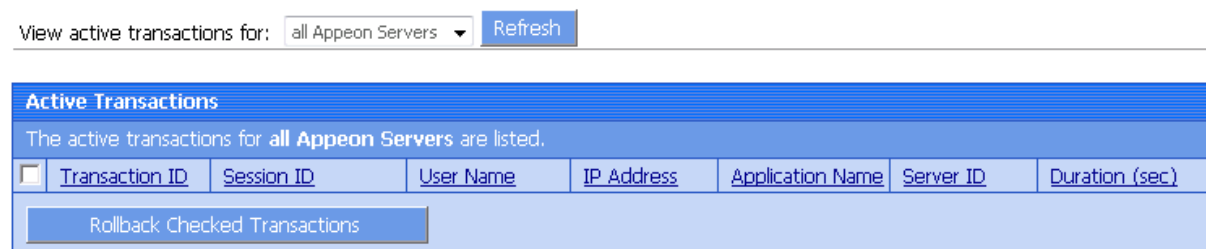
5.3.3.a Viewing active transactions on an Appeon Server

By default, the Active Transactions table lists the current active transactions on all Appeon Servers. If you want to view active transactions on an Appeon Server, select the Appeon Server from the "Viewing active transactions for" dropdown list, and click the Refresh button. The dropdown list displays all the servers configured in the AEM Appeon Server Cluster tool.

You can sort the Active Transactions table by clicking any heading of the following columns: Transaction ID, Session ID, User Name, IP Address, and Process Time.

5.3.3.b Rolling back active transaction(s)

You can roll back a single or multiple active transactions in the Active Transactions table to release Appeon Server resources or in case of a database deadlock.

Step 1 – Check the active transaction(s) that you want to roll back.

Proceed with caution when checking transactions you want to roll back.

Step 2 – Click the Rollback Checked Transactions button.

A message box displays for you to confirm the action. Once you confirm the action, the selected sessions are immediately killed and the Active Sessions table is refreshed.

5.3.4 Web

The AEM Web tool provides configuration for PDF Printing of Appeon Server for Web applications.

This setting is only effective for Appeon Server installed to EAServer on Windows. You can specify the name of the printer for PDF printing (PDF Printing), after making any change to the configuration, click the Save button . By default, the printer name is "Appeon PDFPrinter" in AEM. Note: The printer name specified in AEM should be identical to the name of the PDFPrinter that is added to the list of printers in Appeon Server by the Appeon PDFPrinter installation program. The PDFPrinter will not work if the two names do not match. If you change the name of the PDFPrinter in Appeon Server, update the printer name with the new name in the PDF Printing box.

Figure 5-7: Web tool in Server Properties

5.3.5 Log Files

Appeon Server creates three different log files for record keeping and for future use in troubleshooting (Figure 5-8). You can view these log files using the Log Viewer tool or directly locate them in the %appeon%\repository*instancename*\log folder.

On the Log Files page, you can configure two log file settings:

- Log Mode
- Replace Log Files

Click the *Save Settings* button to save changes.

Figure 5-8: Log Files

AEM Console > Server Properties > Log Files

Log Files Path

Appeon log files are stored in %AppServer%\appeon\repository\%Instance%\log.

Log Mode

- ○ Off
- ⊙ Standard mode (default)
- ○ Developer mode
- ○ Debug mode

Replace Log Files

- ⊙ Never replace log files
- ○ Replace log files...
  - ☑ When size exceeds 2   MB
  - ☐ Every 1   day(s)
- ☑ Backup log files before replacing

Save

5.3.5.a Log mode

Select one of the following four modes for log file operation.

- Mode 1: Off

  Off mode does not generate any log files **except** error log files. It offers the fastest performance.

- Mode 2: Standard mode

  Standard mode is the default mode, and should be used when the system is stabilized. It generates standard log files that are sufficient for providing basic system activity information and notifies you if errors have occurred. This mode may be inadequate for detailed troubleshooting.

- Mode 3: Developer mode

  Developer mode generates detailed log files that are sufficient for routine checking and troubleshooting. Performance speed decreases when using this mode.

- Mode 4: Debug mode

  Debug mode generates log files that record every system activity in detail and provide the user with information for troubleshooting **obscure** or **hard to find** issues. Debug mode log files are useful for technical support. There is a noticeable slowdown in performance when using this mode.

5.3.5.b Replace log files

Log files accumulate over time, and if they become too large, they can decrease Appeon Server performance. Select the "Replace log files…" option to replace the log files periodically.

To configure log file settings:

Step 1 – Decide whether the log files should be replaced.

- Option 1: Never replace log files

If you select this option, the log files will never be replaced. This option may compromise system performance when the log files become large, in which case they should be manually deleted.

- Option 2: Replace log files …

  If you select this option, this option will replace log files according to conditions configured in Step 2. **It is highly recommended that you use this option**. To create and keep an archive of all logs, check the "Backup log files before replacing" option.

Step 2 – Set the condition for replacing log files by checking one of the options.

- Option 1: Replace log files when size exceeds ___ MB.

  The system automatically replaces the log files when the file size exceeds the value set here.

- Option 2: Replace log files every ___ day(s).

  The system automatically replaces the log files as stipulated by the value set here.

Step 3 – Decide whether the log files should be backed up.

- This setting allows Appeon Server to back up the log files before replacing them. If this option is checked, all log files are backed up before they are replaced so an archive of the log files is maintained. Maintaining this archive does not compromise system performance, but there must be adequate hard disk space for the backup log files.

- All backup log files are named according to the following format: Log File name ("LogSystem") + an underscore ("_") + the time of the creation of the backup file (yyyy/mm/dd/hh/mm) + ".bak". For example: LogSystem_200504081213.bak.

5.3.6 Log Viewer

The Log Viewer gives you direct access to the log files created by Appeon Server and the host application server of Appeon Server, such as EAServer.

Figure 5-9: Log Viewer

- Appeon Server Logs

  Server Log – the main log file. Records messages logged from services and the core Appeon Server runtime.

  Error Log – the error log.

  Deployment Log – records messages logged during application deployments.

- Application Server Log

  Server Log – the main log file of the host application server.

The Log Viewer tool provides the following manipulations:

- To view a log file

  Click *View* to view the detailed information in the browser, as shown in Figure 5-9. The log file will be shown in a new window, as shown in Figure 5-10.

  If the size of the specified log file exceeds 2 MB, a message will pop up indicating that the file should be downloaded before viewing.

Figure 5-10: Deployment Log
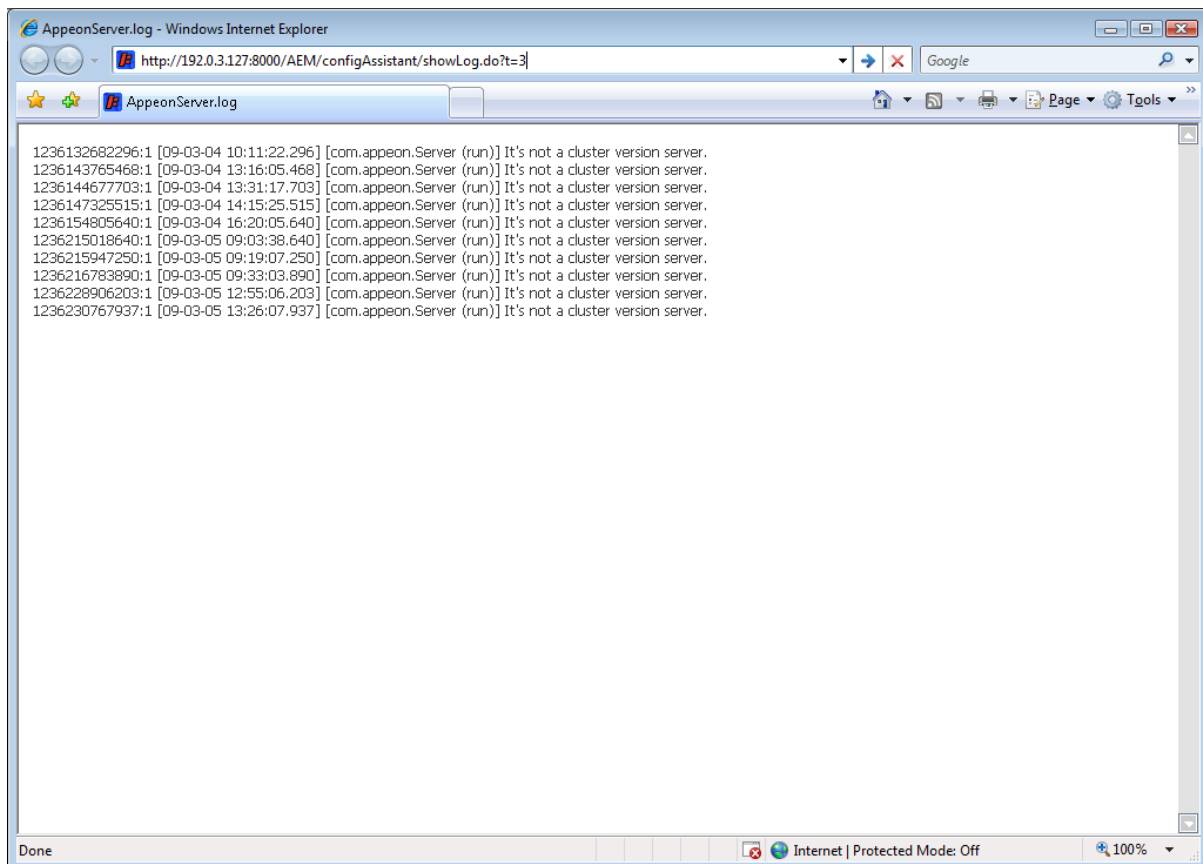
- To download a log file

  Click *Download* and click *Save* on the popup dialog.

- To clear a log file

  Click *Clear* to remove the contents in the Appeon Server log files.

Contents in the application server log file cannot be cleared, because the application server log file may contain records that are not related with Appeon operations.

5.3.7 Temporary Files Cleanup

Temporary Files Cleanup helps you manage the temporary files cleanup automatically or manually. Refer to Figure 5-11.

Figure 5-11: Temporary Files Cleanup

5.3.7.a Auto cleanup

To perform an auto-cleanup for temporary files in the "Cleanup Periodically" group box:

Step 1 – Select the file types to clean up and specify cleanup time.

- Option 1: Clean up DataWindow data files, DataWindow image files, PDF files

  This option is only available for Appeon Server installed to EAServer.

- Option 2: Clean up temp register and profile config files

  Both Option 1 and Option 2 are checked by default. You can choose whether or not to perform these two cleanup jobs by selecting or deselecting these two options.

- Option 3: Clean up the temporary files _____ day(s) ago at ___ am/pm.

  This option is only available for Appeon Server installed to EAServer.

  Use this option to specify a particular time for temporary DataWindow data files, DataWindow image files, and PDF files to be cleaned up. For example, "Clean up the temporary files 2 days ago at 8:00 am" denotes that all temporary files generated 2 days ago will be cleaned up everyday at 8:00 am.

- Option 4: Clean up the info that is last accessed: ___ day(s) ___ hours ago.

  Use this option to specify a particular time based on which the temporary register and profile configuration files will be cleaned up. For example, "Clean up the info that is last accessed: 2 days 4 hours ago" denotes that all temporary register and profile configuration files that were accessed over 2 days and 4 hours ago will be cleaned up everyday.

Step 2 – Click the *Save* button to apply changes.

5.3.7.b Manual cleanup

This feature is not usually necessary if the auto-cleanup feature is used, but it can be helpful between scheduled cleanups if a sudden increase in activity on the system causes an influx of temporary files resulting in declines in performance.

To perform a manual cleanup in the "Cleanup Now" group box:

Step 1 – Select the temporary files to be cleaned up.

Determine which temporary files are to be cleaned up by selecting the following options: "Clean up DataWindow data files, DataWindow image files, PDF files", and "Clean up temp register and profile config files". Both of these options are checked by default.

The "Clean up DataWindow data files, DataWindow image files, PDF files" option is only available for Appeon Server installed to EAServer.

Step 2 – Click the *Cleanup Now!* button to commit the cleanup.

The selected temporary files will be deleted immediately from all the Appeon Servers that are configured in the AEM Appeon Server Cluster page.

5.3.8 Deployment Sessions

The Deployment Sessions tool can help you manage and monitor all the active deployment sessions on the system. Refer to Figure 5-12.

Figure 5-12: Deployment Sessions
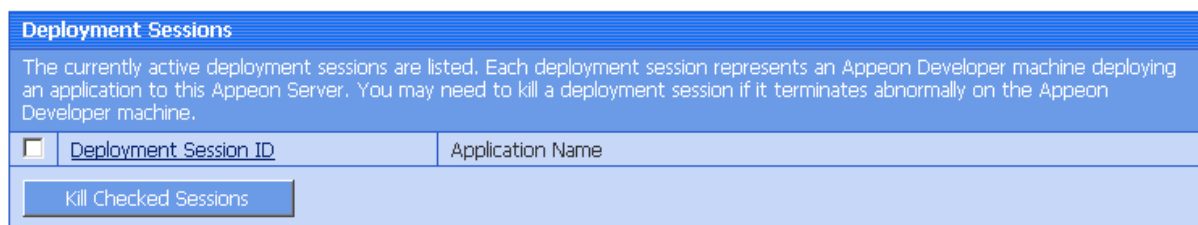
An active deployment session automatically starts and displays in the Deployment Sessions table when Appeon Developer starts to upload the embedded SQL statements, DataWindow SQLs, and INI files of an application to Appeon Server. It ends and disappears automatically from the table when the upload process is completed.

There is one special scenario in which you need to manually kill a deployment session in AEM. If the Deployment Wizard of Appeon Developer abnormally exits during the above-mentioned upload process, the deployment session stays in active status in Appeon Server, and Appeon Developer cannot resume the upload process. Only after you kill the deployment session (by checking the session and clicking the *Kill Checked Sessions* button) or restart Appeon Server can the Deployment Wizard continue its job and upload the application.

Note: Killing a deployment session does not affect the ongoing deployment process. It does not have a negative effect if you kill a deployment session by mistake.

5.3.9 Cluster

Once you installed Appeon Server to several application servers, you can use the AEM Cluster tool to create an Appeon Server cluster and configure the load balancing and failover settings of the cluster.

Note that the load balancing and failover features mentioned in this section are implemented using a plug-in specially provided by Appeon. You will need to configure this Appeon plug-in after creating the Appeon Server cluster in AEM. For detailed instructions, please refer to

the *Configuring for Appeon Server cluster* section of *Web Server Configuration Guide* in Appeon Help.

You can also implement the load balancing feature (but not failover) using the plug-in provided by the application server (such as EAServer). Detailed instructions can also be found in the Web Server Configuration Guide in Appeon Help.

Figure 5-13: Cluster

5.3.9.a Cluster Server List

Use the Cluster Server List to create an Appeon Server cluster. The Appeon Servers listed in the Cluster Server List group share the same AEM settings, and can work as a cluster in supporting the requests from their associated Web server.

Important requirements

- Use the IP address or machine name of the Appeon Server when adding an Appeon Server. Do not use "localhost" or "127.0.0.1".

- The IP address or machine name and port number must match the settings of HTTP listeners in the application server.

- Add the server that the current AEM runs on as the first member of the cluster, and if you want to remove all servers from the list, remove it last.

- To successfully synchronize/save a specific setting to all servers in the list, verify that servers are running before you save it.

- An application must be deployed to all servers in the cluster to make sure the cluster functions properly. Use the Appeon Developer Deployment Wizard to perform the application deployment. For detailed instructions, refer to the *Appeon Developer User Guide*.

- To ensure the most efficiency and stability of the Appeon Server cluster, verify that the environment of all Appeon Servers is identical. For example, the application server (type and version) and Appeon Server (version and license) must be the same.

- If you need to reinstall the operating system of an Appeon Server in the cluster, be sure to remove the Appeon Server from the cluster first.

Adding an Appeon Server

Step 1 – Click the *Add Appeon Server* button on the Cluster Server List page. The Add New Appeon Server page opens.

Step 2 – Verify that the Appeon Server to be configured is running and provide the required information (IP address, port, login username, and AEM login password). For example:

- IP address: 161.0.0.1

- Port: 8080

- User Name: admin

- Password: admin

Step 3 – Click the *Save and Add* or *Save* button. The program will automatically test the connection and add the Appeon Server if the test is successful.

Adding an Appeon Server will succeed only if:

1. The Appeon Server is new to AEM.

2. The information provided is correct.

3. The Appeon Server is running.

4. The first Appeon Server that you add is the one hosting AEM.

5. The password is correct.

Removing an Appeon Server

To remove an Appeon Server from the list:

Step 1 – Click the *Delete* button in the Actions column of the Appeon Server in the Appeon Server Cluster page.

Step 2 – A message box appears requiring confirmation. Choose *OK* to proceed with the deletion, or choose *Cancel* to cancel.

Step 3 – By clicking on the *OK* button, the Appeon Server is removed from the Appeon Server list. AEM no longer interfaces with the Appeon Server.

To remove all Appeon Servers from the list:

Click the *Remove All* button and then click *OK* in the popup message box to confirm the deletion.

Checking status of Appeon Server

An Appeon Server in a cluster must be in the "Running" status in order to handle the requests from Web server. Appeon Server has the following status:

- Shut down: Appeon Server is not started or not available.

- Ready: Appeon Server is preparing itself to accept user requests by taking the essential initialization process.

- Running: Appeon Server is started and accepts user requests.

- Failed: Appeon Server failed to start or failed to verify license.

5.3.9.b Load Balancing Settings

Load Balancing Settings determine how requests will be distributed among the servers in the cluster to optimize system performance and how servers in the cluster will be picked as peer servers. Appeon Server cluster supports the following two load balancing algorithms:

- Random – distributing requests across servers in random order, regardless of the status of servers.

- Sequence – directing requests to servers in an allocated order. The sequence algorithm, which is also known as round-robin, is simple, cheap and very predictable.

Either algorithm can provide optimal performance for servers of similar configuration and specification, because it evenly sends requests to each server in the cluster.

5.3.9.c Failover Settings

Failover Settings determine how the session information in the servers of the cluster is backed up in the system for failover support. With the backup settings, the sessions at a failed server can be continuously supported by the same server after the server is restarted by its Status Monitor, or supported by another server in the cluster. Because session backup does not back up transaction information, there may be some loss to the operations in the sessions, but the users can continue running the sessions without re-login.

Appeon Server cluster provides two major backup options for failover: session backup and heartbeat backup.

Session backup

Session backup options enable a session to be backed up when Appeon Server detects that the session status changes or it receives a request from the same session. You can specify the backup with different levels:

- Session level – backing up a session when Appeon Server detects that the session is created or destroyed, or when a transaction starts or ends in the session.

- Request level – backing up a session each time when Appeon Server receives a request from the same session, regardless of the session status.

Heartbeat backup

Heartbeat backup options enable Appeon Server to automatically back up sessions at the internals you specify.

- Remote backup – backing up all sessions from the local machine to the peer server (another server in the cluster that was picked randomly or in sequence) at the intervals

you specify in the Interval Time box. Remote backup includes mirror backup and rotation backup.

- Mirror backup – periodically backing up all sessions from the local machine to the peer server. A session is backed up at a fixed peer server. If the peer server fails, the session backup no longer works.

- Rotation backup – periodically backing up all sessions from the local machine to the peer server. The peer server at which a session is backed up can be changed. That is, if the first peer server fails, another server will be picked as the peer server for the backup.

- Logical Restore with Status Monitor – backing up all sessions from the local machine to the peer server and allowing both "active" and "passive" sessions to be restored after a failed server is restarted by Status Monitor. If this option is disabled, only "active" sessions on the failed server will be recovered. Each server in the cluster maintains a list of "active" sessions and a list of "passive" sessions. The server recognizes a session as an "active" session if it is created locally and recognizes a session as a "passive" session if it is created in another server and backed up here. The interval of this backup option is specified in the configuration file (monitor.props) of Status Monitor.

5.3.9.d Synchronizing AEM settings to servers in a cluster

Once an Appeon Server is added to the Cluster Server list, you can use the AEM which maintains the list to manage all servers in the cluster. Whenever you change the settings of this AEM and click Save, the settings will be saved to the other servers in the cluster. Therefore, you do not need to repeat the configuration in each AEM. However, not all of the AEM settings can be synchronized, because some settings are not necessary to be the same for all servers. The following settings will not be synchronized:

- Log Viewer: displays the log files on the current server only.

- Temporary Files Cleanup: clears the temporary files of the current server only.

- Deployment Sessions: displays the active deployment sessions of the current server only.

- Licensing: displays the license information and status of the current server only.

- Connection Cache: displays and configures the connection cache related with the current server only.

- DataWindow Data Cache: displays and configures the DataWindow data cache related with the current server only.

- AEM login: displays and configures the login information of AEM on the current server only.

The following action will not be synchronized:

- Killing active sessions: this action will terminate the session on the current server only.

5.3.10 Licensing

The Licensing tool enables you to view the detailed license information. It is also a tool for Appeon to manage the customer, therefore, the three buttons will only work in Appeon Distribution, as shown in Figure 5-14.

Figure 5-14: Licensing

5.3.11 Support

The Support tool is used for Appeon to manage the customer. It only works in Appeon Distribution.

5.3.12 Connection Cache (EAServer 5.x only)

This Connection Cache tool becomes invisible if Appeon Server is installed to EAServer 6.x, WebLogic, and WebSphere. And you would need to configure the connection cache (or data source) in the application server console. For details, please see user documents of the application server.

Appeon provides the AEM Connection Cache tool as a shortcut for configuring EAServer 5.x connection cache. You can add, edit, delete and test a connection cache in AEM, without needing to switch to EAServer Manager to do that as before. To configure connection caches in AEM, follow the sections below.

5.3.12.a Logon

Click Connection Cache in the tree view, and the "Log in to EAServer" page display. Specify the user name and password for the Appeon Server. The default values are "jagadmin" and null, as shown in Figure 5-15. Click Logon to view the connection cache list in the Appeon Server.

Figure 5-15: Logon

5.3.12.b Connection cache list

Each connection cache specifies the settings used to connect to a database at runtime. You can add a new connection cache, edit, delete or test an existing connection cache.

Figure 5-16: Connection cache

Adding a connection cache

Click *Add Connection Cache* below the connection cache list and specify the connection cache settings according to Table 5-1.

Figure 5-17: Add connection cache

Table 5-1: Connection Cache Properties

Connection Cache Name	Type the name of the connection cache.
Driver Type	Select the driver type for the connection cache.
Class Name	Type the driver string. The driver string is case-sensitive
ODBC Data Source Name	Type the data source name only when the driver type is ODBC-JDBC Bridge.
Database Host	Type the database host.
Database Port	Type the database port.
Database/Service Name	Type the database/service name.
Database Server Name	Type the machine name or IP address of the database server.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.
URL	Establish a connection to the database by specifying the DB URL.
Show/Hide Advanced Options	Select to show or hide advanced options, including minimum and maximum connection pool size.

| Minimum Connection Pool Size | Specify the minimum number of connections EAServer opens and pools on startup. |
| Maximum Connection Pool Size | Specify the maximum number of connections EAServer opens and pools on startup. |

For step-by-step instructions on setting up connection caches for various database types, refer to Chapter 4: *Database Connection Setup*.

Editing a connection cache

Click *Edit* and change the settings on the *Edit Connection Cache* page (Figure 5-18). The settings are specified the same way as on the *Add Connection Cache* page.

Figure 5-18: Edit connection cache

Deleting a connection cache

Click *Delete* and you will be prompted whether to delete the specified connection cache. Click *OK* to proceed (Figure 5-19).

Figure 5-19: Delete connection cache
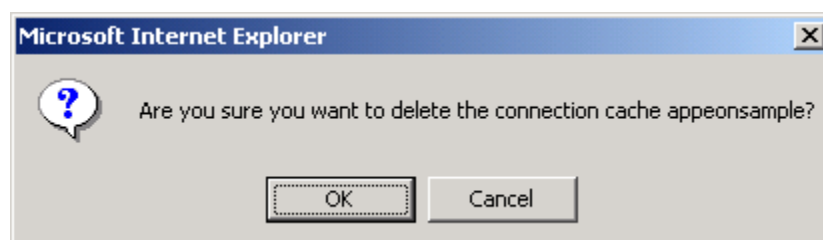
Testing a connection cache

Click *Test Connection* to test if the specified connection cache is successful. If the connection cache fails, click *Edit* to modify the settings until it succeeds (Figure 5-20).

Figure 5-20: Test connection cache

5.4 Application Properties

5.4.1 Overview

Applications deployed to Appeon Server are registered in AEM with their application profile names.

Application Properties are a set of tools for setting the server-related properties for Web applications. There are fifteen tools: Basic Information, Transaction Objects, Timeout Settings, Charset, Application Server Cache, DataWindow Data Cache, DLL/OCX Files Download, Registry Mode, Multi-Thread Download, INI File Settings, Error Message Mode, Run Mode, Transfer Encoding, Decimal Precision, and Client Settings, as shown in Figure 5-21. The settings for each application profile affect Web application(s) deployed from the application profile.

Figure 5-21: Application properties

5.4.2 Basic Information

The Basic Information tool displays the basic information of all deployed Web applications, including the PowerBuilder version, application size and DLL/OCX file size (Figure 5-22).

Figure 5-22: Basic information

AEM Console > Application Properties > Applicaiton Information

Basic Information			
Displays the basic information for all applications.			
Application Name	PowerBuilder Version	Application Size (KB)	DLL Size (KB)
appeon_acf_demo		0.00	0.00
appeon_code_examples		0.00	0.00
sales_application_demo		0.00	0.00

5.4.3 Transaction Objects

A database-driven PowerBuilder application has at least one database connection, which is accomplished with the use of transaction objects. When the PowerBuilder application is deployed to the Web, Appeon Server handles the database connection using connection caches configured in Appeon Server rather than transaction objects defined in the PowerBuilder application.

All transaction objects in the PowerBuilder application must be mapped to a correct Appeon Server connection cache. "Correct" means that the connection cache should be created as a JDBC connection cache in the application server hosting Appeon Server, and it should connect to the same database that the Transaction Object connects to in the application.

There are two types of transaction object to connection cache mapping methods:

- Dynamic Transaction object to connection cache mapping via PowerScript
- Static Transaction object to connection cache mapping in AEM

The dynamic mapping in PowerScript has priority over the static mapping in AEM. This section introduces how to set up the static mapping in AEM. For information about the mapping in PowerScript, refer to Section 4.4.1: *Dynamic transaction object to connection cache mapping*.

5.4.3.a JDBC requirement for transaction object mappings

Appeon Server is based on J2EE architecture and therefore requires JDBC to interface with the database. The JDBC connection caches can use any of the following four types of JDBC drivers: JDBC-ODBC Bridge, Native-API/partly Java driver, Net-protocol/all-Java driver, or Native-protocol/all-Java driver.

Refer to Chapter 4: *Database Connection Setup* for more information on this topic, including recommendations on which JDBC driver to use and instructions for creating connection caches.

5.4.3.b Configuring transaction object mappings for an application

When an application is deployed to Appeon Server, AEM automatically adds the application name into the application list of the Transaction Objects tool.

To view the static transaction object mappings for an application, click the application in the Transaction Objects tool. A new page opens and displays the current transaction mapping(s) for the application, as shown in Figure 5-23.

Figure 5-23: Configuring transaction object mappings for an application

Modifying an existing transaction object mapping

1) To change the connection cache

For each transaction object, there is a dropdown list in the "Connection Cache" column. The list box lists the JDBC connection caches created in Appeon Server.

Make sure the selected connection cache connects to the same database that the transaction object connects to.

You can change the current connection cache by selecting another from the dropdown list. Click *Test Connection* to verify the database connection is successful and then click *Update* to apply the change.

2) To change the database type

If the database the transaction object connects to is changed (for example, if all the data are moved from Oracle to Sybase), AEM must be updated.

Change the current database type by selecting a database from the dropdown list in the "Database type" column. Click *Update* to apply the change.

3) To delete an existing transaction object mapping

Clicking the *Delete* button will delete a transaction object mapping. A pop-up message will ask you to confirm deletion.

By default, a "SQLCA" transaction object is configured in AEM for each application. If the PowerBuilder application does not contain a SQLCA transaction object, you can delete the SQLCA transaction object mapping.

Adding an transaction object mapping

Step 1 – Click the *Add Transaction Object* button in Figure 5-23. The Add Transaction Object page displays as shown in Figure 5-24.

Figure 5-24: Add transaction object

Step 2 – Enter the transaction object name in the "Transaction object" field. The transaction object name is case insensitive and is the same as the one used in the original PowerBuilder application.

Step 3 – Select the connection cache from the "Connection cache" dropdown list. The list displays the JDBC connection caches created in Appeon Server.

Make sure the selected connection cache connects to the same database that the transaction object connects to. Click *Test Connection* button to test the database connection.

Step 4 – Select the database type from the "Database type" dropdown list.

Make sure the selected database type is identical to what the transaction object connects to.

Step 5 – Double-check the information entered because AEM does not validate user-entered data.

Step 6 – Click the *Test Connection* button to test the specified database connection.

Step 7 – Click the *Add Transaction Object* button if testing connection cache succeeded.

To add more transaction object mappings, repeat the above steps.

5.4.4 Timeout Settings

The Timeout Settings provides configuration for four important functions of Appeon Server for Web applications (see Figure 5-25: Timeout settings):

- When the session will timeout (Session Timeout)

- When the transaction will timeout (Transaction Timeout)

- When the file download will timeout (Download Timeout)

- When the message request will timeout (Request Timeout)

Figure 5-25: Timeout settings

Click the application name in the "Application Name" column of the table to configure the settings. After making any changes to the configuration, remember to click the *Save* button. As shown in Figure 5-26.

Figure 5-26: Detailed timeout settings

5.4.4.a Session timeout

A session starts when the user sends a request to load a Web application from the server, and ends if the user closes the application or has not sent any requests to the server during the "session timeout" period.

- By default, the timeout period for a session is 3600 seconds.

- You can set a timeout interval that is shorter or longer than the default setting. The session timeout can be removed altogether by setting the timeout value to 0. This is not recommended because it will eventually exhaust system resources unless old sessions are manually cleared out using the Active Sessions functionality of AEM.

5.4.4.b Transaction timeout

Appeon supports COMMIT and ROLLBACK transaction management statements, and provides a "transaction timeout" setting in AEM that can force a transaction to roll back and release database resource.

The transaction timeout can be removed altogether by setting the timeout value to 0; it is recommended that you set the timeout interval to a small non-0 value, because a small transaction timeout value can prevent:

- Database locking. When a Web application closes abnormally, the active transaction in it can neither commit nor roll itself back.

- Application locking. If an application is deadlocked, other applications cannot proceed.

5.4.4.c Download timeout

Files that are downloaded by the user often include the JS files, Weblibrary.cab package, DLL/OCX files and application files. They may have a considerable size and therefore take a long time to download. If the user has not received any data during the "download timeout" period, AEM will end the download and prompt an error message.

- By default, the timeout period for file download is 3600 seconds.

- You can set a timeout interval shorter or longer than the default setting. It is required to input a whole number within the range from 60 to 7200.

5.4.4.d Request timeout

It takes time for each request to receive response from Appeon Server especially when the server is busy or the bandwidth is low. Requests will queue a while to get the server response. Set a proper request timeout value regarding to the application and network condition. Request will be aborted if when the time for waiting response exceeds the value that specified here.

- By default, the timeout period for receiving data is 3600 seconds.

- You can set a timeout interval shorter or longer than the default setting. It is required to input a whole number within the range from 60 to 7200.

5.4.5 Charset

The character set conversion can be enabled at the connection cache level for each application if you specify the input Charset and database Charset for the cache in AEM. Refer to Figure 5-27.

You will find the Charset tool useful when:

- The database uses non-UTF-8 character set, and

- The language display of the Web application has error code in it

Otherwise, it is unnecessary to use this tool.

Figure 5-27: Charset settings

5.4.5.a Configuring database Charset for a connection cache

Step 1 – Click an application in the Application Name column.

Step 2 – Click the Add Charset button.

Step 3 – Select the connection cache from the dropdown list in the "Connection cache" field.

Step 4 – Select the Database Charset type from the dropdown list in the "Database Charset" field. The Charset should be consistent with the Charset used in the database. This will not change the setting in the database.

Step 5 – Select the Input Charset type from the dropdown list in the "Client-side Charset" field. This setting should match the input Charset type at the client side.

Step 6 – Click the Add Charset button to confirm the configuration.

5.4.5.b Charset options given in the Charset fields

Table 5-2 lists all the Charset options provided in the "Database Charset" field and the "Client-side Charset" field, and provides a brief description of each Charset. If the actual database Charset or the input Charset is not provided as an option, you can use the following method to manually add the type as an option:

Step 1 – Open the file Charset.properties in the directory %EAServer%\deploy\webapps\appeonserver.aem\WEB-INF\classes.

Step 2 – Add the Charset type as an entry into the file, and save the file.

For example, if the Charset type that you want to add is "gbk", you can add a new line "gbk=gbk" in the file.

Step 3 – Refresh AEM and the "gbk" Charset will be added to the Charset lists.

Table 5-2: Charset options

Types	Description
ASCII	American Standard Code for Information Interchange
Cp1252	Windows Latin-1
ISO8859_1	ISO 8859-1, Latin alphabet No. 1
UnicodeBig	Sixteen-bit Unicode Transformation Format, big-endian byte order, with byte-order mark
UnicodeBigUnmarked	Sixteen-bit Unicode Transformation Format, big-endian byte order
UnicodeLittle	Sixteen-bit Unicode Transformation Format, little-endian byte order, with byte-order mark
UnicodeLittleUnmarked	Sixteen-bit Unicode Transformation Format, little-endian byte order
UTF8	Eight-bit Unicode Transformation Format
UTF-16LE	Sixteen-bit Unicode Transformation Format, byte order specified by a mandatory initial byte-order mark
Big5	Big5, Traditional Chinese
Big5_HKSCS	Big5 with Hong Kong extensions, Traditional Chinese
Cp037	USA, Canada (Bilingual, French), Netherlands, Portugal, Brazil, Australia
Cp273	IBM Austria, Germany
Cp277	IBM Denmark, Norway
Cp278	IBM Finland, Sweden
Cp280	IBM Italy
Cp284	IBM Catalan/Spain, Spanish Latin America
Cp285	IBM United Kingdom, Ireland
Cp297	IBM France
Cp420	IBM Arabic
Cp424	IBM Hebrew
Cp437	MS-DOS United States, Australia, New Zealand, South Africa
Cp500	EBCDIC 500V1
Cp737	PC Greek
Cp775	PC Baltic
Cp838	IBM Thailand extended SBCS
Cp850	MS-DOS Latin-1
Cp852	MS-DOS Latin-2
Cp855	IBM Cyrillic
Cp856	IBM Hebrew

Cp857	IBM Turkish
Cp858	Variant of Cp850 with Euro character
Cp860	MS-DOS Portuguese
Cp861	MS-DOS Icelandic
Cp862	PC Hebrew
Cp863	MS-DOS Canadian French
Cp864	PC Arabic
Cp865	MS-DOS Nordic
Cp866	MS-DOS Russian
Cp868	MS-DOS Pakistan
Cp869	IBM Modern Greek
Cp870	IBM Multilingual Latin-2
Cp871	IBM Iceland
Cp874	IBM Thai
Cp875	IBM Greek
Cp918	IBM Pakistan (Urdu)
Cp921	IBM Latvia, Lithuania (AIX, DOS)
Cp922	IBM Estonia (AIX, DOS)
Cp930	Japanese Katakana-Kanji mixed with 4370 UDC, superset of 5026
Cp933	Korean Mixed with 1880 UDC, superset of 5029
Cp935	Simplified Chinese Host mixed with 1880 UDC, superset of 5031
Cp937	Traditional Chinese Host mixed with 6204 UDC, superset of 5033
Cp939	Japanese Latin Kanji mixed with 4370 UDC, superset of 5035
Cp942	IBM OS/2 Japanese, superset of Cp932
Cp942C	Variant of Cp942
Cp943	IBM OS/2 Japanese, superset of Cp932 and Shift-JIS
Cp943C	Variant of Cp943
Cp948	OS/2 Chinese (Taiwan) superset of 938
Cp949	PC Korean
Cp949C	Variant of Cp949
Cp950	PC Chinese (Hong Kong, Taiwan)
Cp964	AIX Chinese (Taiwan)
Cp970	AIX Korean

Cp1006	IBM AIX Pakistan (Urdu)
Cp1025	IBM Multilingual Cyrillic: Bulgaria, Bosnia, Herzegovinia, Macedonia (FYR)
Cp1026	IBM Latin-5, Turkey
Cp1046	IBM Arabic – Windows
Cp1097	IBM Iran (Farsi)/Persian
Cp1098	IBM Iran (Farsi)/Persian (PC)
Cp1112	IBM Latvia, Lithuania
Cp1122	IBM Estonia
Cp1123	IBM Ukraine
Cp1124	IBM AIX Ukraine
Cp1140	Variant of Cp037 with Euro character
Cp1141	Variant of Cp273 with Euro character
Cp1142	Variant of Cp277 with Euro character
Cp1143	Variant of Cp278 with Euro character
Cp1144	Variant of Cp280 with Euro character
Cp1145	Variant of Cp284 with Euro character
Cp1146	Variant of Cp285 with Euro character
Cp1147	Variant of Cp297 with Euro character
Cp1148	Variant of Cp500 with Euro character
Cp1149	Variant of Cp871 with Euro character
Cp1250	Windows Eastern European
Cp1251	Windows Cyrillic
Cp1253	Windows Greek
Cp1254	Windows Turkish
Cp1255	Windows Hebrew
Cp1256	Windows Arabic
Cp1257	Windows Baltic
Cp1258	Windows Vietnamese
Cp1381	IBM OS/2, DOS People's Republic of China (PRC)
Cp1383	IBM AIX People's Republic of China (PRC)
Cp33722	IBM-eucJP – Japanese (superset of 5050)
EUC_CN	GB2312, EUC encoding, Simplified Chinese

EUC_JP	JIS X 0201, 0208, 0212, EUC encoding, Japanese
EUC_JP_LINUX	JIS X 0201, 0208, EUC encoding, Japanese
EUC_KR	KS C 5601, EUC encoding, Korean
EUC_TW	CNS11643 (Plane 1-3), EUC encoding, Traditional Chinese
GBK	GBK, Simplified Chinese
ISO2022CN	ISO 2022 CN, Chinese (conversion to Unicode only)
ISO2022CN_CNS	CNS 11643 in ISO 2022 CN form, Traditional Chinese (conversion from Unicode only)
ISO2022CN_GB	GB 2312 in ISO 2022 CN form, Simplified Chinese (conversion from Unicode only)
ISO2022JP	JIS X 0201, 0208 in ISO 2022 form, Japanese
ISO2022KR	ISO 2022 KR, Korean
ISO8859_2	ISO 8859-2, Latin alphabet No. 2
ISO8859_3	ISO 8859-3, Latin alphabet No. 3
ISO8859_4	ISO 8859-4, Latin alphabet No. 4
ISO8859_5	ISO 8859-5, Latin/Cyrillic alphabet
ISO8859_6	ISO 8859-6, Latin/Arabic alphabet
ISO8859_7	ISO 8859-7, Latin/Greek alphabet
ISO8859_8	ISO 8859-8, Latin/Hebrew alphabet
ISO8859_9	ISO 8859-9, Latin alphabet No. 5
ISO8859_13	ISO 8859-13, Latin alphabet No. 7
ISO8859_15_FDIS	ISO 8859-15, Latin alphabet No. 9
JIS0201	JIS X 0201, Japanese
JIS0208	JIS X 0208, Japanese
JIS0212	JIS X 0212, Japanese
JISAutoDetect	Detects and converts from Shift-JIS, EUC-JP, ISO 2022 JP (conversion to Unicode only)
Johab	Johab, Korean
KOI8_R	KOI8-R, Russian
MS874	Windows Thai
MS932	Windows Japanese
MS936	Windows Simplified Chinese
MS949	Windows Korean
MS950	Windows Traditional Chinese

MacArabic	Macintosh Arabic
MacCentralEurope	Macintosh Latin-2
MacCroatian	Macintosh Croatian
MacCyrillic	Macintosh Cyrillic
MacDingbat	Macintosh Dingbat
MacGreek	Macintosh Greek
MacHebrew	Macintosh Hebrew
MacIceland	Macintosh Iceland
MacRoman	Macintosh Roman
MacRomania	Macintosh Romania
MacSymbol	Macintosh Symbol
MacThai	Macintosh Thai
MacTurkish	Macintosh Turkish
MacUkraine	Macintosh Ukraine
SJIS	Shift-JIS, Japanese
TIS620	TIS620, Thai

5.4.6 Application Server Cache

Every time a Web application starts, Appeon Server loads the DataWindow syntax and embedded SQLs of the application to its memory. If Appeon Server is supporting multiple applications and loads all the syntax and SQLs of the applications into the memory, too much server memory is consumed. This result is a performance reduction of all applications.

AEM provides the Application Server Cache tool for you to leverage Appeon Server resources and make sure it has enough resources for supporting important applications.

Figure 5-28: Application Server Cache

5.4.6.a What is Application Server cache?

An Application Server cache is a portion of Appeon Server memory that is allocated for temporarily storing DataWindow syntax and embedded SQLs of an application.

Depending on the cache size specified for an application, Appeon Server loads part or all of the application DataWindow syntax and embedded SQLs when the application starts. If Appeon Server only loads part of the DataWindow syntax and embedded SQLs of an

application to the cache, the application runtime performance is affected because Appeon Server needs to read certain DataWindow syntax and embedded SQLs from the database instead of reading from the memory.

Make sure that the cache size is large enough for essential applications and those frequently accessed by users. If the Appeon Server memory is tight, you can consider decreasing the cache size for minor applications.

5.4.6.b Modifying the Appeon Server cache setting for an application

In the Cache Settings table of Figure 5-28, the Cache column shows the Appeon Server cache size allocated for the corresponding application, while the Cache Usage column shows how much cache the application currently occupies in the Appeon Server memory.

Take the following steps if you want to change the cache size for an application:

Step 1 – Click an application listed in the Cache Settings table of Figure 5-28. A new page opens and displays the current cache setting for the application, as shown in Figure 5-29.

Figure 5-29: Modify Cache Setting

AEM Console > Application Properties > Application Server Cache > [appeon_acf_demo_ax]
Click to return to the previous page.

Modify Cache Setting

Please specify the cache size for storing the DataWindow syntax and SQL statements of the application. The default size is 3 MB. Setting the size to "0" means that no cache is available for the application. Setting the size to less than "0" means that the cache size has no limit.

| Cache size: | 3 | MB |

Save

Step 2 – Modify the cache size. You can:

- Set the size to a figure bigger than "0". By default, the cache size is 3MB. This is suitable for a common application.

  For example, suppose there are two applications, appA (which is less important) and appB (which is important). You can set the memory limit for appA as 3MB, and set the memory limit for appB as 10MB. If the client runs appA, Appeon Server loads a maximum of 3MB syntax and SQL into its memory; if the client runs appB, Appeon Server loads a maximum of 10MB syntax and SQL into its memory. If the actual size of appA syntax and SQL is very large (more than 10MB), the running of appA will not affect the running of appB.

- Set the size to "0", which means that no cache is available for loading DataWindow syntax or Embedded SQLs. Appeon Server always reads the DataWindow syntax and embedded SQLs from the database.

- Set the size to less than "0" (-3, for example), which means that the cache has no limit. Appeon Server will load all the DataWindow syntax, DataWindow SQLs, and Embedded SQLs of the application into the cache.

Setting the size to "0" is not recommended because it will result in slow performance. If the server has enough memory and the number of the deployed applications is less than 10, it is recommended that you set the size for all applications to less than "0". If the server does not have enough memory, but it contains many deployed applications, it is recommended that you set all important applications, as well as applications using many DataWindows and

Embedded SQL, to less than "0" or much higher than 3M. Keep all other applications at the default setting.

Step 3 – Click the *Save Settings* button to save changes.

5.4.7 DataWindow Data Cache

You can apply the DataWindow Data Cache tool to cache DataWindow data that are frequently used on the Web server and/or the client.

- DataWindow Data Cache at the Web server stores the data in the memory. The cached data will be available unless the server memory is cleared (for example, by restarting the Web server).

- DataWindow Data Cache at the client stores and encrypts data in the Temporary Files folder of the Internet Explorer. The cached data will be available unless the Temporary Files folder is emptied.

Therefore, this tool can significantly reduce server load and network traffic, boosting performance and scalability.

Important:

1) DataWindow Data Cache is unsupported for Informix and Oracle 8i (though supported for Oracle 9i and 10g) databases.

2) Disable DataWindow Data Cache in AEM if the application is set to the Test Mode in the Run Mode page.

3) Do not cache DataWindows whose SQL statements contains non-table related expressions and the result of the expressions is dynamically generated. If these DataWindows are cached, the display result on the Web may be different from that in PowerBuilder.

4) DataWindows created dynamically cannot cache data on the Web server. Even though the Cache tool is enabled for such DataWindows, data will still be retrieved from the database.

5) DataWindow Data Cache at the Web server or at the client will not be effective until you fulfill all the configuration requirements described in the following sections:

- Configuration required for database servers

- Configuration required for Web servers (for Web server cache only)

- Configuration for DataWindow Data Cache in AEM

6) There is a restriction on the database table where a cache-enabled DataWindow retrieves data: the first twenty characters in the table name must be different from those in the other tables in the database. If the first twenty characters in two tables are the same, the Cache tool cannot correctly identify the table that the DataWindow uses.

7) The DataWindow Data Cache tool works with Web servers running on Windows (such as the Apache Web server running on Windows), and does not work with Web servers running on Unix\Linux (such as the Apache Web server running on Solaris).

5.4.7.a Configuration required for database servers

Appeon provides six SQL files respectively for the supported database servers (except Informix). You need to **execute** the SQL file of a database server for the server to support the DataWindow data-caching feature.

Note: DataWindow data-caching feature is unsupported for Informix.

Table 5-3 lists the SQL file that should be executed for each database server. The SQL files reside in the %appeon%\sql\cache\ folder, where %appeon% indicates the Appeon Server installation directory.

Table 5-3: SQL files need be executed for each database server

Database Type	SQL File
Oracle	To enable the feature for Oracle, install install_appeon_cache_ORACLE.sql. To disable the feature for Oracle, uninstall uninstall_appeon_cache_ORACLE.sql.
Microsoft SQL Server	To enable the feature for Microsoft SQL Server, install install_appeon_cache_MSSQL.sql. To disable the feature for Microsoft SQL Server, uninstall uninstall_appeon_cache_MSSQL.sql.
ASE	To enable the feature for ASE, install install_appeon_cache_ASE.sql. To disable the feature for ASE, uninstall uninstall_appeon_cache_ASE.sql.
ASA	To enable the feature for ASA, install install_appeon_cache_ASA.sql. To disable the feature for ASA, uninstall uninstall_appeon_cache_ASA.sql.
Sybase IQ	To enable the feature for Sybase IQ, install install_appeon_cache_IQ.sql. To disable the feature for Sybase IQ, uninstall uninstall_appeon_cache_IQ.sql.
DB2	To enable the feature for DB2, install install_appeon_cache_DB2.sql. To disable the feature for DB2, uninstall uninstall_appeon_cache_DB2.sql.

Important notes

1) The SQL file for Oracle database does not work with 8i databases, though it works with 9i and 10g databases.

2) Executing the SQL files provided by Appeon is the same as executing any other SQL files, but you need to be aware of the following notes:

- If a database server has multiple users, executing the SQL file under the login of one user will be effective for that user only. To make sure all users can use the DataWindow data-caching feature, you should use different logins to execute the SQL file.

- When you execute the SQL for a database server, the current login user of the server must have the right to execute stored procedures and create functions.

- There are two ways to execute SQLs in a database server - from the database server console or from the command line. Sometimes one way will fail while the other works. For example, executing the SQL for Microsoft SQL Server from the command line may result in "parameter –D" error, while executing the SQL from the server console is successful, if the server computer has both Microsoft SQL Server and Sybase ASE server installed.

5.4.7.b Configuration required for Web servers

The configuration of Web server is required for Web server cache only.

If the application server is also used as the Web server, you do not need to do any special configuration, and the DataWindow data-caching feature is automatically enabled for the Web server.

If you use a third-party Web server as the Web server, you need to configure Web server for the DataWindow data-caching feature. For detailed instructions, refer to the *Web Server Configuration Guide*.

5.4.7.c Configuration required for AEM

This section takes the sales_application_demo as an example to show configuration in AEM that will enable the DataWindow Data Cache at the Web server and/or the client.

Step 1 – Select Application Properties | DataWindow Data Cache on the left pane of the AEM Console. The DataWindow Data Cache page displays on the right pane of the Console, as shown in Figure 5-30.

Figure 5-30: DataWindow Data Cache

Step 2 – Click "sales_application_demo" listed in the "Application Name" column of the table. The sales_application_demo page displays as shown in Figure 5-31.

Figure 5-31: DataWindow Data Cache for sale_application_demo

Step 3 – In the Application Cache Setting box, select the "Server Side" option and/or "Client Side" option to enable the cache setting for the application DataWindows.

Step 4 – In the DataWindow Object Cache Setting box, check the DataWindow object(s) on which you want to have the data-caching feature.

You cannot select different DataWindow objects for server cache and client cache, for example, you cannot select DataWindow object A for server cache only while object B for client cache only, instead, you should select object A and/or B for both.

Notes: 1) If a DataWindow object has a Child DataWindow object, its Child DataWindow will also be listed in the table. Checking either of them will enable the data caching for them both. 2) It is recommended that you check the DataWindow objects that do not have frequent data updates, and leave unchecked the DataWindow objects that have frequent data updates.

Step 5 – Click the *Save* button to save changes.

5.4.8 DLL/OCX Files Download

If your application calls to any DLL or OCX files, make the following two configurations to make sure the deployed Web application can successfully call the DLL or OCX files:

- Configure the DLL or OCX files in the application profile, to deploy the files to Web server with the application. Refer to the *Additional Files* Section in the *Appeon Developer User Guide* on how to configure and deploy DLL or OCX files to Web server.

- Configure how the DLL or OCX files are downloaded to the Client using the AEM DLL/OCX Files Download tool.

Figure 5-32: DLL/OCX Files Download

5.4.8.a Viewing default DLL/OCX Files Download Install Settings

View the current install settings for all applications in the DLL/OCX Files Download page (as shown in Figure 5-32).

- Application Name – Lists the names of all deployed applications. The names are automatically added in the page when applications are deployed by Appeon Developer to Appeon Server.

- Install Mode – Shows the configured custom library install mode for each of the application. By default, the mode is set to "Install automatically without asking user".

5.4.8.b Modifying DLL/OCX Files Download Install Settings

By clicking an application name in the DLL/OCX Files Download page, you can enter the DLL/OCX Files Download install mode configuration page of the application and modify the configuration.

Figure 5-33: Modify DLL/OCX Files Download install settings

"Install Mode" defines how the DLL or OCX files of the selected application should be installed to a client browser. Whichever install mode is selected, when a DLL or OCX file is downloaded to a client, the folder for keeping the DLL or OCX file at the client is %WINDOWS%\system32\AppeonPlugin\appname, where *appname* stands for the name of the Web application. You can select the install mode that is most suitable for the application according to the description in Table 5-4.

Table 5-4: Install mode options

Install Mode	Description
Install automatically without asking user	Default. Before the Web application runs, the DLL and OCX files of the application are automatically downloaded and installed without giving any notification.
Confirm with user, then install automatically	Before the Web application runs, a message box will prompt the user to install the DLL and OCX files. If the user confirms this action, those files will be automatically installed.
Install manually (no automatic installation)	With this option, Appeon does not handle the DLL and OCX files installation for the application. Users must manually install the DLL and OCX files of the application before accessing the application.
	This option is recommended if the DLL and OCX files used by the application are large size and take a long time to be downloaded over the network.

"Conflict Resolution Mode" defines how to resolve file conflicts when a different file with the same file name already exists in the folder to which a DLL or OCX is downloaded. There are three mode options.

Table 5-5: Conflict resolution mode options

Conflict Resolution Mode	Description
Install anyway without asking user	Default. Directly replaces the file of the same name without notifying you.
Do not install; use existing file	Continues using the existing file.
Ask the user what to do	Displays a message box for the user to select whether to replace or keep the existing file.

After the install and conflict resolution modes are selected, click the *Save Settings* button to apply the settings to the selected application, or click the *Apply to all applications* button to apply the settings to all available applications.

5.4.9 Registry Mode

The Registry Mode tool determines whether Appeon deployed applications would read client machine Windows registry or Appeon emulation registry to execute registry functions.

Appeon emulation registry refers to the mock registry file stored in the Appeon Server database. It keeps the registry settings users specify when executing RegistrySet. Because it initially has no values, with the Appeon emulation registry method, users must first set values using RegistrySet before reading values with RegistryGet or RegistryValues.

Figure 5-34: Registry Mode

Figure 5-35: Registry Functions Execution Mode

You can click an application link in the Registry Mode page to set the registry mode for the application.

By default, all applications are set to "use client machine Windows registry". This option is recommended because it enables the Web application to directly interact with the client registry, same as in PowerBuilder. You can also change an application to "use Appeon registry emulation", so that the execution of registry functions can avoid the possible differences between client registries, and achieve the same results.

5.4.10 Multi-Thread Download

The Multi-thread Download setting specifies how many threads a client will take for simultaneously downloading application Web files from the Web server. This option makes full use of the network bandwidth between clients and Web server, and shortens the time that clients must wait during the Web files downloading process.

Figure 5-36: Multi-thread download

AEM Console > Application Properties > Multi-Thread Download

Multi-Thread Download Settings	
Download static resources with multi-threads to boost performance. The static resources refer to resources that exist on the Web server as files, such as the JS files, image files, and HTML files.	
Application Name	Maximum Threads
appeon_acf_demo	2
appeon_code_examples	2
sales_application_demo	2

Figure 5-37: Maximum Threads

AEM Console > Application Properties > Multi-Thread Download > [appeon_acf_demo_ax]

Click to return to the previous page.

Maximum Threads	
Specify the maximum number of download threads for the application. The valid number must be within the range from 1 to 6; the default value is 2.	
Maximum Threads:	2

Save

Before setting the thread number, you should take full consideration of the network condition where the application will be run, and the capability of the Web server that supports the application – whether the network and the Web server can support a large number of threads at the same time without jeopardizing the overall performance.

It is best to set the thread number in [1, 6].

5.4.11 INI File Settings

5.4.11.a INI file mode

The INI File Settings tool determines whether Appeon Web applications would download XML files that emulate INI files to the clients for profile functions, or directly use the XML files stored in Appeon Server database, and it also provides the function to allow you to modify the INI file contents of the application. As shown in Figure 5-38.

Figure 5-38: INI file settings

Click the application name in the "Application Name" column of the table to select the deployment mode for the Web application and view or modify the contents of the INI Files. As shown in Figure 5-39.

Figure 5-39: Manipulation mode and download mode

5.4.11.b INI file deployment

In the "server-side manipulations" mode, the Appeon Server database creates an XML file for each application client, and differentiates the XML files for different clients with the client cookie information.

In the "client-side manipulations" mode the XML file that stores the client profile information is kept in the %Windows%\system32\AppeonINI\ directory at the client side.

Select the appropriate mode by balancing the advantages and disadvantages of the two modes:

(1) The "server-side" mode requires that the Internet Explorer cookie is enabled at each client, while the "client-side" mode does not.

(2) The "server-side" mode does not work with Appeon Server cluster. The reason is that the servers in the cluster do not share database information (such as the INI/XML files). The "client-side" can work well with Appeon Server cluster.

(3) The "server-side" mode keeps the confidential profile information in Appeon Server database. It is securer than the "client-side" mode, which stores the profile information in the client computer.

There are two file-downloading methods in the "client-side" mode for downloading the XML files to the clients:

- Auto-download – Default. The XML file is automatically downloaded to the client that executes the relevant profile information.

- Validation – The client Internet Explorer would prompt for the user's validation before it downloads the XML file for executing relevant profile function.

Note: AEM does not allow the user to dynamically create an INI file on the local machine. Instead, AEM transfers the INI file from PowerBuilder into an XML file and allows the user to manipulate the XML file on the local machine. The INI file is transferred by Appeon Developer during the parsing process and deployed to Appeon Server. When the "client-side" mode is selected, the XML file will be downloaded to the local machine on the first time that the user manipulates the INI file.

5.4.11.c INI file contents

The INI file content tool allows you to view and edit the INI files after the deployment by clicking the name of INI file that you need to view or edit. You need to keep the INI content format here is consistent with that in the PowerBuilder. As shown in Figure 5-40.

Figure 5-40: Modify INI file
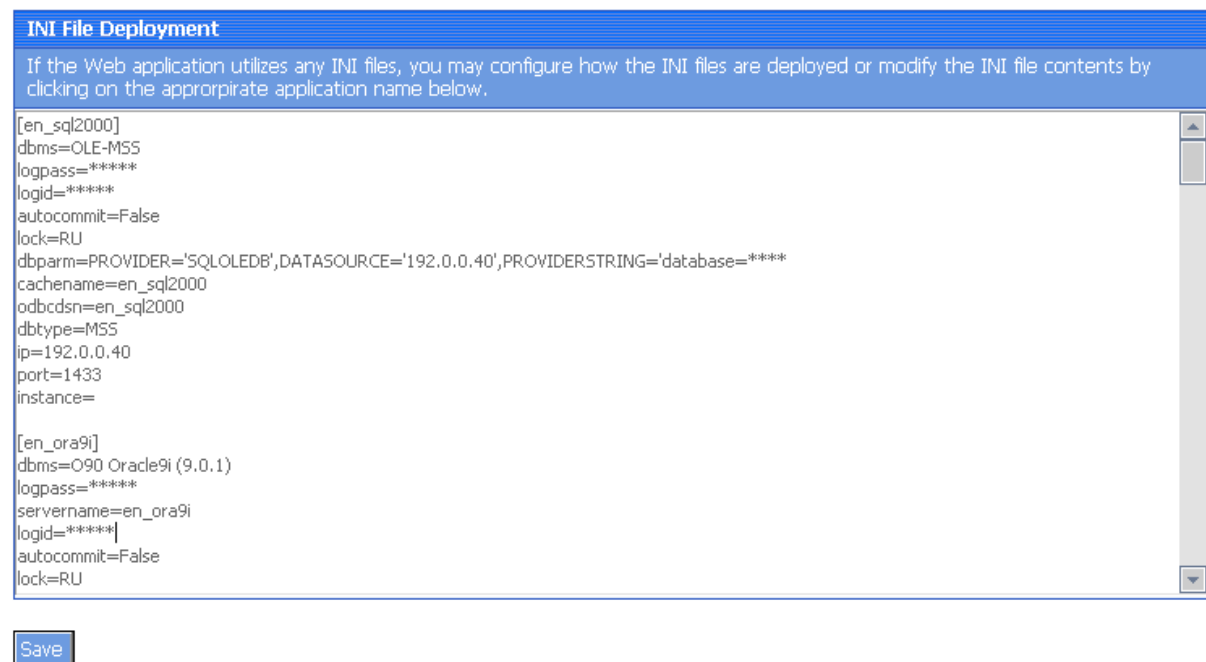
After making any change to the INI file, click the Save button, and then the content in the INI file will be automatically commit to Appeondb.

Notes:

1. If the Registry Mode of the ini-modified application is set to "use Appeon registry emulation", the information of Appeon registry emulation will be cleaned up after the INI modification

2. If the Deployment mode of the INI file is set to Client-side, the modified INI will be redownloaded to the client side, which means the client user may lose all the changes that they made in the previous INI file.

5.4.12 Error Message Mode

The Error Message Mode sets whether the errors occurred at runtime shall block the running of the application or not.

Figure 5-41: Error message mode

Figure 5-42: Error model configuration

"Display in the status bar" mode means that the error displays in the Internet Explorer status bar, and does not require the user to respond to it. The status bar only shows high-level error information.

"Display in a popup message" mode means that the error shows in a popup message box, and requires the user to respond to it first before continuing with the application. The popup message shows all the information available for locating the error, including error ID, error description, most possible cause, solution, and links to the Online Help and Appeon Technical Support.

Appeon Server divides all runtime errors into 4 levels according to their severity, and enables you to specify different display modes for different error levels.

Table 5-6: Error message mode

Error Level	Severity Description	Recommended Display Mode
0	Not severe. The error has little impact to the functions of the application.	Display in the status bar
1	Quite severe. The error is caused by incorrect configuration, and affects the running of the application. For example, no connection cache is set for the application.	Display in popup message
2	Very severe. The error is caused by incompatibility with Appeon product. For example, the specification of invalid Web	Display in popup message

	URL.	
10	Most severe. The error reflects a bug in the Appeon product.	Display in popup message

5.4.13 Run Mode

The Run Mode sets whether the parameters transferred between the Web application and the server can be read and analyzed by stress-testing tools such as LoadRunner.

Figure 5-43: Run mode configuration

Figure 5-44: Run mode

There are two Run Mode options:

- Normal mode – This is the default and recommended mode for running Appeon Web applications.

- Test mode – This is the mode specifically for applications under performance testing. It enables the script to be recorded and transferred in the plain-text format, so that the script can be modified or parameterized to simulate a more realistic stress scenario.

Note: 1) If the Test mode is selected, be sure to disable the data cache in the Application Properties | DataWindow Data Cache page before the application is run. 2) If the settings in the Test Mode have been changed, restart the Internet Explorer to begin a new session. The changes will not take effect if you only click the "Refresh" button of Internet Explorer.

5.4.14 Transfer Encoding

Transfer Encoding specifies the encoding format for data transferred between the clients and the server, as shown in Figure 5-45 and Figure 5-46:

Figure 5-45: Transfer encoding settings

AEM Console > Application Properties > Transfer Encoding

Transfer Encoding Settings
You are allowed to choose the encoding mode for transferring data in Appeon for PowerBuilder. The network traffic for the same data using different encoding modes varies. If the language of your project is English, it is strongly recommended that you choose the UTF-8 mode. If there are languages other than English in your project, choose the UTF-16LE mode.

Application Name	Transfer Encoding
appeon_acf_demo	UTF-16LE
appeon_code_examples	UTF-16LE
sales_application_demo	UTF-16LE

Figure 5-46: Transfer encoding

AEM Console > Application Properties > Transfer Encoding > [appeon_acf_demo_ax]

Click to return to the previous page.

Transfer Encoding
Transfer Encoding: ⦿ UTF-8   ○ UTF-16LE

Save

The transfer speed varies when the encoding format changes. If the language of the application is pure English, select UTF-8; otherwise, select UTF-16LE.

5.4.15 Decimal Precision

Select a proper decimal precision for the Web application.

AEM Console > Application Properties > Decimal Precision

Decimal Precision Settings
Select a proper decimal precision for the Web application. 15-digit Decimal supports numbers with up to 15 digits and offers high performance. It is available for all PowerBuilder developed applications. 28-digit Decimal supports numbers with up to 28 digits but offers lower performance than 15-digit Decimal. 28-digit Decimal is only available for applications developed with PowerBuilder 10.5 or above. It is not recommended to apply 28-digit decimal unless high precision number is necessary.

Application Name	Decimal Precision
appeon_acf_demo	15-digit Decimal
appeon_code_examples	15-digit Decimal
sales_application_demo	15-digit Decimal

- 15-digit Decimal supports numbers with up to 15 digits and offers high performance. It is available for all PowerBuilder developed applications.

- 28-digit Decimal supports numbers with up to 28 digits but offers lower performance than 15-digit Decimal. 28-digit Decimal is only available for applications developed with PowerBuilder 10.5 or above. It is not recommended to apply 28-digit decimal unless high precision number is necessary.

5.4.16 Client Settings

5.4.16.a Web Application Theme

The Web Application Theme specifies the theme of the Web application that will be used on the client side. Refer to Figure 5-47.

Figure 5-47: Web application theme

There are two options for Web Application Theme:

- Windows Vista/XP: Applying this theme enables Appeon Web applications to show in Windows XP/Vista style. The Windows XP/Vista style also requires the end user set the Windows desktop Theme to Windows XP or Windows Vista.

- Windows Classic: Applying this theme makes Appeon Web application presented in traditional Windows 2000 style.

5.4.16.b Start & Exit Settings

The Start & Exit Settings determines the modes when you start or exit the Web application. It includes the settings for Allow user to select run mode, Default run mode, and Close browser when exiting Web application. Refer to Figure 5-48.

Figure 5-48: Start & Exit settings

Allow user to select run mode

Before you start the Web application, you can set whether to allow the user to set the run mode of the Web application.

- Yes: When you run a Web application, a run mode page will be displayed to allow you to select the running mode of the Web application, there are two options: Run Now or Run After Download. Note: These two options are not related with that are

set in Default run mode, even you set the value of Default run mode, you can also change it and select the running mode according to your actual need in the run mode page.

- No: When you run a Web application, there will be no run mode page being displayed, the Web application is directly running now or running after download according to the value set in Default run mode.

Default run mode

This option provides feasible download modes to the end user if they use slow bandwidth. Depending on the bandwidth, the end user can select from the following run modes when the application starts

- Run now: The application runs immediately and files will be downloaded only when used. This mode is recommended for high speed network.

- Run after download: The application runs after all files are downloaded to the client. This is recommended for clients using low bandwidth

Close browser when exiting Web application

You can set whether to close the Internet Explorer browser in advance when you exit the Web application.

- Yes: When you exit the Web application, the Internet Explorer browser is automatically closed.

- No: When you exit the Web application, the Internet Explorer browser keeps open.

5.4.16.c Client Storage Location

Specify a location to store the Web application files on the client side in the Client Storage Location tool. Refer to Figure 5-49.

Figure 5-49: Client storage location

There are three options. Choose one of them to best fit your environment.

- Default User Profile Location: Unless you remove them manually, choosing this option will store Web application files permanently in the user profiles folder allocated by Windows system, for example %systemdrive%\Documents and Settings\Administrator\Application Data\appeon.
- Browser Cache Folder: The Web application files will be stored in IE cache. When IE cache is cleared, files will be downloaded again the next time the application runs.

- Customized Location: The Web application files will be stored in the location specified here. These files will remain cached even if the IE Browser folder is cleared. You must specify absolute path here (e.g. C:\Appeon\) or use one of the following dynamic paths:

  %system% which stands for Windows System directory
  %userLocation%, which stands for default Windows user profile folder, (e.g. C:\Documents and Settings\Administrator\Application Data).
  %systemDrive% which stands for system drive root, e.g.C:\.

  If this options is selected, the following drop down table shows to allow you specify the storage location for Web files in different types. Note that the System Files Storage Path cannot be empty or null, and the value specified here will be treat as the root path of the following items by default. You can change the path for each file type according to the demand. Refer to Figure 5-54.

Figure 5-50: Customized location

Path Type	Path
Customerized Location	
Specifies where to cache the Web application files.	
System Files Storage Path	%systemDrive%test_beta
Application Object Files Storage Path	%systemDrive%test_beta\AppObject\
OLE Files Storage Path	%systemDrive%test_beta\OLE\
Menu Object Files Storage Path	%systemDrive%test_beta\Menu\
Image File Storage Path	%systemDrive%test_beta\Image\
OCX/DLL Files Stoarege Path	%systemDrive%test_beta\PlugIn\
INI Files Storage Path	%systemDrive%test_beta\INI\
DataWindow Meta Files Storage Path	%systemDrive%test_beta\DataWindow\

Save

5.5 Security

5.5.1 Overview

AEM Security allows you to configure three types of security in the Appeon system:

- Security for accessing AEM. Configures the user name and password for AEM.

- Security for deploying applications to Appeon Servers. Configures the user group that has the right to deploy applications to Appeon Server. By default, all users have the right to deploy applications to Appeon Server.

- Security for accessing deployed applications. You can add an additional layer of security provided by AEM on top of any PowerBuilder security coded in the application. By default, all users have the right to access the Appeon Web applications.

Appeon provides the following six tools for AEM Security: AEM Login, System Settings, Application Security, Group Management, User Management, and Deployment Security. Refer to Figure 5-51.

Figure 5-51: Security
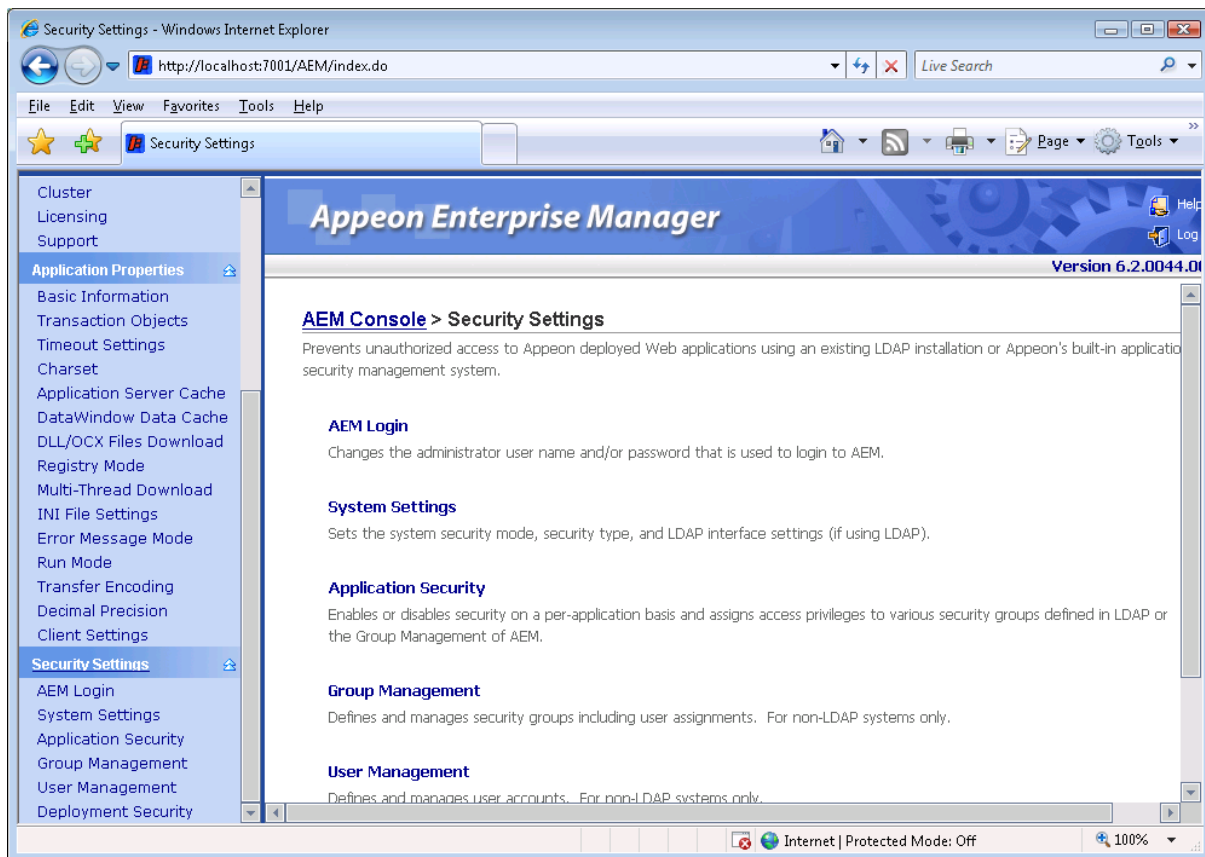
You should verify the System Settings are set as required before configuring Application Security, Group Management, User Management, or Deployment Security.

5.5.2 AEM login

The user can change the default or current username and password to log on to AEM.

Figure 5-52: AEM Login

1) Change AEM Password

The new password will overwrite the user's existing password, but the existing username will be used to login. In order to successfully change the password, the user must enter information in the following fields as shown in Figure 5-52:

- Old password – Correctly enter the current password (case sensitive).

- New password – Enter a new password to replace the old password (case sensitive).

- Confirm password – Retype the new password. The value entered in this field must match the 'New password' field (case sensitive).

2) Change AEM Username

The new username will overwrite the user's existing username, but the existing password will be used to login. In order to successfully change the username, the user must enter information in the following fields as shown in Figure 5-52:

- Old username – Correctly enter the current username (case sensitive).

- New username – Enter a new username to replace the old username (case sensitive).

- Confirm username – Retype the new username. The value entered in this field must match the New username field (case sensitive)

Note that if this is the first time you are using this AEM Login tool, the old username and password are those you specified when installing the Appeon Server. If you did not specify the username and password during the installation, the old user name and password are both "admin" by default. For security purposes, Appeon recommends that you change the username and password after the initial login.

5.5.3 System Settings

Figure 5-53: System Settings

As Figure 5-53 illustrates, the System Settings covers three important issues:

- Security Toggle – Turns application security on and off at the system level. All application security and settings are ignored when set to off, but the settings will not be lost.

- Security Type – Determines which system, Appeon built-in system or LDAP server, is applied to implement the security feature. Note that the Group Management and User Management tools only work with the Appeon built-in system.

- LDAP Interface Settings – If you are using LDAP server, the user must configure LDAP interface settings to connect the LDAP server with Appeon Server.

Table 5-7: LDAP security type and LDAP server type

LDAP types	Requirements
Netscape LDAP	Netscape LDAP 4.2 or above
Sun LDAP	Sun LDAP 5.1 (Sun LDAP is very similar to Netscape LDAP)
Microsoft LDAP	Win 2000 Active Directory
IBM LDAP	Directory Services (LDAP) 5.1

5.5.3.a Security Toggle and Security Type

Table 5-8 shows how the Security Toggle and Security Type settings determine which security tools are applied and what security features are performed.

Table 5-8: Security toggle, Security type and Security Settings

Security Toggle	Security Type	Settings in Security	Security Feature
Off	Not Available	Not Available	Disabled. Unauthorized users have access to load or deploy Web applications.
On	Appeon Security	User Management Group Management Application Security Deployment Security	The Appeon built-in security is enabled. Only authorized groups and users of a deployed Web application are allowed to load or deploy the Web application. Three consecutive invalid logins will result in an exceptional exit of the login dialog from the Web application. In this case, the user can click the *Refresh* button to obtain the login dialog again and re-log in with the correct username and password.
	LDAP Security	LDAP Interface Settings Application Security Deployment Security	Enabled. Any authorized LDAP groups and users of a Web application are allowed to load or deploy the Web application. Three consecutive invalid logins will result in an exceptional exit of the login dialog from the Web application. In this case, the user can click the *Refresh* button to obtain the login dialog again and re-log in with the correct username and password.

- Appeon security and LDAP security provides the user with options of using Appeon Server or LDAP to assign groups to the application. The security groups will be read from either LDAP (if it is LDAP security) or Appeon Server (if it is Appeon security).

- When the user attempts to change the security type, a message box will prompt the user to confirm the change.

5.5.3.b LDAP Interface Settings

If you are using the LDAP security, you must perform additional steps to access and manage the user/group information.

LDAP Interface Settings in AEM

To access the user and group information on your LDAP server, it is necessary to provide the LDAP interface settings in AEM. AEM interfaces with the LDAP server every time it opens the page that displays the users and groups information stored in the server.

All the fields in the LDAP Interface Settings group box are required:

- LDAP host – The IP address or domain name of the LDAP Server.

- LDAP port – Port of the LDAP Server.

- LDAP OU – The LDAP organization unit where the users and groups are created.

  If using Netscape LDAP or Sun LDAP, the LDAP OU should be "ou=*AAA*, o=*BBB*", where *AAA* stands for the organization unit in which all the groups are created, and *BBB* stands for the domain name (DN).

  If using Microsoft LDAP, the LDAP OU should be "DC=*AAA*, DC=*BBB*, (DC=*CCC*)", where *AAA* stands for the domain component (DC) that contains all the groups, and *BBB* stands for the domain component that contains the *AAA* component.

  If using IBM LDAP, the LDAP OU should be "o=*AAA*, c=*BBB*", where *AAA* stands for the organization suffix, and *BBB* stands for the country.

- LDAP type – Type of the LDAP server.

  There are four options (the LDAP servers that Appeon supports): Netscape LDAP, Microsoft LDAP, Sun LDAP, and IBM LDAP.

- Admin username – The administrator username.

  If using Microsoft LDAP, the username should be the username for the domain of the LDAP (The username has access rights to the specified LDAP domain component).

- Admin password – The administrator password.

- Use SSL -- If Yes is selected, the communication between Appeon Server and LDAP Server will use LDAPS protocol. You need to provide the Certificate Authenticated file of LDAPS. If No is selected, the communication between Appeon Server and LDAP server will use LDAP protocol.

- Certificate File -- The Certificate authenticated file of LDAPS.

After all the fields are filled, do the following:

- Click the *Test LDAP Settings* button to test whether the settings are correct or not. If the message indicates that the settings are incorrect, continue to verify the settings until the LDAP settings are correct.

- Click the *Save Settings* button.

User and group management at LDAP server side

Managing users and groups "at the LDAP server side" means that the administrator adds/removes/modifies users and groups in the LDAP server rather than in the user management and group management of AEM. The following are the steps to perform LDAP user and group management:

1. Set up the LDAP server in the system

   Refer to the documentation supplied by the LDAP server vendor for installation and setup instructions for your LDAP server.

2. Create an organization unit in the LDAP server.

   Only a single organization unit can be used to host all the groups and users for the Appeon Web application.

3. Create/manage users and groups in the organization unit in accordance with the LDAP server documentation.

5.5.4 Application Security

Figure 5-54: Application Security

5.5.4.a Viewing the current settings

1) View the current application security settings for all applications available in the Application Security page (as shown in Figure 5-54).

- Application Name – Lists the names of all the deployed applications. The names are automatically registered with AEM when an application is deployed by Appeon Developer to the Appeon Server.

- Configured Groups – The number of groups with access rights to the Web application.

  To view the names of the groups, click the link at the application name. To view details of the groups, go to the Group Management page.

- User Authentication – Shows the security mode for user authentication.

  "Security on" explicates that the user will be prompted to enter the username and password when accessing the selected application, while "Security off" requires no username and password for the application access. You can click the link of an application name listed in the Application Security Settings table and switch the security mode in the page that displays subsequently.

2) View the details of the current application security settings for a single application, by clicking an application. The detailed security settings for the selected application are displayed as shown in Figure 5-55.

Figure 5-55: Detailed security settings for an application

As Table 5-9 shows, different application security settings determine different security behaviors in a Web application.

Table 5-9: Application security settings and security behaviors in a Web application

User Authentication	A Given Group	Security behaviors in a Web application
Off	Assigned	All users can access to a Web application without being prompted for a username or password.
	Unassigned	
On	Assigned	Users of an assigned group have access rights to a Web application and they are prompted for usernames and passwords when loading a Web application.
	Unassigned	Users of an unassigned group do not have access rights to the Web application.

5.5.4.b Modifying the security settings of an application

The user can enter the security-setting page of the application by clicking an application name link in the Application Security page.

With the LDAP security type selected, the security-setting page automatically loads the latest user and group information from the specified LDAP server. If changes are made to users and groups at the LDAP server, you can use the *Refresh* button (on the Internet Explorer toolbar) to include the latest update to the page.

With the Appeon security type selected, the security-setting page loads user and group information from AEM Group Management and User Management.

In this page, you are able to:

1. Skip the login window when loading the application…

   Set the user authentication to **Security Off** in the Application Security group box. By default, the "Security Off" option is selected. This assumes that all users can access an application without user authentication.

2. Display a login window before loading the application …

   Set the user authentication to **Security On** by selecting the *Security On* radio button.

3. Display a custom login window before loading the application…

   Set the user authentication to **Security Off** in the Application Security group box; keep the System Security setting as On and set the Security Type setting to LDAP Security in the System Settings tool; write codes in the PowerBuilder program to call "appeonldaplogon" function to display a custom login window for LDAP security login. For details, please refer to "appeonldaplogon" function description in Appeon Workarounds Guide.

4. Assign a group to the application…

   Select a group from the Unassigned Groups list. Click the forward button (">>>") to shift the group to the Assigned Groups list.

   By default, all the groups are listed in the Unassigned Groups list. The groups are read from the Appeon Server (if the security type is Appeon security) or the LDAP server (if the security type is LDAP security) in use.

5. Unassign a group from the application…

   Select a group from the Assigned Groups list. Click the back button ("<<<") to shift the group to the Unassigned Groups list.

Click the *Save Changes* button to apply changes.

5.5.5 Group Management

If the security type is Appeon security, you can use the Group Management tool of AEM to set up various security groups and assign user accounts to the groups. This feature is not applicable to LDAP systems. For LDAP systems, use LDAP to add or remove security groups.

Figure 5-56: Group Management

5.5.5.a Viewing groups

The group information and associated user information can be viewed in the following two ways:

1) Click the *Show All* button to display all the groups.

2) Specify filter criteria to view groups:

Step 1 – Select "Group" or "Description" in the dropdown list as the type of the filter criteria.

Step 2 – Enter the contents that are expected to be included in the item specified in the dropdown list. Based on the criteria, groups that contain the specified information will be displayed.

Step 3 – Enable or disable the "Exact search".

Step 4 – Click the *Filter* button and the groups that meet the criteria will be displayed.
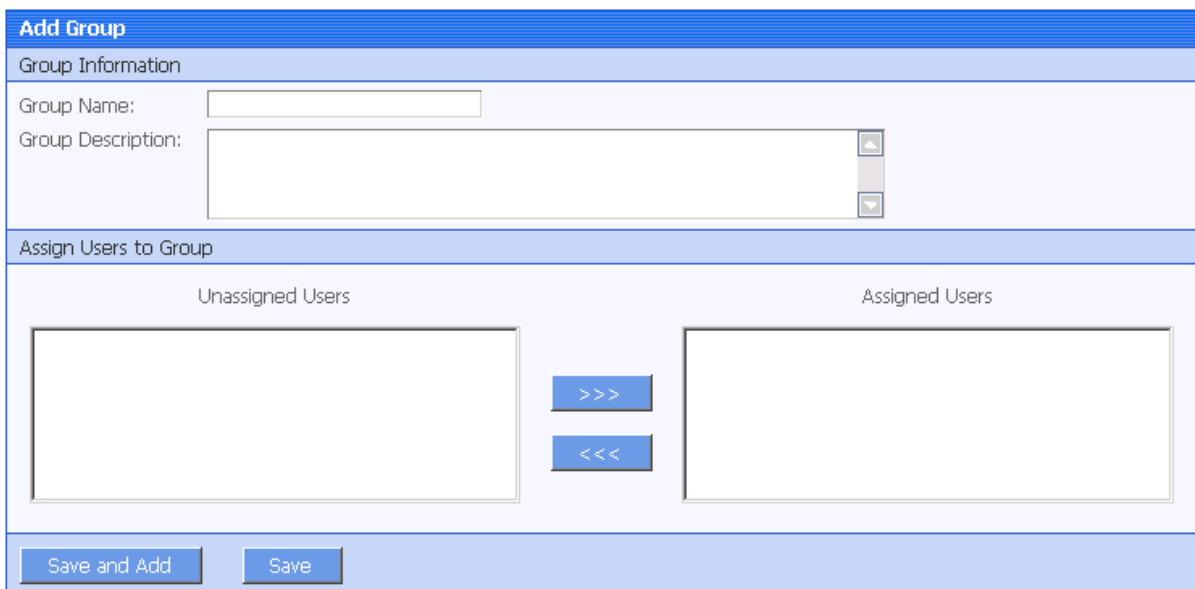
5.5.5.b Adding a new group

To add one or more groups, click the *Add Group* button in the Group Management page (as shown in Figure 5-56) and the Add Group page will be displayed as shown in Figure 5-57.

Figure 5-57: Add a group

- Group name – The group identifier. This field is required. Chinese characters are unsupported.

- Group description – Some explanation about the group. This field is optional.

- Assign or unassign users to the group.

  1. To assign a user to the group…

     Select a user from the Unassigned Users list. Click the forward button to shift the user to the Assigned Users list.

     By default, all the users are listed in the Unassigned Users list. The users are configured in AEM User Management.

  2. To unassign a user from the application.

> Select a user from the Assigned Users list by clicking it. Click the back button to shift the user to the Unassigned Users list.

5.5.5.c Editing an existing group

To edit a specific group, click the *Edit* button in the Group Management page (as shown in Figure 5-56) and enter the Edit Group page.

The Edit Group page is similar to the Add Group page except that the group name is not editable. You can modify the group description, or assign (unassign) users to the group in the same way as instructed in Section 5.5.5.b: *Adding a new group*.

5.5.5.d Deleting a group

Delete a group by clicking the *Delete* button in the Group Management page (as shown in Figure 5-56). A message box will prompt you to confirm the action.

Click the *OK* button to confirm the deletion or the *Cancel* button to cancel the deletion.

5.5.6 User Management

If the security type is Appeon security, you can use the User Management tool of AEM to set up user accounts. This feature is not applicable to LDAP systems. For LDAP systems, use LDAP to add or remove security groups.

Figure 5-58: User Management

In the User Management page, you can view which users are currently in the system and whether their accounts are enabled or disabled. By default, all existing users are displayed.

User names and associated user information can be viewed in the following two ways:

1) Click the *Show All* button to display all users.

2) Specify filter criteria to view users:

Step 1 – Select "User name", "Full Name", "Account Status", or "Description" in the dropdown list as the type of filter criteria.

Step 2 – Enter the contents that are expected to be included in the item specified in the dropdown list.

Step 3 – Enable or disable the "Exact search".

Step 4 – Click the *Filter* button. Users that meet the criteria will be displayed.
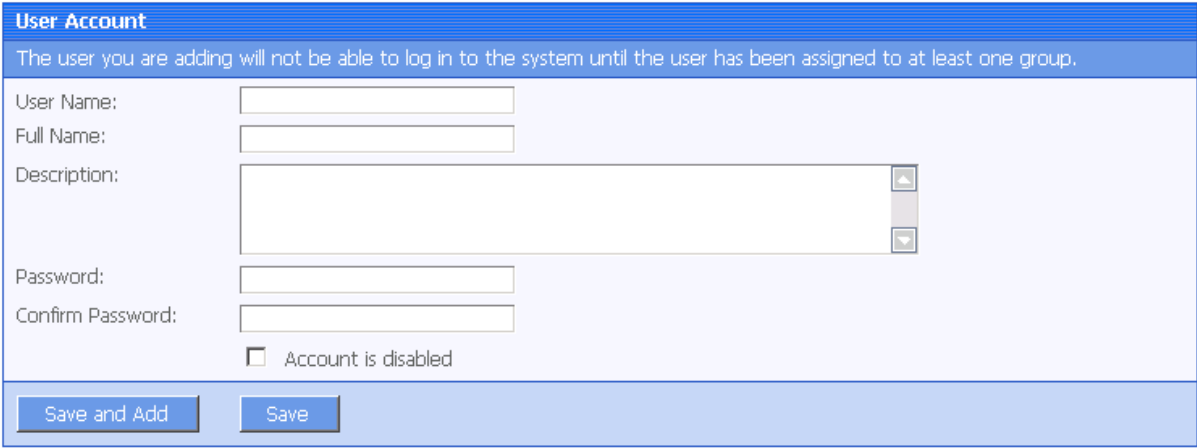
5.5.6.a Adding a new user

If you want to add one or more users, click the *Add User* button in the User Management page (refer to Figure 5-58) and the Add User page will be displayed as shown in Figure 5-59.

Figure 5-59: Add a user

- Username – The user identifier. This field is required. Chinese characters are unsupported

- Full name – The full name of the user. This field is optional. Chinese characters are unsupported.

- Description – Any appropriate user information. This field is optional.

- Password – The password of the new user. This field is required.

- Confirm password – The user must enter the new password again to confirm the password. This field is required.

- Account is disabled – If this checkbox is checked, the user account is disabled.

  When the account status is disabled, the user cannot load any application with the username and password if the application requires user authentication.

  When the account status is enabled, the user can load an application with the username and password if the account is assigned to a group that is in turn assigned to the application (with application access status enabled).

5.5.6.b Editing an existing user

By clicking the *Edit* button in the User Management page (refer to Figure 5-58), you can enter the Edit User page to edit an existing User.

The Edit User is similar to the Add User page except that the user name is not editable. You can modify the full name, the description, or change the password or account status in the same way as you were instructed in Section 5.5.6.a: *Adding a new user*.

After making any changes, click the *Save Changes* button. The changes are updated in Appeon Server.

5.5.6.c Deleting a user

Delete a user by clicking the *Delete* button in the User Management page in Figure 5-58. A message box will prompt you to confirm the action:

Click the *OK* button to confirm the deletion or the *Cancel* button to cancel the deletion.

5.5.7 Deployment Security

You can use the Deployment Security tool to manage Appeon Server deployment security, which controls what PowerBuilder developers are allowed to deploy applications to Appeon Server.

Corresponding to the Deployment Security in AEM, Appeon Developer requires PowerBuilder developers to specify deployment user name and password in the Appeon Server profile configuration. If the user name and password of the Appeon Server profile does not match the setting in Deployment Security, the Appeon Server profile will not take any application deployments.

Figure 5-60: Deployment Security

The Deployment Security tool enables you to do the following:

1) Disable deployment security for Appeon Server

Select the "Security Off" radio button in the "Application Deployment Security Settings" group box. When the deployment security is off, the user name and password in the Appeon Server profile will be ignored, and the Appeon Server profile will always work for application deployments.

2) Enable deployment security for Appeon Server

Step 1 – Select the "Security On" radio button.

Step 2 – Select a group from the Unassigned Groups list and click the forward button ("»»»") to shift the group to the Assigned Groups list. By doing this, that group obtains the permission to deploy applications to Appeon Server. If a user name and password that belongs to the group is specified in the Appeon Server profile configuration in Appeon Developer, the profile will work for application deployments. Otherwise, application deployments to the Appeon Server profile give an error message "Failed to call methods in Appeon Server; cannot find the user…"

By default, all groups are listed in the Unassigned Groups list. The groups are read from the Appeon Server (if the security type is Appeon security) or the LDAP server (if the security

type is LDAP security) in use. You can use back button ("<<<") to shift the group to the Unassigned Groups list.

Index

adding, 121
deleting, 122
editing, 122
username, 65
using Status Monitor, 14

V

viewing active sessions, 67
viewing active transactions, 67

viewing Application Security, 116
viewing group, 119

W

Web
session timeout, 88
transaction timeout, 88
working around database auditing, 61