PowerServer Configuration Guide for J2EE

Appeon® PowerServer® 2017 (on J2EE)

FOR WINDOWS & UNIX & LINUX

DOCUMENT ID: ADC20239-01-0700-01

LAST REVISED: October 27, 2017

Appeon Limited, 1/F, Shell Industrial Building, 12 Lee Chung Street, Chai Wan District, Hong Kong.

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 PowerServer 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 PowerServer.

Chapter 3: PowerServer Status Monitor

Describes how to configure and use PowerServer Status Monitor.

Chapter 4: Database Connection Setup

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

Chapter 5: AEM User Guide

Describes how to configure AEM.

1.3 Related documents

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

- Introduction to Appeon:

  Gives general introduction to Appeon PowerServer and its editions.

- Getting Started (for PowerServer Mobile):

  Guides you though installing PowerBuilder and Appeon PowerServer, and developing and deploying a mobile application.

- New Features Guide:

  Introduces new features and changes in Appeon PowerServer.

- PowerServer Mobile Tutorials:

  Gives instructions on deploying, running, and debugging the mobile application, distributing native mobile apps, and configuring the PowerServer cluster.

- PowerServer Mobile (Offline) Tutorials:

  Gives instructions on setting up the PowerServer Mobile (Offline) environment, and configuring, deploying, running, updating, and debugging the offline application.

- Appeon Installation Guide:

  Provides instructions on how to install Appeon PowerServer successfully.

- Mobile UI Design & Development Guide:

  Introduces general guidelines on designing and developing the mobile app and UI.

- Migration Guidelines for PowerServer Web:

  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 you through the entire process of deploying a small PowerBuilder application to the Web.

- Supported PB Features:

  Provides a detailed list of supported PowerBuilder features which can be converted to the Web/Mobile with Appeon as well as which features are unsupported.

- PowerServer Toolkit User Guide:

  Provides instructions on how to use the PowerServer Toolkit in Appeon PowerServer.

- Workarounds & API Guide:

  Provides resolutions for unsupported features and various APIs to facilitate you to implement the features (including Web and mobile) that are not easy or impossible to implement in the PowerBuilder IDE.

- Appeon Workspace User Guide:

  Gives a general introduction on Appeon Workspace and provides detailed instructions on how to use it.

- PowerServer Configuration Guide:

  Provides instructions on how to configure PowerServer Monitor, establish connections between PowerServer and database servers, and configure AEM for maintaining PowerServer and the deployed applications.

- Web Server Configuration Guide:

  Describes configuration instructions for different types of Web servers to work with the PowerServer.

- Troubleshooting Guide:

  Provides information on troubleshooting issues; covering topics, such as product installation, application deployment, AEM, and Appeon application runtime issues.

- Appeon Performance Tuning Guide:

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

- Testing Appeon Web Applications with UFT:

Provides instructions on how to test Appeon Web applications with UFT.

1.4 If you need help

If you have any questions about this product or need assistance during the installation process, access the Technical Support Web site at http://www.appeon.com/support.

2 Server Configuration Tasks

Server configuration for n-tier 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, PowerServer can be installed to WebLogic, WebSphere, JBoss, SAP NetWeaver Application Server, or JEUS. A number of configuration tasks must be performed before an Appeon application can work on the Web or Mobile, 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.

2.1 Scope of configurations discussed in this book

Appeon architecture is a typical n-tier 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 Installation Guide for .NET and the Web Server Configuration Guide, and therefore, will not be addressed in this guide.

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.

2.2 Configuration stages and tasks

Server configuration is divided into several stages as shown in the following table. 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: Server 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.

Configuration During...	For the Purpose of ...
Performance Management	Improving server performance.
Server Information Management	Managing server-related information.
Emergency Control	Restarting PowerServer automatically when it shuts down.

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

2.2.1 Configuration during application deployment

The following table 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 data sources.	Database Connection Setup
(In AEM) Transaction Object	Set up static mapping between application transaction objects and data sources.	Transaction Objects
(In AEM) Decimal Precision	Select a proper decimal precision for the Appeon application.	Decimal Precision
(In AEM) DLL/OCX Files	Configure the mode for installing and downloading DLL and OCX files used in an application.	DLL/OCX Files
(In AEM) Registry Mode	Enable the Appeon Web or Appeon mobile applications to directly access the client machine Windows registry or use Appeon registry emulation, so that PowerBuilder registry functions will work properly.	Registry Mode
(In AEM) INI File Mode	Make the Appeon Web or Appeon mobile applications manipulate the INI files at the client or by Appeon emulation, so that INI file function will work properly.	INI File Mode
(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.	Error Message Mode
(In AEM) Charset	Specify the input charset and database charset to ensure characters in applications display correctly.	Charset

2.2.2 Configuration during debugging

The following table lists the server configuration tasks for efficient debugging in case of abnormal behavior of the Appeon Web or Appeon mobile applications.

Table 2.3: Configuration tasks during debugging process

Task	Description	See section
(In AEM) Log Mode	Set the log file generation mode.	Log Mode
(In AEM) Logging	View the log files generated by PowerServer or the application server.	Viewing Logs
(In AEM) Run Mode	Set the run mode for Web or mobile applications.	Run Mode

2.2.3 Configuration during security management

The following table 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	Database security
(In AEM) AEM Login	Modify the AEM user name and password.	AEM Login
(In AEM) System Security	Set the system security mode and type.	System Security
(In AEM) Client Security	Limit the accessibility of an Appeon Web application or Appeon mobile application to the selected groups.	Client Security
(In AEM) Group Management	Create groups and grant access rights.	Group Management
(In AEM) User Management	Create user profiles and grant access rights.	User Management
(In AEM) Deployment Security	Limit the number of users permitted to deploy applications to PowerServer.	Deployment Security

2.2.4 Configuration during performance management

The following table 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.	Active Sessions
(In AEM) Active Transactions	Monitor all active transactions in the system. Some active transactions can be killed if necessary.	Active Transactions
(In AEM) Maintenance	Set the schedule for automatically clearing temporary files, or manually deleting temporary files, and the backing up configurations.	Maintenance
(In AEM) Deployment Sessions	Monitor all active deployment sessions in the system. Some active deployment sessions can be killed if necessary.	Deployment Sessions
(In AEM) Application Server Cache	Allocate server cache between deployed applications. Ensures that important applications are cached.	PowerServer Cache
(In AEM) DataWindow Data Cache	Cache DataWindow data on the server and/or client to improve data-reading performance.	DataWindow Data Cache
(In AEM) Multi-Thread Download	Download static resources with multi-threads to boost performance.	Multi-Thread Download
(In AEM) Encoding	Choose the proper encoding mode to reduce network traffic.	Encoding

2.2.5 Configuration during server information management

The following table 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) Timeout	Set session timeout, transaction timeout, download timeout, and request timeout.	Timeout
(In AEM) Licensing	View license information, and activate or de-activate an PowerServer.	Licensing
(In AEM) Support	view the valid product support period and renew the support.	Support

2.2.6 Configuration for emergency control

The following table lists the server configuration task with which PowerServer can be started automatically when it shuts down.

Table 2.7: Configuration for emergency control

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

3 PowerServer Status Monitor

3.1 Overview

Note

PowerServer Status Monitor does not work with JEUS.

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

3.2 Configuring Status Monitor

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

Table 3.1: Files for status monitor

PowerServer	Windows	Unix\Linux
WebLogic/WebSphere/JBoss/ NetWeaver Application Server	<Appeon Home>\bin \appeonmonitor.bat	<Appeon Home>/bin/ appeonmonitor.sh
	<Appeon Home>\lib \powerserver.jar	<Appeon Home>/lib/ powerserver.jar
	<Appeon Home>\bin \appeonserver.bat	<Appeon Home>/bin/ appeonserver.sh
	<Appeon Home>\config \monitor.props	<Appeon Home>/config/ monitor.props

Notes:

1. <Appeon Home> indicates the installation path of PowerServer.
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 3.2: Configure appeonmonitor.bat

Settings	Description
JBOSS_HOME	Specifies the path of JBoss. For example, JBOSS_HOME=C:\Program Files\jboss-eap-6.1.
JAVA_HOME	Specifies the JDK location, which must be the same one used by PowerServer. For example, JAVA_HOME=C:\Program Files\Java \jdk1.6.0_18. Note: 1) If PowerServer 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 PowerServer works on WebSphere, only when the IBM JDK is used can Status Monitor function properly.
APPEON_HOME	Specifies the PowerServer home directory. WebSphere: <WAS_HOME>\appeon WebLogic: <WL_HOME>\appeon JBoss: <JB_HOME>\appeon Note: <WAS_HOME> indicates the home directory of WebSphere server; <WL_HOME> indicates the home directory of WebLogic; and <JB_HOME> indicates the home directory of JBoss. For example, If PowerServer works on WebLogic 9.2, the PowerServer home directory is: APPEON_HOME= C:\bea\weblogic92\appeon. For example, if Appeon Server works on JBoss, the PowerServer home directory is: APPEON_HOME= C:\Program Files\jboss-eap-6.1\appeon.
J2EE_JAR	Changes the default setting according to the PowerServer in use: WebLogic: <WL_HOME>\server\lib\weblogic.jar WebSphere: <WAS_HOME>\lib\j2ee.jar JBoss EAP: <JB_HOME>\modules\system\layers\base\javax\mail\api \main\mail-1.4.5-redhat-1.jar, <JB_HOME>\modules\system\layers\base \javax\ejb\api\main\jboss-ejb-api_3.1_spec-1.0.2.Final-redhat-2.jar JBoss 7: <JB_HOME>\modules\system\layers\base\javax\mail\api\main \mail-1.4.4.jar, <JB_HOME>\modules\javax\ejb\api\main\jboss-ejb-api_3.1_spec-1.0.1.Final.jar Note: In different JBoss builds, the name of jboss-ejb-api_3.1_spec-1.0.1.Final.jar may be slightly different. For example, if Appeon Server works on JBoss EAP 6.1, the J2EE_JAR directory is: J2EE_JAR=C:\Program Files\jboss-eap-6.1\modules\system\layers\base \javax\ejb\api\main\jboss-ejb-api_3.1_spec-1.0.1.Final.jar; C:\Program Files\jboss-eap-6.1\modules\system\layers\base\javax\mail\api\main \mail-1.4.5-redhat-1.jar.
CLASS_PATH	Default setting:

Settings	Description
	CLASS_PATH=%APPEON_HOME%\lib\appeonserver.jar;%J2EE_JAR% You do not need to make any changes to the default setting.
NeedToEncryptedEASPWD	Specify the administrator password of the application server. For example, NeedToEncryptedEASPWD=appeon123. After you set the password, comment out the following script in appeonmonitor.bat, then run appeonmonitor.bat to encrypt the password, and after you get the encrypted password, make sure to clean the password here and then input the encrypted password to EASPWD below. "%JAVA_HOME%/bin/java.exe" -cp "%CLASS_PATH%" -Dappeon.home="%APPEON_HOME%" com.appeon.server.monitor.StatusMonitor -e "%NeedToEncryptedEASPWD%"
EASUSER	Specify the administrator user name of the application server. For example, EASUSER=admin@system. Note that the user name must be in this format "admin@system".
EASPWD	Input the encrypted password of the application server. The encrypted password is generated after you set NeedToEncryptedEASPWD. Please see "NeedToEncryptedEASPWD" for details. For example, EASPWD=YXBwZW9uMTIz. After you input the encrypted password here, make sure to clean the password in NeedToEncryptedEASPWD.

After you properly configure the above settings, make sure to uncomment the following scripts, so Status Monitor can start normally.

```
"%JAVA_HOME%/bin/java.exe" -cp "%CLASS_PATH%" -Dappeon.home="%APPEON_HOME%"
com.appeon.server.monitor.StatusMonitor -e "%NeedToEncryptedEASPWD%"
"%JAVA_HOME%/bin/java.exe" -cp "%CLASS_PATH%" -Dappeon.home="%APPEON_HOME%"
-Deas.user="%EASUSER%" -Deas.pwd="%EASPWD%" com.appeon.server.monitor.StatusMonitor
```

Here is a sample of a configured appeonmonitor.bat file:

```
@echo off

cls
SETLOCAL

title Appeon Server Status Monitor

REM Please replace <JBOSS_HOME> with the real path of JBOSS

set JBOSS_HOME=C:\Program Files\jboss-eap-6.1

set JAVA_HOME=C:\Program Files\Java\jdk1.6.0_18

set APPEON_HOME=C:\Program Files\jboss-eap-6.1\appeon
```

```
set J2EE_JAR=C:\Program Files\jboss-eap-6.1\modules\system\layers\base\javax
\ejb\api\main\jboss-ejb-api_3.1_spec-1.0.1.Final.jar; C:\Program Files\jboss-
eap-6.1\modules\system\layers\base\javax\mail\api\main\mail-1.4.5-redhat-1.jar

set CLASS_PATH=%JBOSS_HOME%/lib/ext/appeonserver.jar;%J2EE_JAR%

REM Please replace <NeedToEncryptedEASPWD> with the administrator password of
JBoss 6.x. Make sure to clean the password after you have encrypted it.
set NeedToEncryptedEASPWD=

REM Please replace <EASUSER> with the administrator user name of JBoss 6.x
set EASUSER=admin@system

REM Please replace <EASPWD> with the administrator password of JBoss 6.x that
is encrypted
set EASPWD=YXBwZW9uMTIz

REM If you want to encrypt the administrator password of JBoss 6.x, please
uncomment the line below
"%JAVA_HOME%/bin/java.exe" -cp "%CLASS_PATH%" -Dappeon.home="%APPEON_HOME%"
com.appeon.server.monitor.StatusMonitor -e "%NeedToEncryptedEASPWD%"

REM If you want to start status monitor,  please uncomment the line below
"%JAVA_HOME%/bin/java.exe" -cp "%CLASS_PATH%" -Dappeon.home="%APPEON_HOME%"
-Deas.user="%EASUSER%"  -Deas.pwd="%EASPWD%"
 com.appeon.server.monitor.StatusMonitor

echo Appeon Server Status Monitor terminated.

PAUSE
ENDLOCAL
```

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 PowerServer has shut down.

3.2.2.1 Configuring appeonserver.bat (Windows)

The appeonserver.bat file contains the following code:

```
@echo off

REM if use WebLogic, please replace <Domain> with real path and uncomment the line
 below.
REM @start call "<Domain>\startWebLogic.cmd"

REM if use WebSphere, please replace <WebSphere> with real path and uncomment the
 line below.
REM @start call "<WebSphere>\AppServer\bin\startServer.bat" server1

REM if use JBoss, please replace <JBoss> with real path uncomment and the line
 below.
REM @start call "<JBoss>\bin\run.bat"
```

Make the following changes to the file:

1. Remove the notation "REM" before the command line that starts the application server/ PowerServer.
2. Replace the wildcard character string, which stands for the application server, with the home directory of the application server.

For example, if PowerServer works on JBoss WildFly 10, the following script should be modified.

Original script:

```
REM @start call "<JBoss>\bin\run.bat"
```

Modified script:

```
start cmd /c "D:\wildfly-10.0.0.Final\bin\standalone.bat"
```

3.2.2.2 Configuring appeonserver.sh (Unix\Linux)

The appeonserver.sh file contains the following script:

```
#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

#If use JBoss, please uncomment the line below.
#"<Jboss>/bin/run.sh"
```

Make the following changes to the file:

1. Remove the notation "#" before the command line that starts the application server/ PowerServer.

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

For example, if PowerServer is installed to JBoss WildFly 10, the following script should be modified.

Original script:

```
#"<Jboss>/bin/run.sh"
```

Modified script:

```
"/export/home/wildfly-10.0.0.Final/bin/standalone.sh"
```

3.2.3 Configuring monitor.props

The *monitor.props* file contains the property settings of Status Monitor. These property settings work for WebLogic, WebSphere, JBoss, and NetWeaver Application Server, except for

- Scheduled task settings, which are unsupported by WebLogic, WebSphere, JBoss, or NetWeaver Application Server.

Make the following changes to the property settings in *monitor.props*, as shown in the following table.

Note: If you have made changes to the instance names and instance ports, you will need to restart PowerServer to make the settings effective.

Table 3.3: Configure monitor.props

Settings	Descriptions
com.appeon.server.monitor.instance.names	The names of server instances that need to be monitored. Separate multiple instance names with comma (","). Note that changes to this setting will not take effect until PowerServer is restarted.
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 PowerServer. 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 PowerServer is restarted.
com.appeon.server.monitor.instance.files	The files that Status Monitor will check when the server shuts down, for example, D:\wildfly-10.0.0.Final\appeon\repository \standalone\config\aem-config.xml. 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 PowerServer. Default setting: com.appeon.server.monitor.instance.commandlines=appeonserver.bat

Settings	Descriptions
	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 **(Obsolete)**	The cycle for checking memory information. The memory usage detected by Status Monitor may not be necessarily the same as the memory usage shown in the Windows task manager.

Settings	Descriptions
	The unit is second. **Note** This setting is obsolete, because it is effective only for EAServer which Appeon no longer supports.
com.appeon.server.monitor.memory.maxvalue **(Obsolete)**	The maximum value (in percentage) 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. **Note** This setting is obsolete, because it is effective only for EAServer which Appeon no longer supports.
com.appeon.server.monitor.memory.minvalue **(Obsolete)**	The minimum value (in percentage) 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. **Note** This setting is obsolete, because it is effective only for EAServer which Appeon no longer supports.

Settings	Descriptions
com.appeons.erver.monitor.memory.restart **(Obsolete)**	The switch to restart server instance by force when the memory usage reaches the peak. The value can be true or false. **Note** This setting is obsolete, because it is effective only for EAServer which Appeon no longer supports.
com.appeon.server.monitor.scheduled.task.cycle **(Obsolete)**	The cycle for scheduled tasks. The value can be daily, weekly or monthly, among which only the daily mode is supported at present. **Note** This setting is obsolete, because it is effective only for EAServer which Appeon no longer supports.
com.appeon.server.monitor.scheduled.task.when **(Obsolete)**	The moment to start carrying out scheduled tasks. The value ranges from 00:00:00 to 23:59:59. **Note** This setting is obsolete, because it is effective only for EAServer which Appeon no longer supports.
com.appeon.server.monitor.scheduled.task.restart **(Obsolete)**	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. **Note** This setting is obsolete, because it is effective only for EAServer which Appeon no longer supports.

3.2.4 Additional configuration for Status Monitor in PowerServer cluster

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

The "active" sessions for a PowerServer will always be restored if that PowerServer 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 a PowerServer.

3.3 Information backed up by Status Monitor

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

3.3.1 What is backed up?

Status Monitor periodically backs up PowerServer session information that includes:

- User authentication information
- References to PowerServer transaction components

Status Monitor does not back up:

- Information being processed in active transactions

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: D:\wildfly-10.0.0.Final \appeon\bin.

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

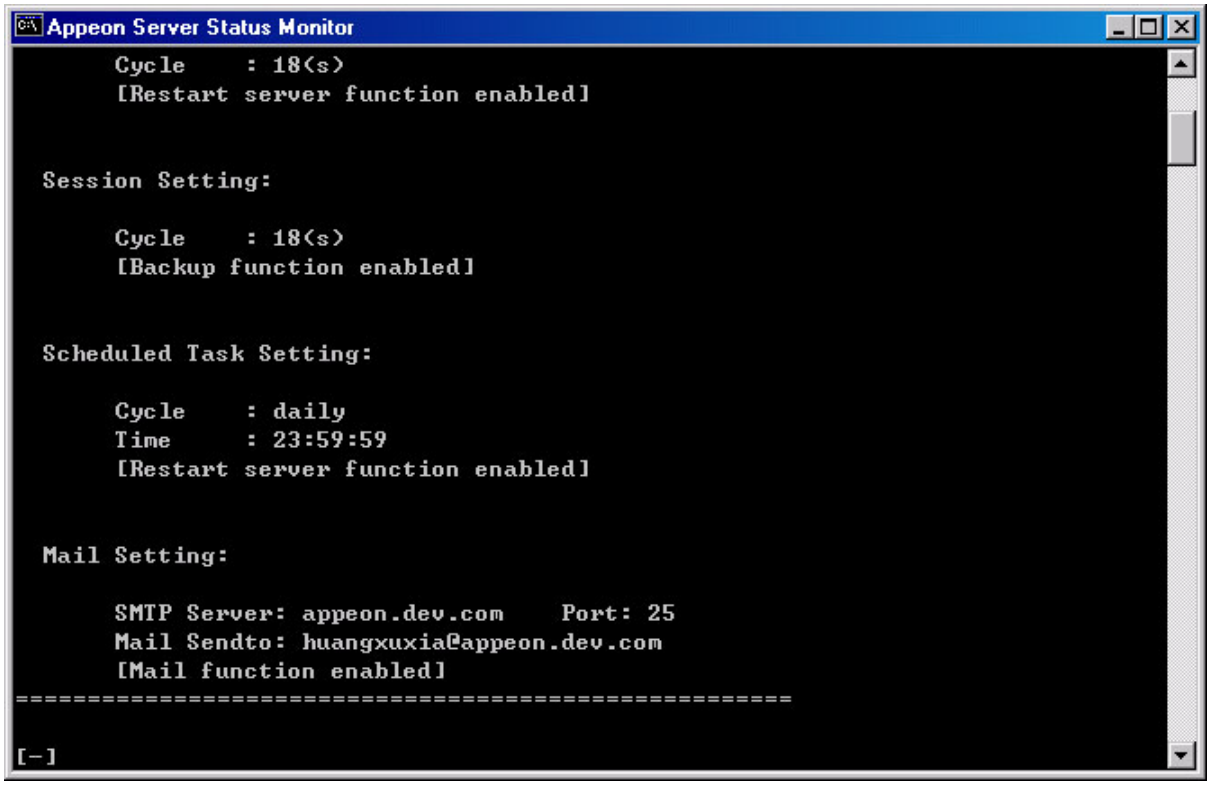
Note: In Unix\Linux, be sure to run Status Monitor in the background by executing the command "nohup statusmonitor.sh &". If Status Monitor runs in the foreground, executing a ctrl-c command for Status Monitor will stop both the Status Monitor and the PowerServer process started by Status Monitor.

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 PowerServer are simultaneously running, the Status Monitor window as well as the configuration information will display as illustrated in the following figure.

Figure 3.1: Information in Status Monitor Window



PowerServer 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 PowerServer data sources.

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 PowerServer. This refers to setting up PowerServer data sources.
- Setting up communication between the deployed application and PowerServer. This refers to setting up the mapping between the application transaction objects and PowerServer 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 PowerServer data source?

PowerServer data source is actually the same terminology as data source in the following mainstream application servers: WebLogic, WebSphere, JBoss, NetWeaver, and JEUS.

PowerServer data source (for WebLogic, WebSphere, JBoss, NetWeaver Application Server, and JEUS) can only be configured in their corresponding application server management console.

For detailed instructions, please refer to the corresponding documents of WebLogic, WebSphere, JBoss, NetWeaver Application Server, or JEUS.

4.2.1 Why PowerServer data source?

The data source for a Web or mobile 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 data sources.

The Appeon Web application and the Appeon mobile application relies on PowerServer data sources to interact with the database servers. When creating a data source, 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 the Appeon Web application and the Appeon mobile application, data-related operations are managed by PowerServer. 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 and the mobile 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 data source, 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 data sources 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, so it is recommended that you evaluate Type 3 or Type 4 for both intranet and Internet 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

4.2.4.1 Checklist for JDBC driver preparation

Before you configure a JDBC data source for your application database, the following JDBC driver file(s) must be copied to the PowerServer computer. Following is the checklist of the JDBC driver file(s) that should be copied to the directory.

Table 4.1: Checklist of JDBC driver files

Database	Driver Type	Driver Files	Availability of the Driver Files
SAP SQL Anywhere 8.0.2, 9.0, 10.0.1, 11.0, 12.0. 16.0, or 17.0	jConnect JDBC driver (Recommended)	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.
	iAnywhere JDBC-ODBC driver	For PowerServer on Windows: dbjodbc8.dll, dbjodbc9.dll, or dbjodbc10.dll jodbc.jar	Available in SAP SQL Anywhere 8.0.2 Build 4361 or above. For earlier versions, you can obtain the files from http://www.sybase.com/downloads.

Database	Driver Type	Driver Files	Availability of the Driver Files
		For PowerServer on Unix\Linux: dbjodbc8.so jodbc.jar	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.
ASE 12.5.x or 15.x	jConnect JDBC driver	jconn2.jar for jConnect 5.5 jconn3.jar for jConnect 6.0 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.
SAP IQ 12.7.x or 15.x	jConnect JDBC driver	jconn2.jar for jConnect 5.5 jconn3.jar for jConnect 6.0	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.
SAP HANA 1.00.36	SAP In-Memory Database JDBC driver	Ngdbc.jar	Available at %SAP HANA%\hdbclient\ngdbc.jar.
Oracle 8i	Oracle JDBC driver	classes12.zip Oracle8i 8.1.7.1 Patch nls_charset12.zip	Available at the Oracle Web site (http://www.oracle.com/technetwork/database/features/jdbc/index-091264.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://www.oracle.com/technetwork/database/features/jdbc/index-091264.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:	Available at the Oracle Web site (http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html).

Database	Driver Type	Driver Files	Availability of the Driver Files
		Ojdbc15.jar	Note: Ojdbc14.jar and ojdbc15.jar cannot be placed in the same location and used at the same time.
Microsoft SQL Server 2000	jTDS JDBC driver (Recommended)	jtds-1.2.jar	Available at SourceForge Web site (http://sourceforge.net/projects/jtds/). 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/downloads/en/details.aspx?FamilyID=99b21b65-e98f-4a61-b811-19912601fdc9&displaylang=en). 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
Microsoft SQL Server 2005, 2008, or 2012	jTDS JDBC driver (Recommended)	jtds-1.2.jar	Available at SourceForge Web site (http://sourceforge.net/projects/jtds/). 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/downloads/en/details.aspx?FamilyID=99b21b65-e98f-4a61-b811-19912601fdc9&displaylang=en).

Database	Driver Type	Driver Files	Availability of the Driver Files
Microsoft SQL Server 2014, or 2016	jTDS JDBC driver (Recommended)	jtds-1.2.2.jar	Available at SourceForge Web site (http://sourceforge.net/projects/jtds/).
	Microsoft SQL Server JDBC driver	sqljdbc4.jar	Available at the Microsoft Web site (http://www.microsoft.com/downloads/en/details.aspx?FamilyID=99b21b65-e98f-4a61-b811-19912601fdc9&displaylang=en).
IBM DB2 UDB 8.1, 8.2, 9.5 or 10.x	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, 10.x or 11.x	IBM Informix JDBC driver	ifxjdbc.jar and/or ifxjdbcx.jar	Available at the IBM Web site (http://www14.software.ibm.com/webapp/download/search.jsp?go=y&rs=ifxjdbc).
MySQL 5.5.x	MySQL Connector/J	mysql-connector-java-5.1.19-bin.jar	Available at %MySQL%\MySQL Connector J\mysql-connector-java-5.x.jar Or download from http://www.mysql.com/products/connector/.
Teradata 13.0	Teradata JDBC driver	terajdbc4.jar tdgssconfig.jar	Available at the Teradata Web site (http://downloads.teradata.com/download/connectivity/jdbc-driver).
PostgreSQL 9.2	PostgreSQL JDBC driver	For use with JDK 1.7 or 1.8: postgresql-9.3-1101.jdbc41.jar For use with JDK 1.6: postgresql-9.3-1101.jdbc4.jar For use with JDK 1.4 or 1.5: postgresql-9.3-1101.jdbc3.jar	Available at the PostgreSQL Web site (https://jdbc.postgresql.org/download.html).

4.2.4.2 Copying drivers to PowerServer

Copy the JDBC driver files to the proper directory in PowerServer. The directory varies with the type of application server that PowerServer is installed to, as shown in the table below.

Note: Configuring JDBC driver files in NetWeaver Application Server is different from those listed. For details on deploying JDBC driver files in NetWeaver Application Server, refer to Setting up data source for NetWeaver.

Table 4.2: Copy drivers to PowerServer

Server Type	Directory for Storing JDBC Files
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
JBoss	For Windows: %JBOSS_HOME%\server\instance\lib (%JBOSS_HOME % indicates the WildFly or JBoss EAP installation path) For Unix\Linux: $JBOSS_HOME/server/instance/lib
JEUS	For Windows: %JEUS_HOME%\lib\datasource (%JEUS_HOME% indicates the JEUS installation path) For Unix\Linux: $JEUS_HOME/lib/datasource

Important Note: Remember to restart PowerServer after copying files.

4.3 Setting up PowerServer data sources

The data source for the Web application and the mobile 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 data sources.

The Appeon Web application or the Appeon mobile application relies on PowerServer JDBC data sources to interact with the database servers. When creating a JDBC data source, you can use different JDBC drivers. However, Appeon has some recommendations on which JDBC driver is to be used for certain types of databases.

This section gives detailed instructions on configuring data sources in WebLogic, WebSphere, JBoss, NetWeaver Application Server, and JEUS. If you have problems creating JDBC data sources, refer to the documentations from the database/JDBC driver vendor or SAP NetWeaver, Oracle WebLogic, IBM WebSphere, JBoss and TmaxSoft JEUS.

4.3.1 Setting up data source for WebLogic

4.3.1.1 Setting up data source for WebLogic 8.1

The following section will take one database type (SQL Anywhere 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 Data source parameters.

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 data source name by PowerServer and AEM.

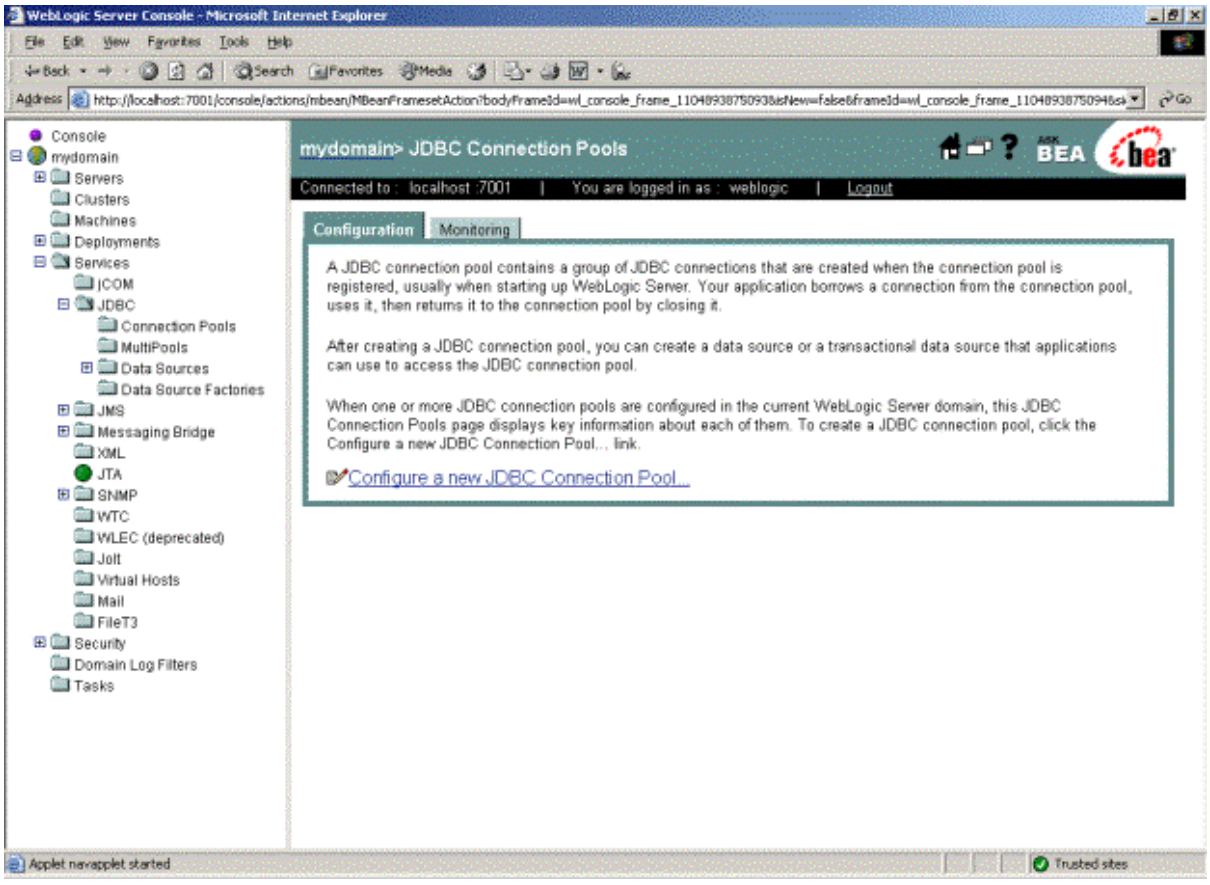
4.3.1.1.1 Creating a JDBC connection pool

1. Start the WebLogic Server for your domain.

2. Log on to the WebLogic Server Console.

3. Go to **Services** > **JDBC** > **Connection Pools**.

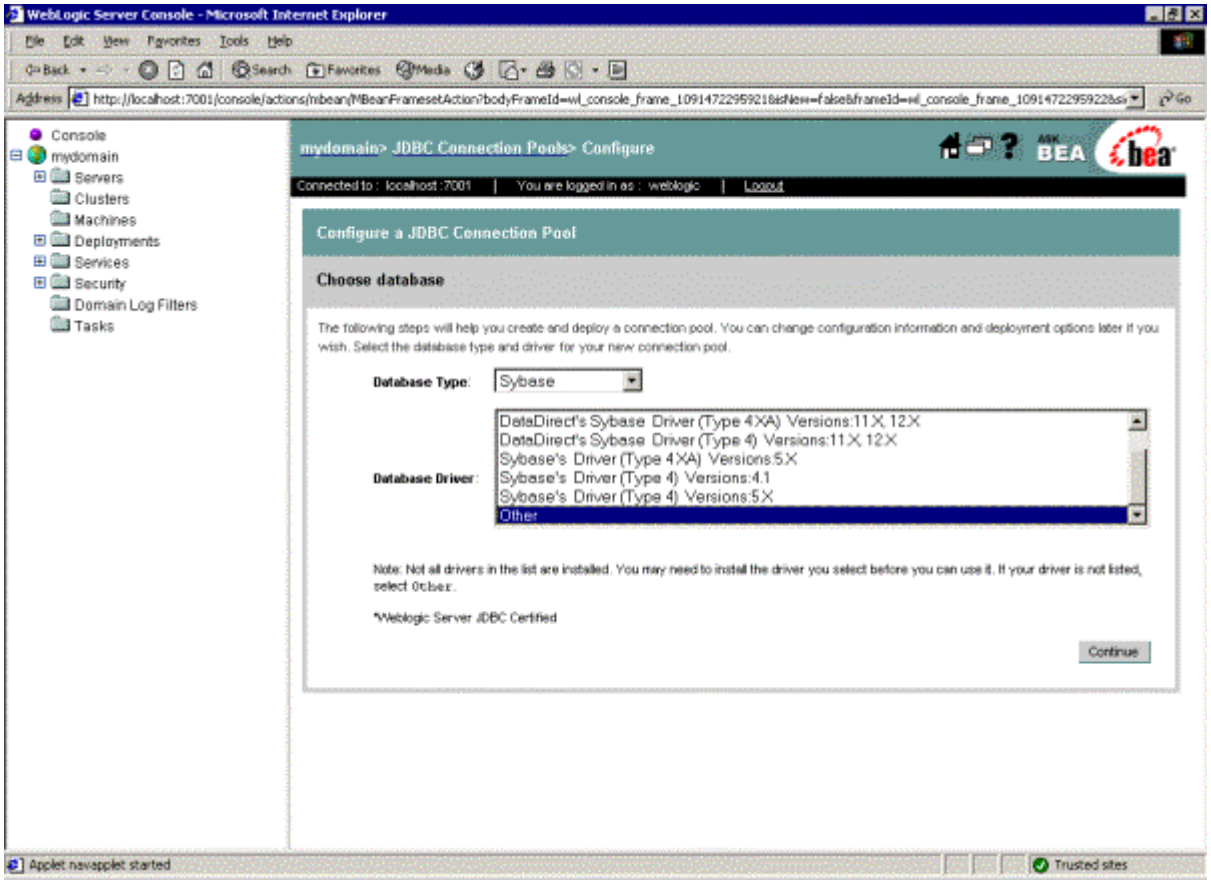
Figure 4.1: Configure a JDBC connection pool



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 4.2: Choose database

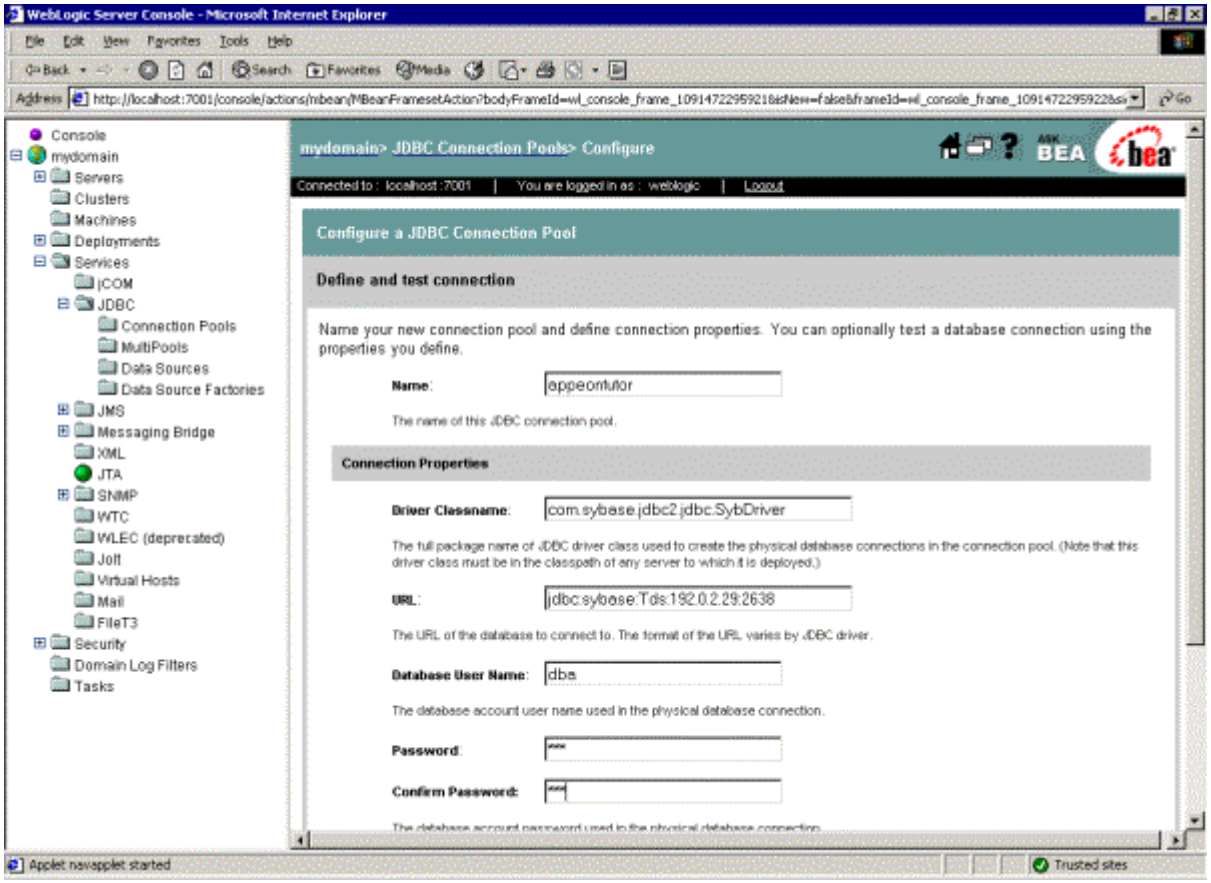


6. Choose a name for the new connection pool (for example, appeontutor) and fill in the blanks for the SQL Anywhere database. Click **Continue**.

Table 4.3: Connection pool properties

Name	Input the name of the new connection pool
Driver classname	com.sybase.jdbc2.jdbc.SybDriver
URL	jdbc:sybase:Tds:*hostname*:2638/*dbname* (The default port of the SQL Anywhere 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 4.3: Data source properties



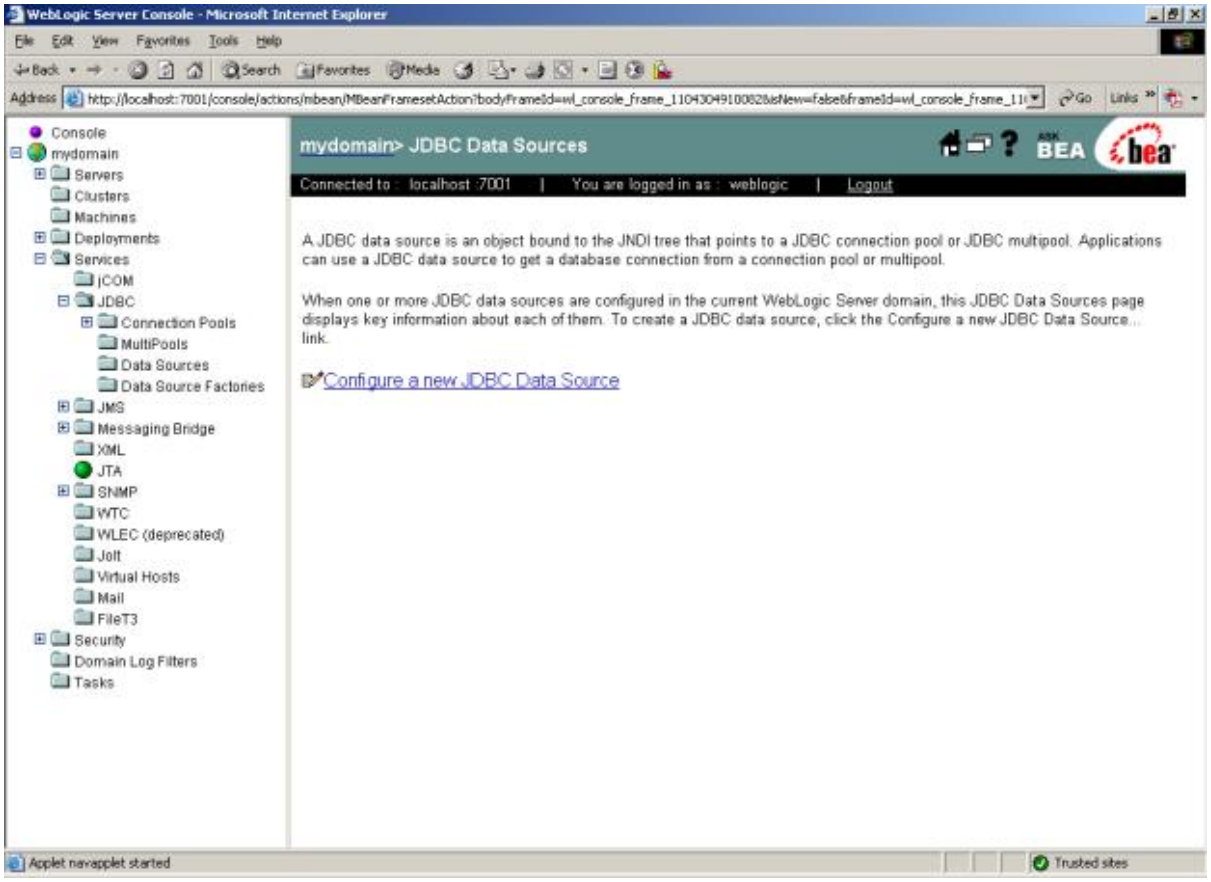
7. Test your connection to verify that you can connect to your database.

8. Create and deploy the new connection pool.

4.3.1.1.2 Configuring a JDBC data source

1. Go to **Services** > **JDBC** > **Data Sources**.

Figure 4.4: Configure a JDBC data source

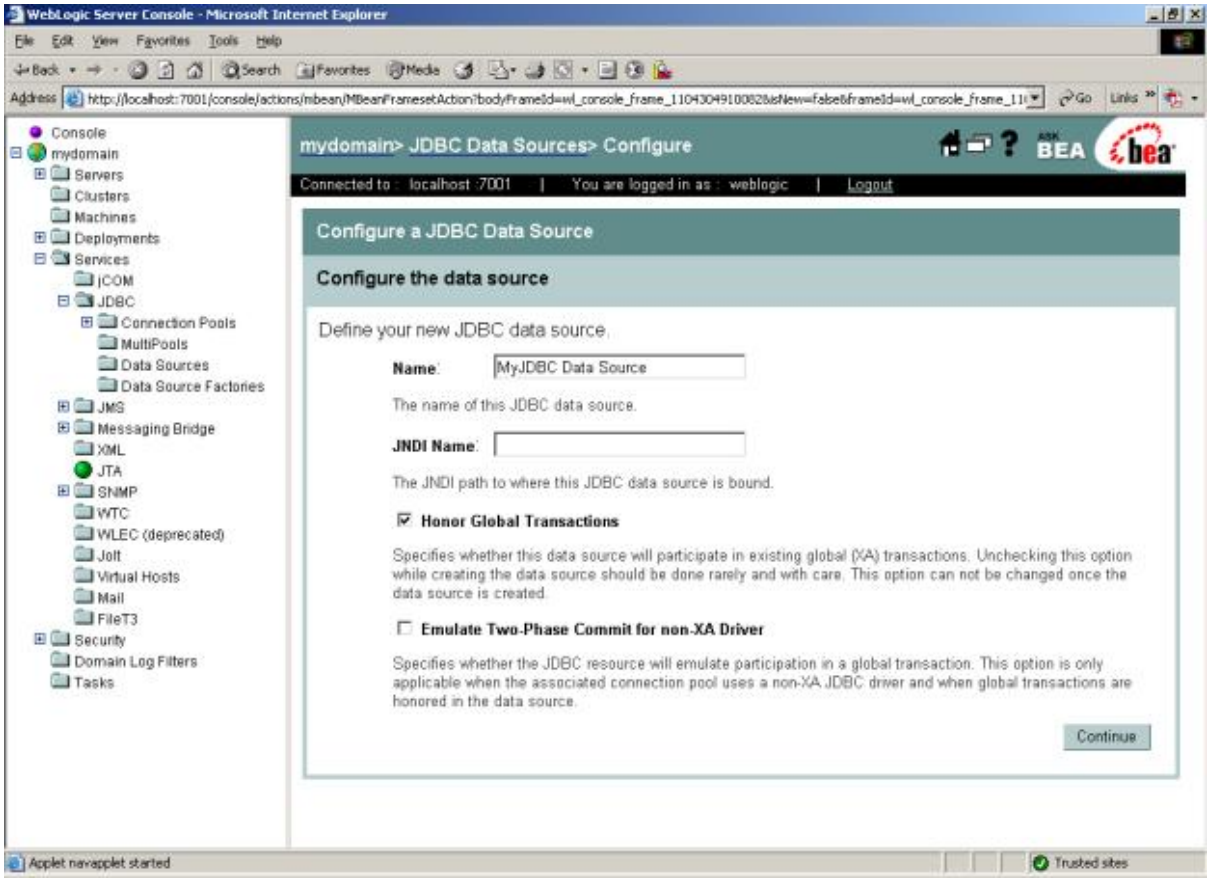


2. Click the **Configure a new JDBC Data Source** link.

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

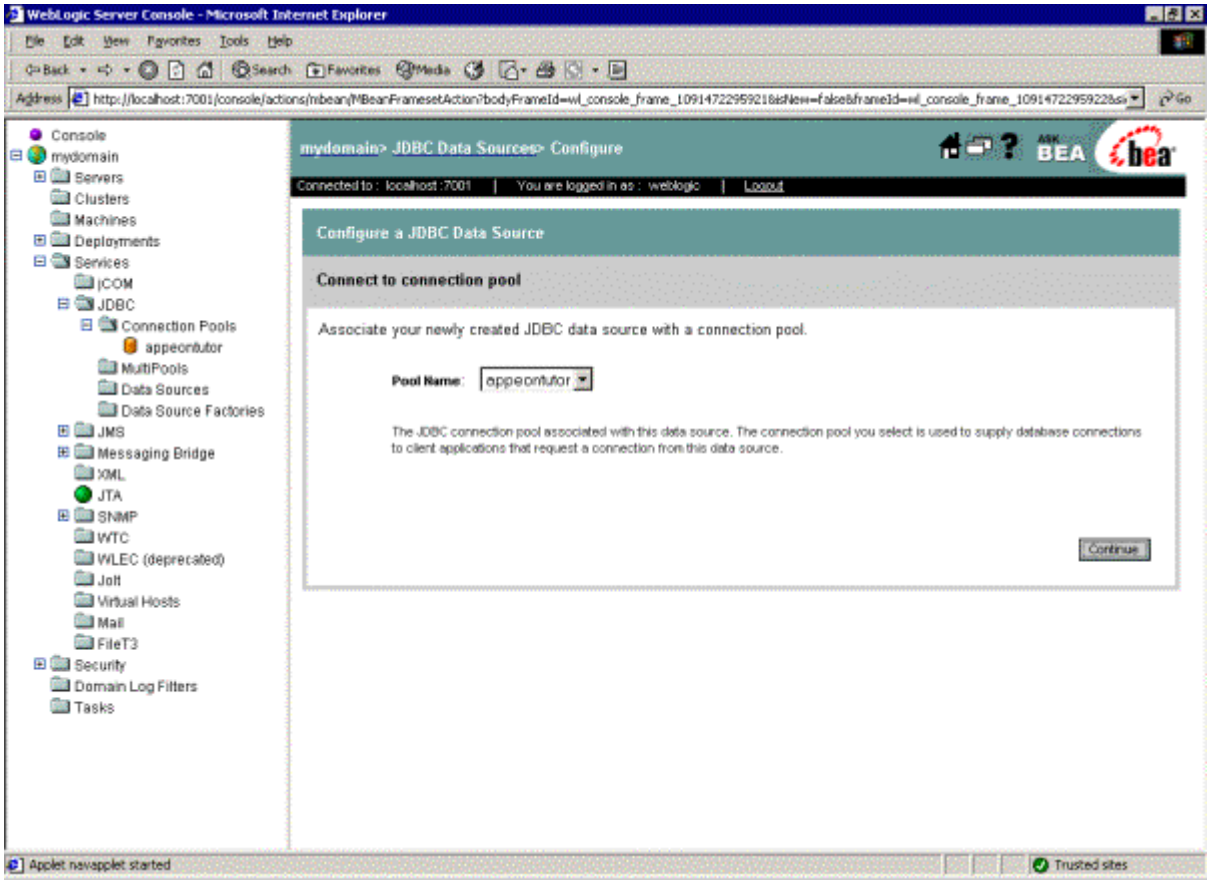
Note: The JNDI name will be used as the data source in AEM.

Figure 4.5: Data source properties



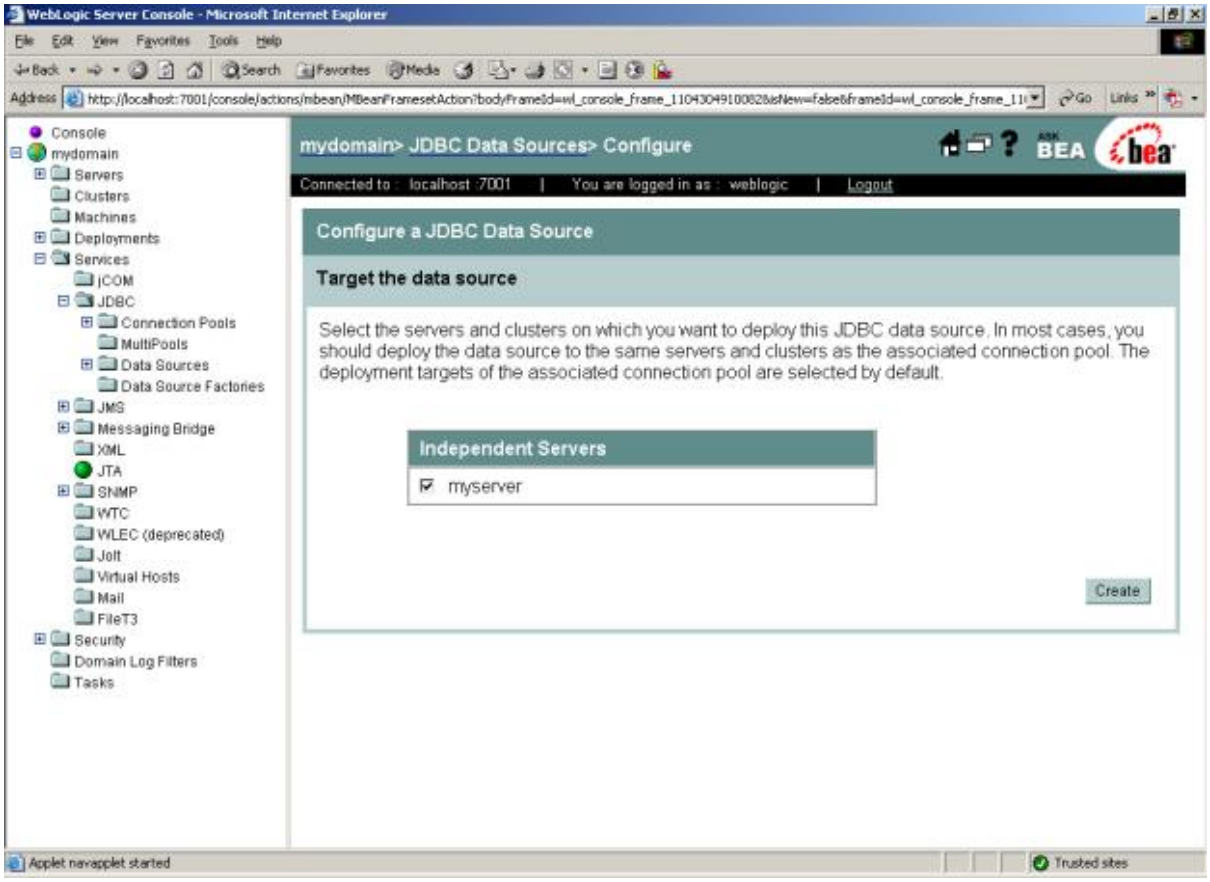
4. Select the newly created connection pool in the dropdown list box and click **Continue**.

Figure 4.6: Select the connection pool



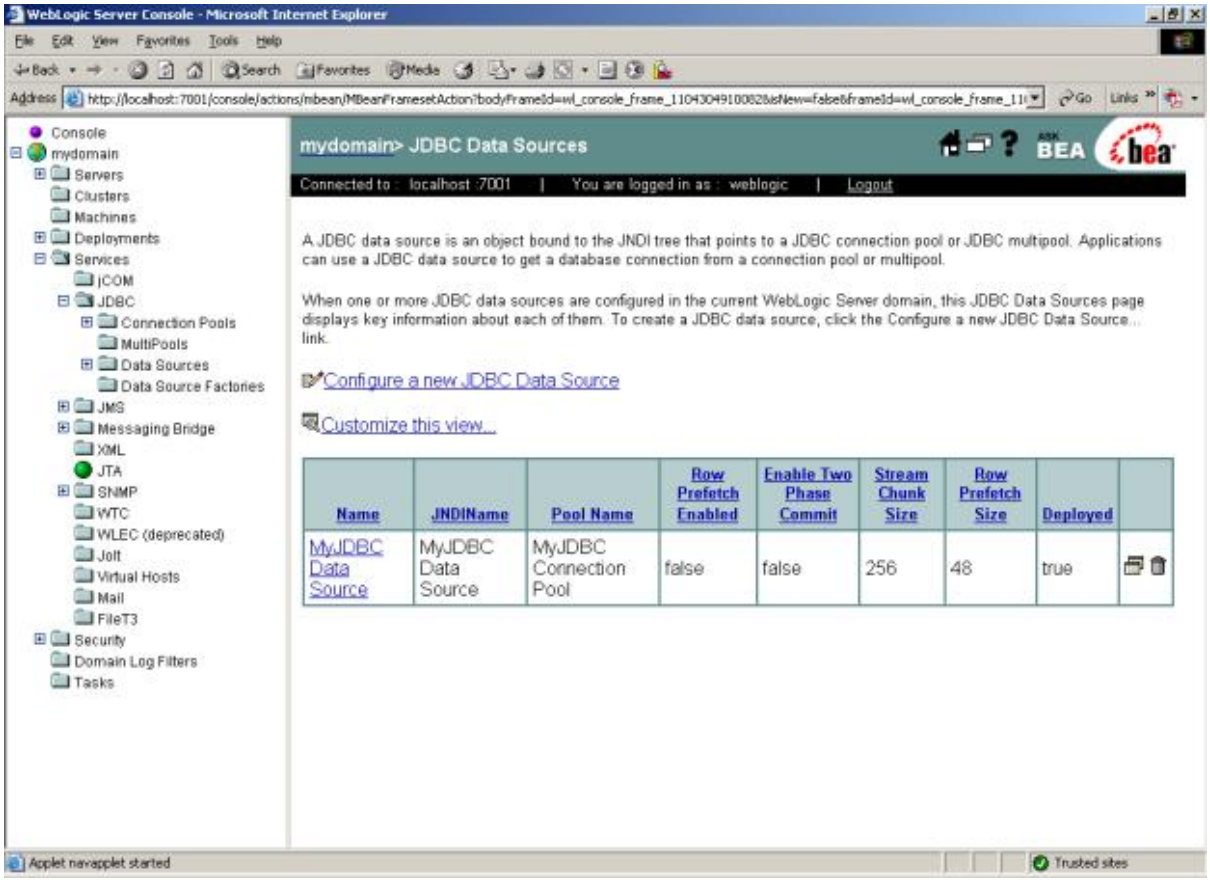
5. Select the server to which you want to deploy the JDBC data source, and click **Create**.

Figure 4.7: Target the data source



6. Confirm the Deployed status of the data source is "true" in the JDBC Data Sources window.

Figure 4.8: Deployed status



4.3.1.2 Setting up data source for WebLogic 11g

The following section will take one database type (SQL Anywhere database with jConnect 6.0 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 Data source parameters.

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

Detailed steps are as below:

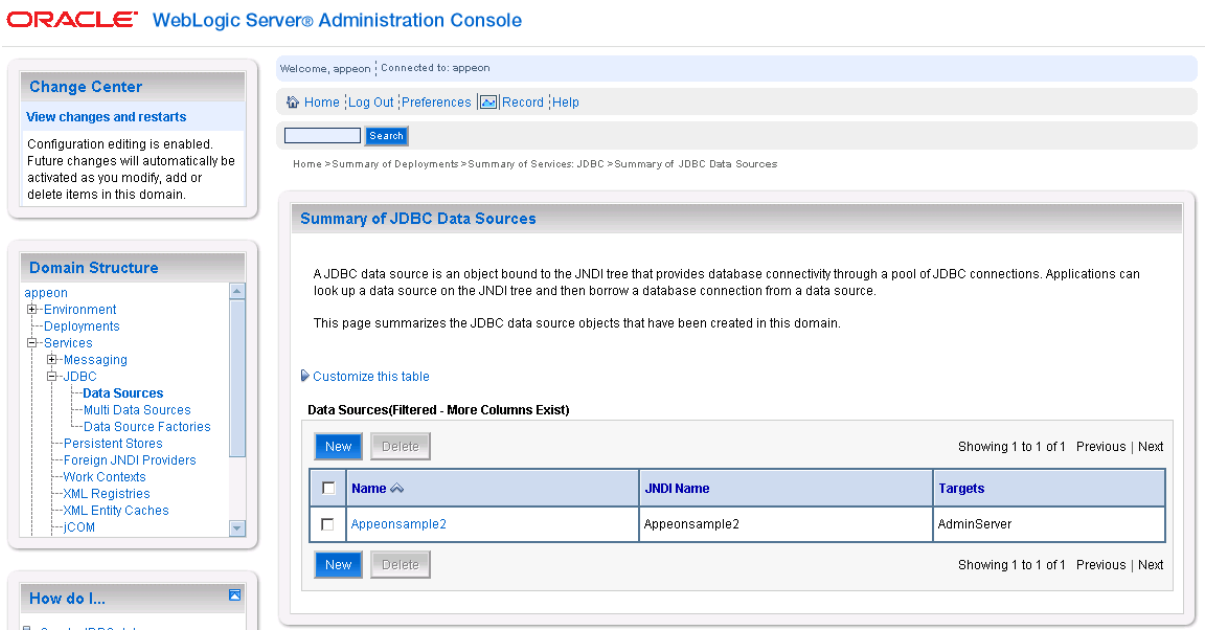
Step 1: Start the Admin Server for WebLogic Server Domain.

Step 2: Log on to the WebLogic Server Administration Console.

Step 3: In the **Domain Structure** section, select **Services** > **JDBC** > **Data Sources**.

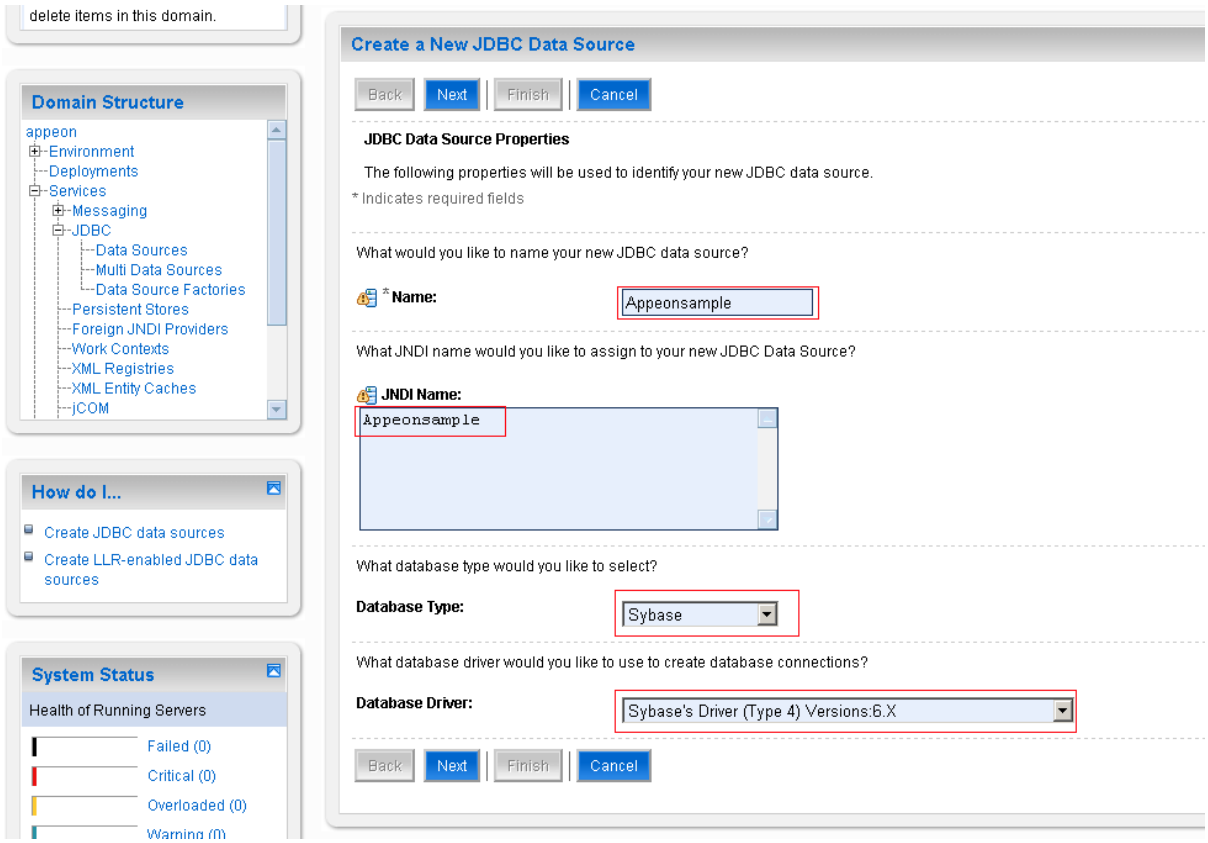
Step 4: On the summary of **Summary of JDBC Data Sources** page, click **New**.

Figure 4.9: The Summary of JDBC Data sources page



Step 5: On the **JDBC Data Source Properties** page, enter or select the following information and then click **Next**.

Figure 4.10: JDBC Data Source Properties page



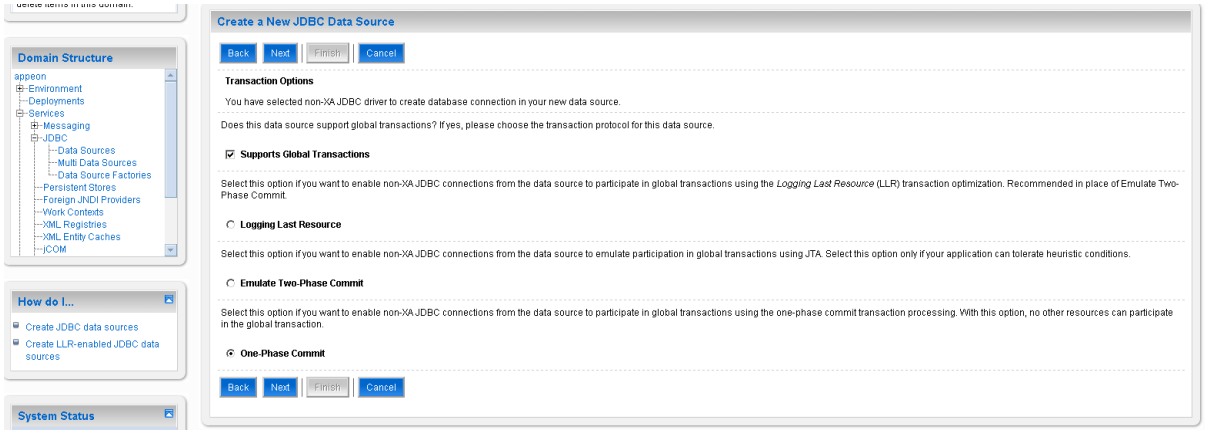
Fill in details as required in the table below.

Table 4.4: JDBC Data Source Properties

Field	Description	Value
Name	Enter a desired new JDBC data source name.	Appeonsample
JNDI Name	Enter a JNDI name that you like to assign to your new JDBC Data Source. Note: The JNDI name will be used as the data source name in AEM.	Appeonsample
Database Type	Select the database type from the dropdown list box.	SAP
Database Driver	Select the database drive from the dropdown list box.	SAP's Driver (Type 4) Versions:6.X

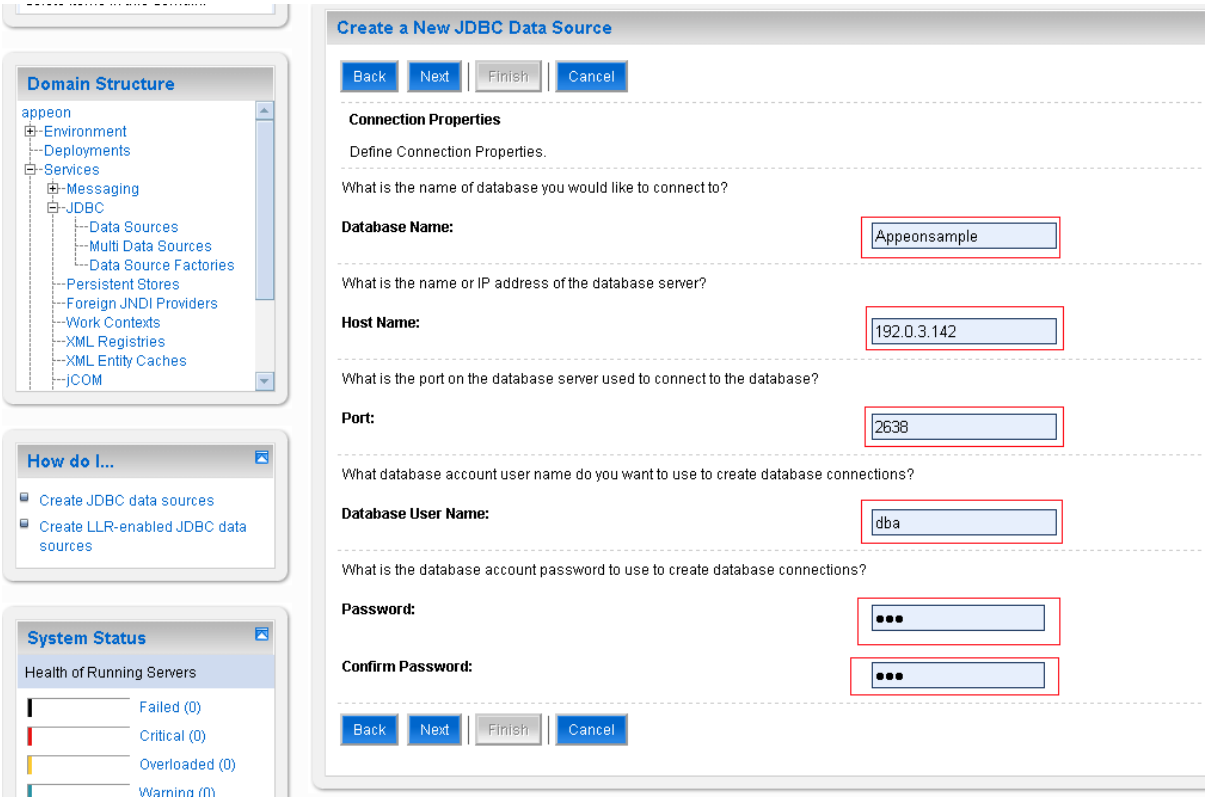
Step 6: On the **Transactions Options** page, check the **Supports Global Transactions** checkbox and select the **One-Phase Commit** radio button, and then click **Next.**

Figure 4.11: Transaction options



Step 7: On the **Connection Properties** page, enter the following information, and then click **Next.**

Figure 4.12: Connection Properties page



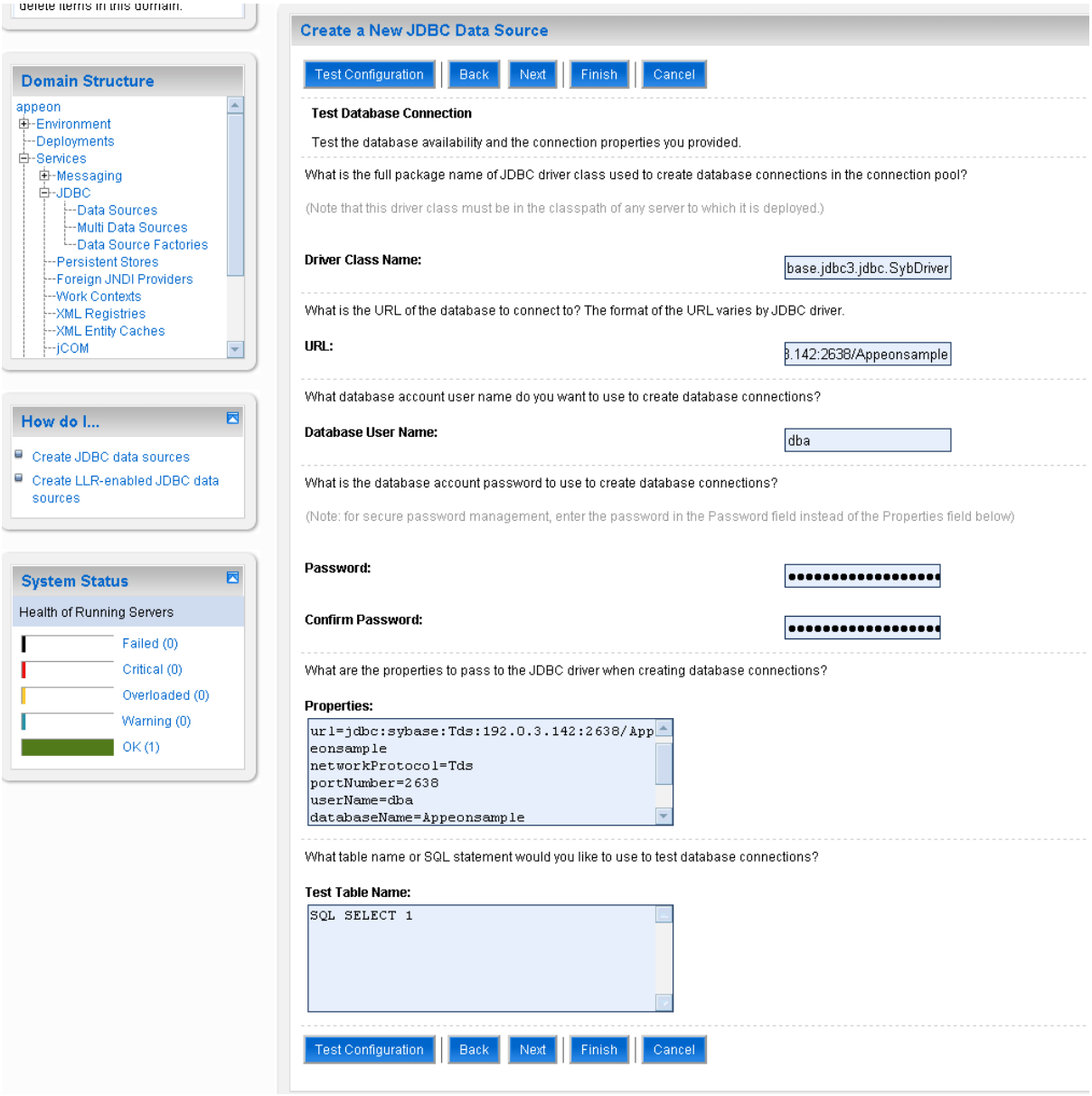
Fill in details as required in the table below.

Table 4.5: Connection Properties page

Field	Description	Value
Database Name	Enter a database name that you would like to connect.	Appeonsample
Host Name	Enter a host name or IP address of the database server.	192.0.3.142
Port	Enter a database port on the database server used to connect to the database.	2638
Database User Name	Enter the database account user name that you want to use to create the database connections.	dba
Password	Enter the database account password that you want to use to create the database connections.	sql
Confirm Password	Enter the same password for confirmation.	sql

Step 8: On the **Test Database Connection** page, specify the **Driver Class Name** and the **URL**, and then click **Test Configuration**. If the test is successful, A "Connection test succeeded" message appears at the top of the page. If the test is unsuccessful, you should correct any configuration errors and retry the test. And then click **Next**.

Figure 4.13: Test Database Connection page



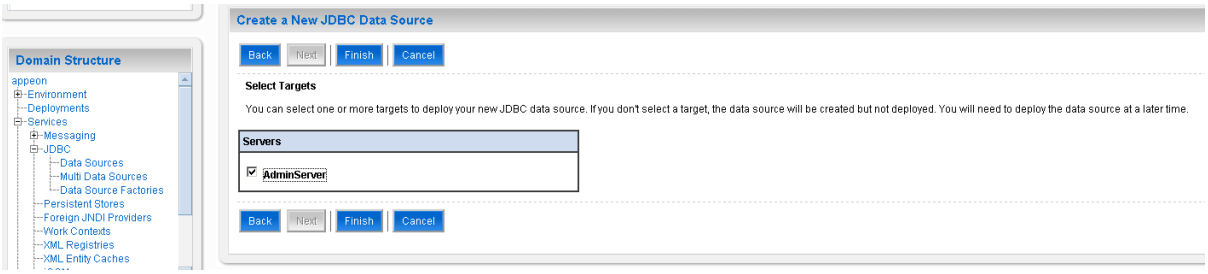
Fill in details as required in the table below.

Table 4.6: Specify the Driver Class Name and the URL

Field	Description	Value
Driver Class Name	Enter the driver name of the database specified.	com.sybase.jdbc3.jdbc.SybDriver
URL	Enter the server name of the database specified.	jdbc:sybase:Tds:Hostname:Port/ServiceName For example: jdbc:sybase:Tds:192.0.3.142:2638/Appeonsample.

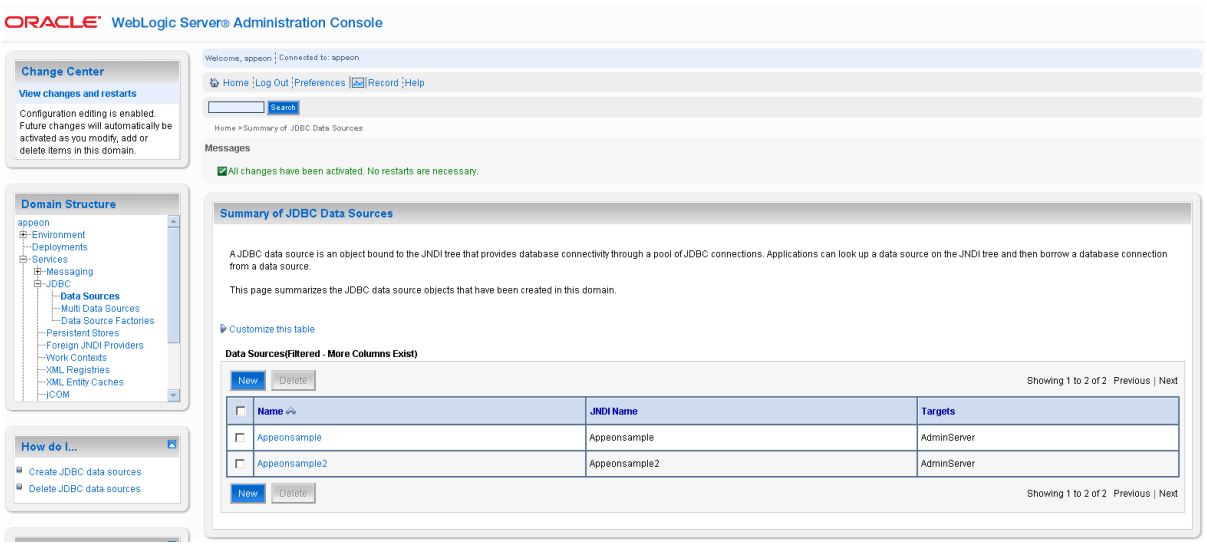
Step 9: On the **Select Targets** page, select the **AdminServer** check box, and then click **Finish**.

Figure 4.14: Select Targets Page



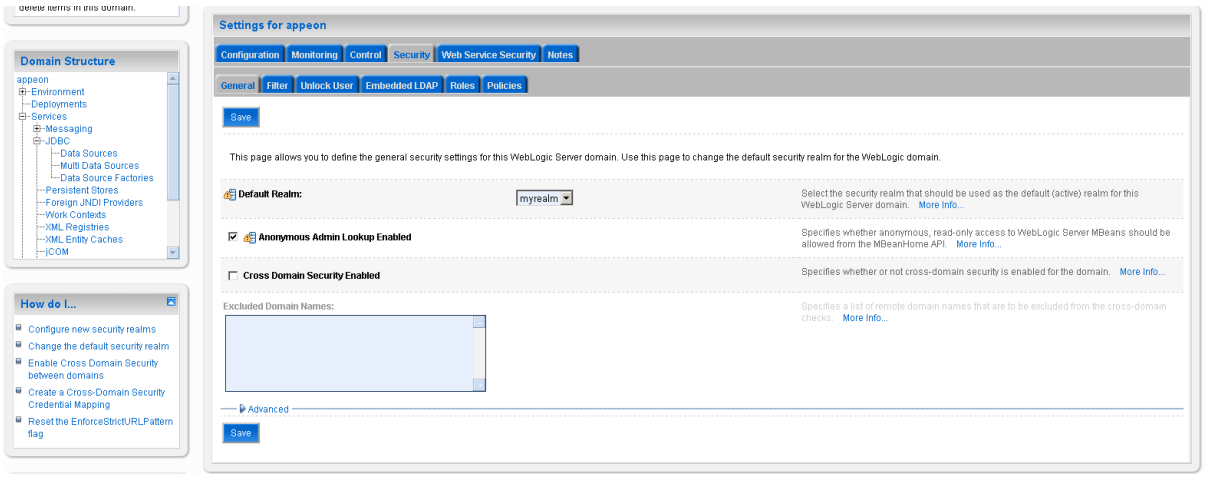
Step 10: On the **Summary of JDBC Data Sources** page, the Data Source that you created appears in the list, and then click the link to the name of the new data source in the **Data Sources** window.

Figure 4.15: Summary of JDBC Data Sources page



Step 11: **(Important)** On the **Settings for the base_domain** page, click **appeon** in the **Domain Structure** section and then select **Security** tab page. Select **Anonymous Admin Lookup Enabled** check box and click **Save**. **This will allow AEM to read the JNDI Names.**

Figure 4.16: Settings for the base_domain page



Step 12: Choose **All Programs** > **Oracle WebLogic** > **User Projects** > **appeon** from the **Windows Start** menu to restart your WebLogic server for configuration changes to take effect.

Step 13: In order to test the connection, please log on to Appeon AEM to configure a Transaction Object and then test it.

4.3.2 Setting up data source for WebSphere

4.3.2.1 Setting up data source for WebSphere 6.1

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 Data source parameters.

Note:

1. The JNDI name specified for the data source will be regarded as the data source name by PowerServer and AEM.

2. If the **global security mode** is turned on in WebSphere, AEM will not be able to access the WebSphere data sources. Please refer to Section 4.3.2.3, “Required configurations when global security is on” for solutions.

4.3.2.1.1 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 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.

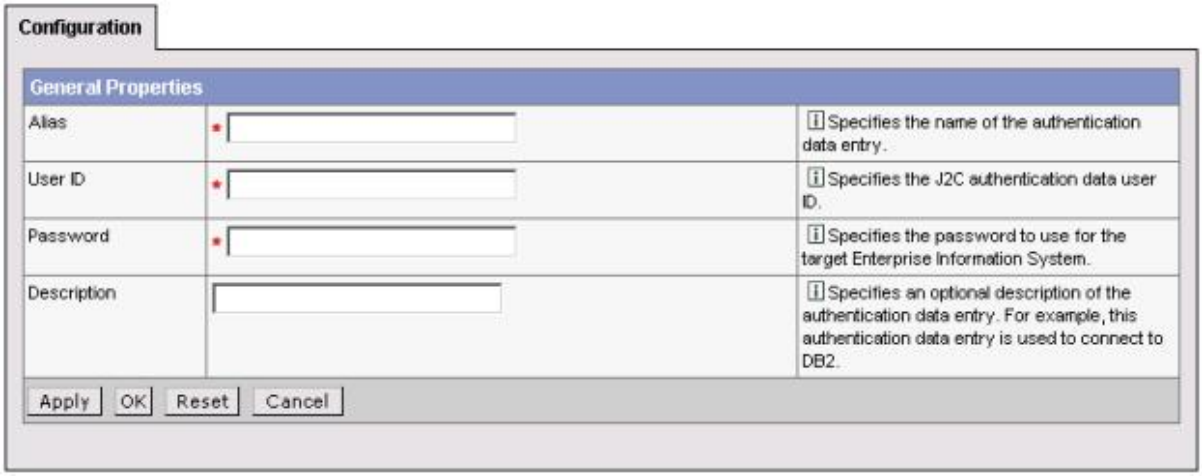
4. Save changes to the ORACLE_JDBC_DRIVER_PATH variable in the master configuration.

4.3.2.1.2 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 4.17: New J2C authentication data entry



Fill in details as required in the table below.

Table 4.7: Details for the new authentication data entry

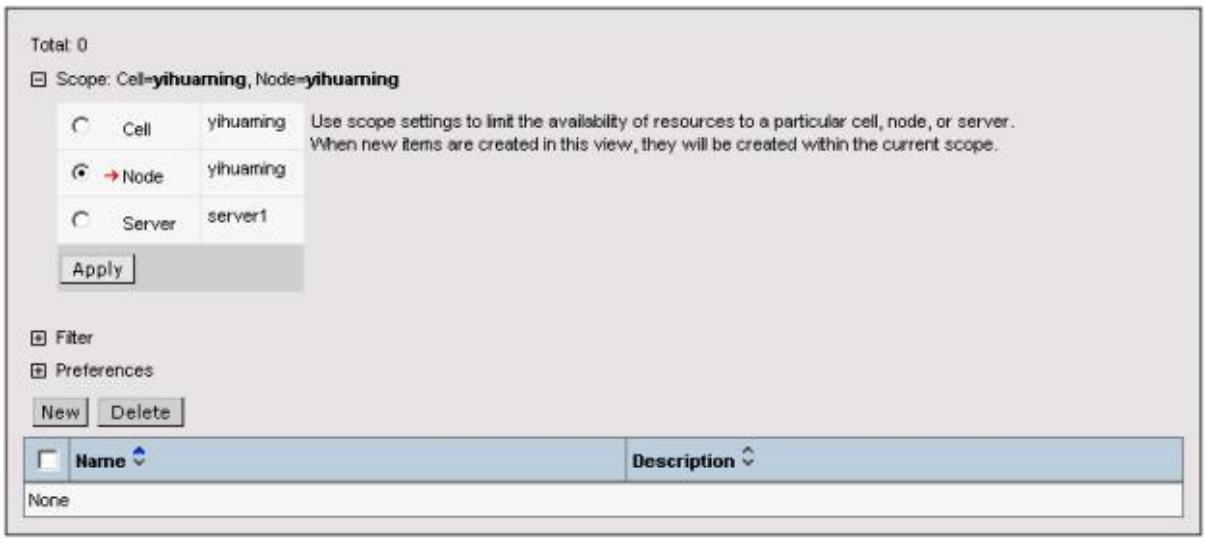
Alias	Enter a suitable (short) name, such as "UDDIAlias"
Userid	Enter the database user ID used to read and write to the UDDI registry database.
Password	Enter the password associated with the user ID specified above.
Description	Enter a suitable description of the chosen user ID or leave it blank.

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

4.3.2.1.3 Creating and configuring a JDBC provider

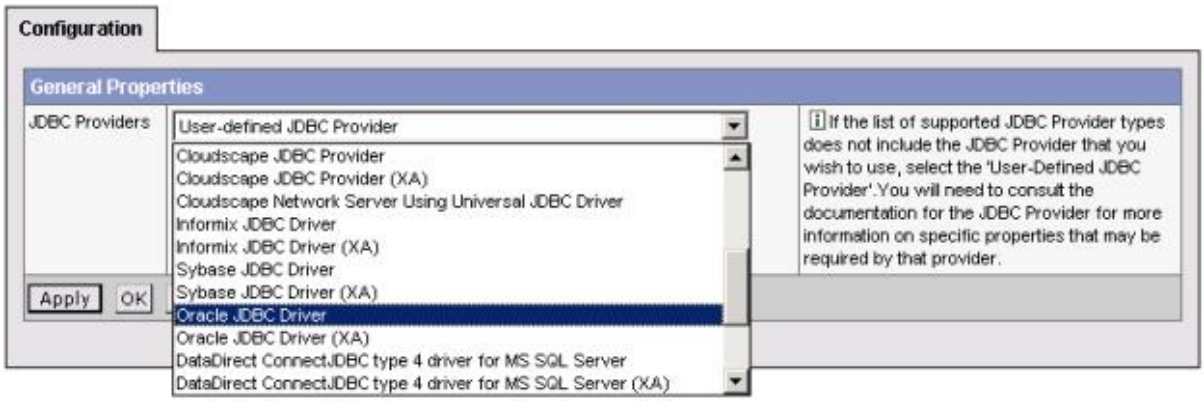
1. Click **Resources** | **JDBC Providers** in the WebSphere administrative console.
2. Click **New**. The JDBC Providers configuration window opens.

Figure 4.18: JDBC Providers configuration window



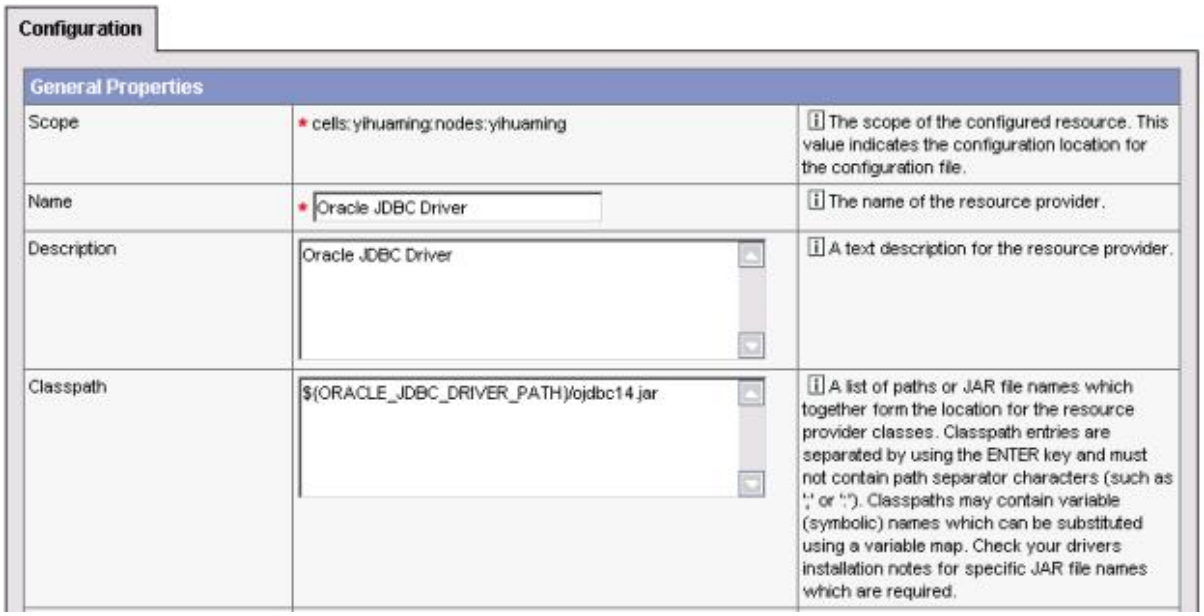
3. Select the correct JDBC provider type. For example, Oracle JDBC Driver.

Figure 4.19: Select JDBC Provider type



4. Select the driver provider and driver file.

Figure 4.20: 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.

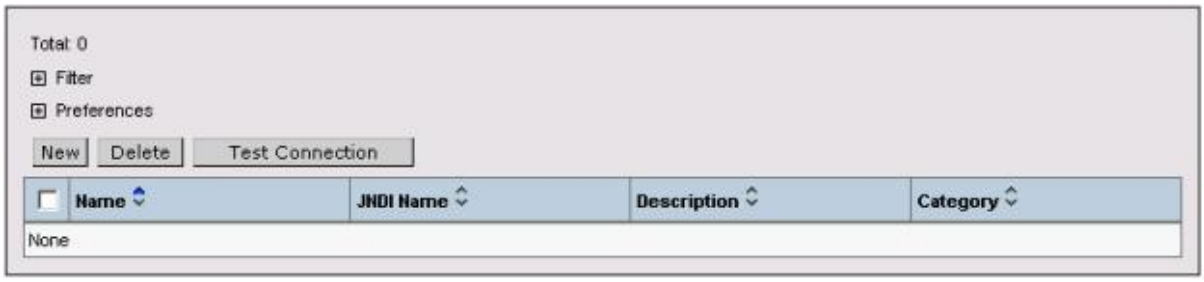
4.3.2.1.4 Creating a data source

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 4.21: Data source page



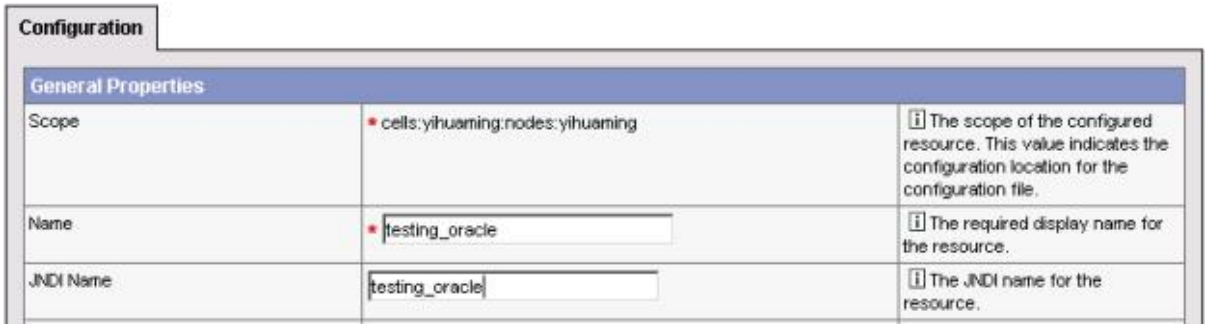
4. Click **New** to display the Data source settings page.

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

Note:

- The JNDI name specified for the data source will be regarded as the data source name by PowerServer and AEM.
- If the **global security mode** is turned on in WebSphere, AEM will not be able to access the WebSphere data sources. Please refer to Section 4.3.2.3, “Required configurations when global security is on” for solutions.

Figure 4.22: Data source properties



6. Select the J2C authentication data entry configured in Creating a new J2C authentication data entry 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.

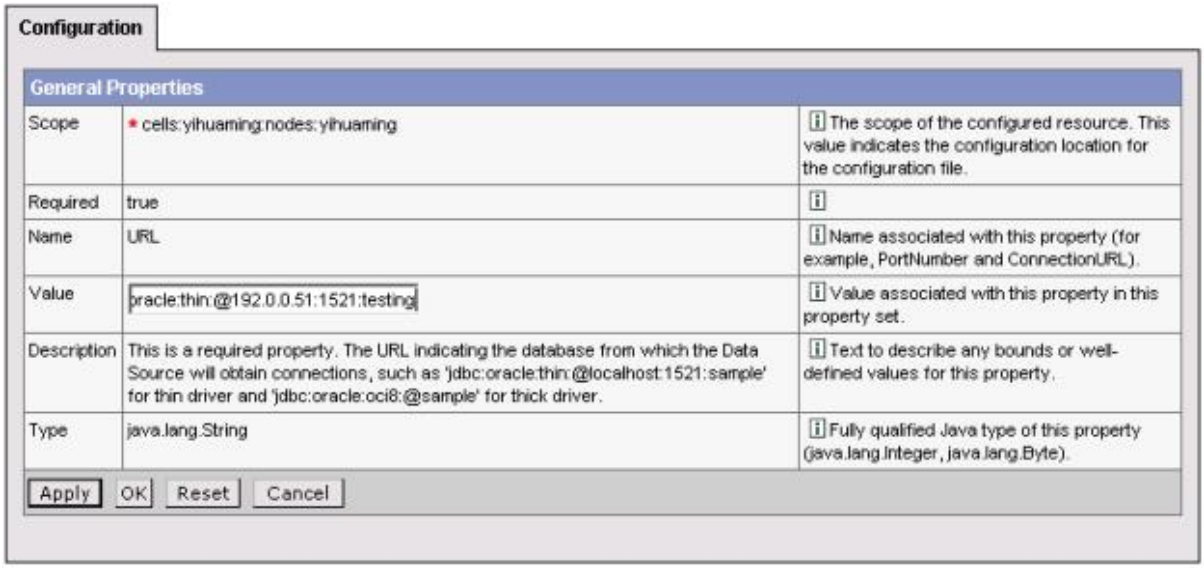
8. Click the name of the new data source in the Data Sources window.

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

Figure 4.23: Additional properties

10. Configure all the required fields according to the instructions in the window. For example, set the URL property to jdbc:oracle:thin:@192.0.0.51:1521:testing if Oracle 9i, 10g, and 11g, or jdbc:oracle:thin:@//192.0.0.51:1521/testing if Oracle 12c.

Figure 4.24: 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.

4.3.2.2 Setting up data source for WebSphere 8.0

The following section will take one database type (Teradata database with Teradata 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 Data source parameters.

Note:

1. The JNDI name specified for the data source will be regarded as the data source name by PowerServer and AEM.

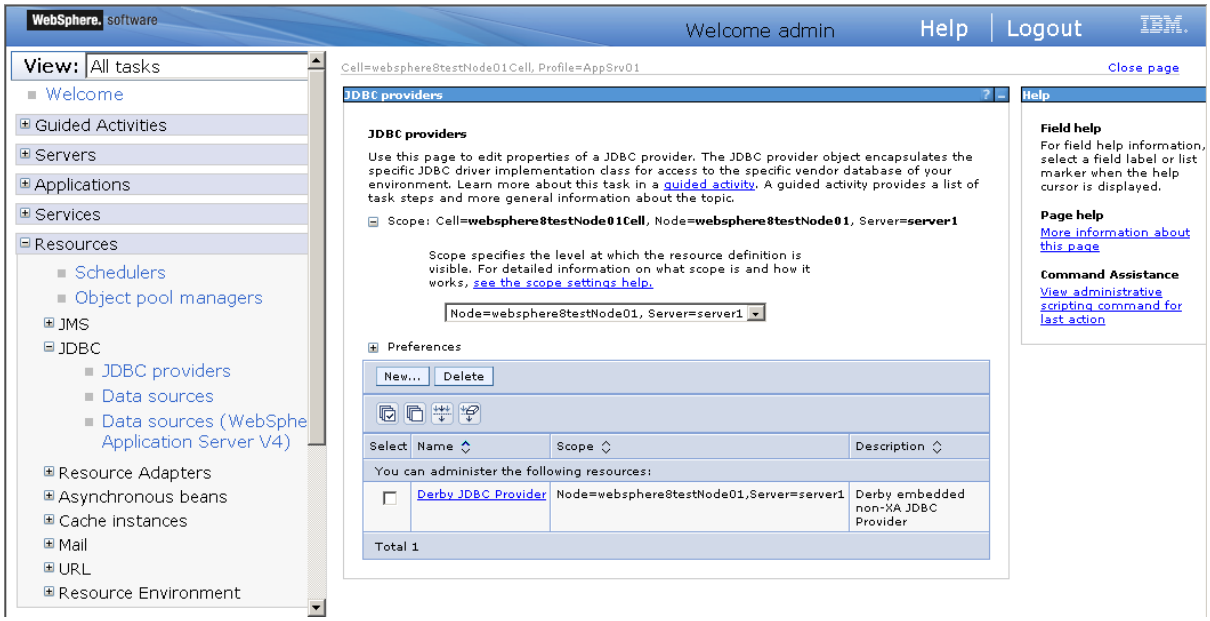
2. If the **global security mode** is turned on in WebSphere, AEM will not be able to access the WebSphere data sources. Please refer to Section 4.3.2.3, “Required configurations when global security is on” for solutions.

4.3.2.2.1 Creating and configuring a JDBC provider

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

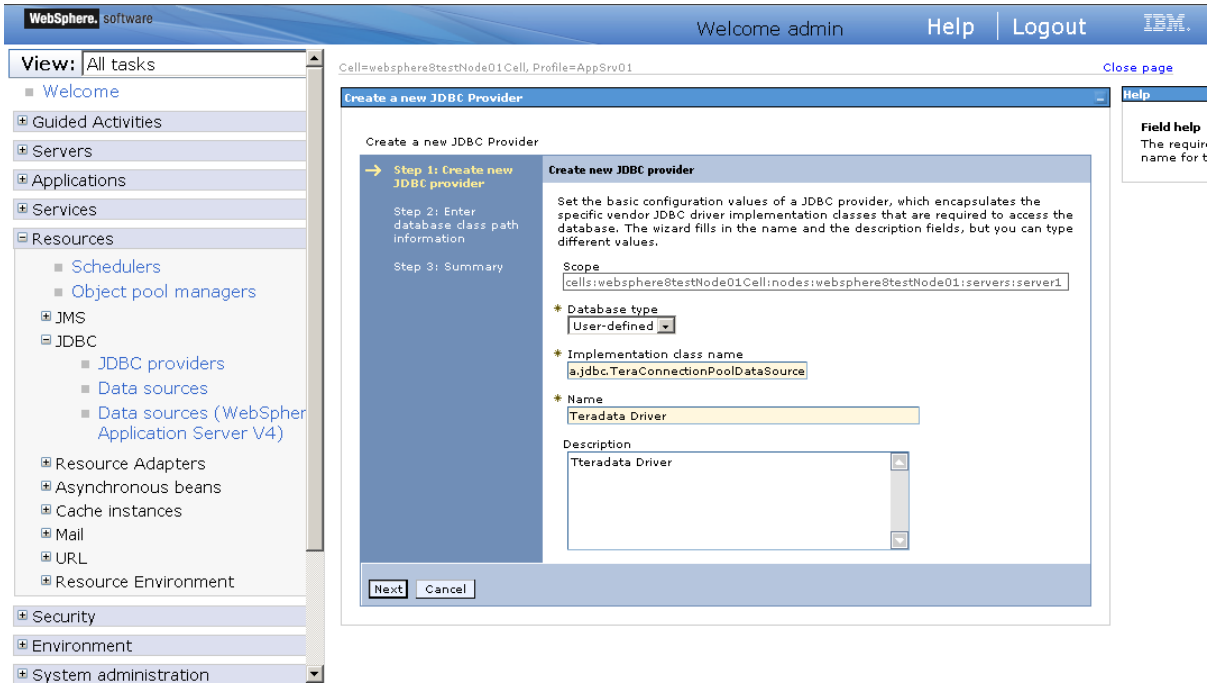
Step 2: Click **Resources** > **JDBC** > **JDBC providers**. In the right pane, select the appropriate scope for the JDBC provider. (This scope becomes the scope of your data source.) You can choose a cell, node, cluster, or server. And then click **New**.

Figure 4.25: JDBC providers page



Step 3: On the Create new JDBC provider page, enter or select the following information, and then click **Next**.

Figure 4.26: Create new JDBC provider page



Fill in details as required in the table below.

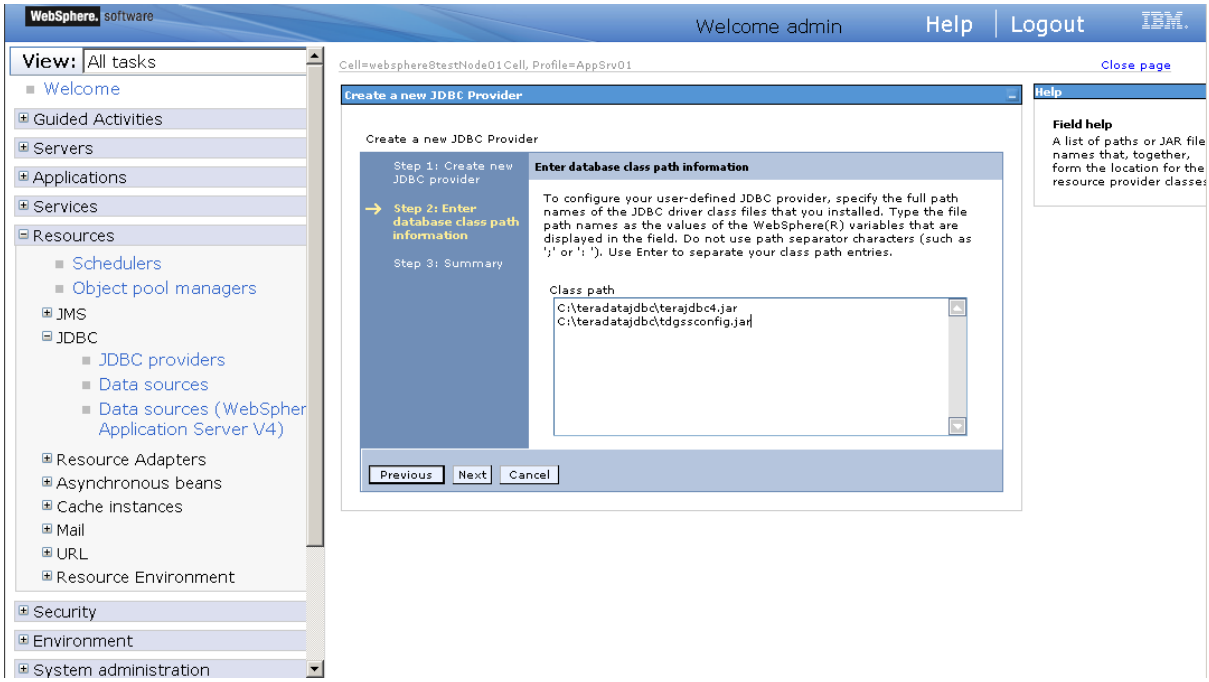
Table 4.8: Create new JDBC provider

Field	Description	Value
Database type	Select the database type of the JDBC provider you need to create from the drop-down list.	User-defined

Field	Description	Value
	Note: If the list of database types does not include the database type that you want to use, select "User-defined".	
Implementation classname	Enter the name of the connection pool driver of the database specified.	com.teradata.jdbc.TeraConnectionPoolDataSource
Name	Enter a desired new JDBC provider name.	Teradata Driver
Description	Enter the description that you like to describe your new JDBC provider.	Teradata Driver

Step 4: On the Enter database class path information page, enter the database class path, and then click **Next**.

Figure 4.27: Enter database class path information page



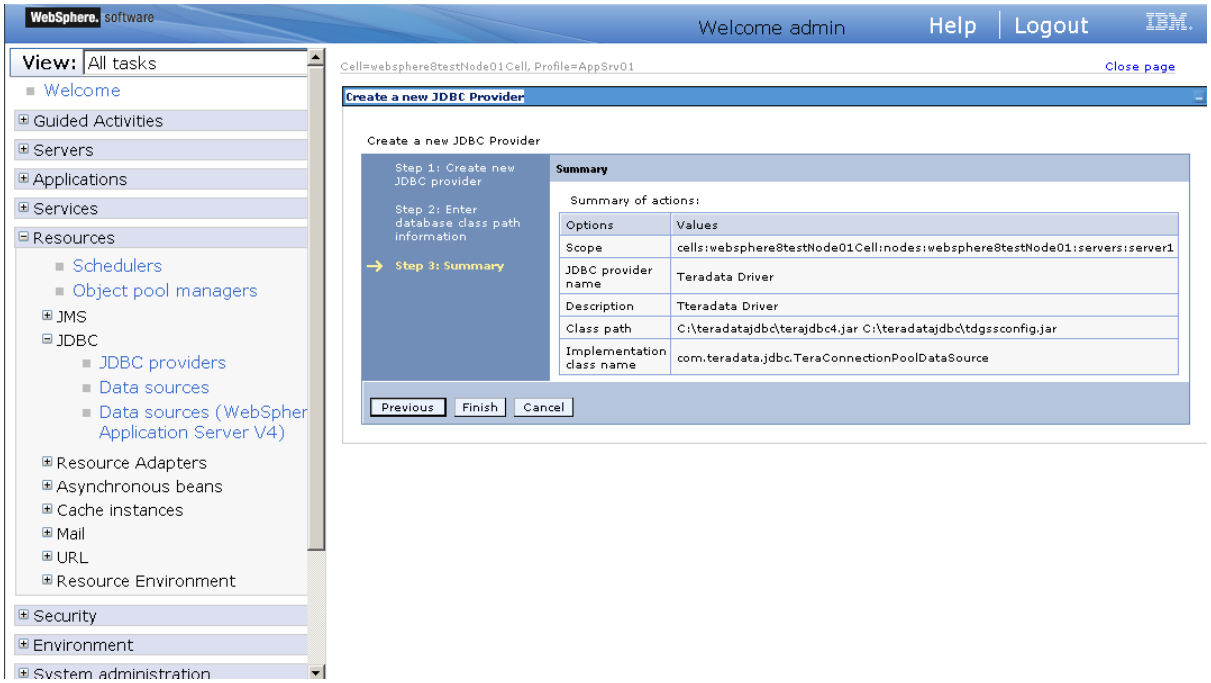
Fill in details as required in the table below.

Table 4.9: Database class path information

Field	Description	Value
Class path	The full name of the jar files that make up the Teradata JDBC Driver. The example assumes that you have copied these files to the C:\teradatajdbc directory on your system. A path on a Unix machine would use forward slashes to separate its components.	C:\teradatajdbc\terajdbc4.jar C:\teradatajdbc\tdgssconfig.jar

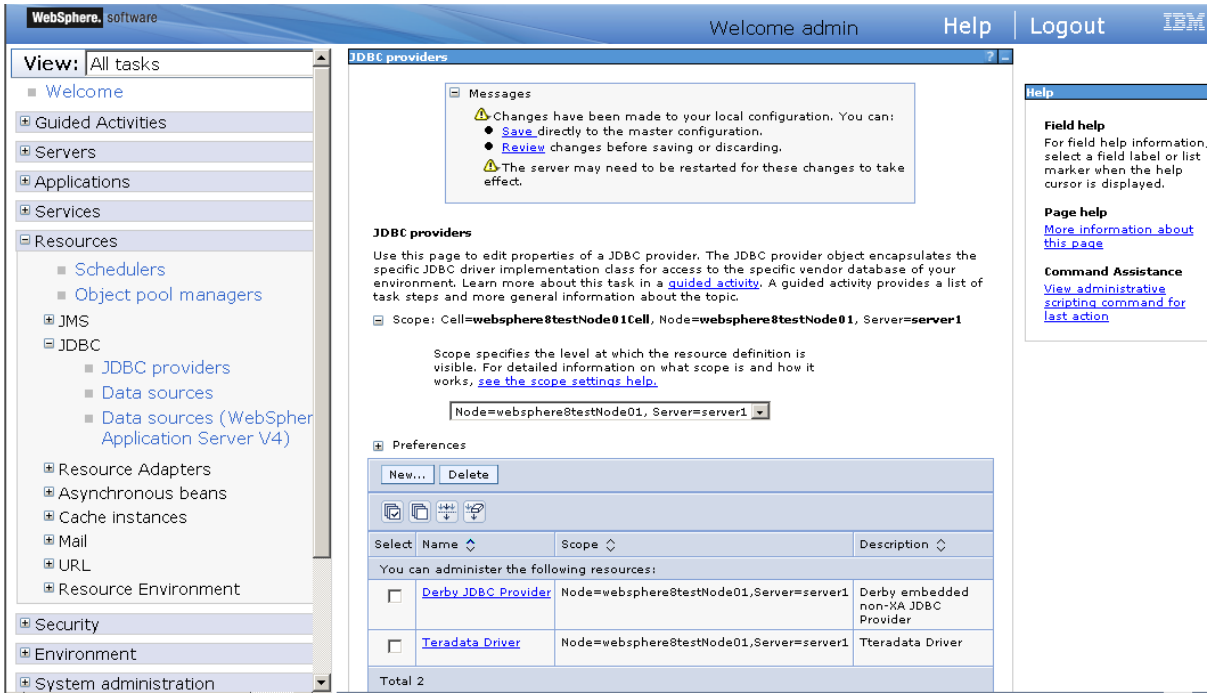
Step 5: On the Summary page, you can review the settings and when done click **Finish**.

Figure 4.28: Summary page



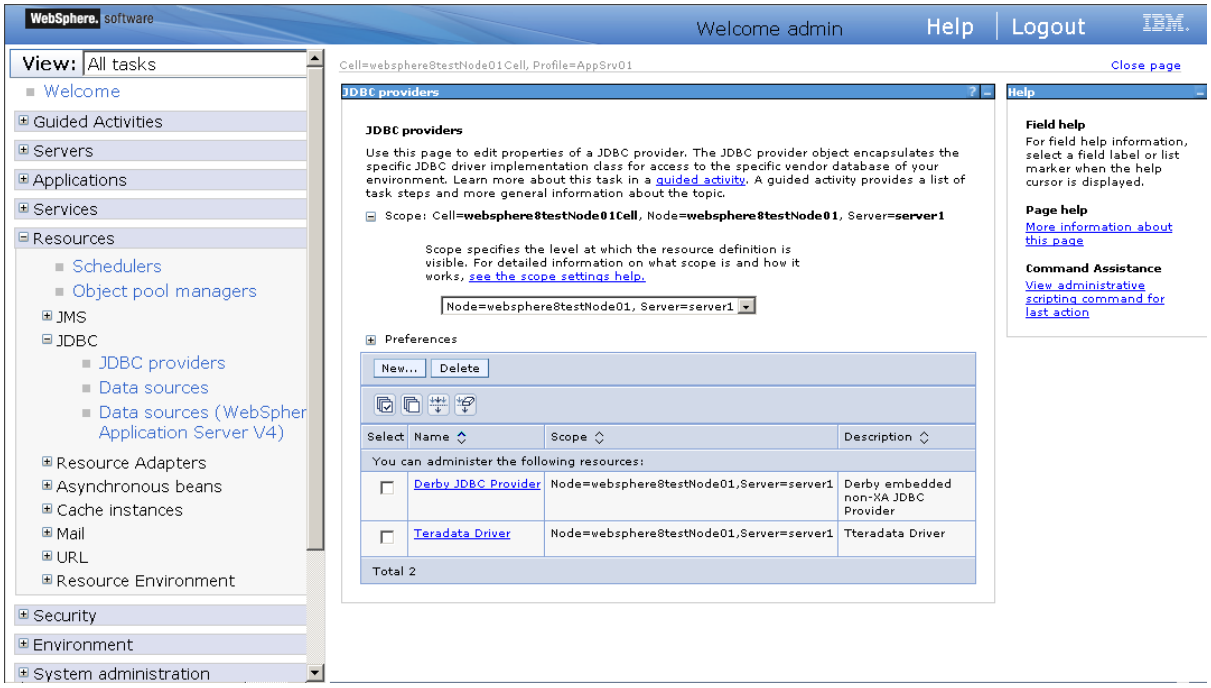
Step 6: On the JDBC providers page, click **Save** to commit these changes to the master configuration and have them go live inside of the server.

Figure 4.29: JDBC providers page



Now the "Teradata Driver" appears in the list of JDBC providers.

Figure 4.30: The newly created JDBC providers page

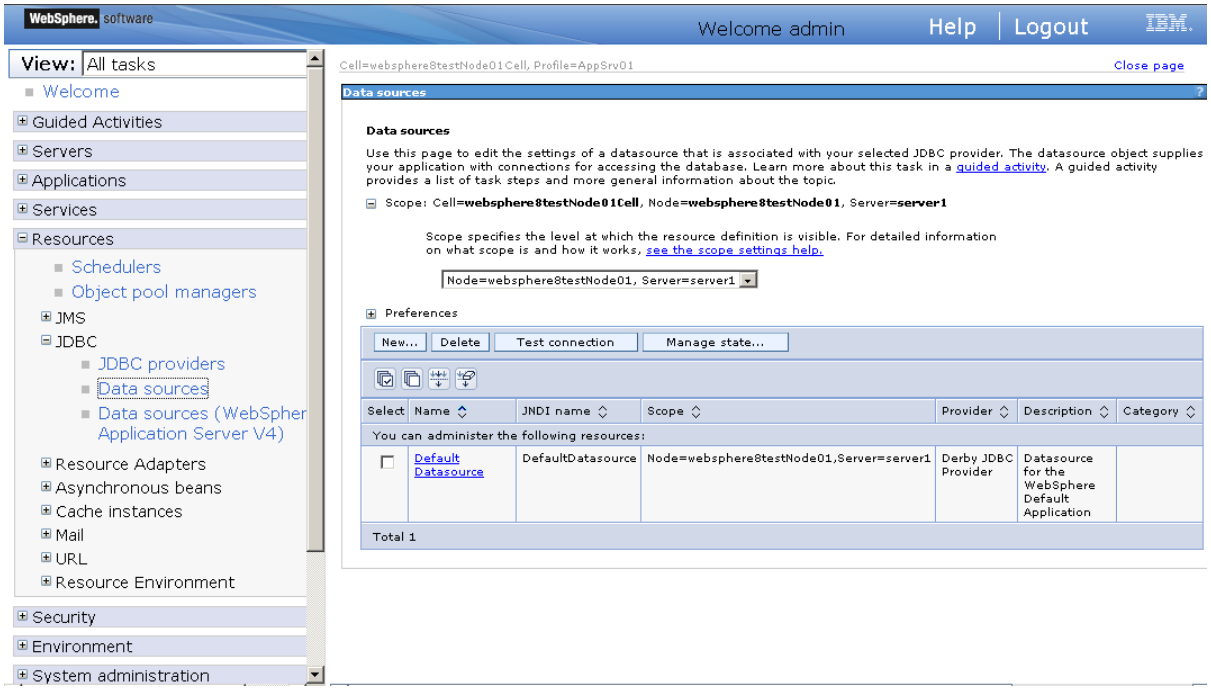


4.3.2.2.2 Creating the Data Source

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

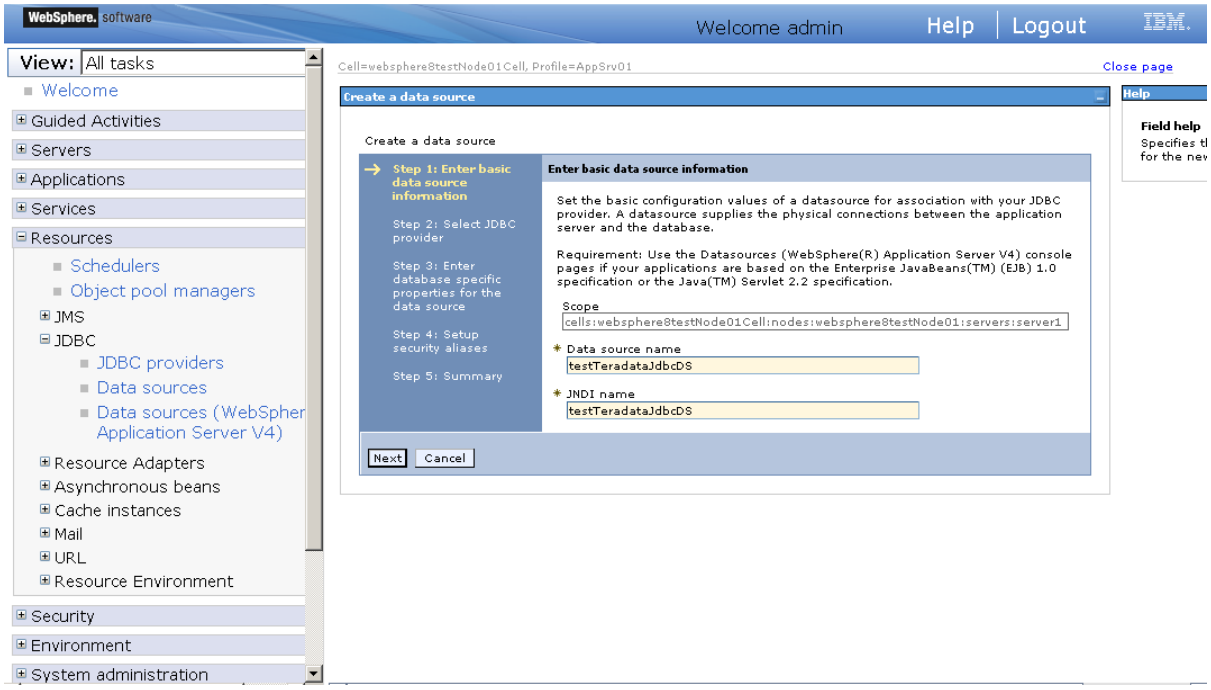
Step 2: Click **Resources** > **JDBC** > **Data sources**. In the right pane, select appropriate scope for the data source. (This scope becomes the scope of your data source.) You can choose a cell, node, cluster, or server. And then click **New**.

Figure 4.31: Create the Data Source page



Step 3: On the Enter basic data source information page, enter the following information. And then click **Next.**

Figure 4.32: Enter basic data source information page



Fill in details as required in the table below.

Table 4.10: The basic Data Source information

Field	Description	Value
Data Source Name	Enter a desired new JDBC data source name.	testTeradataJdbcDS
JNDI Name	Enter a JNDI name that you like to assign to your new JDBC Data Source.	testTeradataJdbcDS

Note:

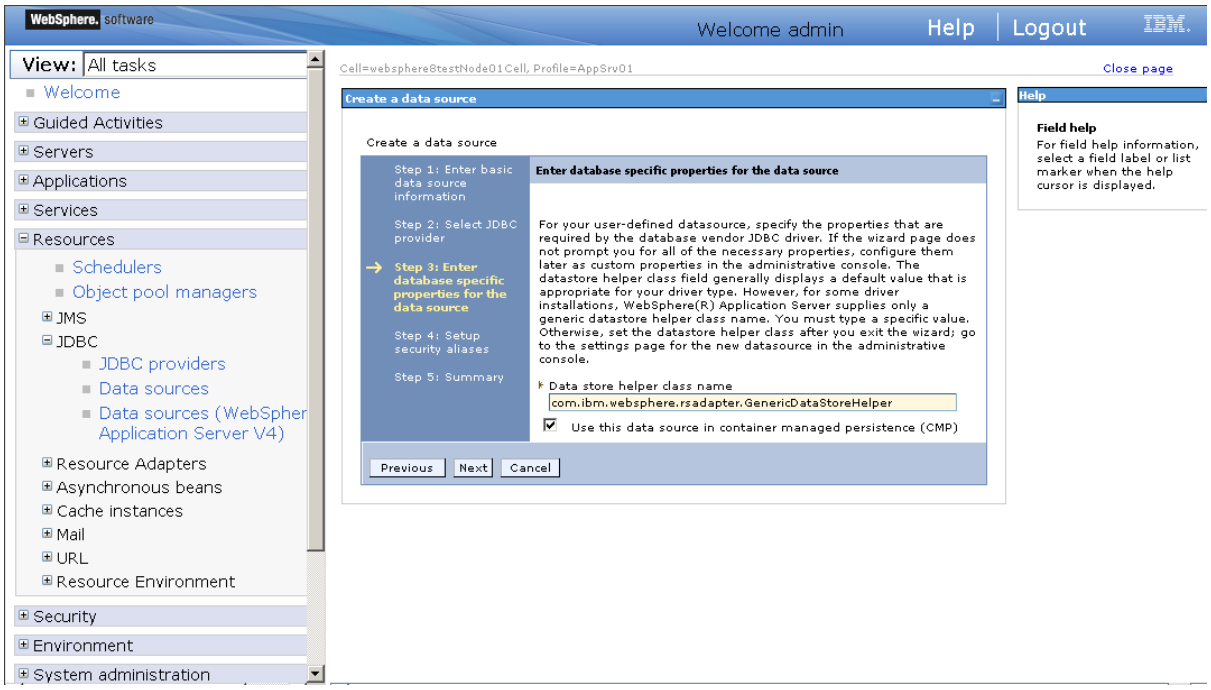
- The JNDI name specified for the data source will be regarded as the data source name by PowerServer and AEM.
- If the **global security mode** is turned on in WebSphere, AEM will not be able to access the WebSphere data sources. Please refer to Section 4.3.2.3, “Required configurations when global security is on” for solutions.

Step 4: On the **Select JDBC provider** page, click **Select an existing JDBC provider** and select **Teradata Driver** from the drop-down list. And then click **Next**.

Figure 4.33: Select JDBC provider page

Step 5: On the Enter database specific properties for the data source page, click **Next**.

Figure 4.34: Enter database specific properties for the data source page



Fill in details as required in the table below.

Table 4.11: Database specific properties for the data source

Field	Description	Value
Data store helper class name	Data store helper classes provided by WebSphere.	Select the default value "com.ibm.websphere.rsadapter.GenericDataStoreHelper".

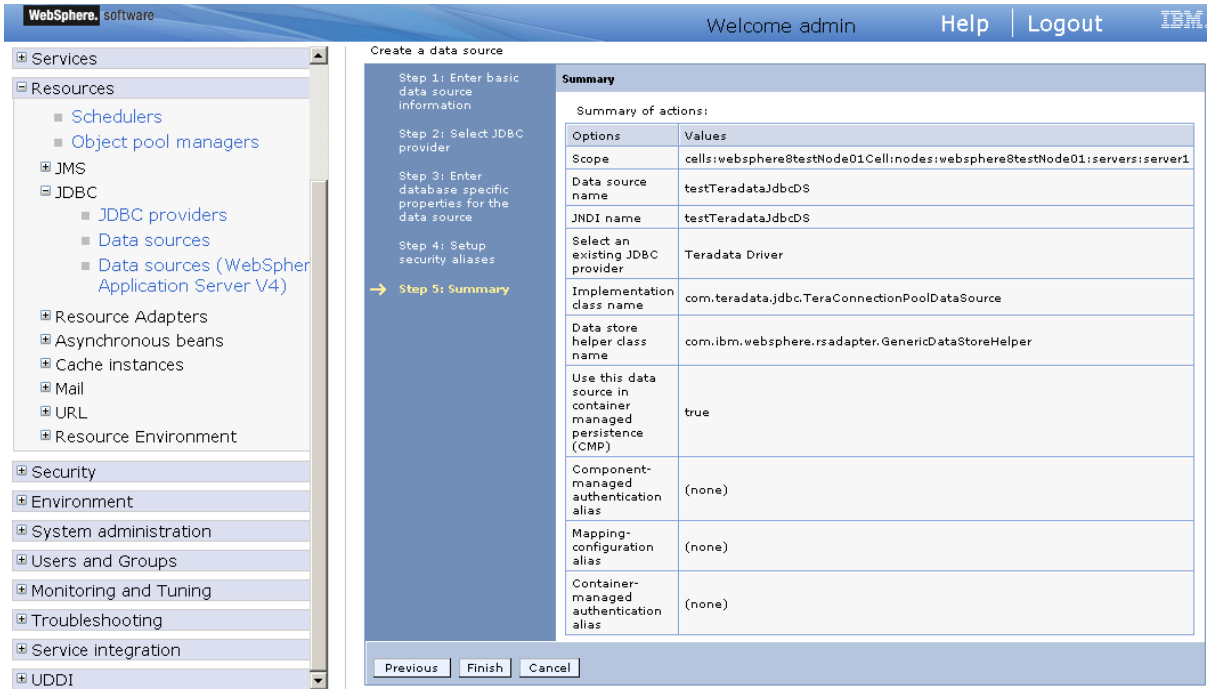
Field	Description	Value
Container Managed Persistence	Set if Data Source is used for CMP of EJBs.	Check this box if the Data Source is used with CMP entity beans. Otherwise, leave it unchecked.

Step 6: On the **Setup security aliases** page, keep the default values as "none", and then click **Next.**

Figure 4.35: Setup security aliases page

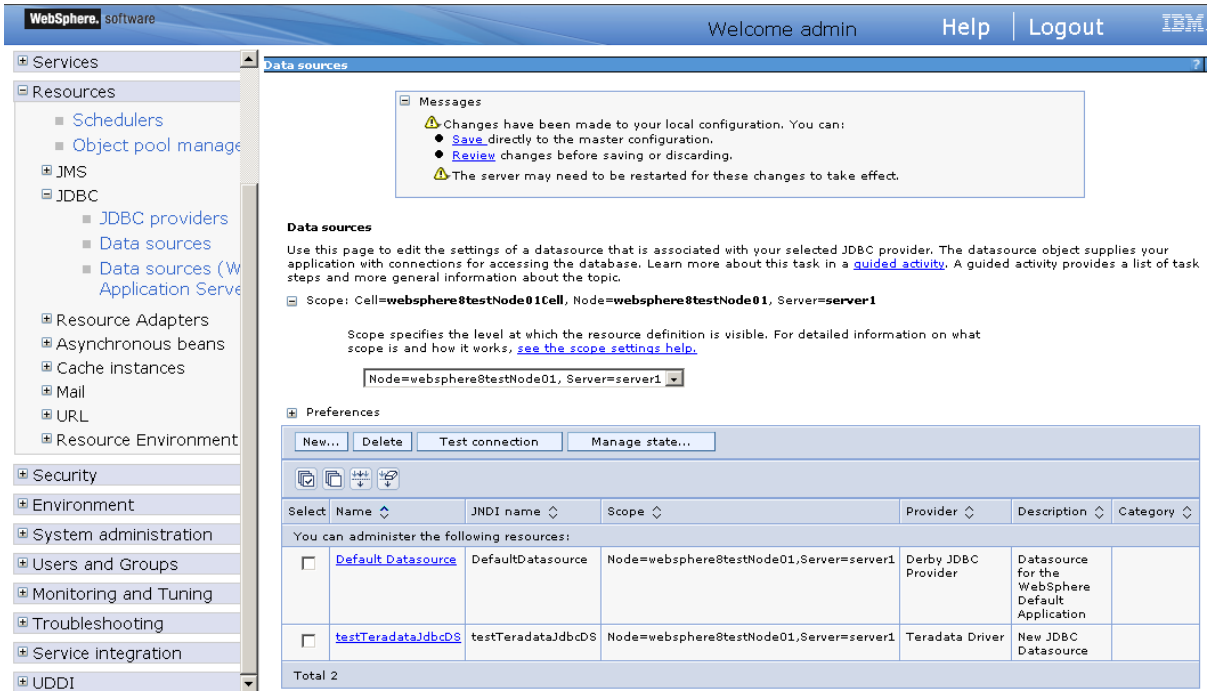
Step 7: On the **Summary** page, you can review the settings and when done click **Finish**.

Figure 4.36: Summary page



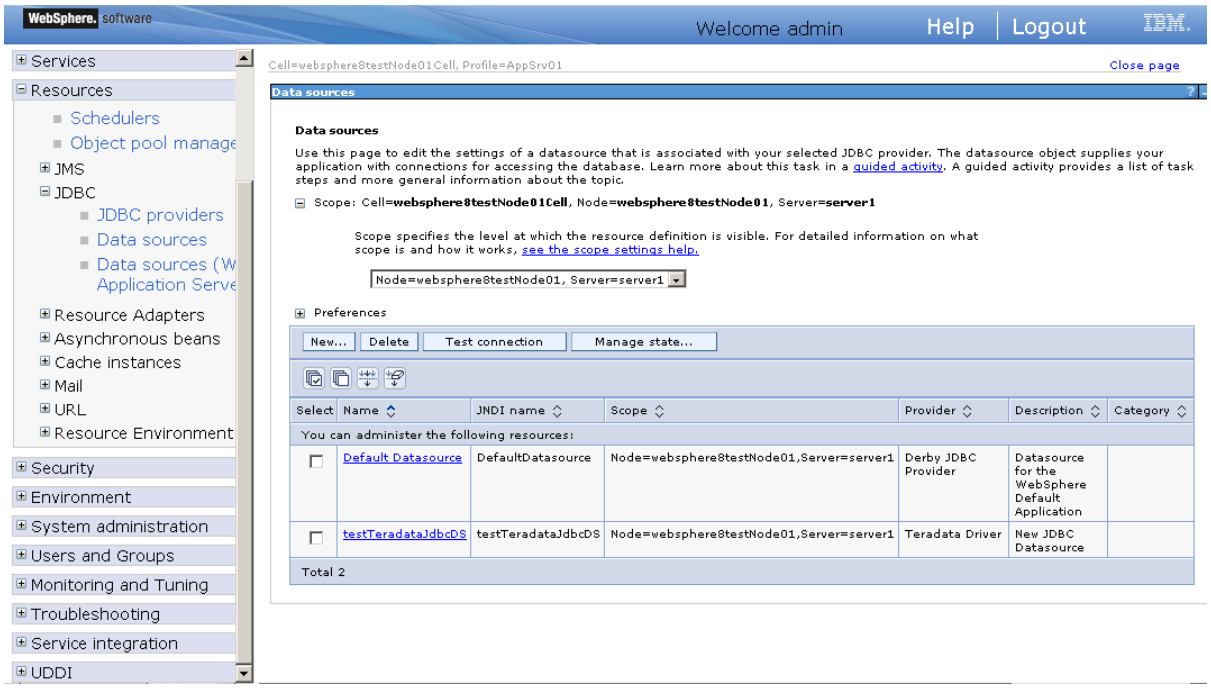
Step 8: On the **Data Sources** page, click **Save** to commit these changes to the master configuration and have them go live inside of the server.

Figure 4.37: Data Sources page



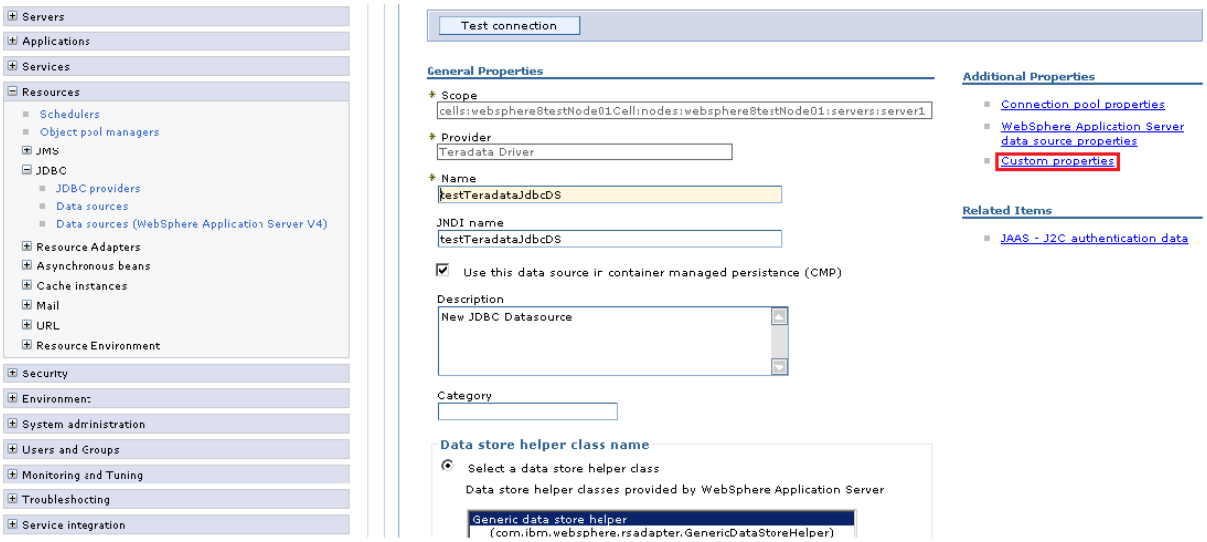
Step 9: On the following page, click **testTeradataJdbcDS** in the **Data Sources** window.

Figure 4.38: The newly created data source information page



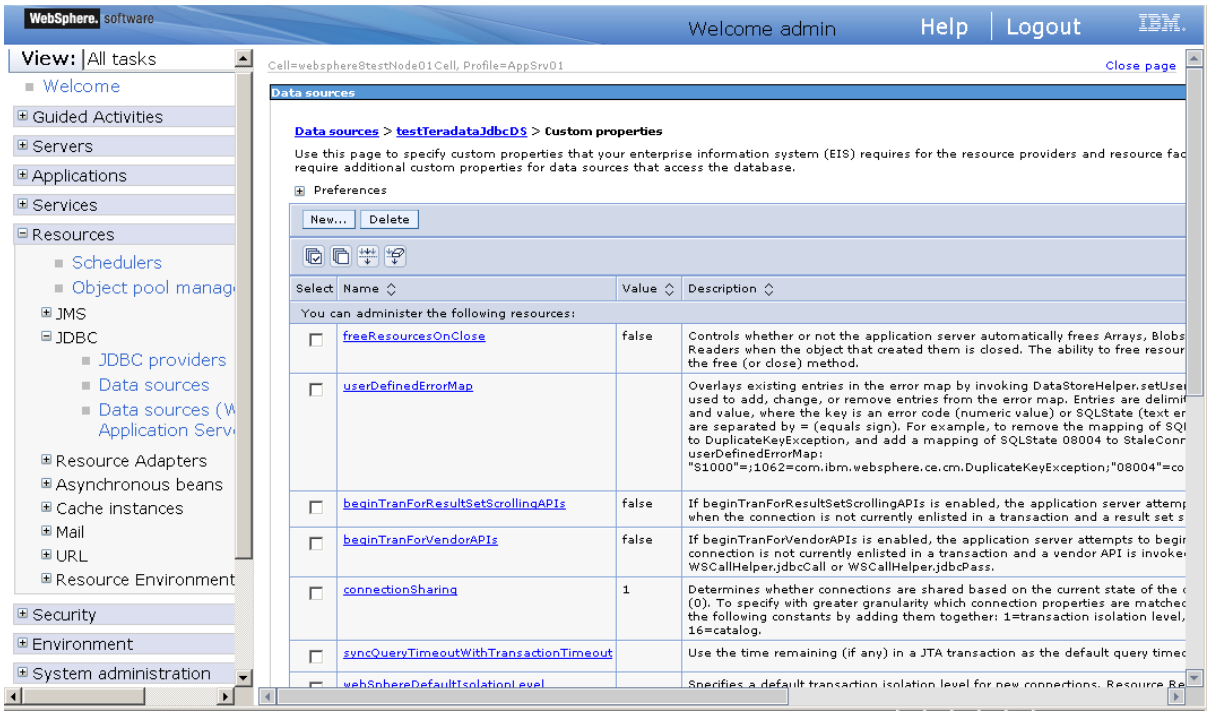
Step 10: On the following page, click the link to Custom properties in the Additional Properties of the data source configuration window.

Figure 4.39: The details of the newly created data source information page



Step 11: On the **Custom properties** page, specify the Custom properties and click **Save**.

Figure 4.40: Custom properties page



Fill in details as required in the table below.

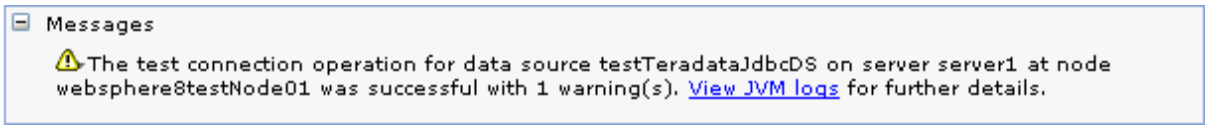
Table 4.12: Custom properties

Name	Description	Value
DSName	Enter a host name or IP address of the database server.	192.0.2.54

Name	Description	Value
USER	Enter the database account user name that you want to use to create the database connections.	DBC
PASSWORD	Enter the database account password that you want to use to create the database connections.	DBC
CHARSET	Enter the session character set utilized to map characters bidirectionally from the client application and the Teradata Database.	UTF8
TMODE	Enter the session mode on a Teradata Database V2R2.0 or later system.	ANSI
account	Enter the database account name that you want to use to create the database connections.	DBC

Step 12: Click **Test Connection** for the new data source. A message will display as follows if the data source is successfully created.

Figure 4.41: Test the connection for the data source



4.3.2.3 Required configurations when global security is on

If the global security mode is turned on in WebSphere, AEM will not be able to access the WebSphere data sources. You can perform the following configurations to resolve this problem.

Step 1: Go to the %user.install.root%\properties directory (%user.install.root% indicates the WebSphere instance installation directory, for example, C:\Program Files\IBM\WebSphere \AppServer\profiles\AppSrv01\), open the sas.client.props file in text editor, and modify the following three properties:

- com.ibm.CORBA.loginUserid: set to the WebSphere account username.
- com.ibm.CORBA.loginPassword: set to the WebSphere account password.
- com.ibm.CORBA.securityServerPort: set to the WebSphere IIOP port, if it is not the default port 2809. You can find out and modify this port number by using the BOOTSTRAP_ADDRESS property in the WebSphere console.

Step 2: Save changes in sas.client.props and then restart WebSphere.

Note: After making the above changes, everytime when a data source is created, you will need to restart WebSphere so the new data source is accessible to AEM.

If the global security mode is turned off, you will need to remove settings of com.ibm.CORBA.loginUserid and com.ibm.CORBA.loginPassword from the sas.client.props file.

4.3.3 Setting up data source for JBoss

4.3.3.1 Setting up data source for WildFly and JBoss EAP

Data source configuration in WildFly 10 and JBoss EAP 6.x is almost the same. Here we take WildFly as am example to show you how to create the data source. You can find more details in the corresponding JBoss Web sites: Datasource configuration for WildFly, and Datasource management for JBoss EAP 6.4.

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

You need to perform two main tasks to define a data source in WildFly and JBoss EAP. First, you must make the JDBC driver available to the application server; then you need to configure the data source that references the driver you installed.

4.3.3.1.1 Installing the JDBC driver

You can install a JDBC driver with the management console or as a Core Module. In this example, we will take the management console approach as an example. If you want to use the Core Module approach, you may refer to the corresponding JBoss documentation.

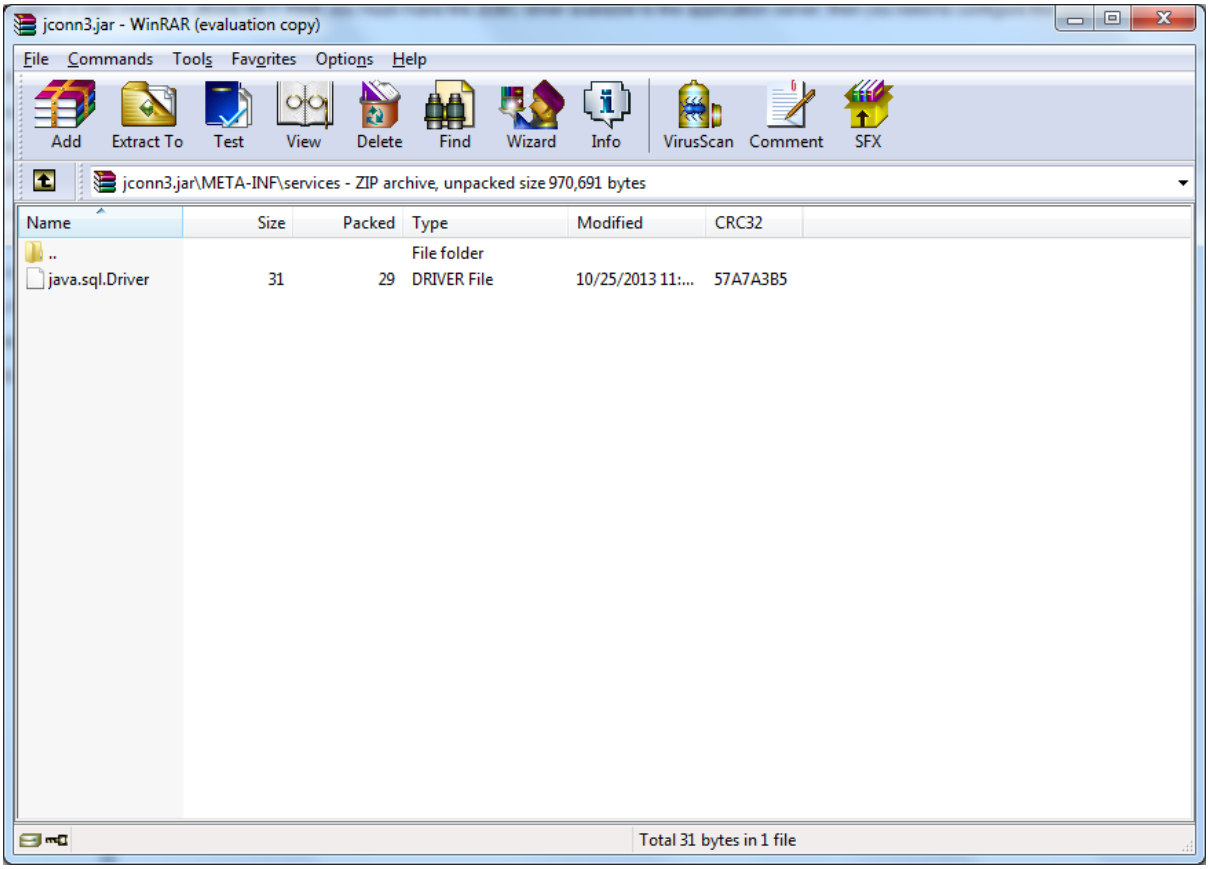
Step 1: Modify the JAR file of the JDBC driver. Take SAP jConnect JDBC driver as an example.

1. Under the same directory as the jconn3.jar file, create a "**META-INF**" subdirectory and a "**META-INF\services**" subdirectory.

2. Under the "**META-INF\services**" directory, create a **java.sql.Driver** file which contains one line - the fully-qualified class name of the JDBC driver, in this example, **com.sybase.jdbc3.jdbc.SybDriver**.

3. Execute the "**jar**" command to update the JAR file: "**jar -uf jconn3.jar META-INF/services/java.sql.Driver**". You can also use WinRAR tool to add the **META-INF\services\java.sql.Driver** directory and file to jconn3.jar, as shown in the following figure.

Figure 4.42: Modify the JAR file

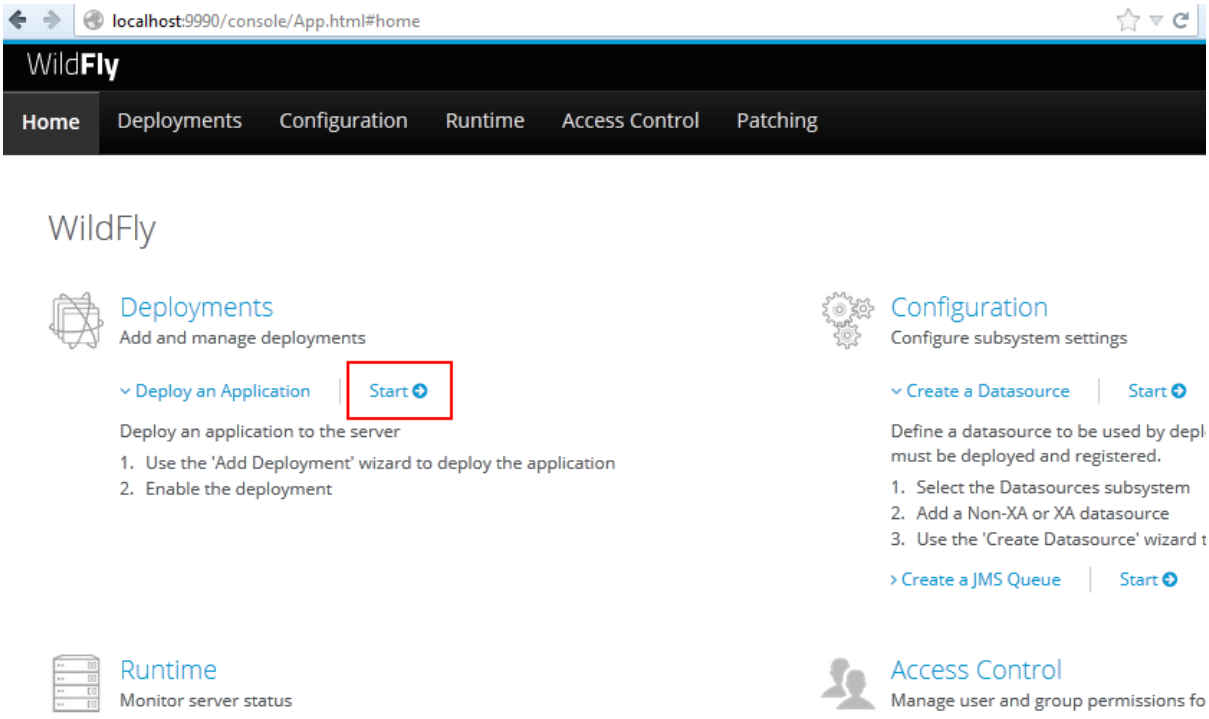


Step 2: Deploy the modified JAR file.

1. Log into the WildFly management console.

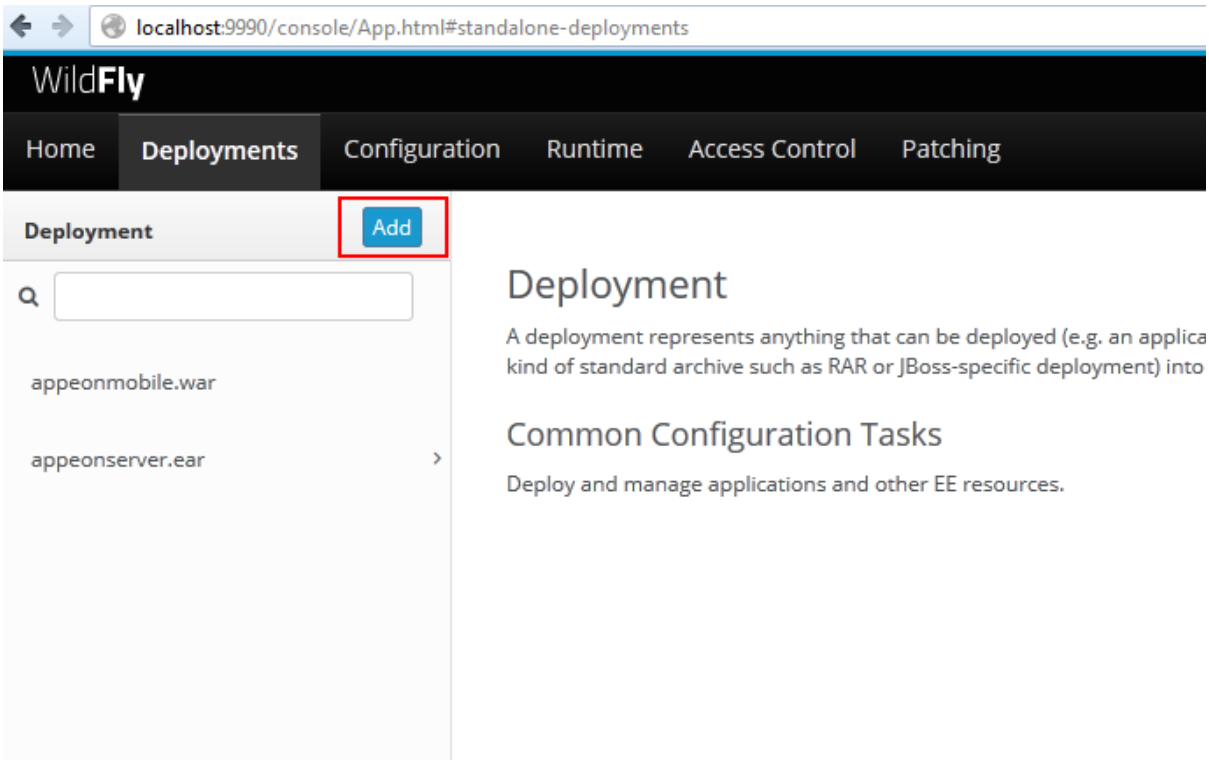
2. Click **Start** for **Deploy an Application** on the home page.

Figure 4.43: Start to deploy the JAR file



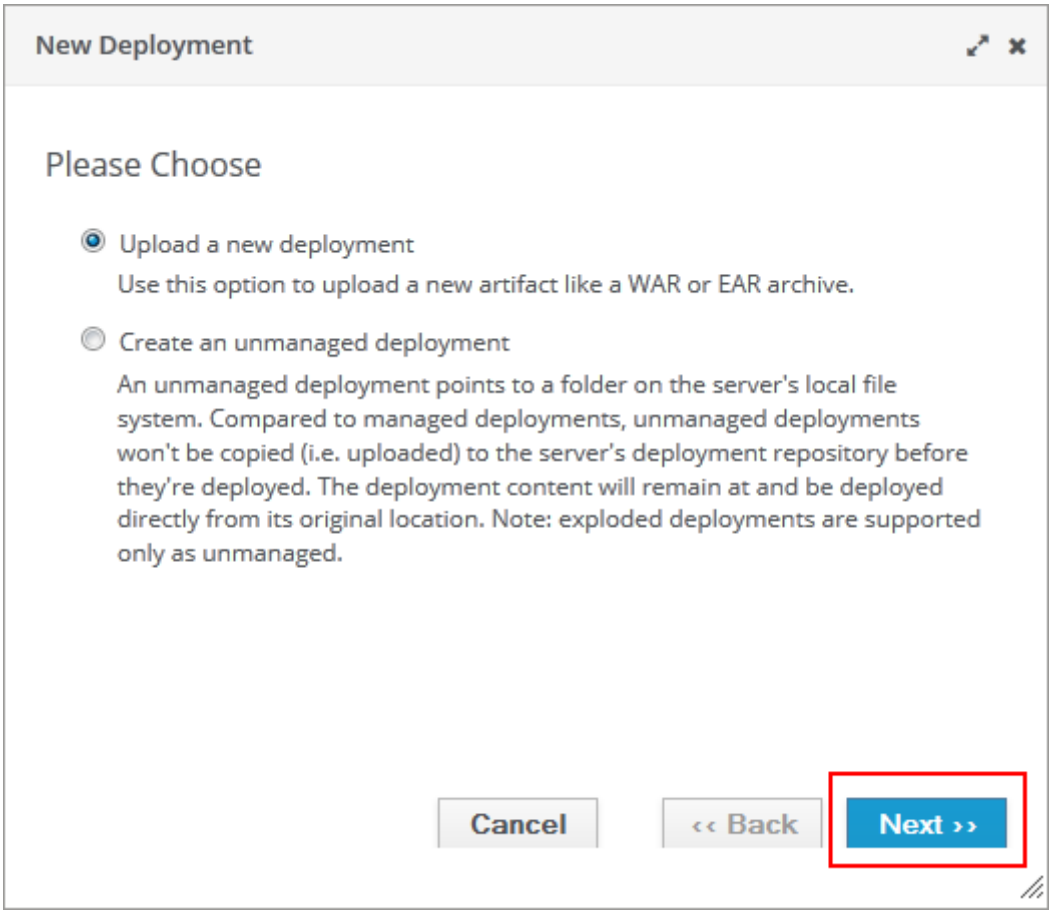
3. Click the **Add** button on the deployment page. The **New Deployment** wizard starts.

Figure 4.44: Add the JAR file



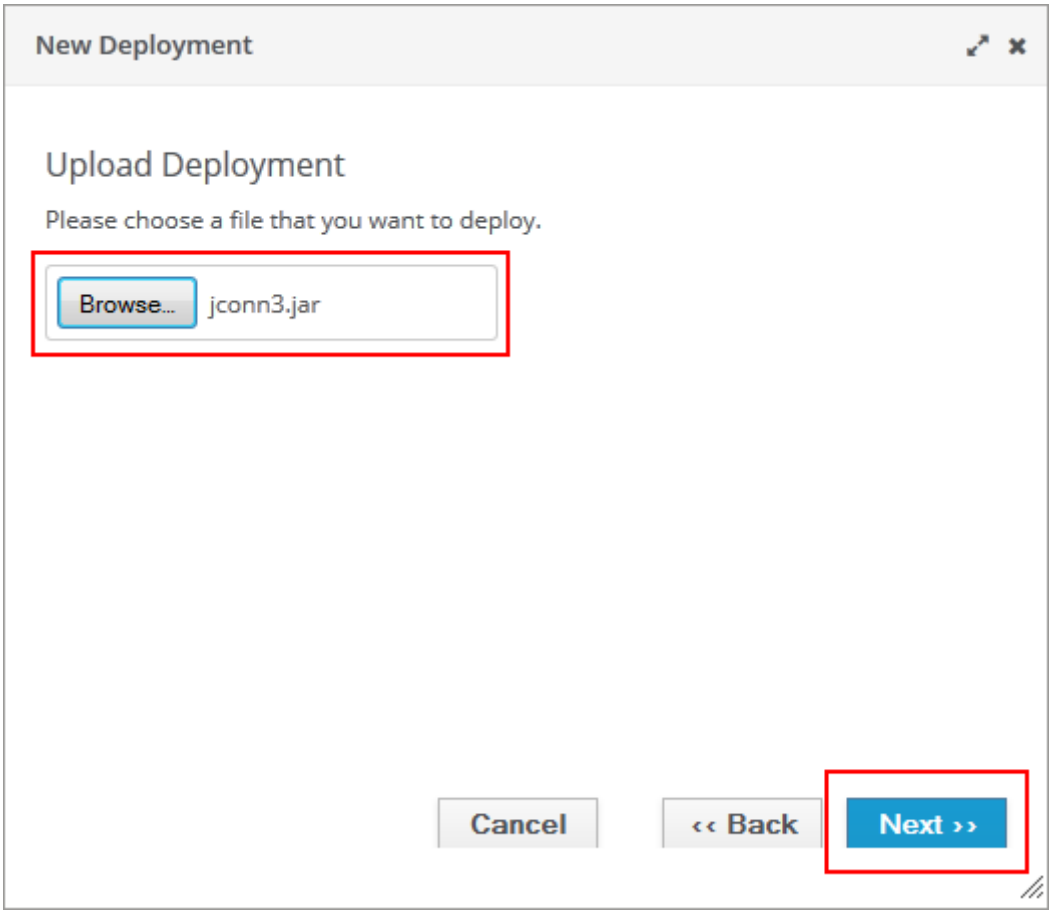
4. In the **New Deployment** Wizard, keep the default option "**Upload a new deployment**" and click **Next**.

Figure 4.45: New Deployment wizard



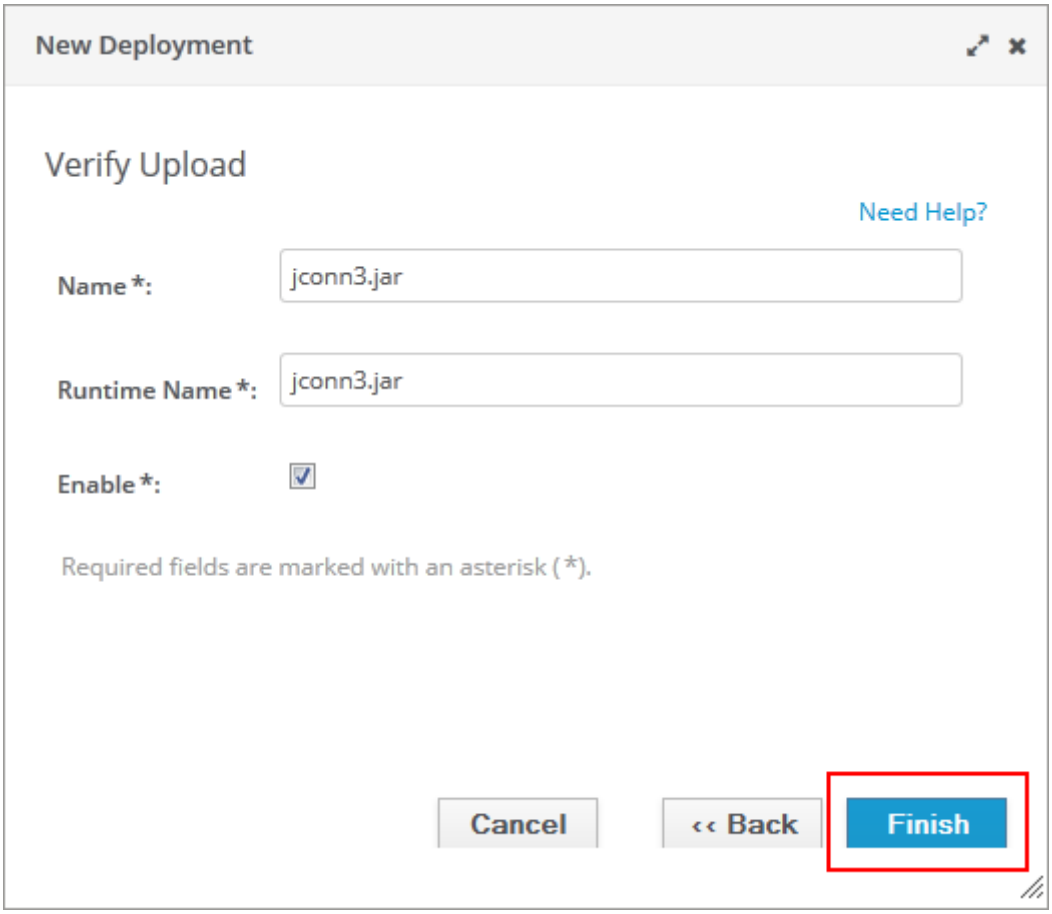
5. Click **Browse** to select the modified JAR file and click **Next**.

Figure 4.46: New Deployment wizard



6. Verify the deployment settings for the JAR file and click **Finish**.

Figure 4.47: New Deployment wizard



7. When deployment is successful, you will be able to see the message "jconn3.jar deployed successfully" and jconn3.jar listed on the deployment page.

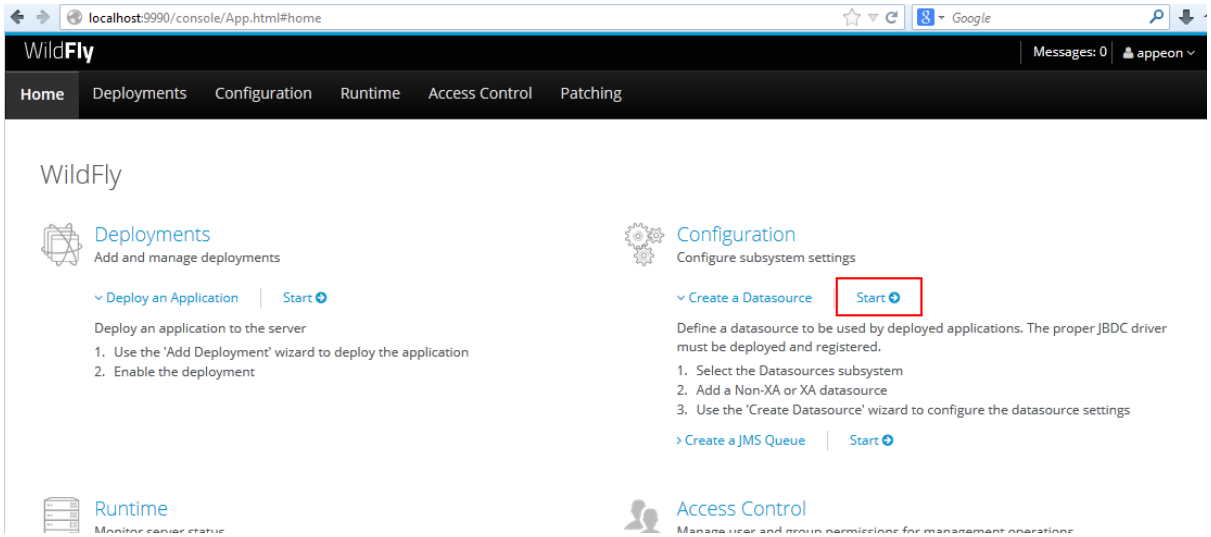
Step 3: Wait a few minutes for the JAR file to be detected and listed in the driver list by WildFly or restart WildFly application server to make the JAR file detected and listed immediately.

4.3.3.1.2 Configuring the data source

You can configure a data source with the management console or the configuration file. In this example, we will take the management console approach as an example. If you want to use the configuration file approach, you may refer to the corresponding JBoss documentation.

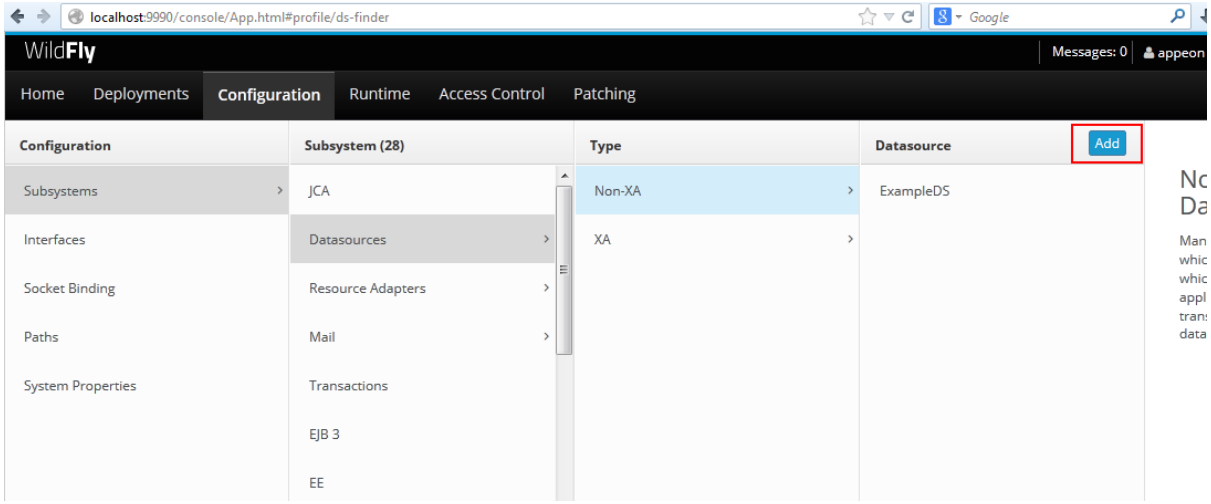
Step 1: On the home page of WildFly management console, click **Start** for **Create a Datasource**.

Figure 4.48: Start to create a new data source



Step 2: On the **Configuration** page, select **Subsystems** > **Datasources** > **Non-XA**, and then click **Add**.

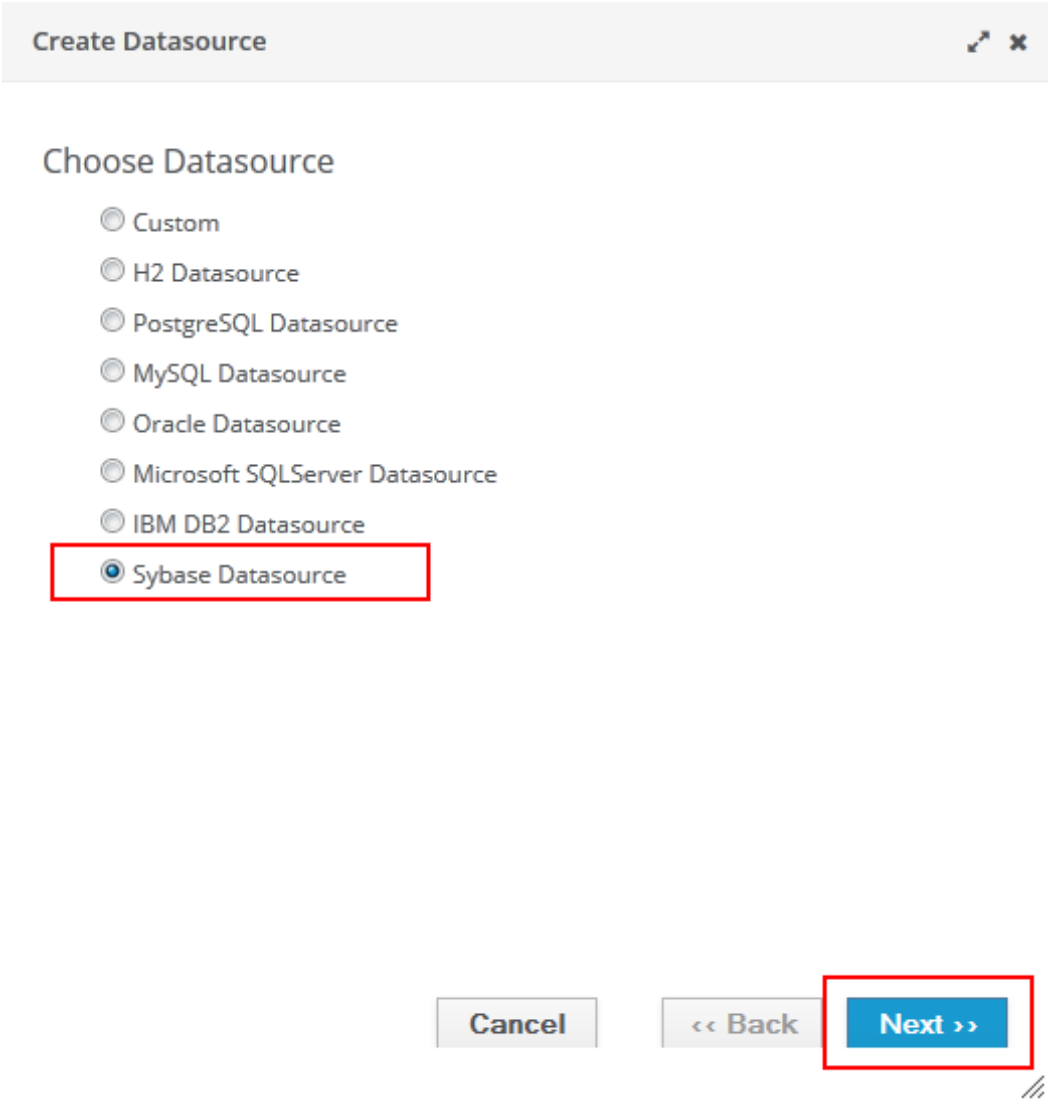
Figure 4.49: Start to create a new data source



Step 3: The **Create Datasource** wizard starts to guide you through creating a data source.

1. Select the data source type. In this example, select **Sybase Datasource** and click **Next**.

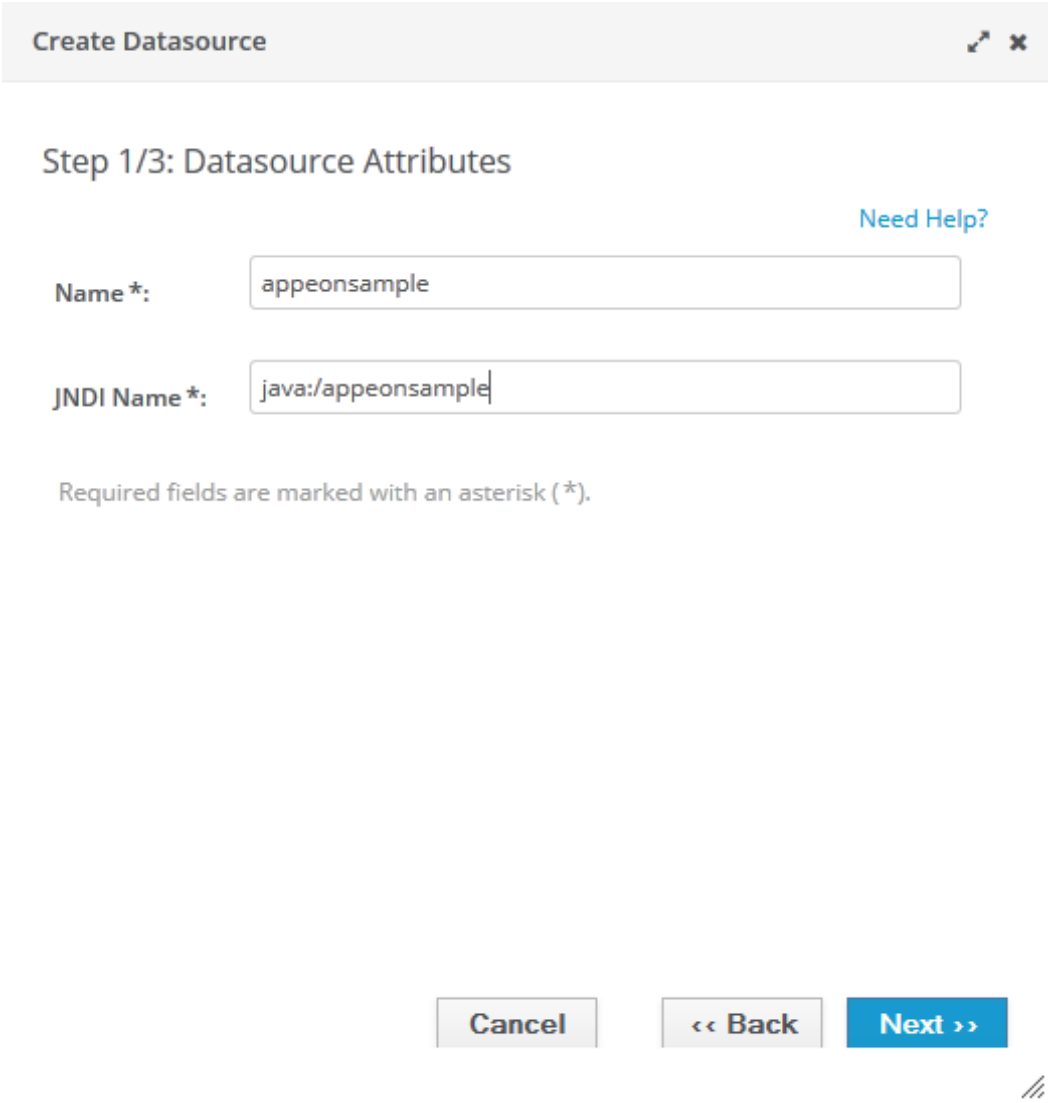
Figure 4.50: Select the data source type



2. Input any text as the data source name and the JNDI name. For example, "java:/appeonsample". Click **Next**.

   Note: The JNDI name will be used as the data source name in AEM.

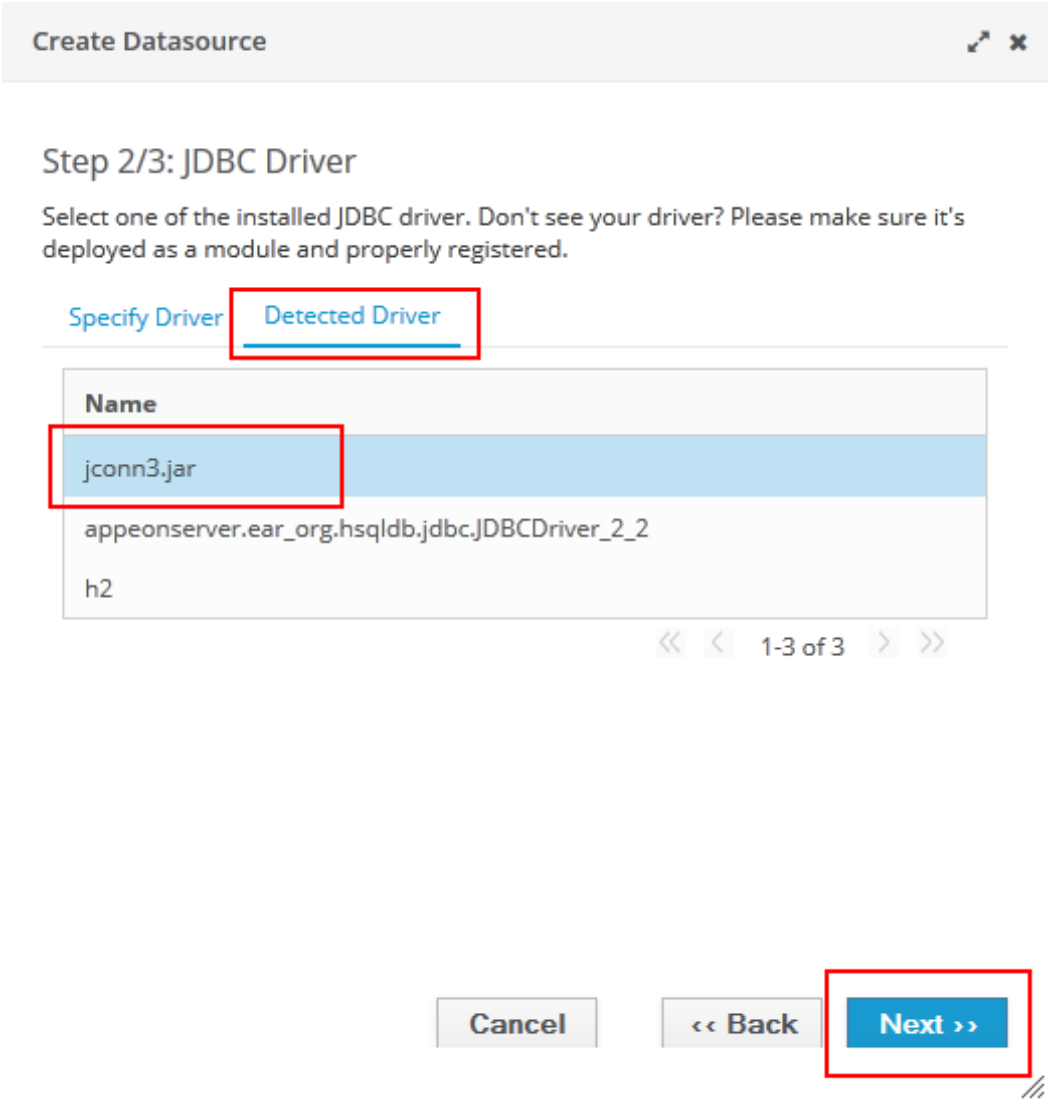
Figure 4.51: Specify the data source attributes



3. Click **Detected Driver**, and then select the JDBC driver, in this example, jconn3.jar. Click **Next**.

   If you do not see the driver, make sure you have installed the driver by following instructions in Installing the JDBC driver.

Figure 4.52: Specify the JDBC driver



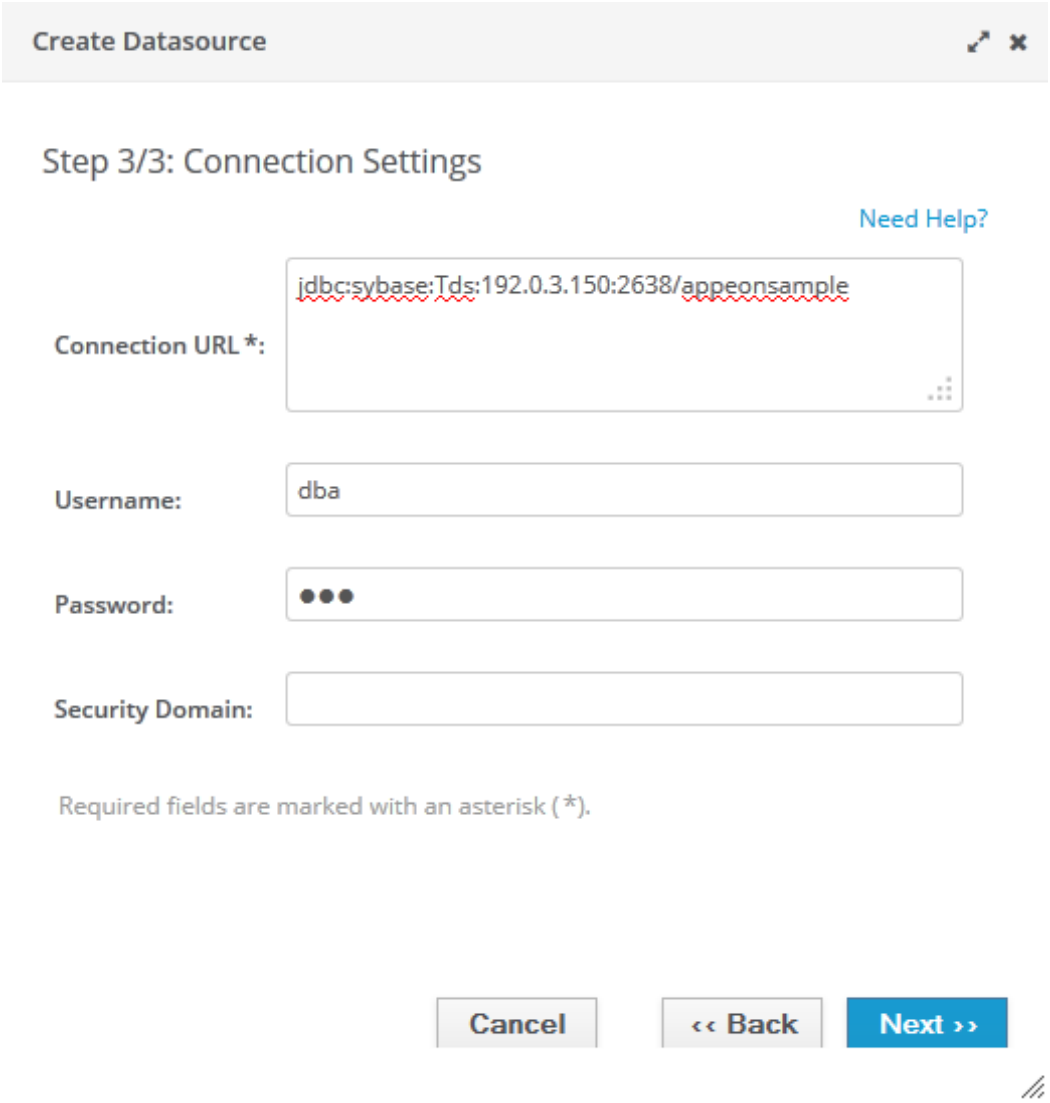
4. Specify the connection information and click **Next**.

   The following table describes how to specify the connection information for SAP SQL Anywhere databases. The values are different according to database types. You can refer to Data source parameters.

Table 4.13: Connection properties

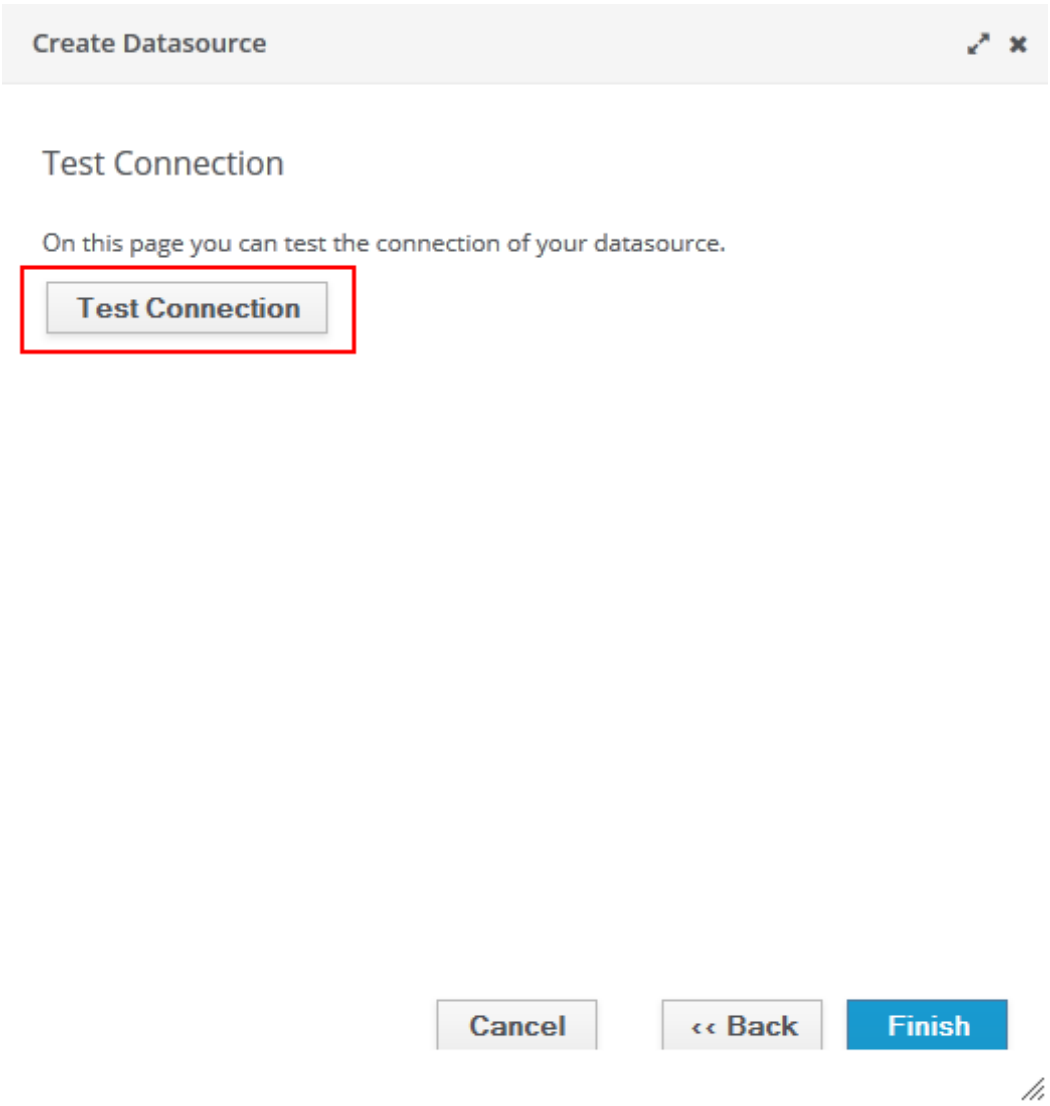
Connection URL	For example, jdbc:sybase:Tds:192.0.3.150:2638/appeonsample
Username	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.

Figure 4.53: Specify the connection information



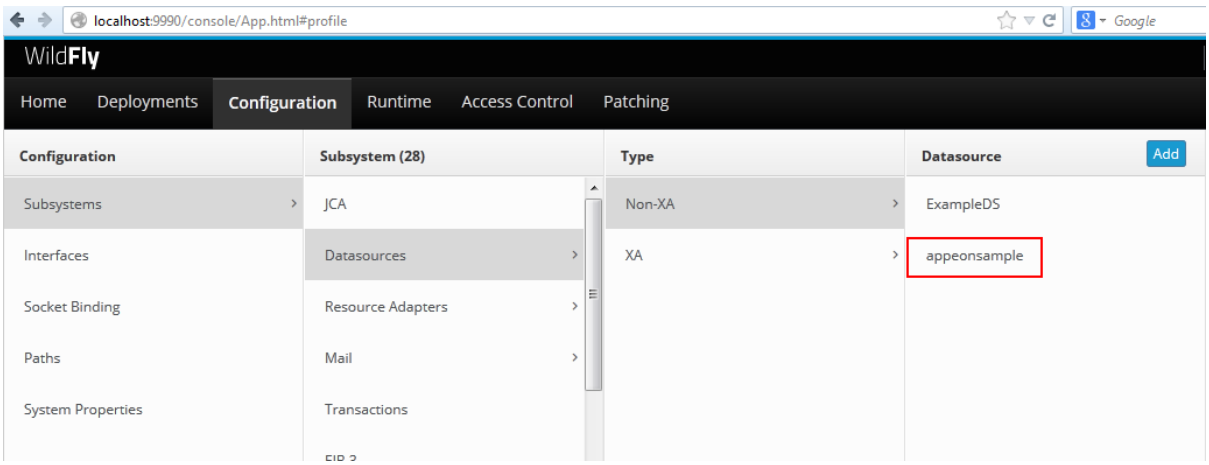
5. Click **Test Connection** to make sure the database can be connected and then click **Finish**.

Figure 4.54: Test the database connection



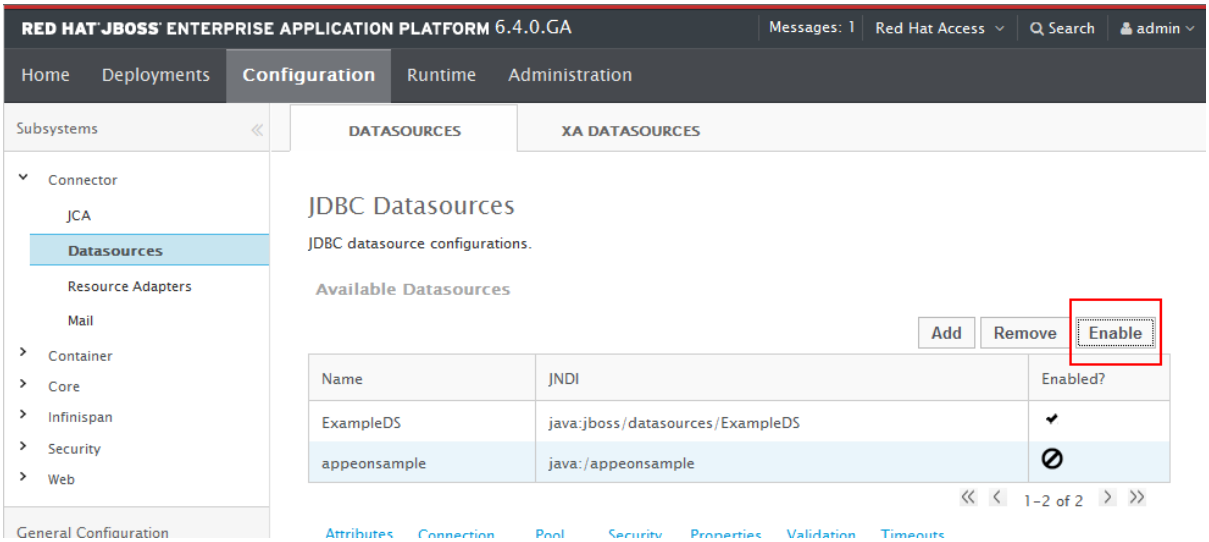
After the data source is created successfully, you will return to the data source page and you will be able to see the new data source in the list.

Figure 4.55: Data source list



In JBoss EAP, you may need to manually enable the newly created data source by clicking the **Enable** button on top of the list.

Figure 4.56: Enable the data source



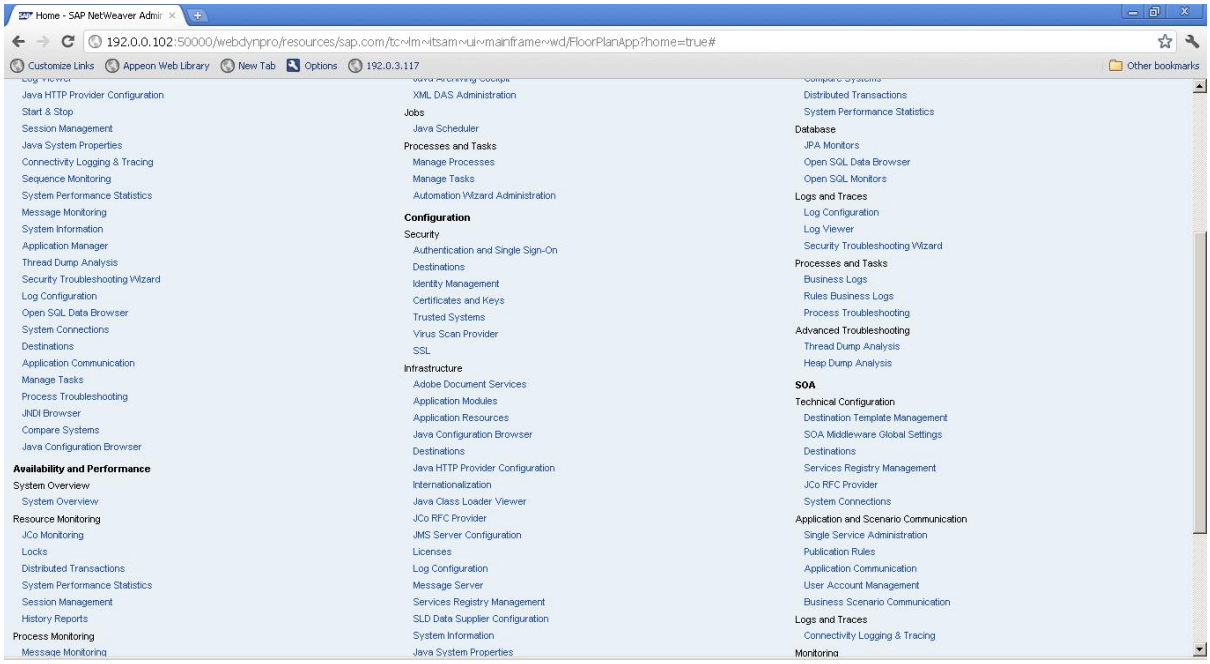
4.3.4 Setting up data source for NetWeaver

The following section will take one database type (SAP HANA database with HANA JDBC driver) as an example to show you how to create a data source for NetWeaver Application Server, you can later create data sources for other database types by taking the same steps below but specifying different parameters according to Data source parameters.

Step 1: Log in to SAP NetWeaver Administrator with the URL http://IP:50000/nwa. The IP here is your server's IP address.

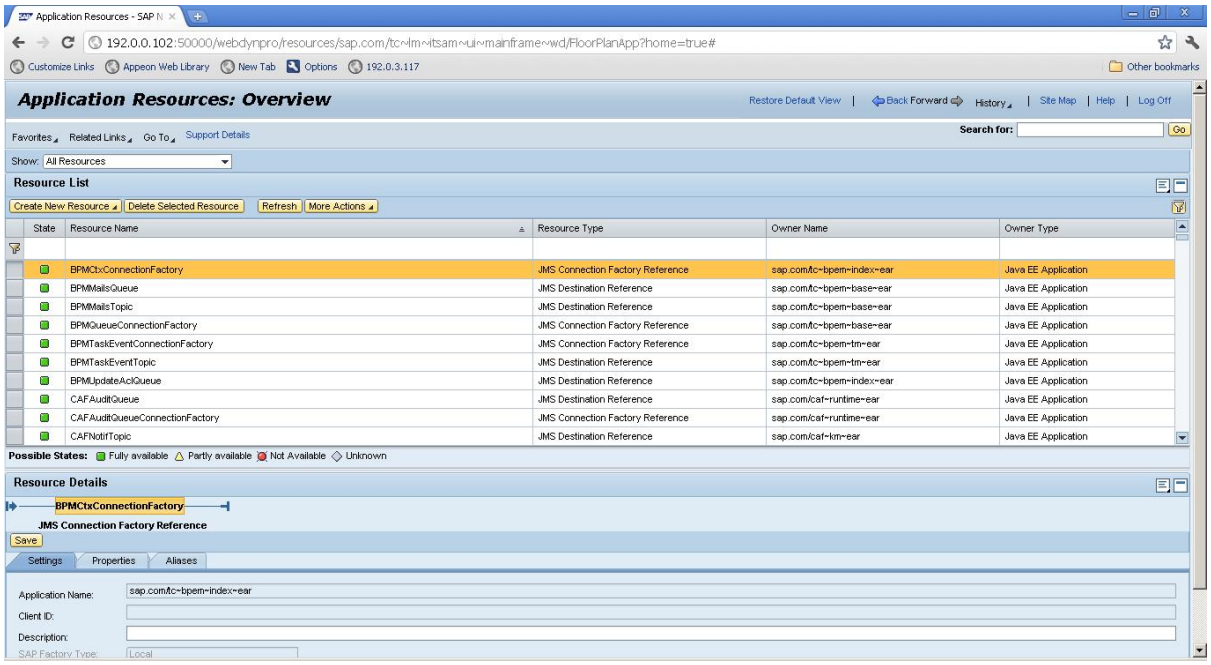
Step 2: Click the **Site Map** in the right top of the page to view site map, as shown in the following figure.

Figure 4.57: View Site Map



Step 3: Click **Application Resources** in the infrastructure of configuration to configure application resources, as shown in the following figure.

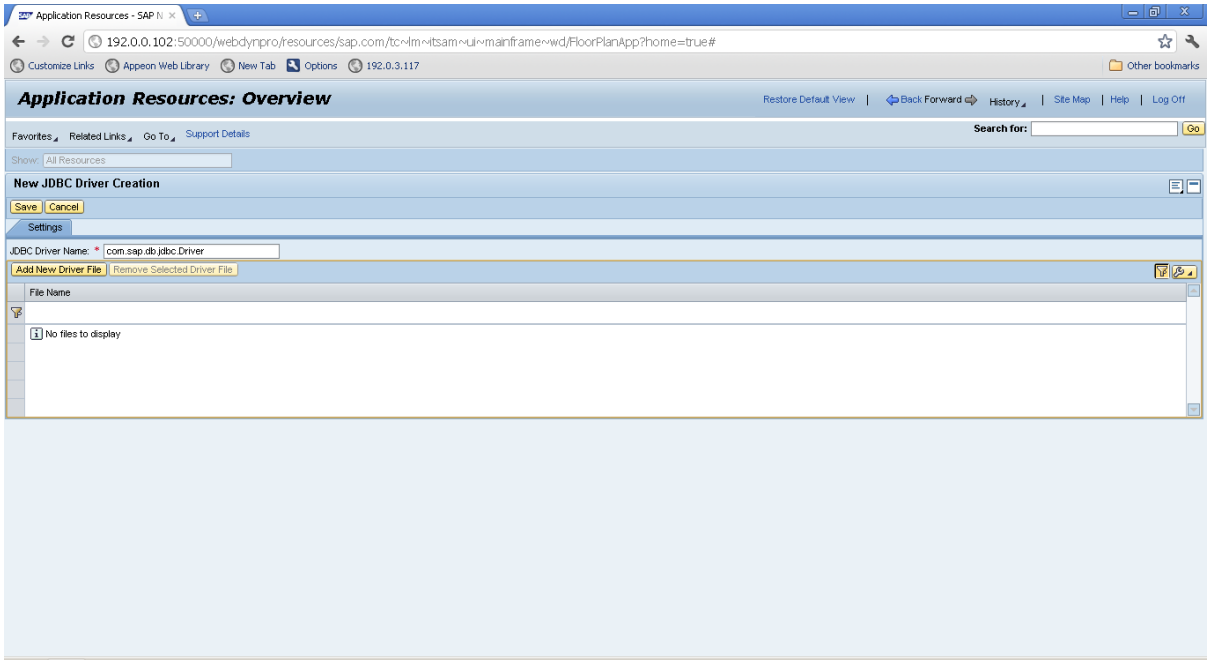
Figure 4.58: Configure Application Resources



Step 4: If it is the first time that you create an SAP HANA database connection in the NetWeaver, you need to deploy the HANA JDBC driver at first.

Click **Create New Resource**, and then select **Deploy New JDBC Driver**. On the page that appears, enter a JDBC driver name in the **JDBC Driver Name** text box. It is required, but you can enter any name, which is only used to identify the type of JDBC drivers. For simplicity, enter “com.sap.db.jdbc.Driver”, and then click **Add New Driver File** to select the JDBC driver jar file. Finally, click **Save** to deploy JDBC driver.

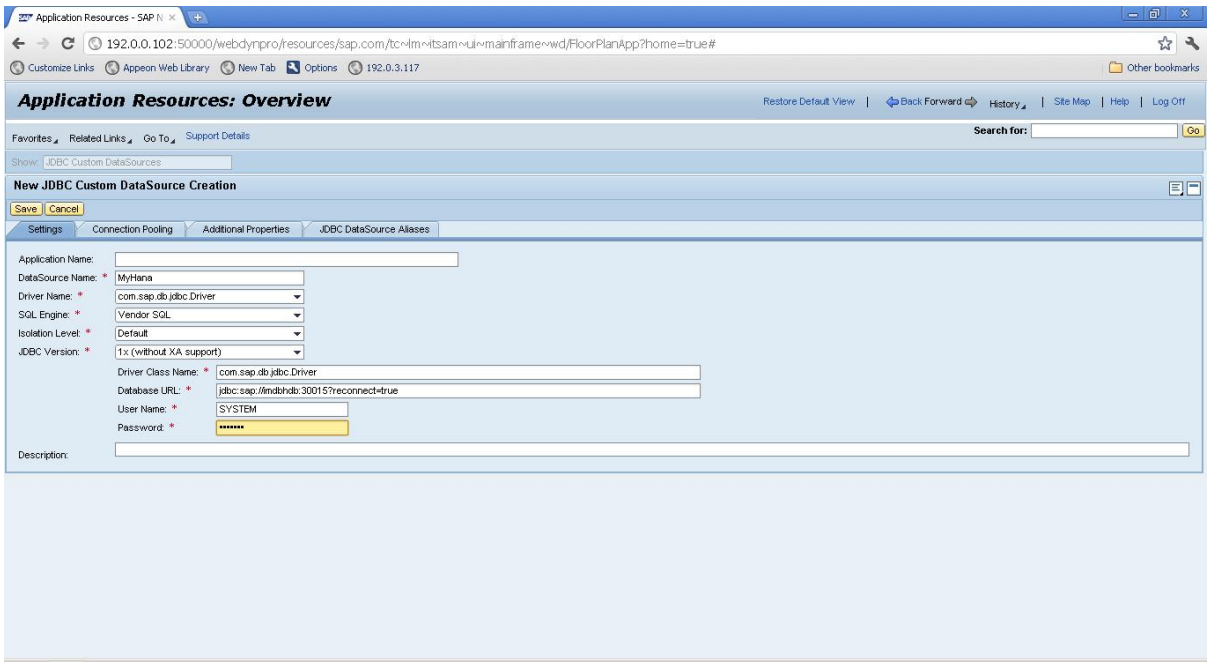
Figure 4.59: Deploy New JDBC Driver



Step 5: After the JDBC driver is deployed successfully, click **Create New Resource** and then select **New JDBC Custom DataSource** to create a new database connection. On the page that appears, do the following:

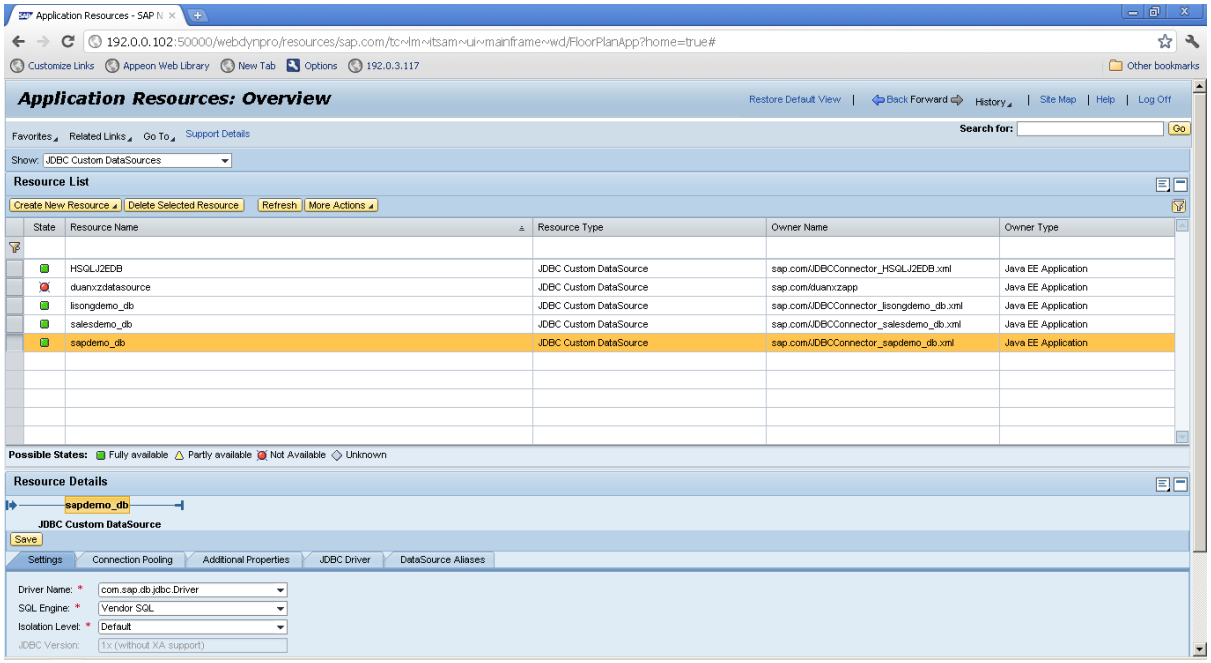
1. In the **Database Name** text box, Enter a DataSource name;
2. In the **Diver Name** dropdown list box, select the correct **Driver Name**;
3. In the **SQL Engine** dropdown list box, select **Vendor SQL**;
4. In the **Isolation Level** dropdown list box, select **Default**;
5. In **JDBC Version** dropdown list box, select **1x (without XA support)**;
6. In **Driver Class Name** text box, enter “com.sap.db.jdbc.Driver”;
7. In **Database URL** text box, enter "jdbc:sap://Host:Port?reconnect=true", for example, enter "jdbc:sap://imdbhdb:30015?reconnect=true".
8. In the **User Name** text box, enter the correct user name, and in the **Password** text box, enter the correct password;
9. Click **Save** to finish creating a database connection.

Figure 4.60: New JDBC Custom DataSource Creation



Step 6: To verify whether it is created successfully, select **JDBC Custom DataSource**, and you can see a list of database connections. If the state of the database connection is a green icon, then it indicates that the database connection is created successfully.

Figure 4.61: Database Connection State



4.3.5 Setting up data source for JEUS

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 JEUS, you can later create data sources for other database types by taking the same steps below but specifying different parameters according to Data source parameters.

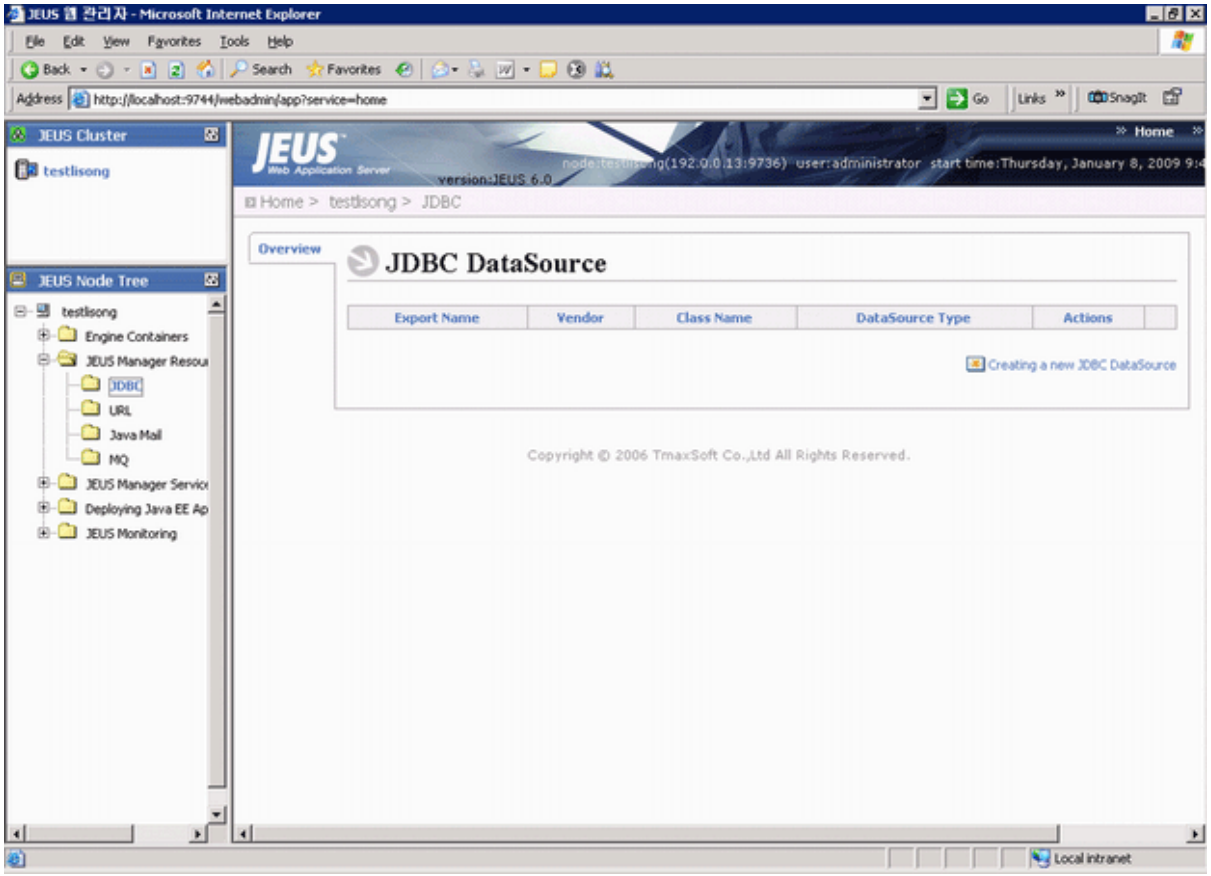
Detailed steps are as below:

Step 1: Start JEUS and log on to the JEUS Manager.

Step 2: Click the node name: **JEUS Manager Resources** > **JDBC** in the JEUS Node Tree.

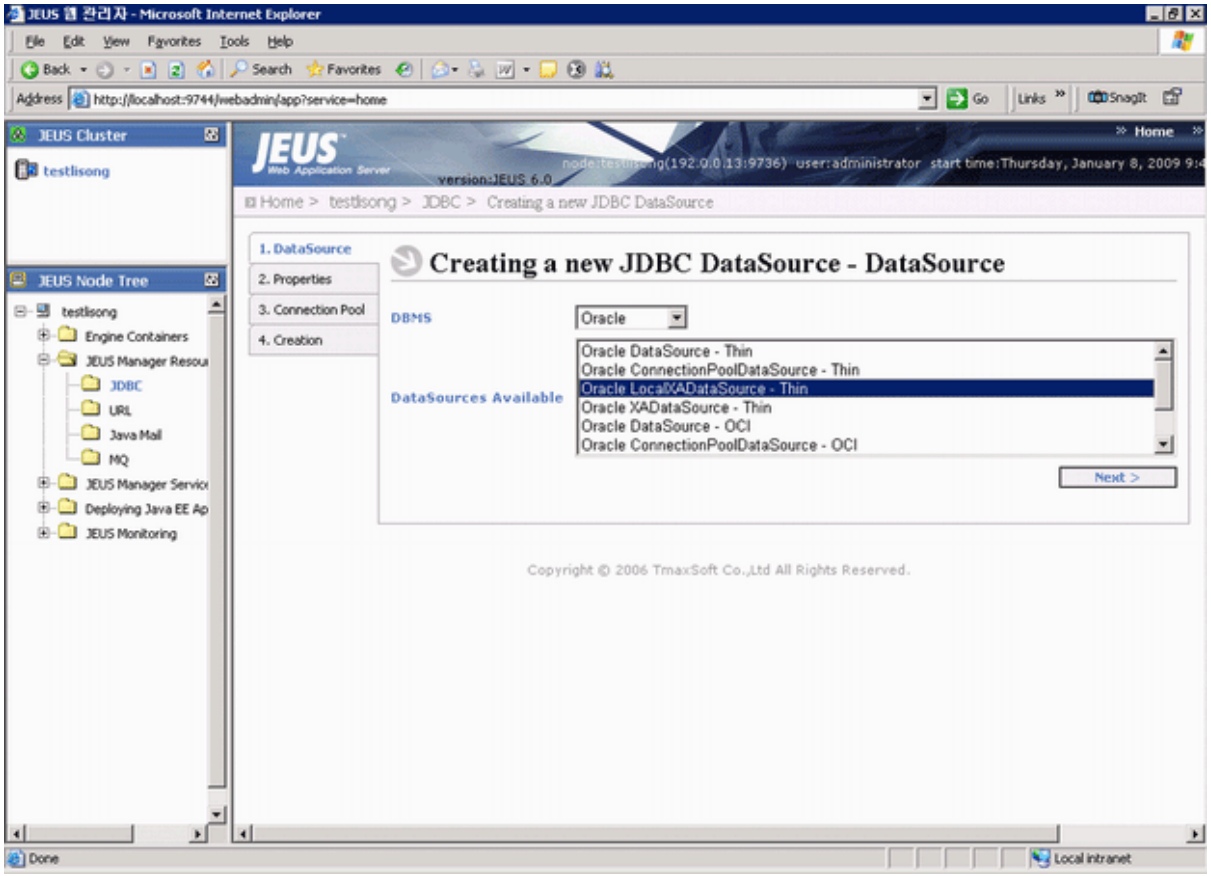
Step 3: Click **Creating a new JDBC DataSource**.

Figure 4.62: JDBC DataSource page



Step 4: In the **DBMS** dropdown list box, select **Oracle**, and in the **DataSources Available** list box, select **Oracle LocalXADataSource -- Thin**.

Figure 4.63: Creating a new JDBC DataSource page

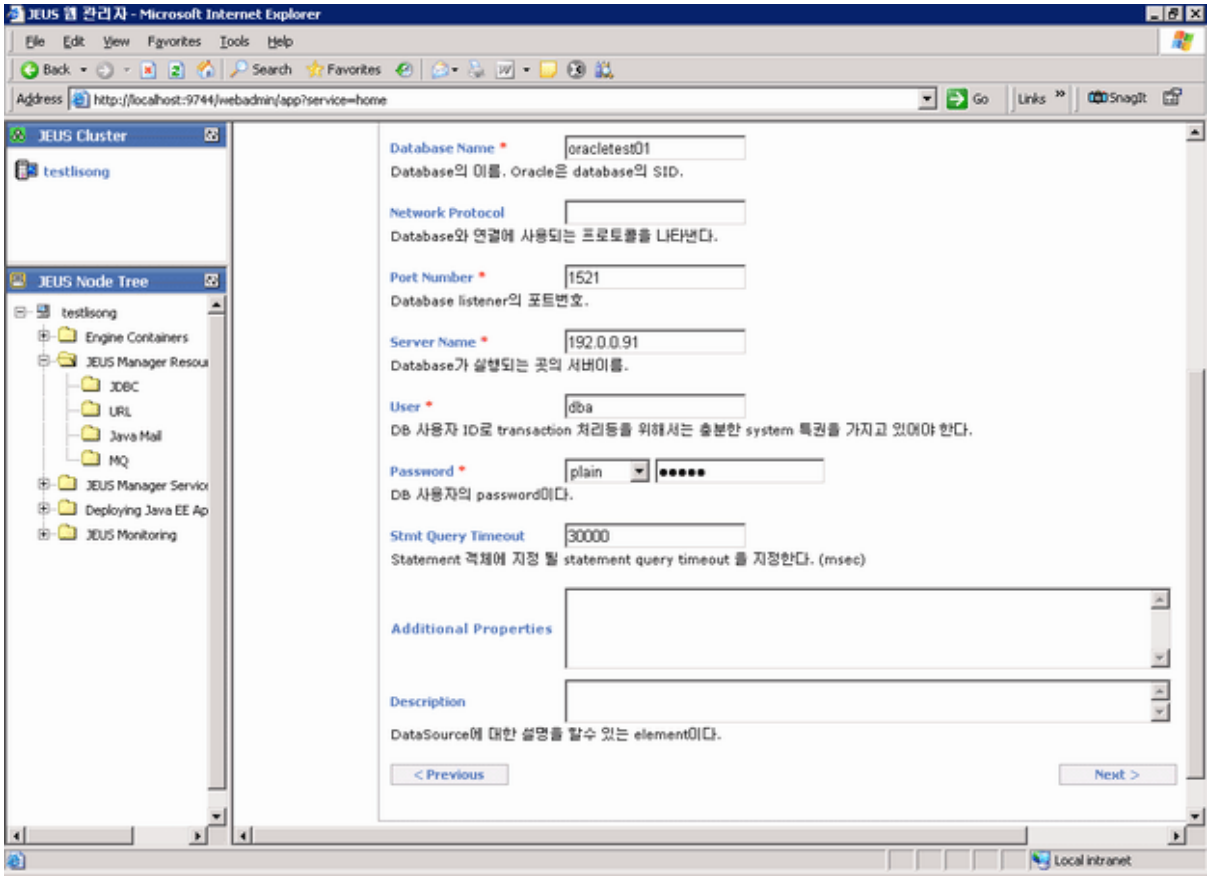


You must select LocalXADataSource or XADataSource. LocalXADataSource is preferable to XADataSource because it improves the application performance. For SQL Anywhere databases, you can only select LocalXADataSource. Following are the recommended datasources for different database drivers:

- MS SQL Server 2000 JDBC driver: MS-SQ LocalXADataSource
- MS SQL Server 2005 JDBC driver: Custom DataSource
- jTDS/IBM JDBC Driver: BlackBox LocalXADataSource
- Oracle JDBC driver: Oracle LocalXADataSource -- Thin, or Oracle XADataSource -- Thin
- jConnect: SAP jConnect 5.5 LocalXADataSource

Step 5: Specify the datasource properties and click **Next** twice.

Figure 4.64: Datasource properties page



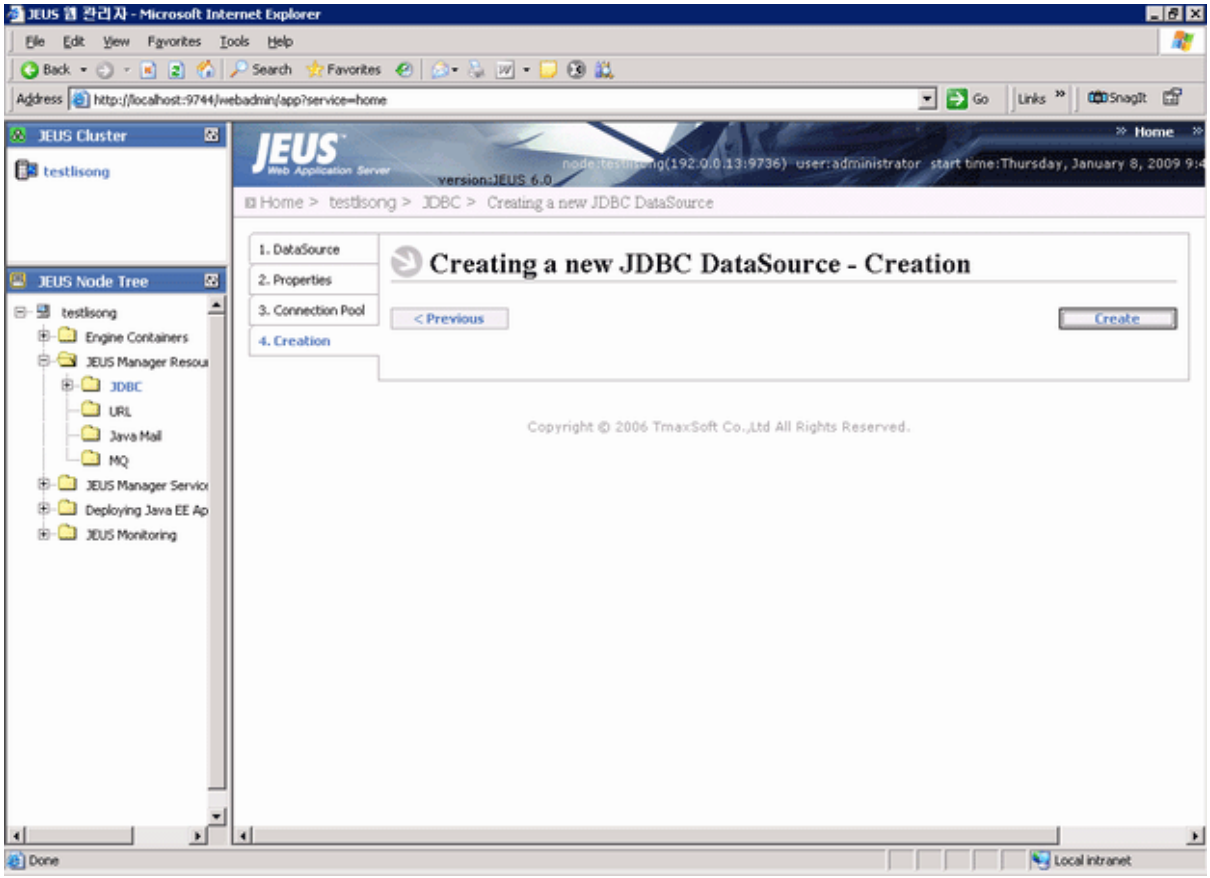
The following table lists instructions for how to specify the properties for a datasource.

Table 4.14: Datasource properties

Export Name	Input any text as the datasource name. For example, "oracle_datasource1". This name will be recognized as the data source name in AEM.
Database Name	Type the database name. For example, "oracletest01".
Port Number	Type the database port. The default port is 1521.
Server Name	Type the database server name. For example, 192.0.0.91.
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. If the password has no effect in the Password field, input "password=password" to the Additional Properties box.

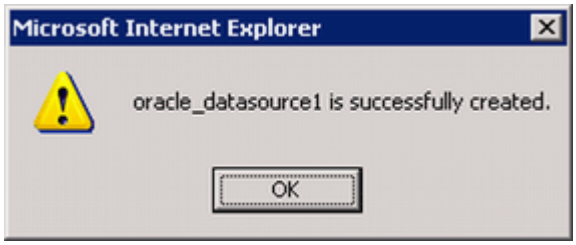
Step 6: Click **Create** and ensure that the JDBC data source is successfully created.

Figure 4.65: Create a new JDBC DataSource page



A message pops up if the JDBC data source is successfully created.

Figure 4.66: Datasource successfully created



4.3.6 Data source parameters

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, WebSphere, JBoss, JEUS, and NetWeaver.

Note that the values of driver class name and Database URL are case sensitive.

4.3.6.1 Data source parameters for SAP SQL Anywhere

SAP SQL Anywhere databases support jConnect (recommended), iAnywhere JDBC-ODBC, and Sun JDBC-ODBC bridge. jConnect is preferable than iAnywhere JDBC-ODBC and Sun JDBC-ODBC bridge because it delivers much better performance at runtime. However, the Appeon Demo uses the Sun JDBC-ODBC bridge because this driver can be automatically configured by the Appeon installation program.

Note:

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

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

3) jConnect 6.0 is preferable to jConnect 5.5.

Table 4.15: Data source parameters for SAP SQL Anywhere

Driver	Parameter	Value	Note
jConnect JDBC driver (Recommended)	Driver class 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 SQL Anywhere port is 2638. *ServiceName* stands for the name of the SQL Anywhere database service specified during configuration. *DSNname* refers to the name of the ODBC DSN that is created for the database.
	Database URL	jdbc:sybase:Tds:Hostname:Port/ServiceName	
iAnywhere JDBC-ODBC driver	Driver class name	For JDBC 2.0: ianywhere.ml.jdbcodbc.IDriver For JDBC 3.0: ianywhere.ml.jdbcodbc.jdbc3.IDriver	
	Database URL	jdbc:odbc:dsn=*DSNname*	
Sun JDBC-ODBC driver	Driver class name	sun.jdbc.odbc.JdbcOdbcDriver	
	Database URL	jdbc:odbc:*DSNname*	

Driver	Parameter	Value	Note
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.)		

4.3.6.2 Data source parameters for ASE

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

Table 4.16: Data source parameters for ASE

Parameter	Value	Note
Driver class 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.
Database URL	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.)	

4.3.6.3 Data source parameters for SAP IQ

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

Table 4.17: Data source parameters for SAP IQ

Driver	Parameter	Value	Note
JConnect JDBC driver (Recommended)	Driver class 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.
	Database URL	jdbc:sybase:Tds:*Hostname*:*Port*/*ServiceName*	
Sun JDBC-ODBC driver	Driver class name	sun.jdbc.odbc.JdbcOdbcDriver	
	Database URL	jdbc:odbc:*DSNname*	

Driver	Parameter	Value	Note
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.)		

4.3.6.4 Data source parameters for SAP HANA

SAP HANA databases support SAP In-Memory Database JDBC driver.

Table 4.18: Data source parameters for SAP HANA

Driver	Parameter	Value	Note
SAP In-Memory Database JDBC driver	Driver class name	com.sap.db.jdbc.Driver	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port.
	Database URL	jdbc:sap://Host:Port?reconnect=true	
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.)		

4.3.6.5 Data source parameters for Microsoft SQL Server

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

Table 4.19: Data source parameters for Microsoft SQL Server

Driver	Parameter	Value	Note
jTDS JDBC driver (Recommended)	Driver class name	net.sourceforge.jtds.jdbc.Driver	*Hostname* stands for the database server name or IP address. *Port* stands for the database server port. The default SQL Server port is 1433. *DBName* stands for the name of the database to which the data source connects. "SelectMethod=cursor" must be specified, otherwise errors will occur when inserting data.
	XA datasource class	net.sourceforge.jtds.jdbcx.JtdsDataSource	
	Database URL	jdbc:jtds:sqlserver://*Hostname*:*Port*/;DatabaseName=*DBName*;SelectMethod=cursor	
WebLogic SQL Server JDBC driver (for WebLogic server only)	Driver class name	weblogic.jdbc.sqlserver.SQLServerDriver	
	Database URL	jdbc:bea:sqlserver://*Hostname*:*Port*	

Driver	Parameter	Value	Note
Microsoft SQL Server JDBC driver	Driver class name	com.microsoft.jdbc.sqlserver.SQLServerDriver	
	Database URL	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.)		

4.3.6.6 Data source parameters for Oracle

Oracle databases support the Oracle JDBC driver only.

Table 4.20: Data source parameters for Oracle

Parameter	Value	Note
Driver class 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.
Database URL	jdbc:oracle:thin:@*hostname*:*port*:*DBName* for Oracle 9i, 10g, and 11g jdbc:oracle:thin:@//*hostname*:*port*/*DBName* for Oracle 12c	
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.)	

4.3.6.7 Data source parameters for IBM DB2

IBM DB2 databases support the IBM JDBC driver only.

Table 4.21: Data source parameters for IBM DB2

Parameter	Value	Note
Driver class 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
Database URL	jdbc:db2://*Hostname*:*Port*/*DBName*	

Parameter	Value	Note
		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.
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.)	

4.3.6.8 Data source parameters for Informix

Informix databases support the IBM Informix JDBC driver only.

Table 4.22: Data source parameters for Informix

Parameter	Value	Note
Driver class 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.
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	
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.)	

4.3.6.9 Data source parameters for MySQL

MySQL databases support MySQL Connector/J driver. Different servers use different driver class names. See the following table for details.

Table 4.23: Data source parameters for MySQL

Application Server	Paramete	Value	Note
JBoss & WebSphere	Driver class name	com.mysql.jdbc.jdbc2.optional.MysqlXADataSource	*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.
	Database URL	jdbc:mysql:*Hostname:Port/ServiceName*	
WebLogic	Driver class name	com.mysql.jdbc.Driver	
	Database URL	jdbc:mysql:*Hostname:Port/ServiceName*	
JEUS	Driver class name	com.mysql.jdbc.jdbc2.optional.MysqlConnection PoolDataSource	
	Database URL	jdbc:mysql:*Hostname:Port/ServiceName*	
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.)		

4.3.6.10 Data source parameters for Teradata

Teradata databases support the Teradata JDBC driver only.

Table 4.24: Data source parameters for Teradata

Parame	Value	Note
Driver class name	For WebLogic/JBoss/JEUS: com.teradata.jdbc.TeraDriver For WebSphere: com.teradata.jdbc.TeraConnectionPoolDataSource	*Hostname* stands for the database server name or IP address. *DBPort* stands for the database server port. The default Teradata port is 1025. *DBName* stands for the name of the database to which the data source connects.
Database URL	jdbc:teradata://*Hostname*/DATABASE=*DBName*, DBS_PORT=*DBPort*,TMODE=ANSI,CHARSET=UTF8	
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.)	

4.3.6.11 Data source parameters for PostgreSQL

PostgreSQL databases support the PostgreSQL JDBC driver only.

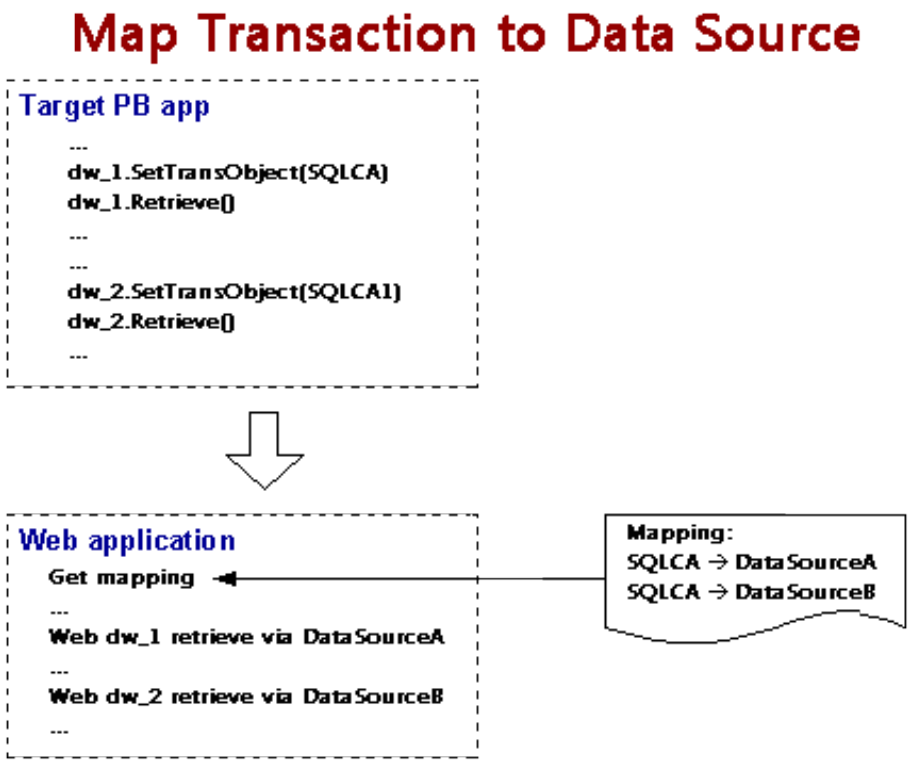
Table 4.25: Data source parameters for PostgreSQL

Parameter	Value	Note
Driver class name	org.postgresql.Driver	*Hostname* stands for the database server name or IP address. *DBPort* stands for the database server port. The default PostgreSQL port is 5432. *DBName* stands for the name of the database to which the data source connects.
Database URL	jdbc:postgresql://*Hostname*:*DBPort*/*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.)	

4.4 Setting up transaction object to data source mapping

The purpose of setting up the mapping is to make sure the configured data source can access the database server for the Appeon Web or mobile application as the replacement of the transaction object in the PowerBuilder application.

Figure 4.67: Map transaction to data source



Once PowerServer data sources are configured, you can set up the transaction object to data source mapping in two different ways:

- Higher priority: Dynamic transaction object to data source mapping via PowerScript.
- Lower priority: Static transaction object to data source 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 data source A via PowerScript and mapped to data source B in AEM, the transaction in effect is mapped to data source A.

Note that if PowerServer is installed to WebLogic, WebSphere, JBoss, NetWeaver Application Server, or JEUS, PowerServer and AEM reads data source JNDI names as data source names.

4.4.1 Dynamic transaction object to data source mapping

Transaction object to data source 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 data source dynamically, code the DBParm property of the Transaction object in this format:

```
SQLCA.DBParm="CacheName='ASEDataSource1'"
```

"ASEDataSource1" can be replaced by the name of the data source 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 the table below.

Table 4.26: Setting the DBMS property based on the database type

Database Type	ODBC Interface	JDBC Interface	OLE Interface	Native Interface
MS SQL Server	ODB-MSS	JDB-MSS	OLE-MSS	MSS
Oracle 8i	ODB-O84	JDB-O84	OLE-O84	O84
Oracle 9i	ODB-O90	JDB-O90	OLE-O90	O90
Oracle 10g/11g	ODB-O10	JDB-O10	OLE-O10	O10
SAP ASE	ODB-SYC	JDB-SYC	OLE-SYC	SYC
SAP SQL Anywhere	ODB-ASA	JDB-ASA	OLE-ASA	-
SAP IQ	ODB-SYI	JDB-SYI	OLE-SYI	-
SAP HANA	ODB-HAN	JDB-HAN	-	-

Database Type	ODBC Interface	JDBC Interface	OLE Interface	Native Interface
IBM DB2 UDB	ODB-DB2	JDB-DB2	OLE-DB2	DIR
Informix	ODB-IN9	JDB-IN9	OLE-IN9	IN9
MySQL	ODB-MYS	JDB-MYS	-	-
Teradata	ODB-TER	JDB-TER	-	-
PostgreSQL	ODB-PGS	JDB-PGS	OLE-PGS	PGS
Other	ODB-Oth	JDB-Oth	OLE-Oth	Oth

In the table above:

- 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 SQL Anywhere. 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 data source mapping

For an Appeon Web or mobile application, you can set up transaction object to data source mapping in the **Applications** settings in AEM. This is a static way for mapping the Transaction object to the data source. For detailed instructions, refer to Transaction Objects.

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

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

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

4.5.1.1 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 and Appeon mobile applications rely on the data sources to interact with the Database Servers. In the Web or mobile application, transaction object to data source 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 data source configuration: the user ID and password of a connection must be pre-configured in AEM or application server console. 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.

4.5.1.1.1 Workaround one: Predefined data sources

You can pre-define in AEM or application server console a certain number of data sources 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 data source mapping to use for establishing the database connection.

You should set up an equal number of data sources in AEM or application server console that connect to the database with different privileges, and map the data sources dynamically using the Transaction DBParm property to the PowerBuilder Transaction objects. Transaction object to data source 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 Dynamic transaction object to data source mapping for the details.

4.5.1.2 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: PowerServer Toolkit deploys the INI files as XML to PowerServer. 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 PowerServer.

- 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 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 the Database Security section.

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 AEM, the Web application that manages the Appeon system and deployed Web or mobile applications. Appeon security is at the application level and is "either or": the user either has or does not have access to the application. By default, Appeon security is turned off for each deployed application.

When the security for a Web or mobile application is turned on, the Appeon Login dialog box pops up at the beginning of the application startup and prompts the user to enter the user name and password. The user name and password are verified by PowerServer 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 application.

For more information on using Appeon security features for Appeon Web or Appeon mobile applications, refer to the Server Security section.

4.5.2.1 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 application runs, the user is prompted to enter the Appeon user name and password in the Appeon Login dialog box.

The Appeon user name can be passed to the application so that it can be utilized to implement script coded security features for the application. You can use the of_getappeonusername function in the Appeon Workarounds PBL to get the Appeon user name. For detailed information, refer to Section 2.3.1, “AppeonExtFuncs Object” in *Workarounds & API Guide*.

4.5.2.2 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 Web applications and Appeon mobile applications run in a three-tier architecture. Each time the Client wants to connect with the database, the call reaches PowerServer first. PowerServer will validate the user ID and password of the call. If the validation passes, PowerServer 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.

4.5.2.2.1 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

AEM is a Web-based application that is automatically installed with PowerServer to manage the PowerServer and the Appeon deployed applications (including both the Web application and the mobile application).

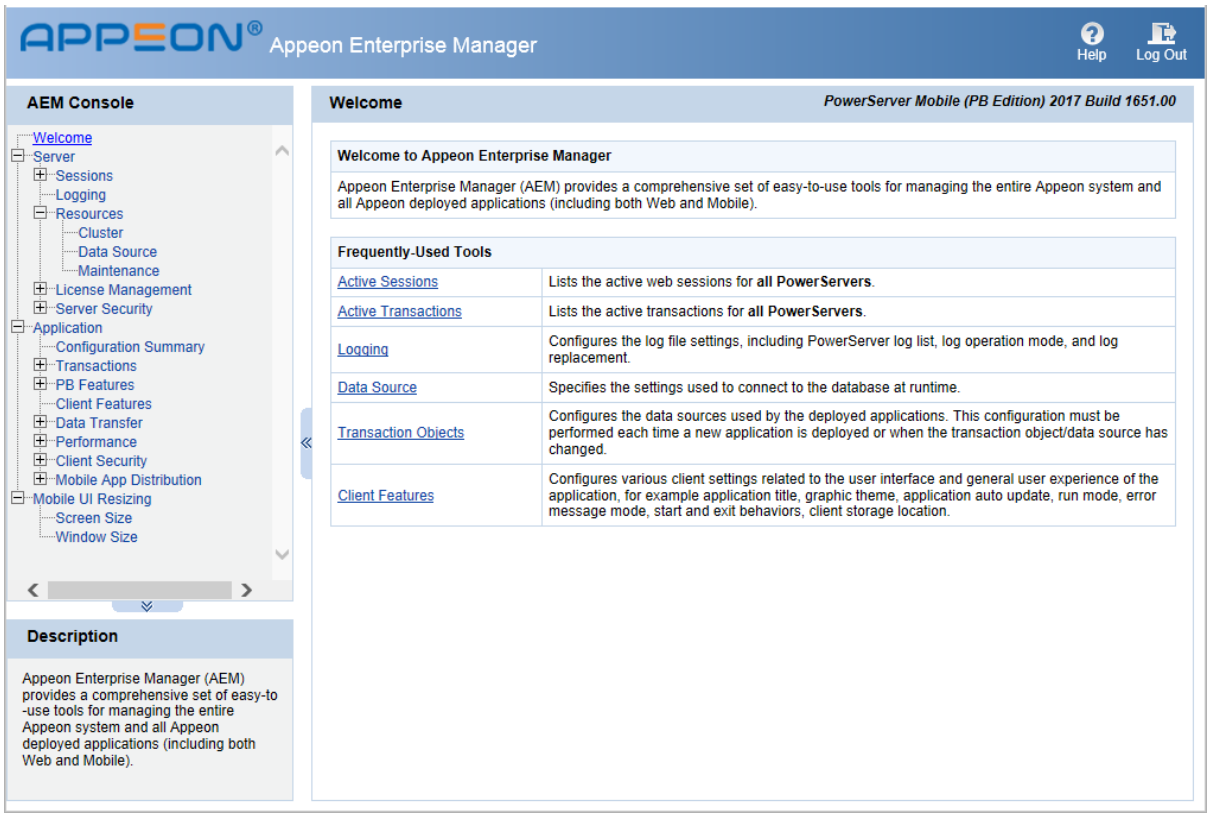
AEM is designed to manage both single-server installations and multiple-server installations with the same ease and power, and it provides an additional layer of security to the existing security already coded into your PowerBuilder applications. It also allows the administrator to use the built-in Appeon 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 <AppeonHome>\repository\<instancename>\config folder. For example, if PowerServer runs on JBoss, the XML files are saved in the %jboss%\appeon\repository\<instancename>\config folder, where %jboss% stands for the installation path of JBoss on the computer.

5.1.2 AEM Tools

AEM contains three sets of tools: Server, Application, and Mobile UI Resizing. After login, you can access each tool from the treeview window on the left.

Figure 5.1: AEM Console



5.1.3 Supported Web browsers

AEM can be viewed on the following Web browsers and versions.

- Microsoft Internet Explorer 10/11
- Google Chrome 35 or later

Considering that Web browsers are usually downward compatible, versions higher than the above listed may also be supported.

If you view your AEM using Web browsers other than those listed above, you may run into errors, such as that UI cannot be displayed properly or some functions may not be available.

5.2 Getting started

5.2.1 Running PowerServer

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

Start PowerServer, which means starting the application server (JBoss, JEUS, WebLogic, or WebSphere) that PowerServer is installed to.

For example, if PowerServer is installed to JBoss, you can start PowerServer with the following method:

In Windows: choose **Programs** > **Appeon PowerServer 2017** > **PowerServer for JBoss** > **Instances** > *InstanceName* > **Start JBoss** from the **Windows Start** menu.

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

5.2.2 Starting AEM

5.2.2.1 AEM URL

The URL for launching AEM for a given PowerServer 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 default ports for JBoss, JEUS, WebLogic, and WebSphere are:

- JBoss: 8080
- JEUS: 8088
- WebLogic: 7001
- WebSphere: 9080

5.2.2.2 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 PowerServer.

- On the computer where PowerServer is installed, select **Programs** > **Appeon** > **PowerServer** > **Appeon Enterprise Manager** from the **Windows Start** menu.

- On the computer where PowerServer Toolkit is installed, click the **AEM** button () in the PowerServer Toolkit. Before doing this, ensure that the AEM URL has been configured correctly in PowerServer Toolkit.

5.2.2.3 AEM user name and password

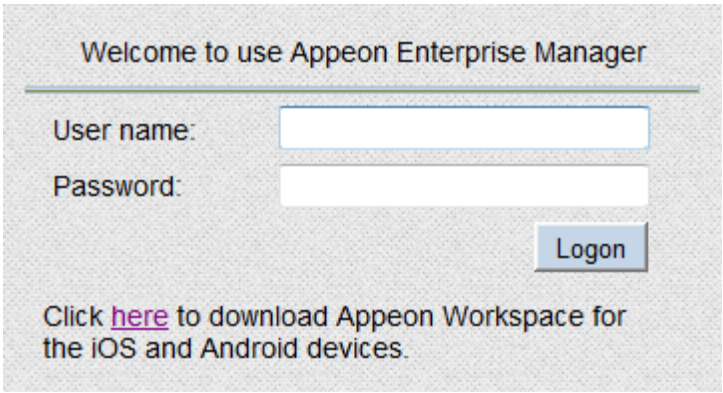
Enter a valid user name and password for AEM. During the PowerServer installation, you can specify the user name and password. If you did not specify the user name and password during the installation, you can use the default user name and password (both "admin") to log in to AEM. For security purposes, Appeon recommends that you change the user name and password after the initial login. Refer to AEM Login for more information about changing the user name and password.

5.2.2.4 Installing Appeon Workspace

If you click the link on the AEM login page, the Appeon Workspace download center (http://*server_ip_address*/aws/) will display and allow you to download the built-in version of Appeon Workspace from there.

If you are a server administrator, it is highly recommended that you read through Chapter 3, *Installing Appeon Workspace* in *Appeon Workspace User Guide* carefully, as it talks about how to prepare and deploy Appeon Workspace to the Web server in great details.

Figure 5.2: AEM login

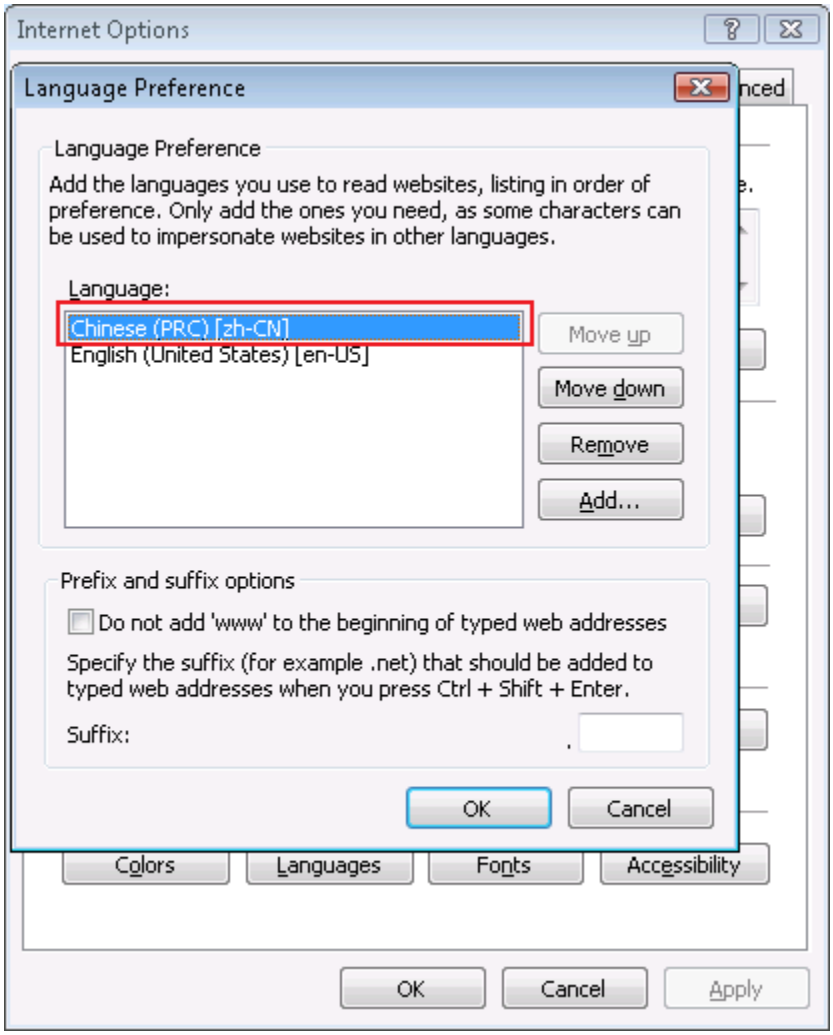


5.2.2.5 AEM language

AEM supports to display its content in multiple languages, such as English (en/en-us), Japanese (ja), Simplified Chinese (zh-cn) and Traditional Chinese (zh-hk/zh-tw).

The AEM language is determined by the language settings of the Web browser. Take Internet Explorer as an example. Select menu **Tools** > **Internet Options** from Internet Explorer. Click the **Languages** button on the **General** tab. Add the language and move it to the top of the list. For example, if you want to display the AEM contents in simplified Chinese, select **Chinese (PRC) [zh-CN]** and move it to the top, as shown in the following figure.

Figure 5.3: Language settings



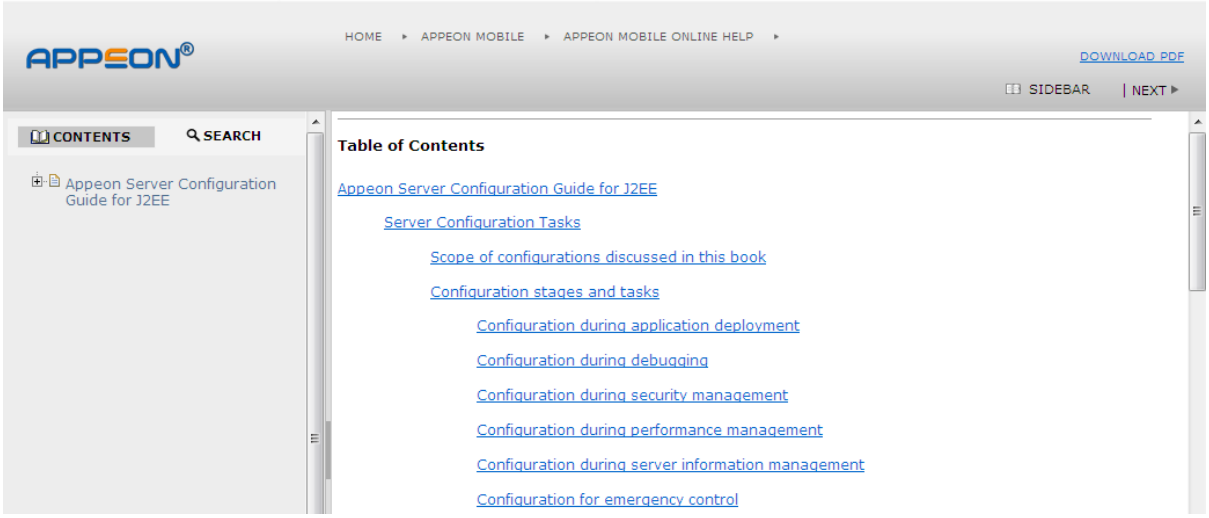
5.2.3 AEM Help

On the index page of AEM, the **Help** button provides easy access to AEM Help:

Figure 5.4: Help button

Click the **Help** button, find the topic on the left pane, and view the content on the right pane.

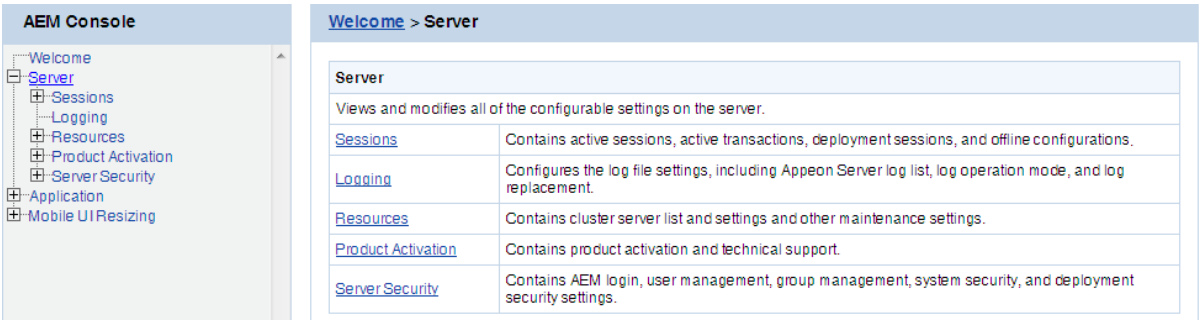
Figure 5.5: PowerServer Help



5.3 Server

Server is a set of tools for viewing and modifying all the configurable system settings. There are five tools: Sessions, Logging, Resources, Product Activation, and Server Security.

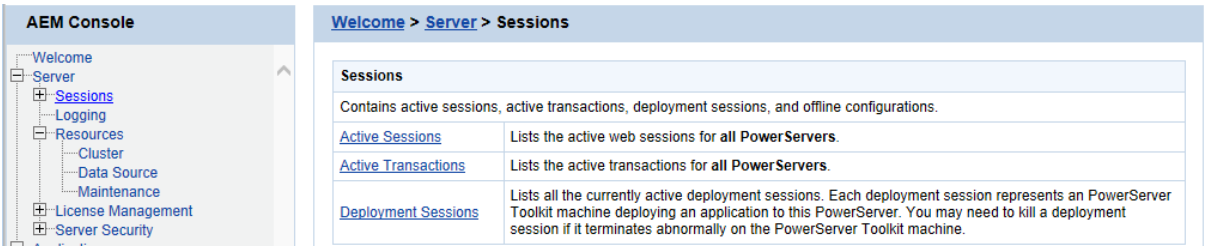
Figure 5.6: Server



5.3.1 Sessions

Sessions is a set of tools for viewing and modifying all the sessions and the transactions. There are three tools: Active Sessions, Active Transactions, and Deployment Sessions.

Figure 5.7: Sessions

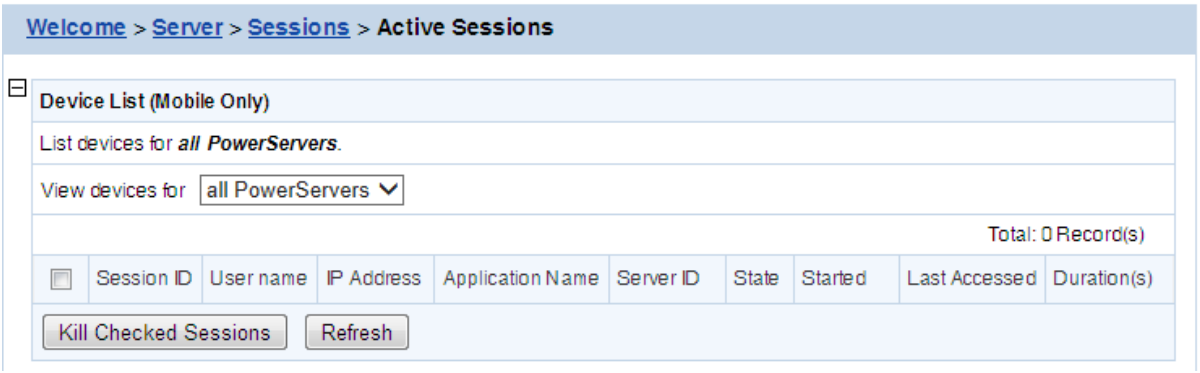


5.3.1.1 Active Sessions

The AEM Active Sessions tool helps you manage and monitor all the active sessions and the mobile devices (for mobile apps) in the system.

Figure 5.8: Active Sessions

Figure 5.9: Active Sessions



5.3.1.1.1 Viewing active sessions and devices on a PowerServer

Viewing active sessions

Note: This part is only for Web applications.

By default, the Active Sessions table lists the current active and passive sessions on all PowerServer. If you want to view sessions on a particular PowerServer, select the PowerServer from the **View active sessions for** dropdown list box, 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 a PowerServer, the session will be recognized as an active session for that PowerServer.
- Passive sessions: if the session is backed up in another PowerServer (randomly picked according to the load balancing algorithm), the session will be recognized as a passive

session for that PowerServer. The passive sessions only exist when you enable session backup in the Cluster tool.

Viewing active devices and sessions that belong to the device(s)

Note: This part is only for mobile applications.

By default, the Device List table lists all the active devices and sessions that belong to the device(s) on all PowerServer.

A device may have several sessions depending on the applications the device is accessing.

If you want to view devices on a particular PowerServer, select the PowerServer from the **View devices for** dropdown list box, and then click the **Refresh** button.

You can sort the **Device List** table by clicking any heading of the columns.

Each session of a device will have the following two states:

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

5.3.1.1.2 Killing session(s) and device(s)

Killing session(s)

Note: This part is only for Web applications.

You can kill a single or multiple sessions in the Active Sessions table to release PowerServer 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 you want to kill.

Proceed with caution when checking sessions 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.

Killing device(s) or session(s) that belong to the device(s)

Note: This part is only for mobile applications.

You can kill a single or multiple devices and/or sessions that belong to the device(s) in the Device List table to release PowerServer resources or if you want to perform database maintenance. Each session may include several transactions. When you kill an active device, the active transactions that belong to the session will be rolled back.

Step 1: Check the device(s) or the session(s) that belong to the device(s) you want kill.

If you kill a device, the session(s) that belong to the device will be killed correspondingly.

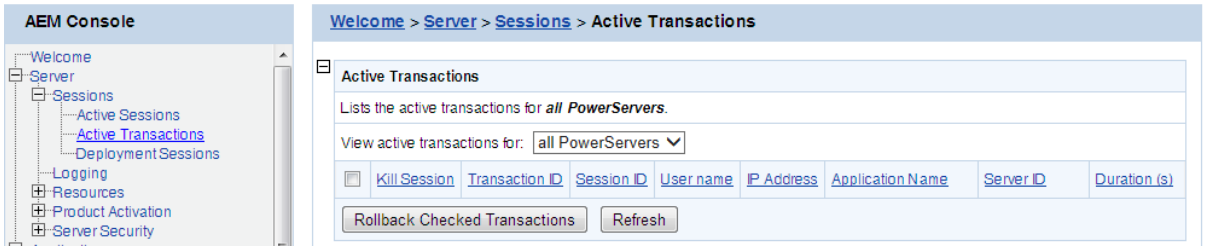
Step 2: Click the **Kill Checked Sessions** button.

A message box appears for you to confirm the action. Once you confirm the action, the selected devices or sessions are immediately killed and the Device List table is refreshed.

5.3.1.2 Active Transactions

The AEM Active Transactions tool helps you manage and monitor all active transactions in the system.

Figure 5.10: Active Transactions



5.3.1.2.1 Viewing active transactions

By default, the Active Transactions table lists the current active transactions on all PowerServer. If you want to view active transactions on a particular PowerServer, select the PowerServer from the "**View active transactions 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 Transactions table by clicking any heading of the following columns: Transaction ID, Session ID, User Name, IP Address, Application Name, Server ID, Client Type, and Duration.

5.3.1.2.2 Rolling back active transaction(s)

You can roll back a single or multiple active transactions in the Active Transactions table to release PowerServer 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.

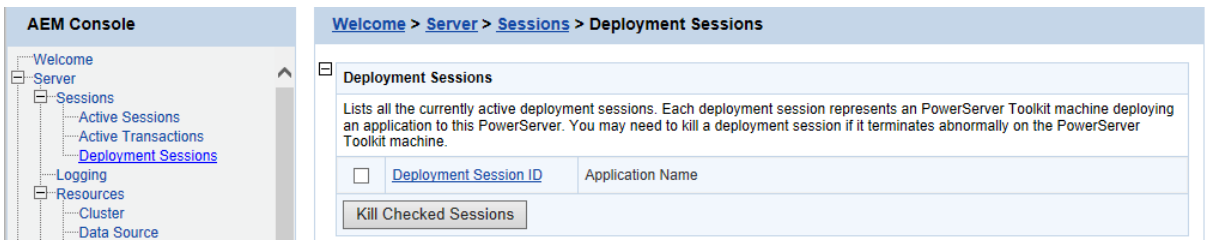
Step 2: Click the **Rollback Checked Transactions** button.

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

5.3.1.3 Deployment Sessions

The Deployment Sessions tool can help you manage and monitor all the active deployment sessions in the system.

Figure 5.11: Deployment Sessions



An active deployment session automatically starts and displays in the Deployment Sessions table when PowerServer Toolkit starts to upload the embedded SQL statements, DataWindow SQLs, and INI files of an application to PowerServer. It ends and disappears automatically from the table when the upload process is complete.

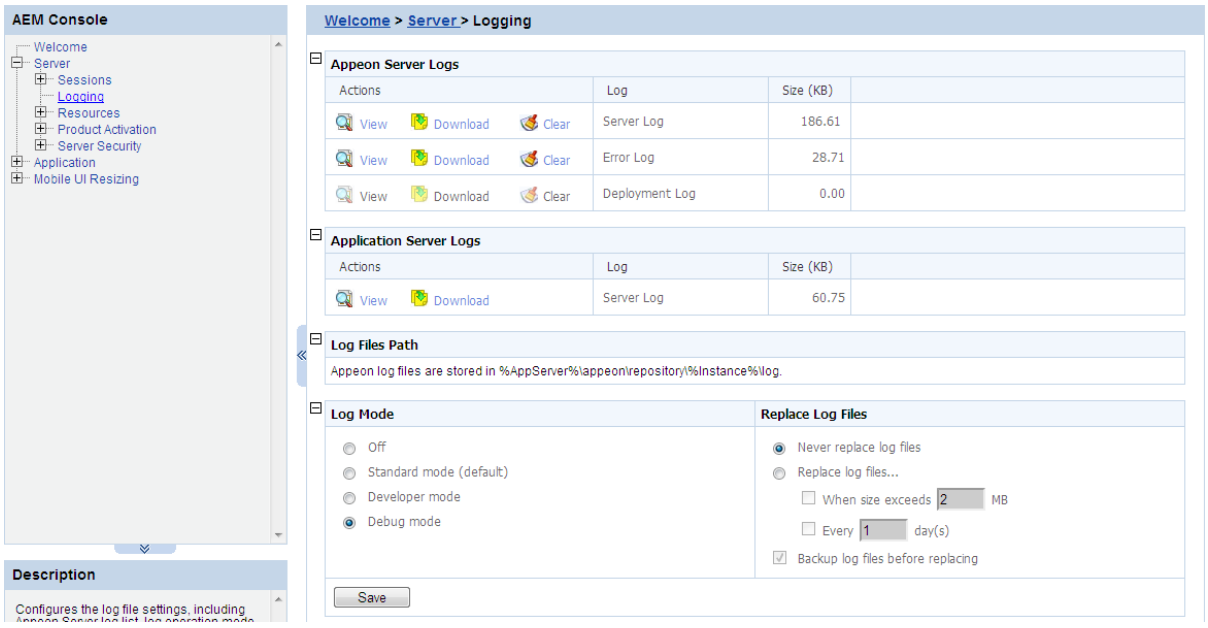
There is one special scenario in which you need to manually kill a deployment session in AEM. If the Deployment Wizard of PowerServer Toolkit abnormally exits during the above-mentioned upload process, the deployment session stays in active status in PowerServer, and PowerServer Toolkit cannot resume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

5.3.2 Logging

Logging is a set of tools for viewing and configuring all the logs.

Figure 5.12: Logs



5.3.2.1 Viewing logs

PowerServer creates three different log files for record keeping and for future use in troubleshooting. You can view these log files using the **View** button or directly locate them in the <AppeonHome>\repository\<InstanceName>\log folder.

On a click on a **View** button either in the **PowerServer Logs** table or in the **Application Server Logs** table, you direct access the log files created by PowerServer and the host application server of PowerServer, such as JBoss.

- PowerServer Logs

  Server Log: the main log file. Records messages logged from services and the core PowerServer 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.

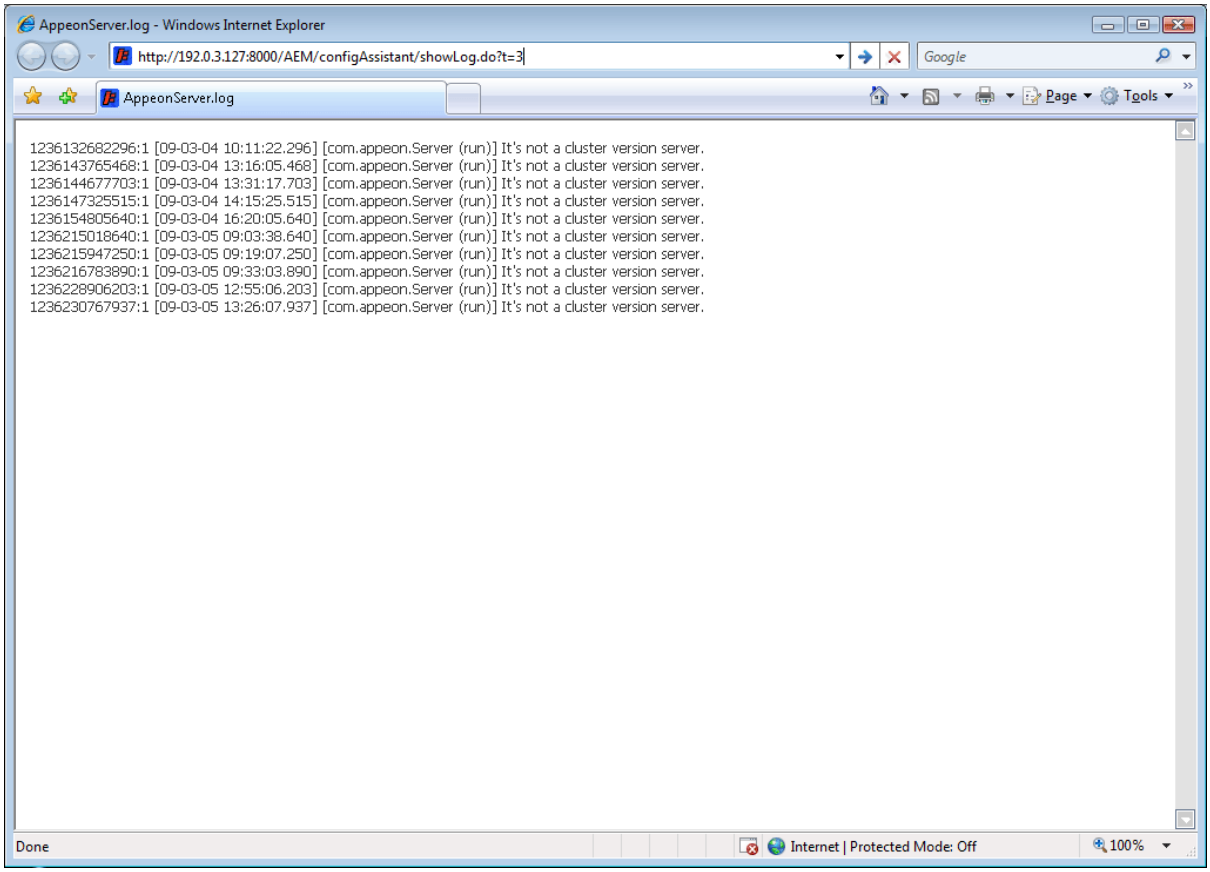
The Log Viewer tool provides the following manipulations:

- To view a log file

  Click **View** to view the detailed information in the browser. Click the links of different log files to switch between them.

  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 5.13: View log files



- 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 PowerServer 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.

5.3.2.2 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.

5.3.2.3 Replace log files

Log files accumulate over time, and if they become too large, they can decrease PowerServer performance. Select the "Replace log files..." option to replace the log files periodically. This section is specifically applicable to AppeonServer.log, AppeonDev.log files and AppeonError.log file.

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.

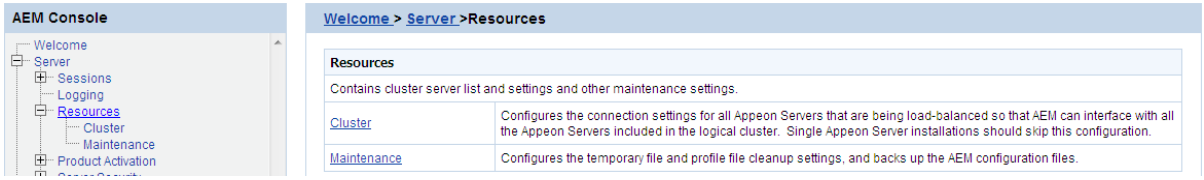
- This setting allows PowerServer to back up the log files before replacing them. If this option is checked, all log files are backed up before they are replaced so an archive of the log files is maintained. Maintaining this archive does not compromise system performance, but there must be adequate hard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

5.3.3 Resources

Resources is a set of tools for viewing and configuring the servers cluster, temporary files and configuration backups. There are two tools: Cluster and Maintenance.

Figure 5.14: Resource



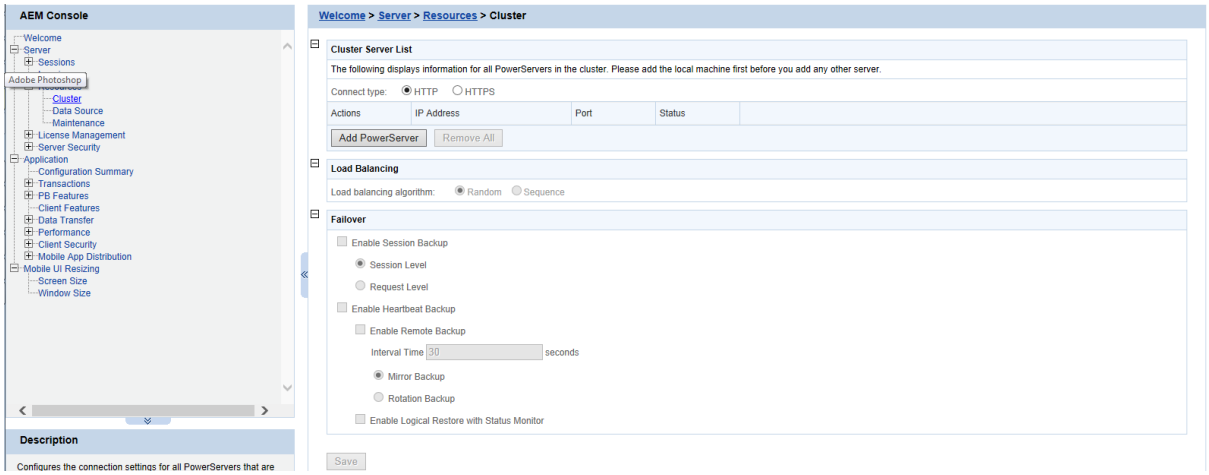
5.3.3.1 Cluster

Once you installed PowerServer to several application servers, you can use the AEM Cluster tool to create a PowerServer 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 PowerServer cluster in AEM. For detailed instructions, refer to Chapter 6, *Tutorial 5: Configure PowerServer Cluster* in *PowerServer Mobile Tutorials*.

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

Figure 5.15: Cluster



5.3.3.1.1 Cluster Server List

Use the **Cluster Server List** to create a PowerServer cluster. The PowerServer 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

- All of the PowerServer to be added into the cluster must have the same connection type: HTTP or HTTPS; it cannot be a mix.
- Use the IP address or machine name of the PowerServer when adding a PowerServer. Do not use "localhost" or "127.0.0.1".
- The IP address or machine name and port number must match the HTTP or HTTPS settings 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 Deployment Wizard to perform the application deployment. For detailed instructions, refer to the Chapter 6, *Deploying PowerBuilder Applications* in *PowerServer Toolkit User Guide*.
- To ensure the most efficiency and stability of the PowerServer cluster, verify that the environment of all PowerServer is identical. For example, the application server (type and version) and PowerServer (version and license) must be the same.
- If you need to reinstall the operating system of a PowerServer in the cluster, be sure to remove the PowerServer from the cluster first.

Adding a PowerServer

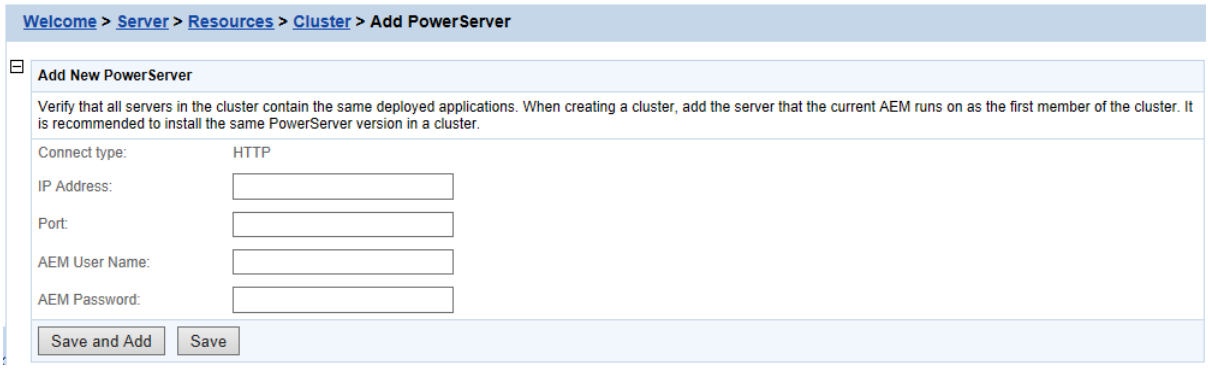
Make sure you add the server that the current AEM runs on as the first member of the cluster.

Step 1: Select the connection type (HTTP or HTTPS) for the PowerServer cluster.

All of the PowerServer to be added into the cluster must have the same connection type: HTTP or HTTPS.

Step 2: Click the **Add PowerServer** button in the **Cluster Server List** table. The Add PowerServer page opens.

Figure 5.16: Add PowerServer



Step 3: Verify that the PowerServer to be configured is running and provide the required information (IP address, port, and the AEM login user name and password). For example:

- IP address: 161.0.0.1
- Port: 80
- AEM User Name: admin
- AEM Password: admin

Step 4: Click the **Save** and **Save and Add** button. The program will automatically test the connection and add the PowerServer if the test is successful.

Adding a PowerServer will succeed only if:

1. The PowerServer is new to AEM.
2. The information provided is correct.
3. The PowerServer is running.
4. The first PowerServer that you add is the one hosting the current AEM.
5. The password is correct.

Removing a PowerServer

Make sure you remove the server that the current AEM runs on first.

To remove a PowerServer from the list:

Step 1: Click the **Delete** button in the Actions column of the PowerServer in the PowerServer Cluster table.

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 PowerServer is removed from the PowerServer list. AEM no longer interfaces with the PowerServer.

To remove all PowerServer from the list:

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

Checking status of PowerServer

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

- Shut down: PowerServer is not started or not available.
- Ready: PowerServer is preparing itself to accept user requests by taking the essential initialization process.
- Running: PowerServer is started and accepts user requests.
- Failed: PowerServer failed to start or failed to verify license.

5.3.3.1.2 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. PowerServer 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.

5.3.3.1.3 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.

PowerServer 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 PowerServer 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 PowerServer 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 PowerServer receives a request from the same session, regardless of the session status.

Heartbeat backup

Heartbeat backup options enable PowerServer 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 which 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 here 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.

5.3.3.1.4 Synchronizing AEM settings to servers in a cluster

Once a PowerServer 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:

- Logging: displays the log files on the current server only.
- Auto cleanup and Manual cleanup in Maintenance: 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.
- Data Source: displays and configures the data source 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.

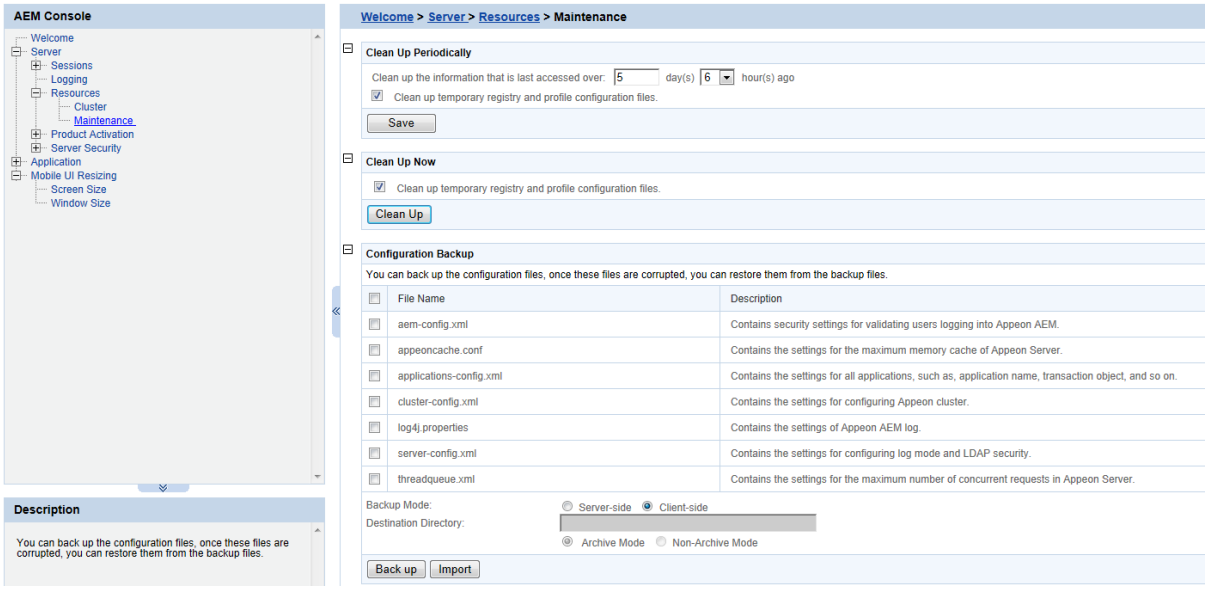
The following action will not be synchronized:

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

5.3.3.2 Maintenance

Maintenance is a set of tools for clearing temporary files and backing up configurations.

Figure 5.17: Maintenance



5.3.3.2.1 Auto cleanup

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

Step 1 -- Specify to clean up files that have not been accessed for the specified period.

For example, "Clean up the information that is last accessed over: 2 days 4 hours ago" denotes that files that were accessed over 2 days and 4 hours ago will be cleaned up everyday.

Step 2 -- Choose whether to clean up the temporary register and profile configuration files by selecting or de-selecting the check box for "Clean up temporary register and profile configuration files".

Step 3 -- Click the *Save* button to apply changes.

5.3.3.2.2 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 -- Choose whether the temporary register and profile configuration files to be cleaned up by selecting or de-selecting the check box for "Clean up temporary register and profile configuration files".

Step 2 -- Click the *Clean Up* button to commit the cleanup.

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

5.3.3.2.3 Configuration Backup

The AEM configuration files can be backed up and restored easily using the Configuration Backup tool.

To back up the AEM configuration files:

Step 1: Select one or more configuration file from the file list.

Step 2: Select the backup mode.

- Server Mode -- Backs up the configuration files and stores on the PowerServer machine.
- Client Mode -- Backs up the configuration files and stores on the local client machine. You will be prompted to specify the location to store the backup file after clicking the **Back Up** button.

Step 3: If you select Server Mode in Step 2, then specify the destination location for the backup files. The destination location must be an existing directory on the PowerServer machine.

Step 4: Specify the archive mode for the backup files.

- Archive Mode indicates the backup files will be packaged into a zip file. If Client Mode is selected as the backup mode, Archive Mode will be used by default.
- Non-Archive Mode indicates the backup files will be existing in separate files.

Step 5: Click the **Back Up** button to back up files.

To import the AEM configuration files:

Step 1: Click the **Import** button.

Step 2: In the **Import Configuration File** page, click **Browse** to select the backup file to import. The backup file can be a single file or a zip file which contains multiple files.

Step 3: Click **Import** to import the selected backup file.

5.3.4 Product Activation

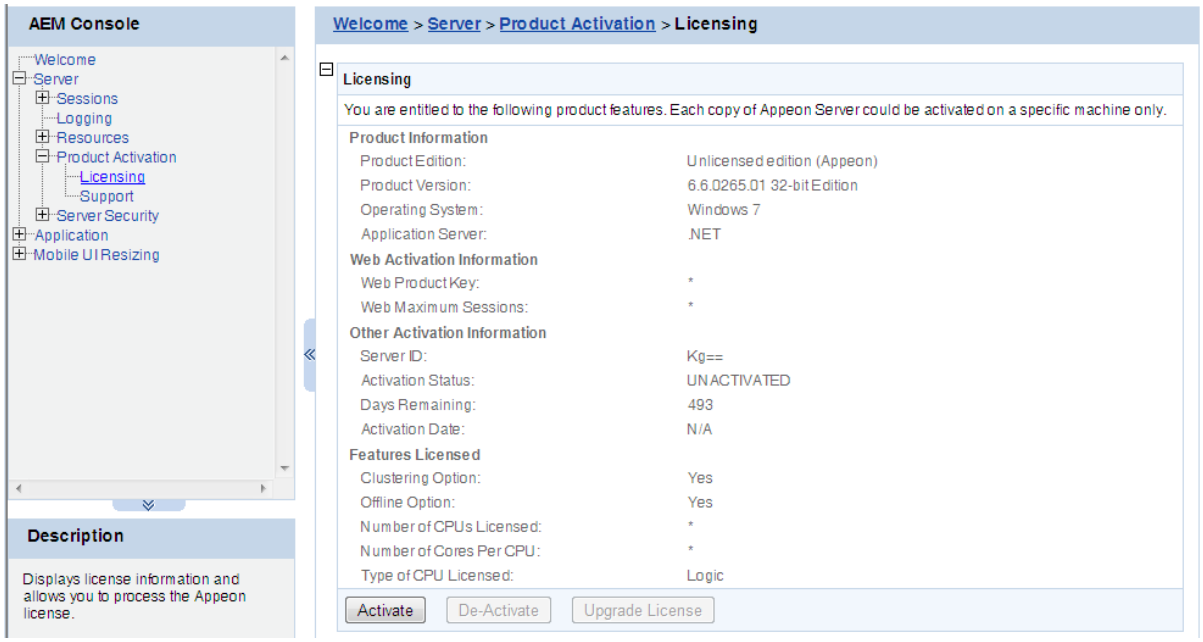
Product Activation is a set of tools for viewing product license information and activating products. There are two tools: Licensing and Support.

Figure 5.18: Product Activation

5.3.4.1 Licensing

The Licensing tool enables you to view the detailed license information, activate or de-activate a PowerServer, and update the license.

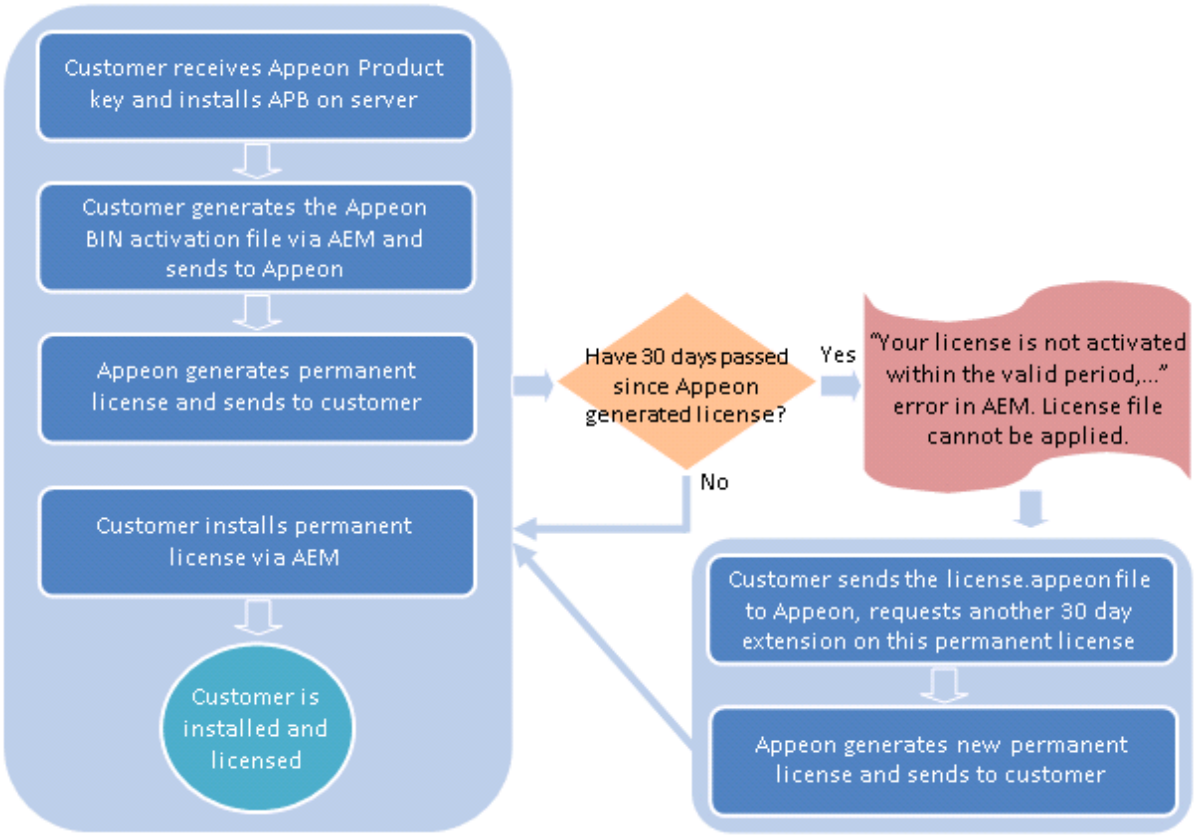
Figure 5.19: Licensing



5.3.4.1.1 Product Activation

After you purchase the product, you will need to activate PowerServer for permanent use. See the following flowchart for the activation process.

Figure 5.20: Activation process



The following are detailed instructions for you to activate the product via AEM:

Step 1: Generate the activation request (the Appeon BIN activation file).

1. On the **Licensing** page, click the **Activate** button.

2. On the **Product Activation** page, do the following:

   - From the **Product Key Type** dropdown list box, select the product type that you have purchased.

     The difference between **PowerServer Web & PowerServer Mobile** and **PowerServer Web & Mobile** is mainly the way of allocating the sessions/devices. For **PowerServer Web & Mobile**, Web apps and mobile apps can share the unused sessions/devices; while for **PowerServer Web & PowerServer Mobile**, the Web apps and the mobile apps are strictly limited by their own session counts. For example, if the Web session is set to 5, and the Mobile session is set to 10, then for **PowerServer Web & PowerServer Mobile**, the Web sessions cannot exceed 5 and the Mobile sessions cannot exceed 10, while for **PowerServer Web & Mobile**, so long as the total sessions do not exceed 15, the Web session can go over 5 if there are unused Mobile sessions, or the Mobile sessions can go over 10 if there are unused Web sessions.

   - From the **Control Type** dropdown list box, select a control type.

     a. Application: it controls how many applications on this PowerServer can be accessed at a particular time.

b. Session/Device: it controls how many sessions and/or devices can access the apps on this PowerServer at a particular time. For Web applications, each application instance running on the client is considered as one session, for mobile applications, each mobile device that is accessing the app (no matter how many apps) is considered as one device.

   The Appeon mobile app will need to get the device ID when running on the mobile device, so that the app as well as other Appeon mobile apps running on the same mobile device can be recognized as running on one device by the Appeon license file, not running on multiple devices.

About App ID for iOS apps

For iOS apps, to enable the app to get the device ID successfully, you will need to correctly specify the App ID Prefix and the App ID Suffix (Bundle ID):

i. App ID Prefix: you should always input the same App ID Prefix for all Appeon mobile apps.

   You can specify the App ID Prefix when packaging the mobile project in the PowerServer Toolkit Package tool in *PowerServer Toolkit User Guide*.

ii. App ID Suffix (Bundle ID): Bundle ID is used to identify the application, therefore it must be unique for different applications.

   You can specify the Bundle ID when packaging the mobile project in the PowerServer Toolkit Package tool in *PowerServer Toolkit User Guide*.

   You should specify the consistent Bundle ID in the Xcode project for the same application. For details, refer to Section 5.2.3.1, “Task 3.1: Set App ID and Bundle Identifier” in *PowerServer Mobile Tutorials*.

- In the product key field(s), double check the product key and modify it if it is incorrect.
- From the **Server Type** list, select **Dedicated Server** if the server is running on hardware that is dedicated for your use; select **Azure Virtual Machine** if the server is running on a virtual machine created in Windows Azure; select **AWS Virtual Machine** if the server is running on a virtual machine created in Amazon Web Services.
- When **Azure Virtual Machine** server type is selected, select the appropriate deployment model for the Azure virtual machine.
  - **Resource Manager VM** -- You will need to provide the following information: **Azure Subscription ID**, **Directory ID**, **Application ID**, **Key Value**, and **Virtual Machine Name**.

    In order to get these information, you will need to first make configurations according to https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal.

- **Classic VM** -- You will need to provide the following information: **Azure Subscription ID**, and **Deployment Label**.

- **Upload Package** -- You will need to provide the following information: **Azure Subscription ID**, and **Deployment Label**.

  You can get the information of **Subscription ID** and **Deployment Name** by selecting the proper service name from the Azure website portal.

  IMPORTANT: If **Classic VM** or **Upload Package** deployment model is selected, you will also need to log into the Azure administration portal (https://manage.windowsazure.com/), download the certificate file (https://manage.windowsazure.com/publishsettings), rename the file to *credentials.publishsettings* and copy the file to the local PowerServer installation directory \%appeon%\AEM\Cert. If the *Cert* folder does not exist, please manually create it.

  Please make sure you complete these steps before you apply the Appeon license file, and keep the certificate file exist in the specified directory whenever PowerServer is activated and running.

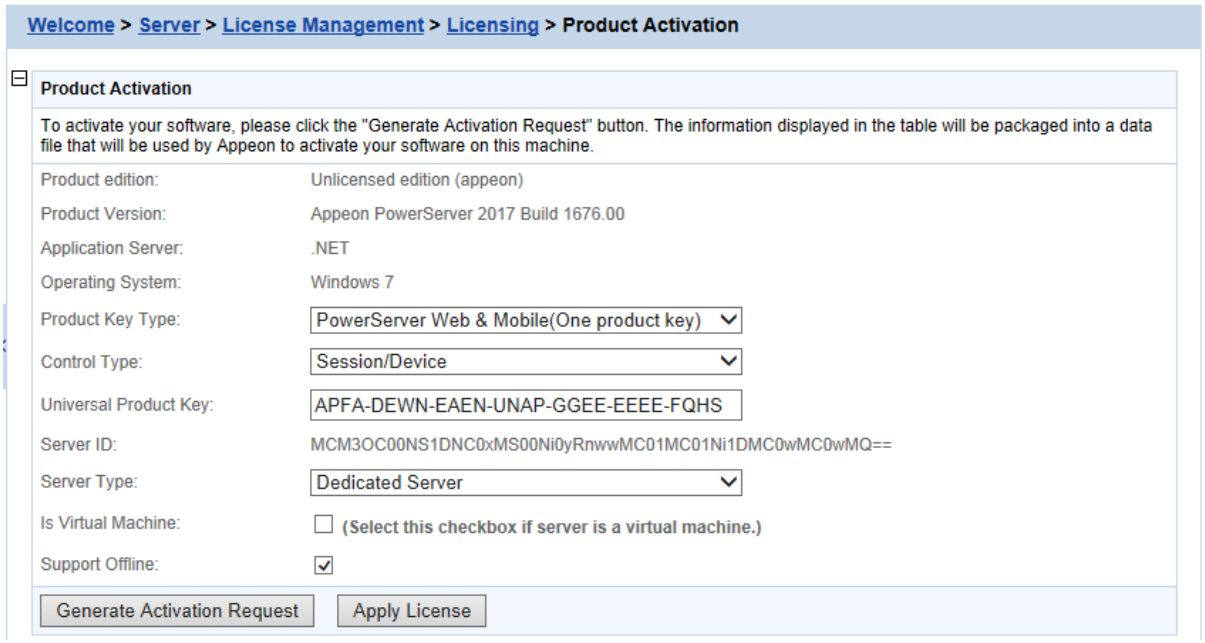
- When **AWS Virtual Machine** server type is selected, specify the settings for the server instance created in Amazon Web Services. These settings can be obtained from the AWS console. For detailed instructions, see AWS server instance settings.

- (Optional) Check the **Is Virtual Machine** checkbox, if the dedicated server is running on a virtual machine rather than a physical machine.

- (Optional) Check the **Support Offline** checkbox, if your license supports offline features.

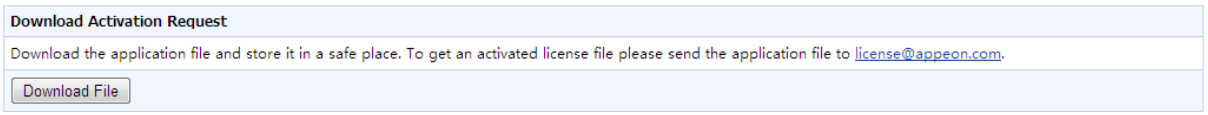
- Click the **Generate Activation Request** button.

Figure 5.21: Product activation



3. Click the **Download File** button to download the request file which is by default named as license.activation.bin and send it to <license@appeon.com>. The request will be processed in Appeon and an activated permanent license (license.appeon) will be sent to you later.

Figure 5.22: Download activation request

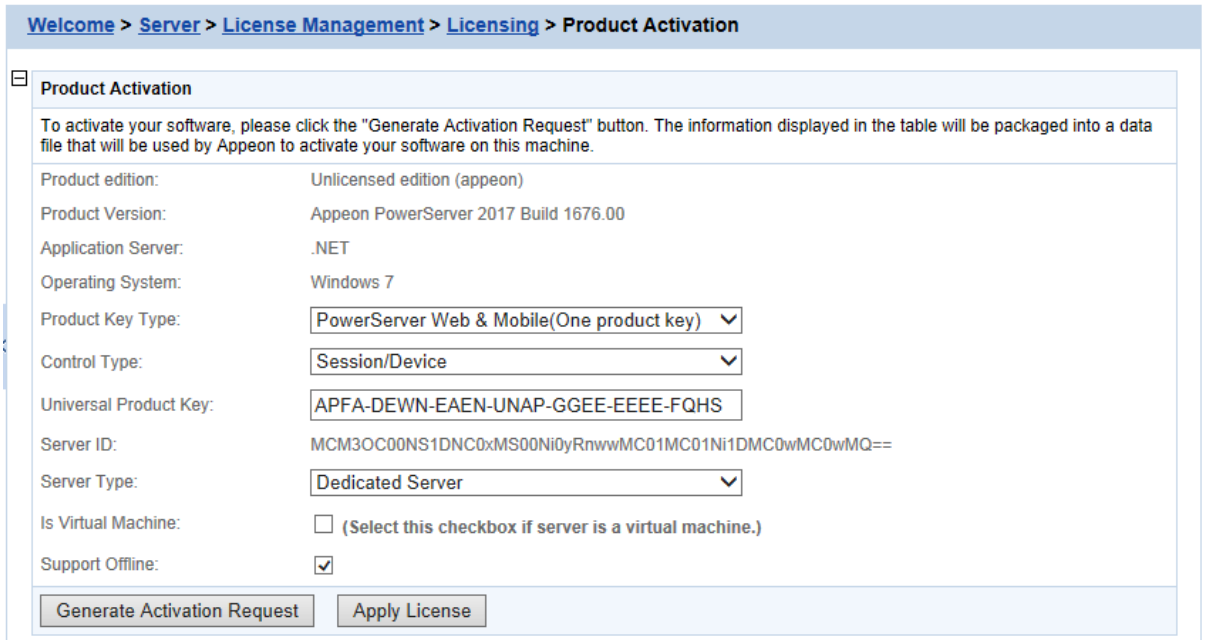


Step 2: Install the permanent license file.

The license file must be installed within 30 days after it's generated. If this 30-day install period has expired, the license file cannot be installed, and there will be an error in AEM when you try to install it. In this case, you will need to send the license file back to Appeon and have Appeon extend the install period for this file. Once you get the license file, follow the steps below to install it via AEM.

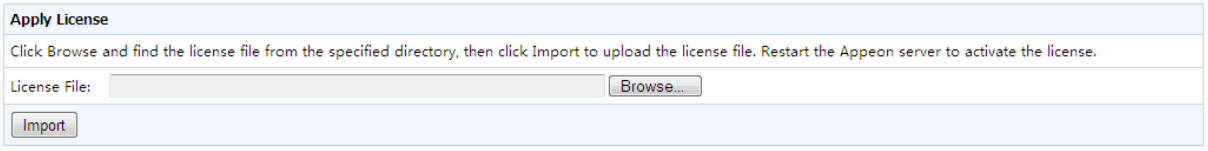
1. After getting the permanent license (license.appeon) from Appeon, click the **Apply License** button.

Figure 5.23: Product activation



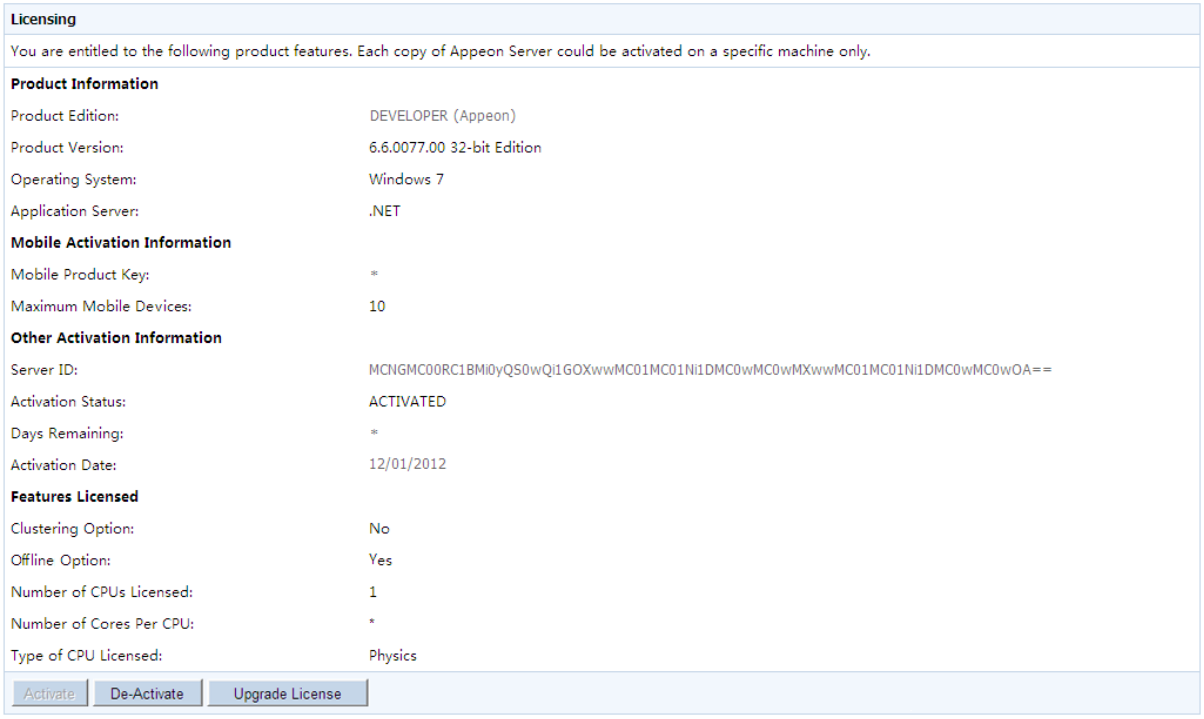
2. Click the **Browse...** button and select the license.appeon file. The file name must be exactly license.appeon, and it is case-sensitive. Click the **Import** button to import the license file. Please make sure the license file is imported successfully, and then restart PowerServer.

Figure 5.24: Apply license



3. After you restart PowerServer, go back to the **Licensing** page, and verify that **Activation Status** is shown as **Activated**.

Figure 5.25: Licensing



4. Back up your permanent license file so you can use it again in case you will reinstall PowerServer within the 30-day install period.

AWS server instance settings

The information required for activating PowerServer on AWS includes: the region code of the account, the key ID and secret key of the user, the keyword prefix of the server instance, and the number of instances allowed for deploying PowerServer. All these information (except for the number of instances) can be obtained from the AWS console, as highlighted below.

- **Region**: the region code (NOT the region name) of the AWS account.

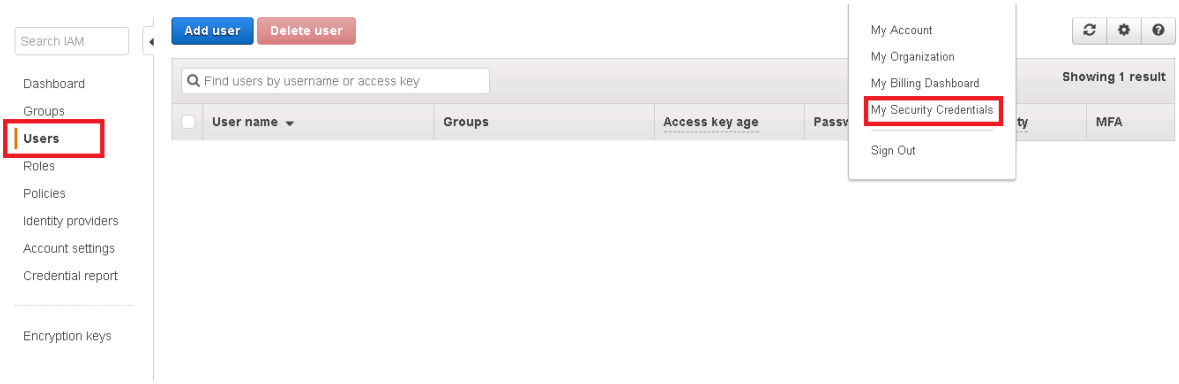
  To get the region code of the AWS account, first log into the AWS console and get the region name on the top right corner of your account center, then search the region name on the Web page: http://docs.aws.amazon.com/general/latest/gr/rande.html#apigateway_region to get the corresponding region code.

- **Key ID**: The access key ID of the AWS user.

- **Secret Key**: The access secret key of the AWS user.

  To get the access key ID and the access secret key of the AWS user, first log into the AWS console and go to the **Users** area.

Figure 5.26: Users area



When you add a new user, be sure to select the **Programmatic access** type, and assign the user to the group with **AmazonEC2ReadOnlyAccess** permissions.

Figure 5.27: Access type

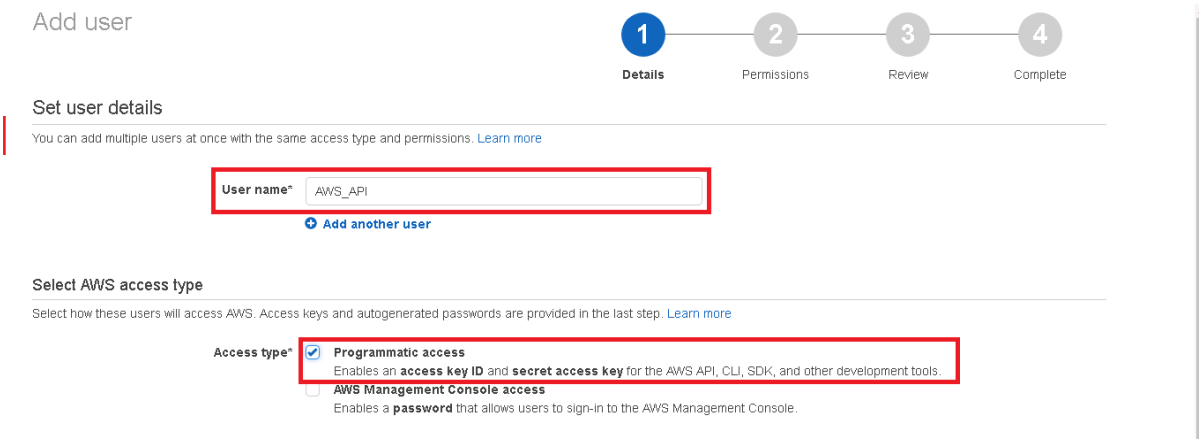
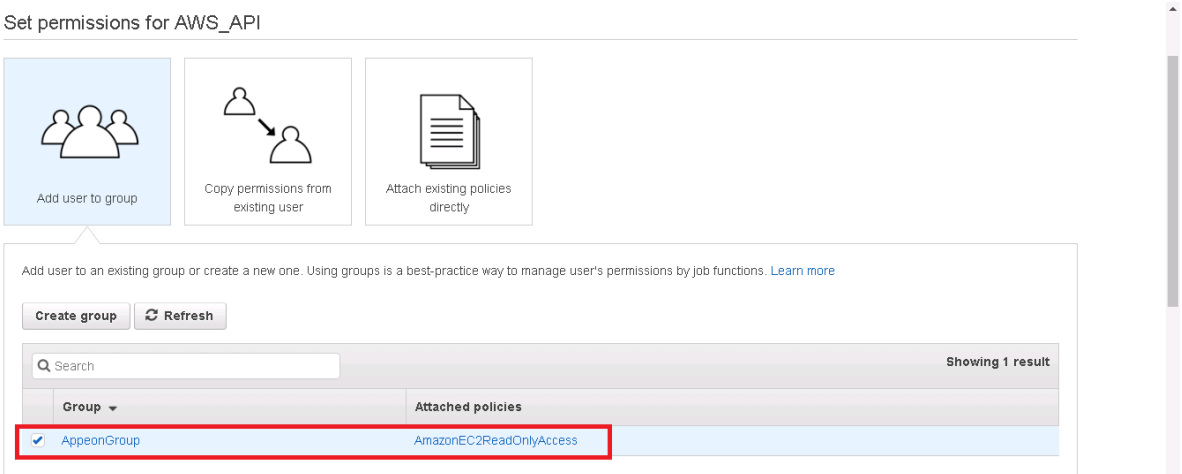
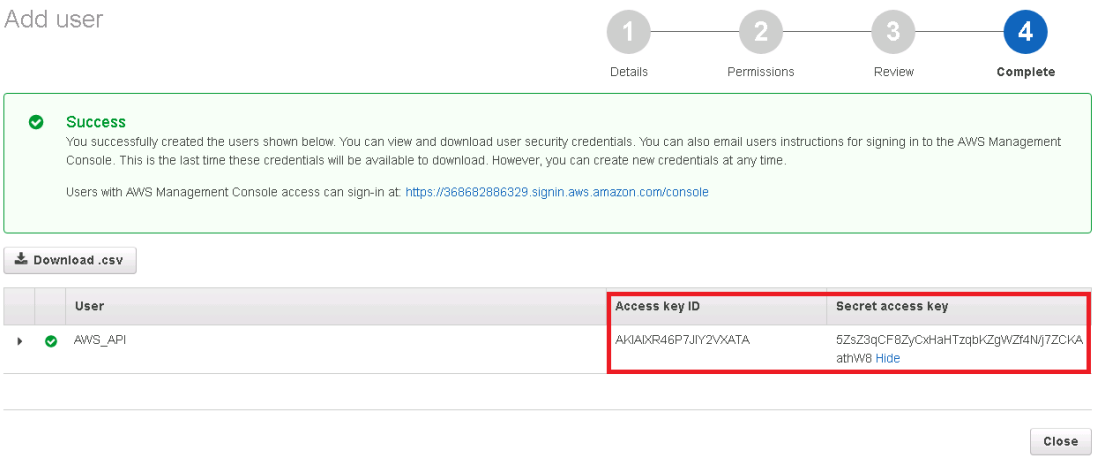


Figure 5.28: User group



After the user is added, you can get the access key ID and the access secret key.

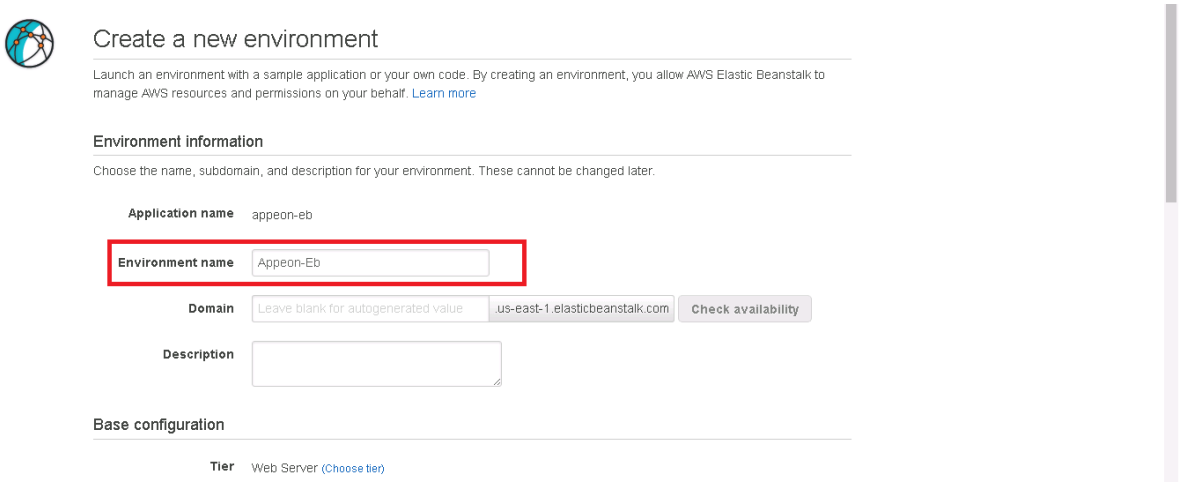
Figure 5.29: Access key ID and secret key



- **Keyword Prefix**: A string that matches with the name prefix of the server instance(s) where PowerServer is deployed. There are two types of server instance where PowerServer can be deployed: **Elastic Beanstalk(EB)** and **Amazon Elastic Compute Cloud(EC2)**.

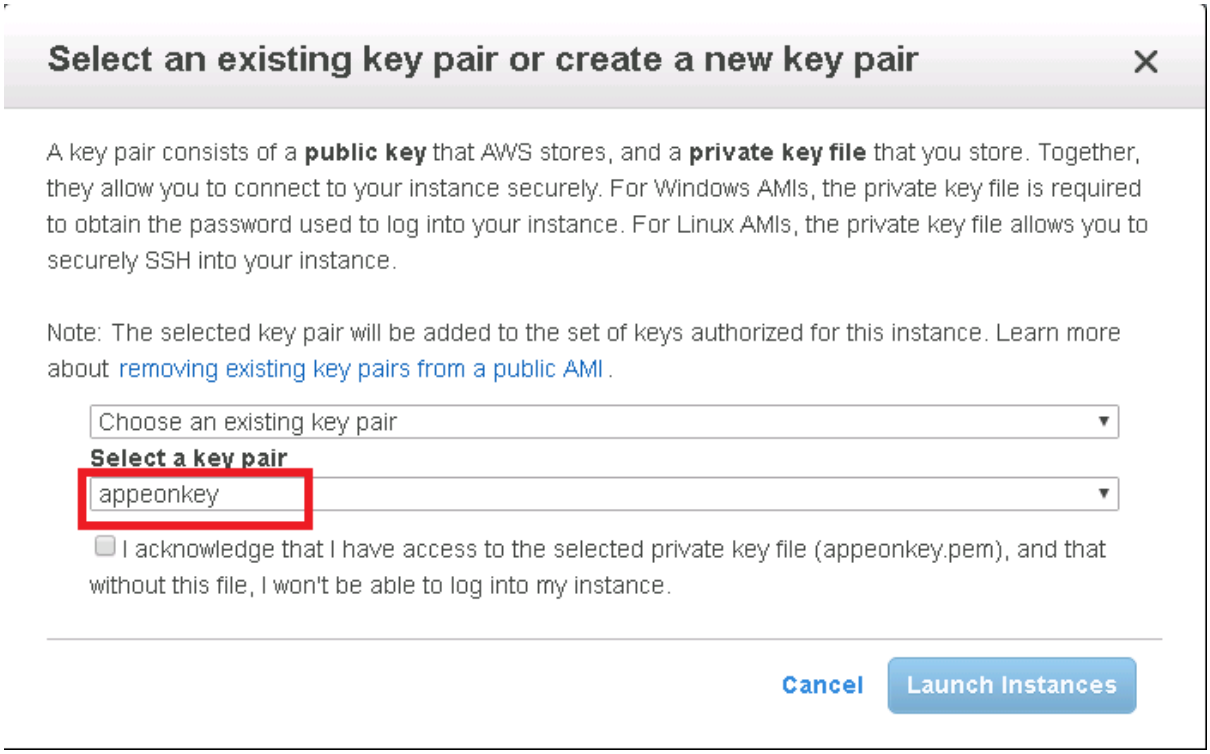
  When creating an instance of **Elastic Beanstalk(EB)**, the **Environment name** must start with the keyword prefix specified for the PowerServer license activation. For example, "Appeon" is the keyword prefix.

Figure 5.30: Environment name



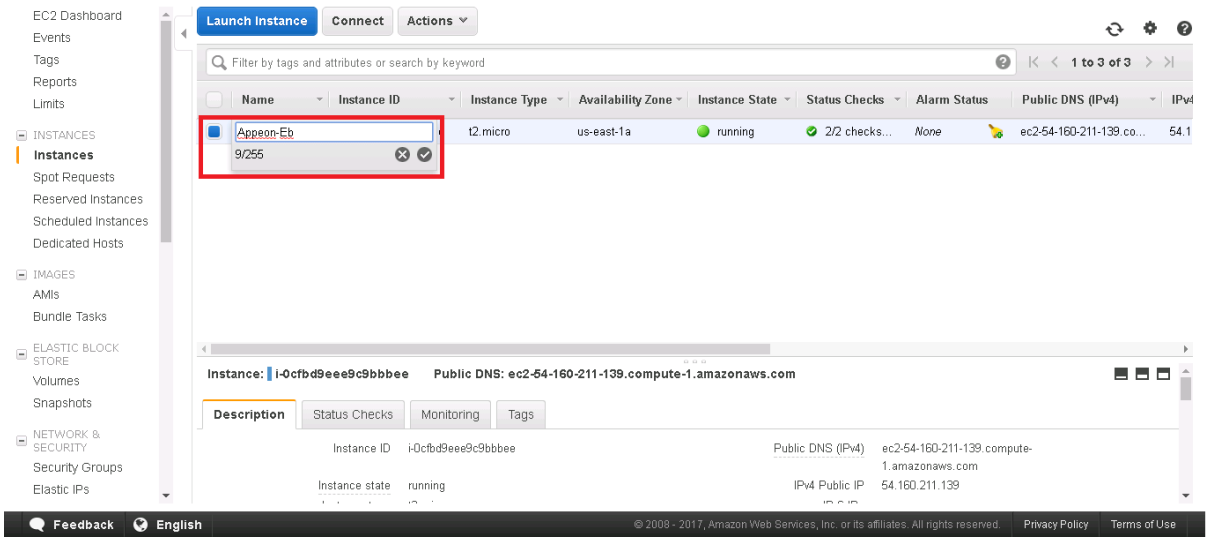
When creating an instance of **Amazon Elastic Compute Cloud(EC2)**, the key pair must start with the keyword prefix specified for the PowerServer license activation. For example, "appeon" is the keyword prefix.

Figure 5.31: Key pair



After you create an instance (either **Elastic Beanstalk(EB)** or **Amazon Elastic Compute Cloud(EC2)**), you can modify the instance name. Make sure the prefix of the instance name matches with the keyword prefix specified for the PowerServer license activation.

Figure 5.32: Instance name



- **Numbers of Services**: The maximum number of service instances allowed for deploying PowerServer under the current AWS account. Simply specify a number in the AEM page.

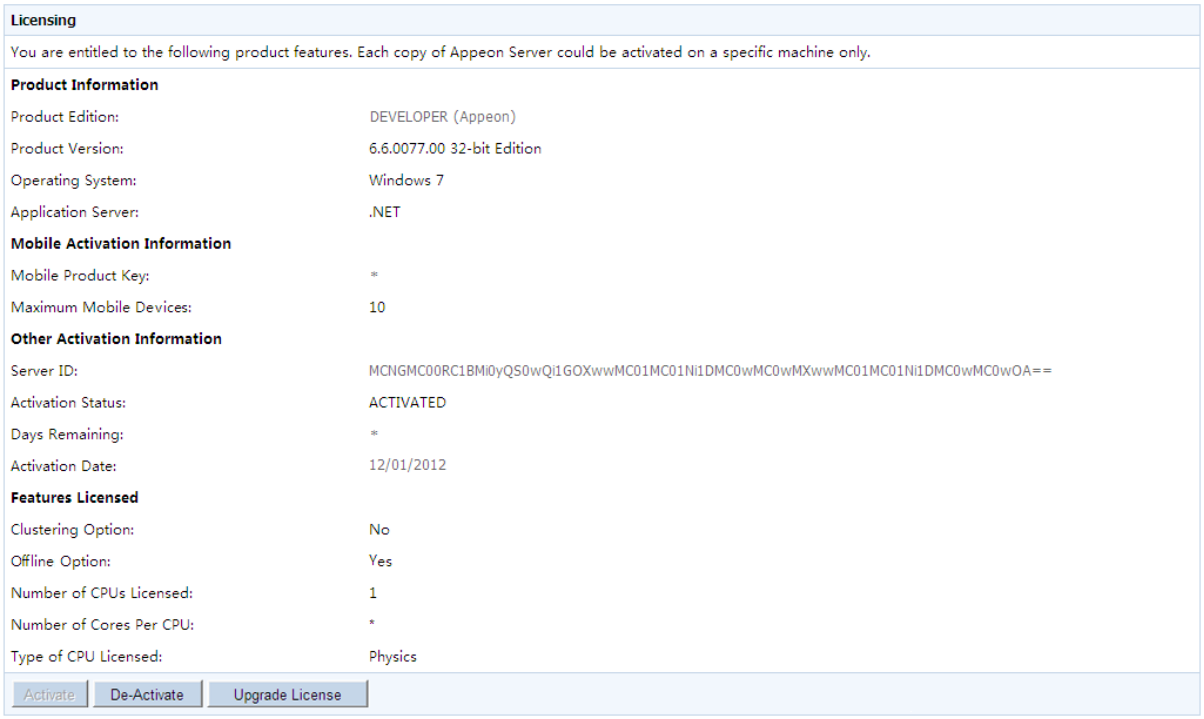
5.3.4.1.2 Re-activation

Each copy of PowerServer can only be activated on one machine. If you want to activate a PowerServer on a different machine, you would need to de-activate PowerServer on the previous machine first and then activate it on the new machine, by following the instructions below.

Step 1: De-activate PowerServer on the previous machine.

1. Click the **De-Activate** button in the **Licensing** page.

Figure 5.33: License deactivation



2. You will be prompted by two sequential messages to confirm whether you want to deactivate PowerServer on this machine. **IMPORTANT**: Please be cautious with this action, as it is irreversible, and once you click **OK**, the license file will become invalid and can no longer be installed on this machine unless it is re-generated. Click **OK** to continue if you are sure to de-activate this PowerServer.

Figure 5.34: Product De-activate

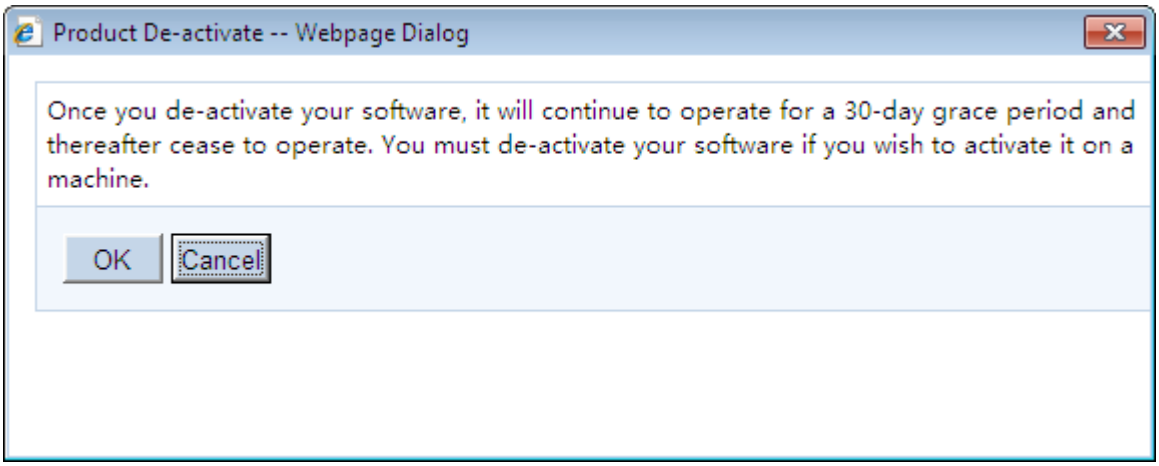
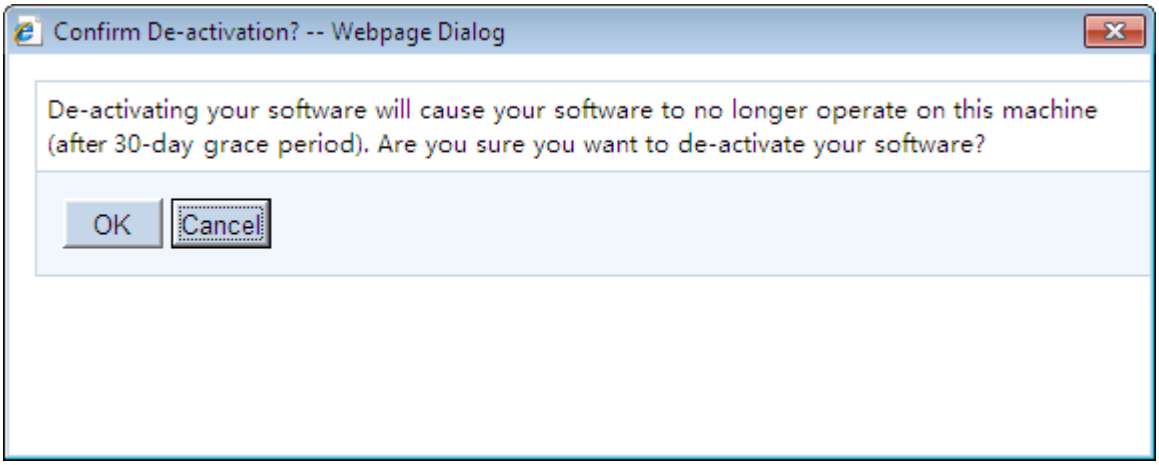
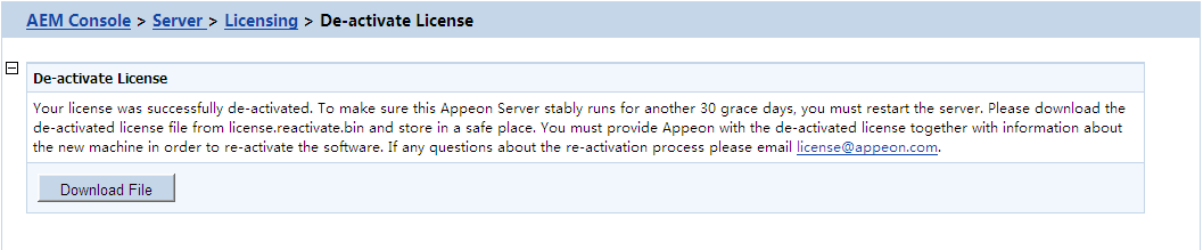


Figure 5.35: Confirm De-activation



3. Click the **Download File** button to download the file whose name is license.reactivation.bin by default.

Figure 5.36: De-activate License



Step 2: Generate the activation request for PowerServer on the new machine.

Follow the steps in Generate the activation request to get the license.activation.bin file and save it in a safe place.

Step 3: Email Appeon to generate the license file for the new server.

You should send both the license.reactivation.bin file and the license.activation.bin file to `<license@appeon.com>` to apply a reactivated license for the new server.

Step 4: Install the license on the new server.

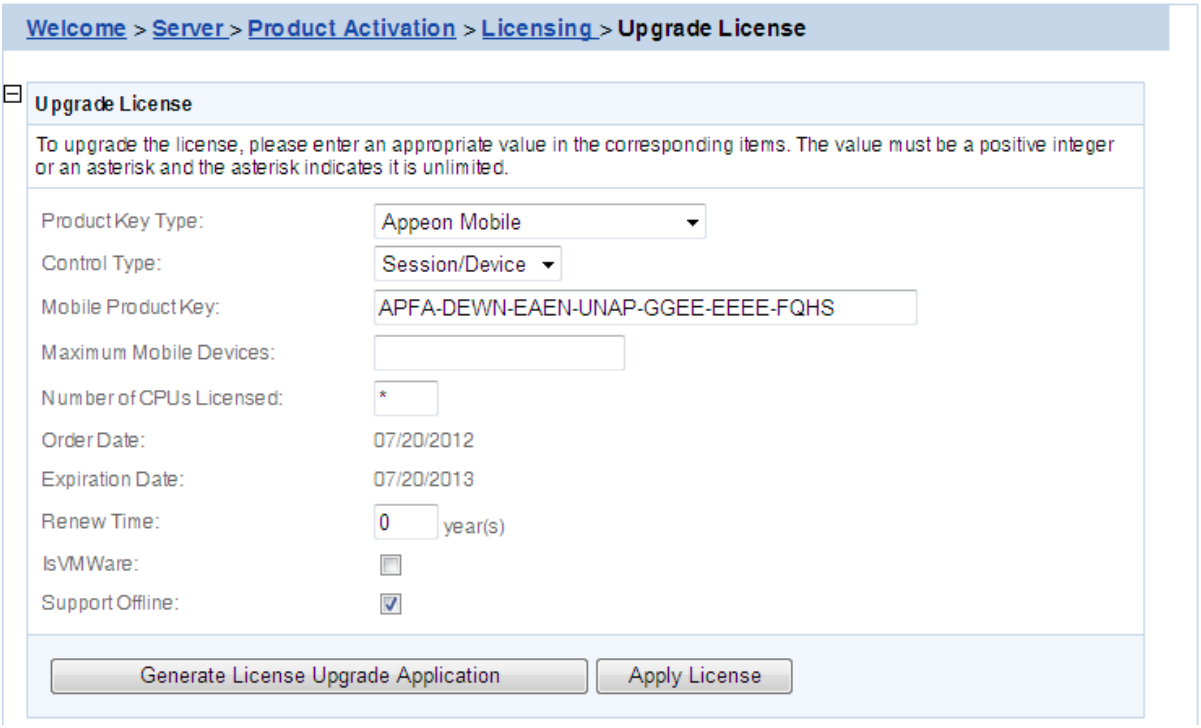
Appeon will process the reactivation request and send you a valid reactivated license file (license.appeon). You need to install this license file on the new server. For detailed instructions, please refer to Install the permanent license file.

5.3.4.1.3 Upgrade license

Step 1: On the **Licensing** page, click the **Upgrade License** button.

Step 2: On the **Upgrade License** page, input the information for upgrading the license.

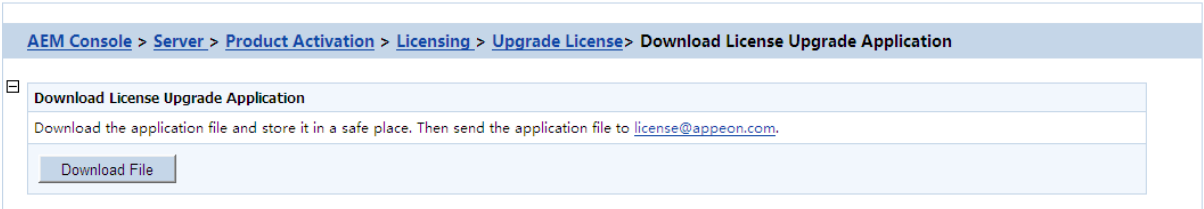
Figure 5.37: Upgrade license



Step 3: Click the **Generate License Upgrade Application** button.

Step 4: Click the **Download File** button to download the request file which is by default named as license.update.bin and send it to `<license@appeon.com>`. The request will be processed in Appeon and an upgraded license will be sent to you later.

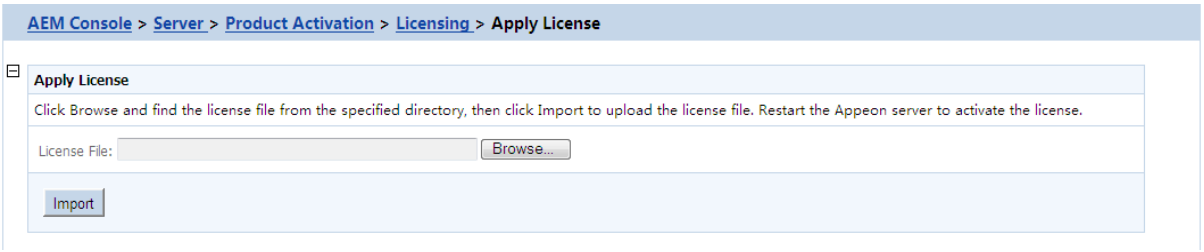
Figure 5.38: Download license upgrade request



Step 5: After receiving the upgraded license from Appeon, click the **Apply License** button in the **Upgrade License** page.

Step 6: Click the **Browse...** button and select the license.appeon file. Click the **Import** button to import the license file. Please make sure the license file is imported successfully, and then restart PowerServer.

Figure 5.39: Apply license



Step 7: After you restart PowerServer, go back to the **Licensing** page, and verify that the license information is updated, and the **Activation Status** is shown as **Activated**.

5.3.4.2 Support

The Support tool enables you to view the valid product support period, which starts from the day you place the product order and expires in 1 year later. You can renew the support before or after the license expires, and apply the renewed license to extend the support period. **Renew Support** and **Apply License** will be enabled when the product is activated.

Figure 5.40: Support

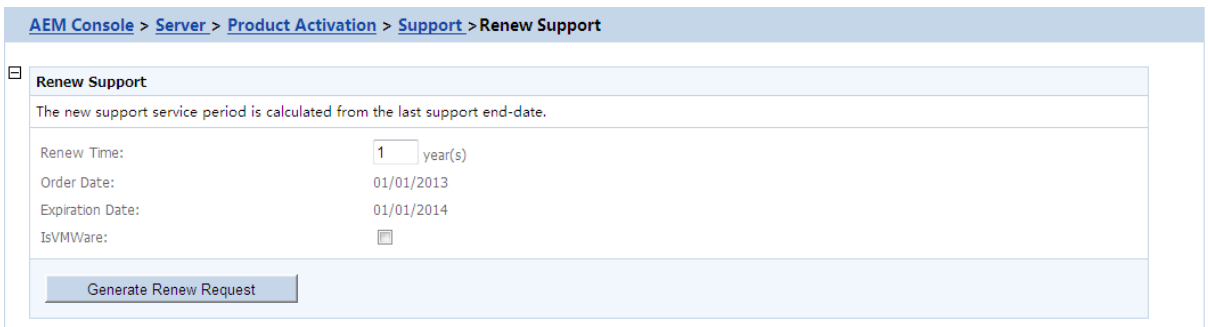
5.3.4.2.1 Renew Support

Support Expiration will not affect the normal running of Appeon. However, after the expiration you are no longer entitled to install product upgrades/EBFs or get technical support assistance from Appeon. You can renew your product support prior to the expiration date to ensure you are benefiting from the latest product enhancements, maintenance releases and the technical support assistance.

If you want to extend the Support, follow the steps below:

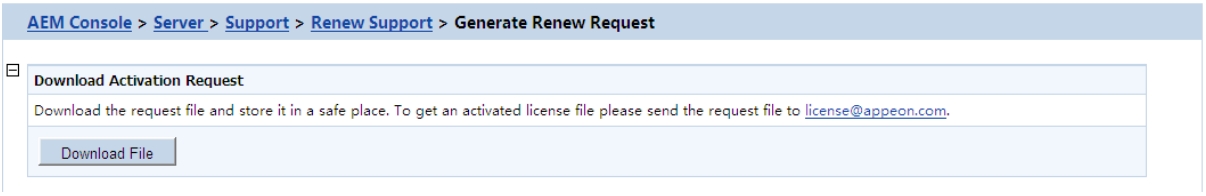
Step 1 - Click the **Renew Support** button. In the **Renew Support** page, enter the time you want to extend, which should only be an integer. Click the **Generate Renew Request** button. Note: The order date is counted from the first date when your last license expired.

Figure 5.41: Renew support



Step 2 - Click the **Download File** button to download the request file which is by default named as license.support.bin and send it to `<license@appeon.com>`. The request will be processed in Appeon and a new license with extended support period will be sent to you later.

Figure 5.42: Generate renew request

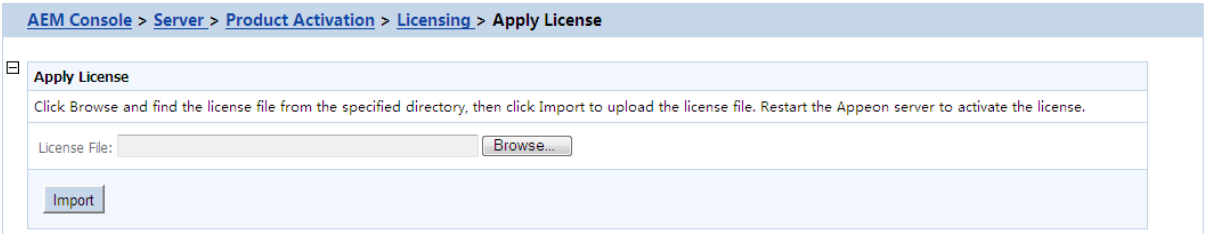


Step 3 - When you get the new license named license.appeon, click the **Apply License** button.

Figure 5.43: Product support

Step 4 - In the **Apply License** window, click the **Browse...** button to select the license.appeon file delivered by Appeon. Click the **Import** button to import your license file.

Figure 5.44: Apply license for support

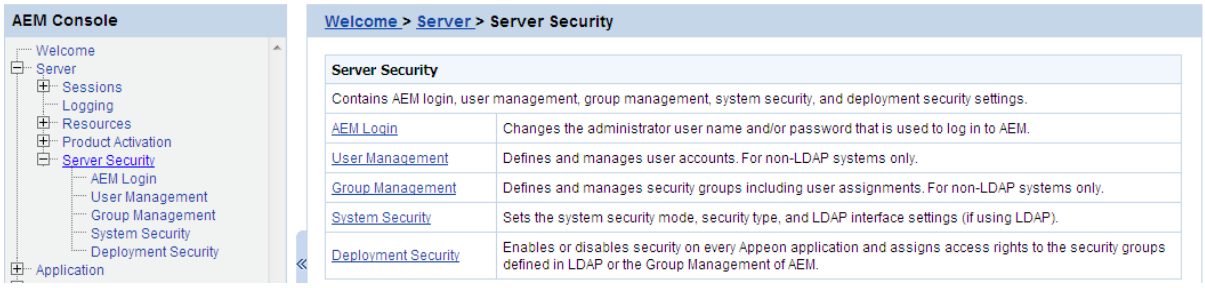


Step 5 - Restart PowerServer after importing the license file, and go back to the **Support** page to ensure the support is correctly extended.

5.3.5 Server Security

Server Security is a set of tools for viewing and modifying all the security on the server side and prevents unauthorized access to the Appeon Web application or the Appeon mobile application using an existing LDAP installation or Appeon's built-in application security. There are five tools: AEM Login, User Management, Group Management, System Security, and Deployment Security.

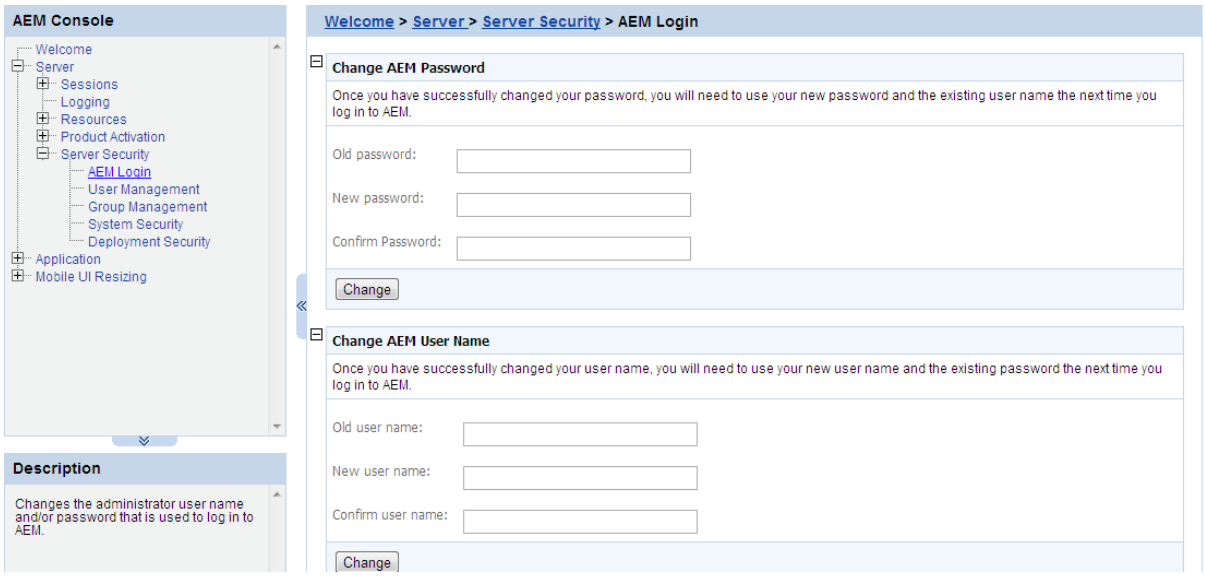
Figure 5.45: Server Security



5.3.5.1 AEM login

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

Figure 5.46: 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:

- 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:

- 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 PowerServer. 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.

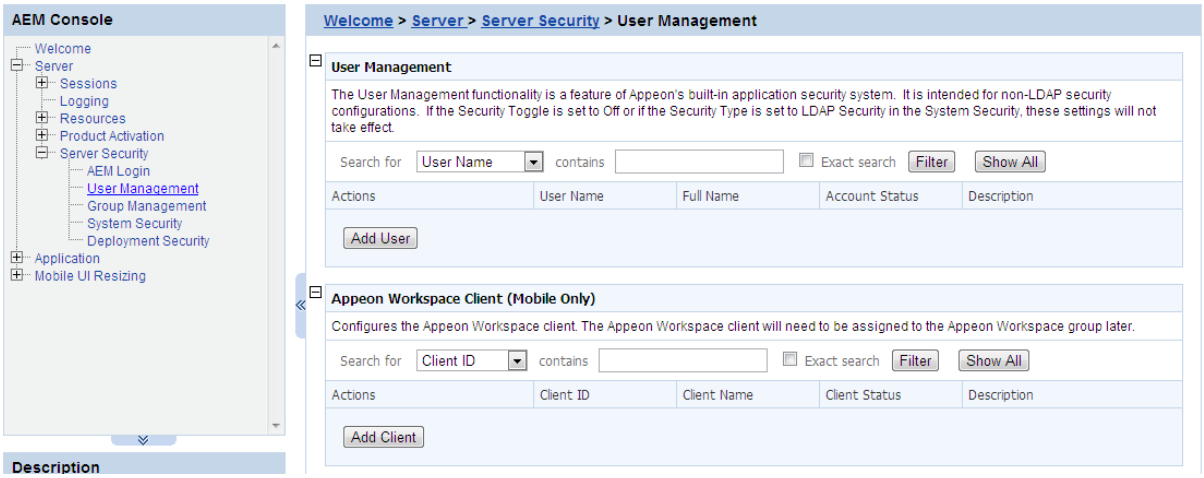
5.3.5.2 User Management

The **User Management** tool in AEM can be used to manage two types of users:

1. user accounts for all Appeon applications including Web apps and mobile apps
2. Appeon Workspace clients for the Appeon mobile application running in Appeon Workspace

You can create, edit and remove users in this tool. After you create the user, you can assign the users to groups in the Group Management tool.

Figure 5.47: User Management



5.3.5.2.1 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.

On 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.

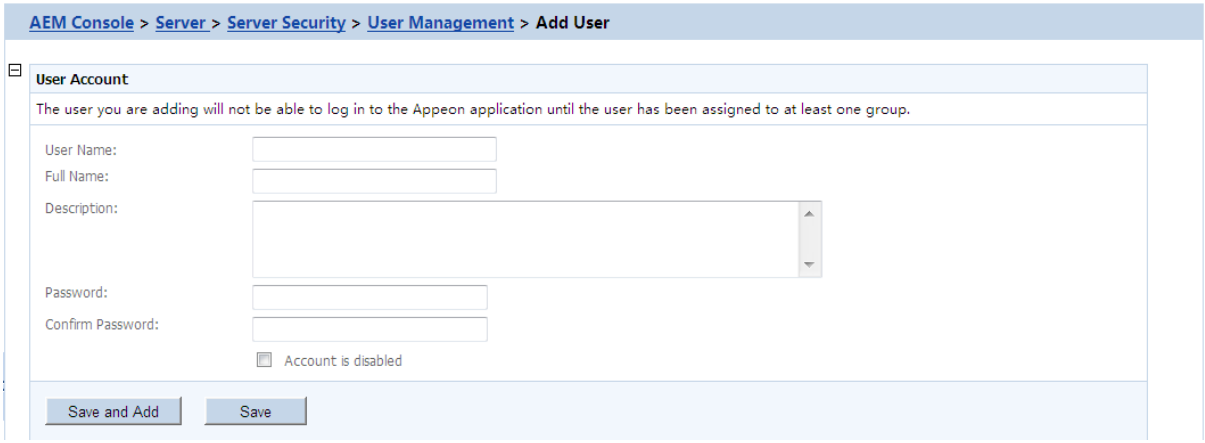
   Step 3: Enable or disable the "**Exact search**".

   Step 4: Click the **Filter** button. Users that meet the criteria will be displayed.

Adding a new user

If you want to add one or more users, click the **Add User** button on the **User Management** page and the **Add User** page will be displayed.

Figure 5.48: 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.

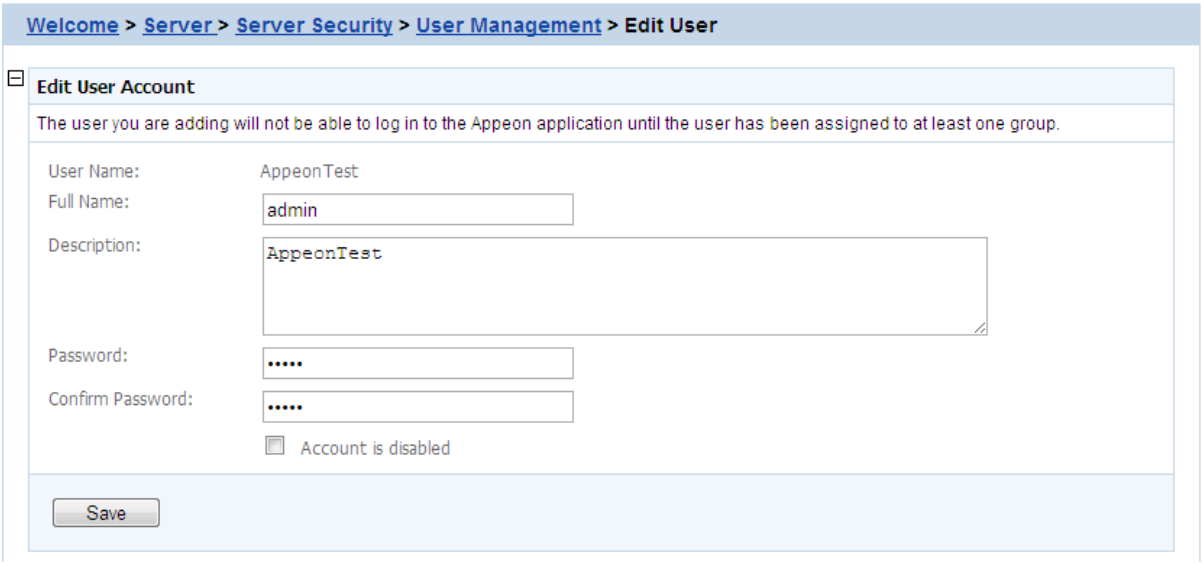
  When the account status is disabled, the user cannot load any application with the username and password if the application requires user authentication.

  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).

Editing an existing user

By clicking the **Edit** button on the **User Management** page, you can enter the **Edit User** page to edit an existing User.

Figure 5.49: Add a 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 Adding a new user.

After making any changes, click the **Save** button. The changes are updated in PowerServer.

Deleting a user

Delete a user by clicking the **Delete** button on the **User Management** page. 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.

5.3.5.2.2 Appeon Workspace Client (Mobile only)

Appeon Workspace Client is intended for security configurations for mobile applications. It works along with Appeon Workspace Group to add extra security to your Appeon Workspace applications.

Viewing Appeon Workspace clients

In the **Appeon Workspace Client** table on the **User Management** page, you can view all the existing clients and associated client information in the system. And you can view them in the following two ways. By default, all the existing clients are displayed.

1. Click the **Show All** button to display all the clients.
2. Specify a filter criteria to view certain clients:

   Step 1: Select **Client ID**, **Client Name**, **Client Status**, or **Description** from the **Search Field** dropdown list box.

Step 2: Type your relevant keywords in the keyword text box.

Step 3: Enable or disable the **Exact Search** check box.

Step 4: Click **Search**. Clients that meet the criteria will be displayed.

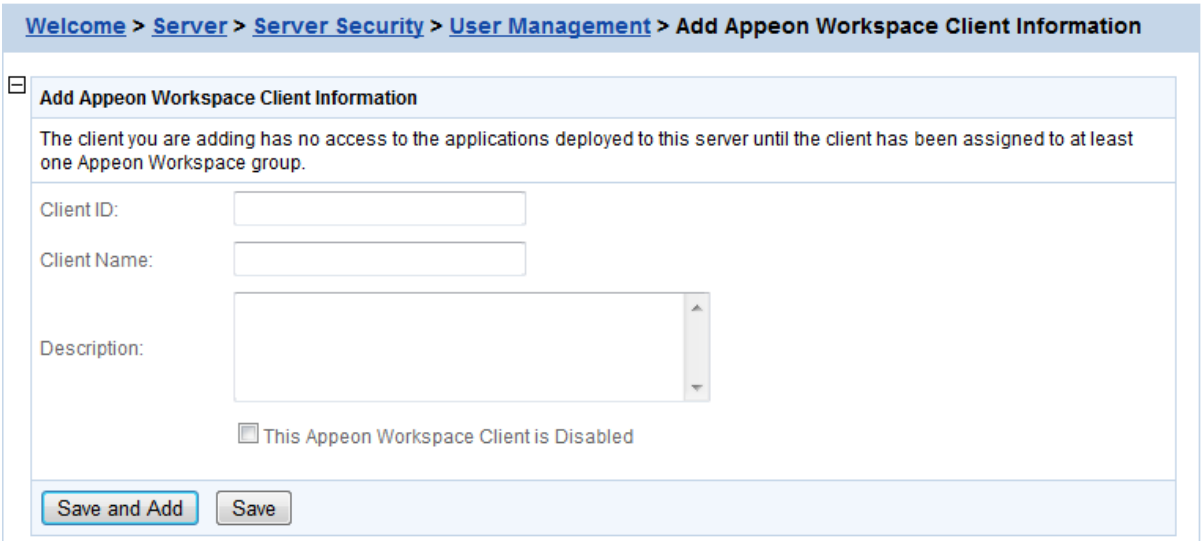
Adding an Appeon Workspace client

To add an new Appeon Workspace client:

Step 1: Click **Add Client** in the **Appeon Workspace Client** table.

Step 2: On the **Appeon Workspace Client ID** page that displays, type a client ID in the **Client ID** text box; enter a client name in the **Client Name** text box; and then enter some descriptions for the client in the **Description** text box.

Figure 5.50: Add Appeon Workspace Client



Step 3: (Optional) If you want to disable the Appeon Workspace client so that it cannot access any Appeon mobile application on this PowerServer, select the **This Appeon Workspace Client is Disabled** checkbox.

Detailed configuration descriptions are shown in the following table.

Table 5.1: Add Appeon Workspace Client Items

Items	Descriptions
Client ID	The unique identifier to identify the mobile device. It must be the same value as the Appeon Workspace ID which can be obtained from the **About** window of **Appeon Workspace**. See the Appeon Workspace User Guide for details.
Client Name	The display name of the mobile client. It can be any text you like.
Description	Any other information for this mobile client. This field is optional.
This Appeon Workspace Client is Disabled	The client's accessbility to the Appeon mobile application on this PowerServer.

Items	Descriptions
	You can select this checkbox to disable the client account, instead of deleting it. The disabled client cannot access any mobile application on this PowerServer.

Step 4: Click the **Save** button to add the client, or click **Save and Add** to save the client and begin to add another one.

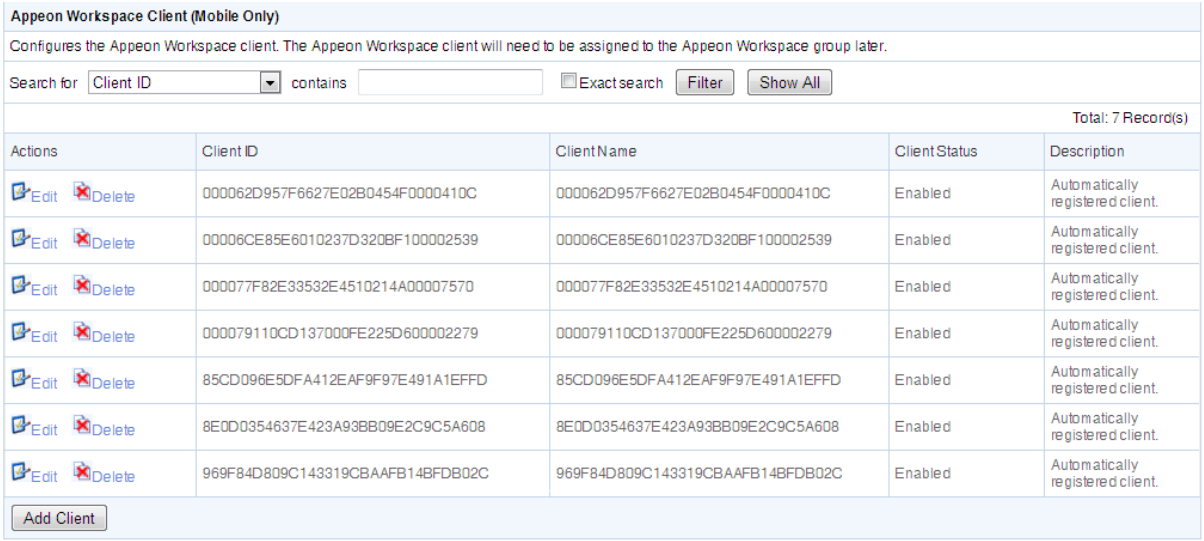
Editing an Appeon Workspace client

To edit an Appeon Workspace client:

Step 1: In the **Appeon Workspace Client** table, click the **Edit** button associated with an Appeon Workspace client ID, and then make the changes you intend to.

You can only change the Appeon Workspace client name and description, and/or you can also enable or disable a client by selecting or deselecting the **This Appeon Workspace Client is Disabled** checkbox.

Figure 5.51: Edit Appeon Workspace Client



Step 2: Click **Save** to save the changes.

Deleting an Appeon Workspace client

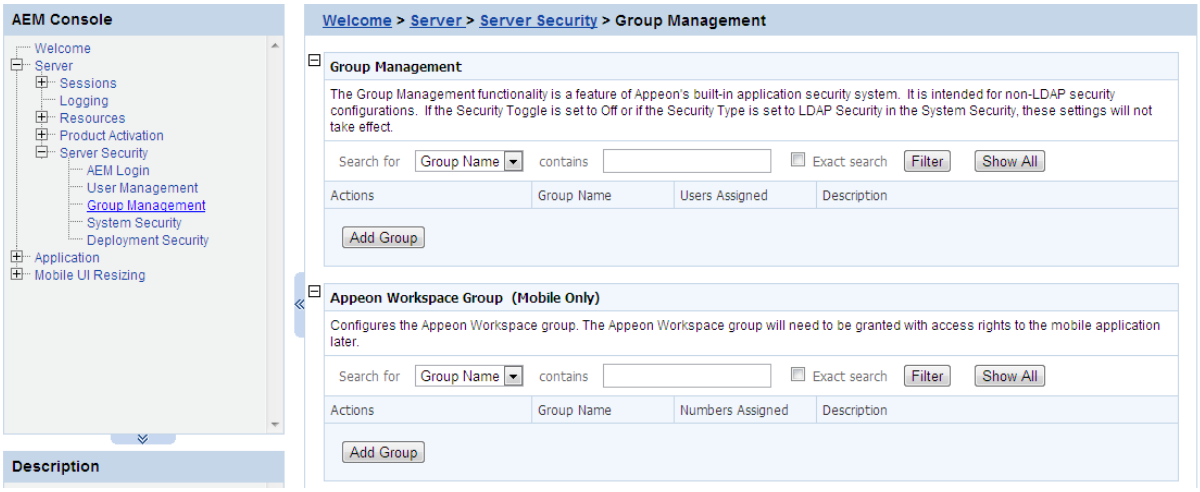
To delete an Appeon Workspace client, click the **Delete** button associated with an Appeon Workspace client ID in the **Appeon Workspace Client** table, and click **OK** to confirm the deletion in the popup dialog box.

You can only delete the Appeon Workspace client one by one.

5.3.5.3 Group Management

The **Group Management** tool in AEM is used to manage user groups and Appeon Workspace groups.

Figure 5.52: Group Management



5.3.5.3.1 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.

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.

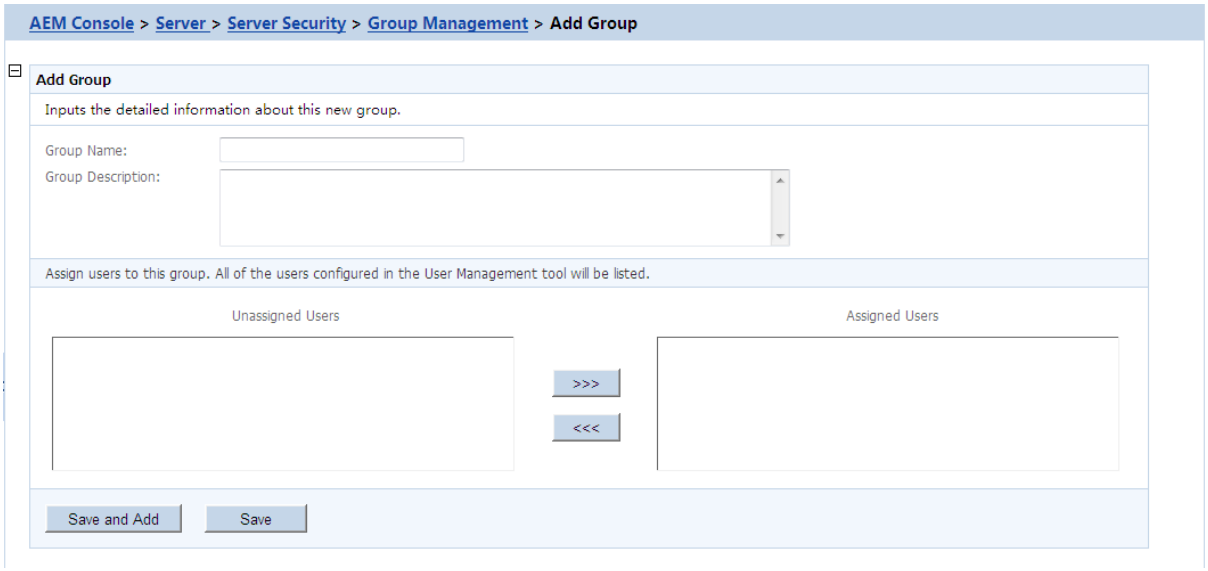
   Step 3: Enable or disable the **Exact search**.

   Step 4: Click the **Filter** button and the groups that meet the criteria will be displayed.

Adding a new group

To add one or more groups, click the **Add Group** button in the **Group Management** table and the **Add Group** page will be displayed.

Figure 5.53: 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 the User Management tool.

  2. To unassign a user from the group

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

Editing an existing group

To edit a specific group, click the **Edit** button in the **Group Management** page 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 Adding a new group.

Deleting a group

Delete a group by clicking the **Delete** button in the **Group Management** page. 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.

5.3.5.3.2 Appeon Workspace Group

Appeon Workspace Group is intended for security configurations for mobile applications.

Viewing Appeon Workspace user groups

In the **Appeon Workspace Group** table, you can view all the groups and associated group information in the system. And you can view them in the following two ways. By default, all the existing groups are displayed.

1. Click the **Show All** button to display all the groups.
2. Specify a filter criteria to view certain groups:

   Step 1: Select **Group Name** or **Description** from the **Search Field** dropdown list box.

   Step 2: Type your relevant keywords in the keyword text box.

   Step 3: Enable or disable the **Exact Search** check box.

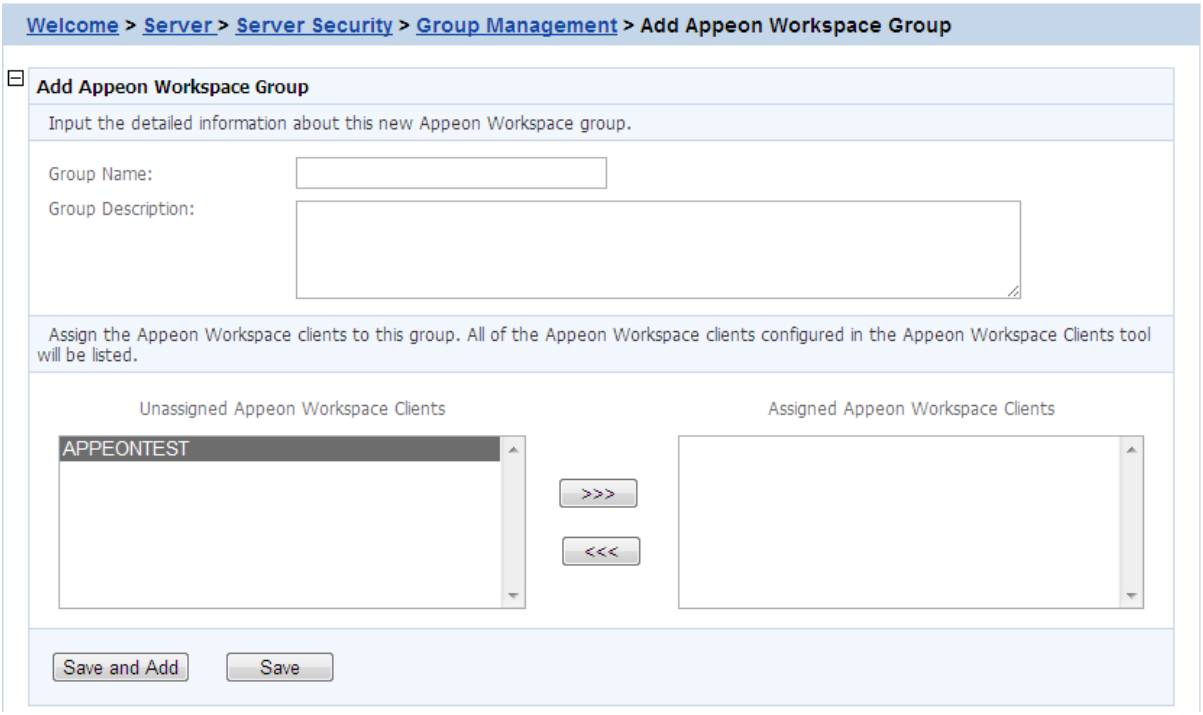
   Step 4: Click **Search**. Groups that meet the criteria will be displayed.

Adding an Appeon Workspace group

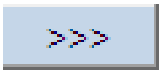
To add a new Appeon Workspace group:

Step 1: In the **Appeon Workspace Group** table, click **Add Group**.

Figure 5.54: Add Appeon Workspace Group



Step 2: On the **Add Appeon Workspace Group** page that displays, type a group name in the **Group Name** text box, and then enter a description in the **Group Description** text box.

Step 3: Assign users into the **Assigned Appeon Workspace Clients** group by selecting a client name from the **Unassigned Appeon Workspace Clients** list box and then clicking the forward  icon. You can create clients in the Appeon Workspace Client tool.

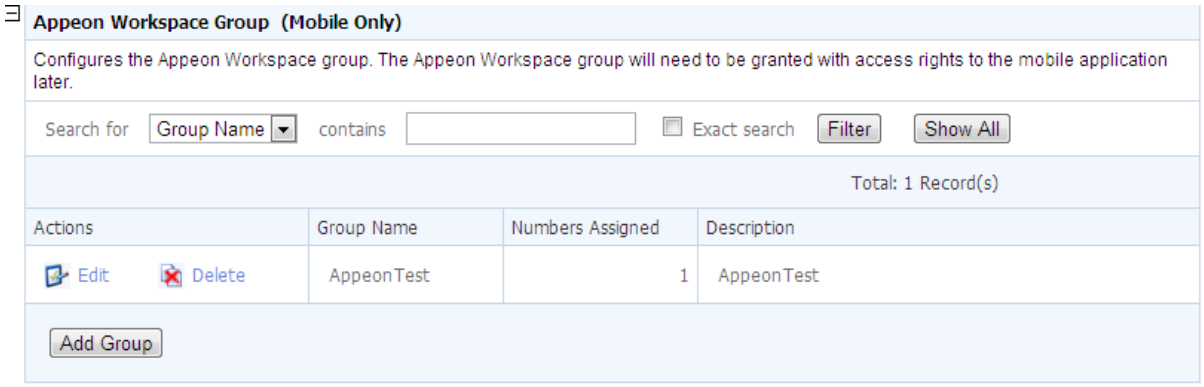
Step 4: Click the **Save** button to save the group, or click **Save and Add** to save the group and begin to add another one.

Editing an Appeon Workspace Group

To edit an Appeon Workspace Group:

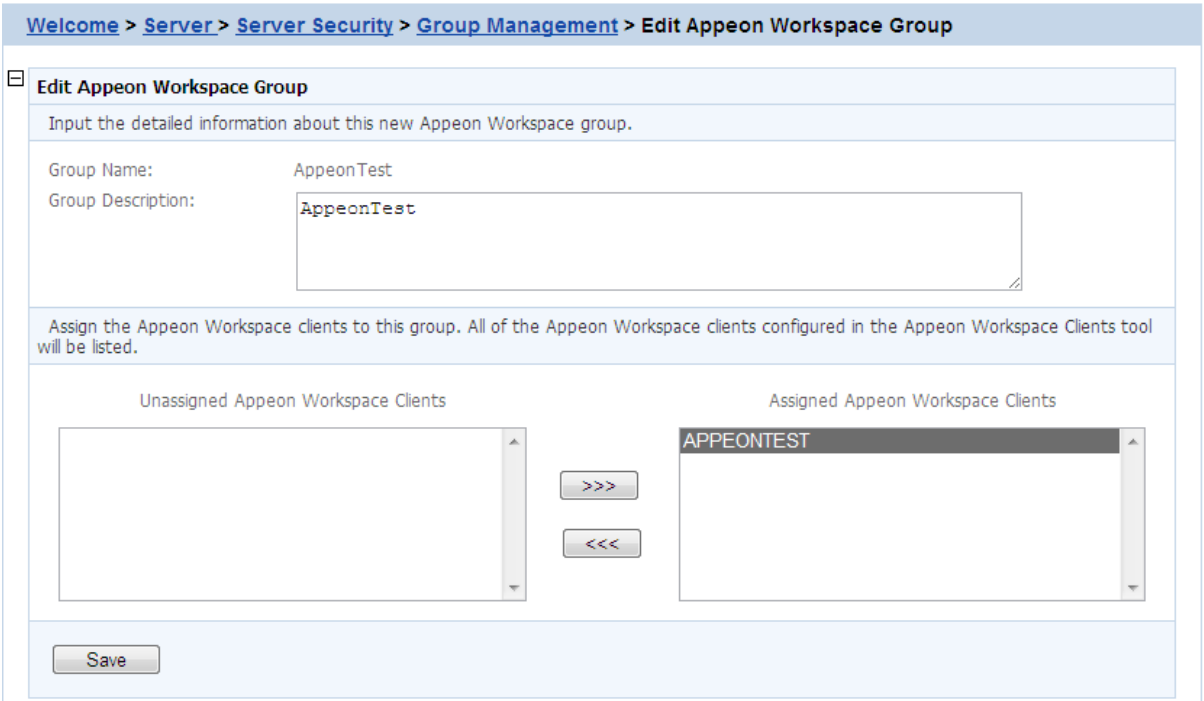
Step 1: In the **Appeon Workspace Group** table, click the **Edit** button associated with an Appeon Workspace group, and then make the changes you intend to.

Figure 5.55: Appeon Workspace Group



You can only change the descriptions and assign new users into the group or delete assigned users from the group, as showing in the following figure.

Figure 5.56: Edit Appeon Workspace Group



Step 2: Click **Save** to save the changes.

Deleting an Appeon Workspace Group

To delete an Appeon Workspace Group, click the **Delete** button associated with an Appeon Workspace group in the **Appeon Workspace Group** table, and then click **OK** to confirm the deletion in the popup dialog box.

You can only delete the Appeon Workspace Group one by one.

5.3.5.4 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/LDAPS server rather than in the user management and group management of AEM. The following are the steps to perform LDAP/LDAPS user and group management:

1. Set up the LDAP/LDAPS server in the system

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

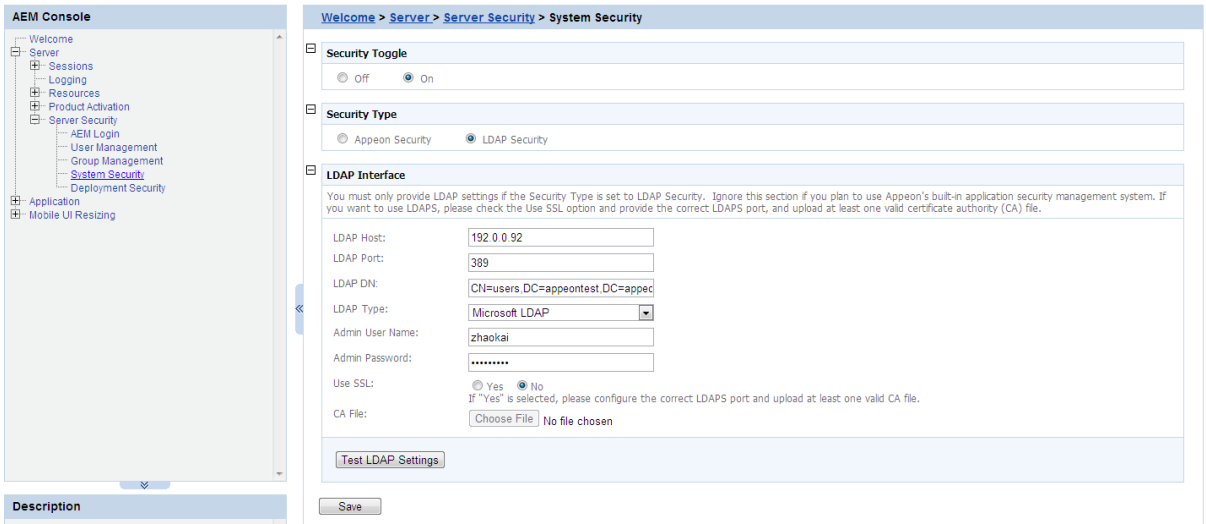
2. Create an organization unit in the LDAP server.

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

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

5.3.5.5 System Security

Figure 5.57: System Security



As the above figure illustrates, the System Security covers three important settings:

- Security Toggle -- Turns application security on and off at the system level. All application security and settings in Client Security 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 PowerServer.

5.3.5.5.1 Security Toggle and Security Type

The following table shows how the Security Toggle and Security Type settings determine which security tools are applied and what security features are performed.

Table 5.2: 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 applications.
On	Appeon Security	User Management Group Management Client Security Deployment Security	The Appeon built-in security is enabled. Only authorized groups and users of a deployed application are allowed to load or deploy the application. Three consecutive invalid logins will result in an exceptional exit of the login dialog from the 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 Client Security Deployment Security	Enabled. Any authorized LDAP groups and users of an application are allowed to load or deploy the application. Three consecutive invalid logins will result in an exceptional exit of the login dialog from the 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 PowerServer or LDAP to assign groups to the application. The security groups will be read from either LDAP (if it is LDAP security) or PowerServer (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.

5.3.5.5.2 LDAP Interface Settings

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

Limitations

There are several limitations about using LDAP with PowerServer:

1. One PowerServer can be configured with only one LDAP domain, which means, all the users and groups must be in a single domain.
2. Only the "Security" type of LDAP Group is supported, not the "Distribution" type.
3. Only "User logon name" (not the "Display name") can be used in the LDAP Logon Dialog when running the application.

For detailed information, please refer to the Appeon LDAP Security Configuration Guide at http://support.appeon.com/index.php?/Knowledgebase/Article/View/22/0/appeon-ldap-security-configuration-guide/.

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 DN -- The distinguished name uniquely identifies the LDAP directory.

  If using Netscape LDAP or Sun LDAP, the LDAP DN 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.

  For Microsoft LDAP, the LDAP DN 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 DN 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, Sun LDAP, Microsoft LDAP, and IBM LDAP.

  Table 5.3: Supported LDAP types

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	Windows 2000, 2003, & 2008 Active Directory
IBM LDAP	Directory Services (LDAP) 5.1

- 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 PowerServer and LDAP Server will use LDAPS protocol. You need to provide the Certificate Authenticated file of LDAPS. If No is selected, the communication between PowerServer and LDAP server will use LDAP protocol.
- Certificate File -- The Certificate authenticated file of LDAPS.

After all the fields are filled, do the following:

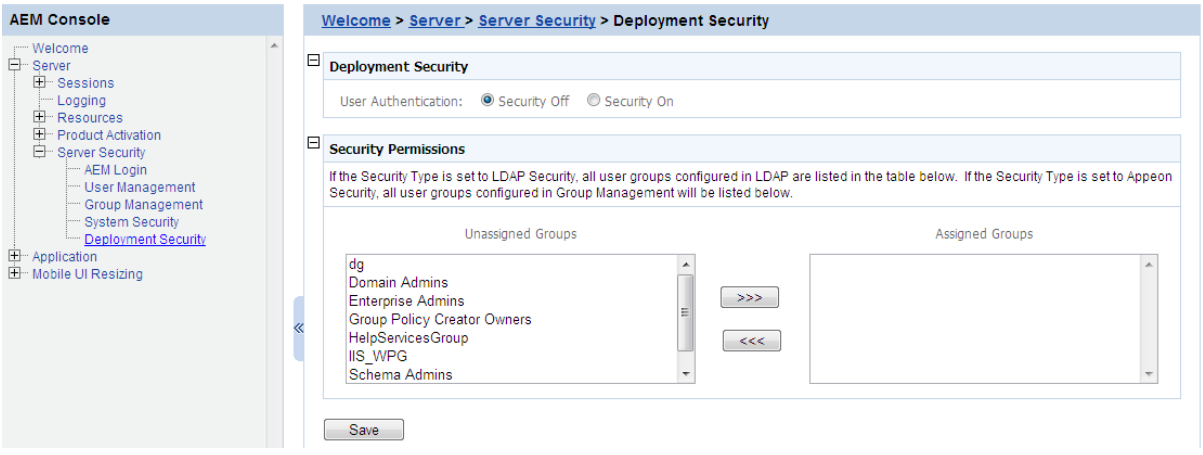
1. Click the **Test LDAP Settings** button to test whether the settings are correct or not. If the message indicates that the settings are incorrect, continue to verify the settings until the LDAP settings are correct.
2. Click the **Save** button.

5.3.5.6 Deployment Security

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

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

Figure 5.58: Deployment Security



The Deployment Security tool enables you to do the following:

1. Disable deployment security for PowerServer

   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

PowerServer profile will be ignored, and the PowerServer profile will always work for application deployments.

2. Enable deployment security for PowerServer

   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 PowerServer. If a user name and password that belongs to the group is specified in the PowerServer profile configuration in PowerServer Toolkit, the profile will work for application deployments. Otherwise, application deployments to the PowerServer profile give an error message "Failed to call methods in PowerServer; cannot find the user..."

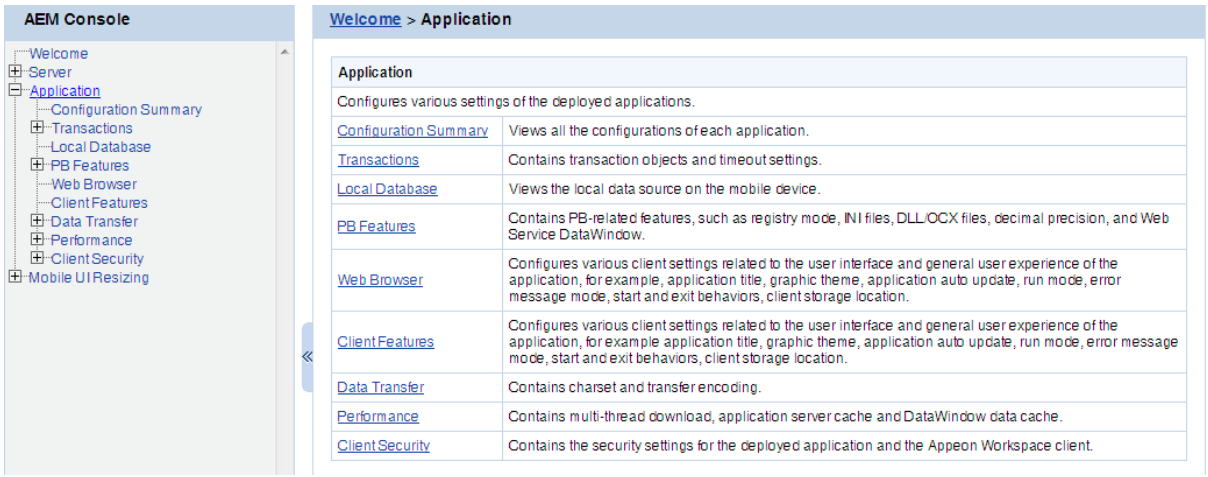
   By default, all groups are listed in the Unassigned Groups list. The groups are read from the PowerServer (if the security type is Appeon security) or the LDAP server (if the security type is LDAP security) in use. You can use back button ("<<<") to shift the group to the Unassigned Groups list.

5.4 Application

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

Application are a set of tools for setting the server-related properties for the Appeon Web application or the Appeon mobile application. There are eight tools: Configuration Summary, Transactions, Local Database, PB Features, Web Browser, Client Features, Data Transfer, Performance, and Client Security. The settings for each application profile affect application(s) deployed from the application profile.

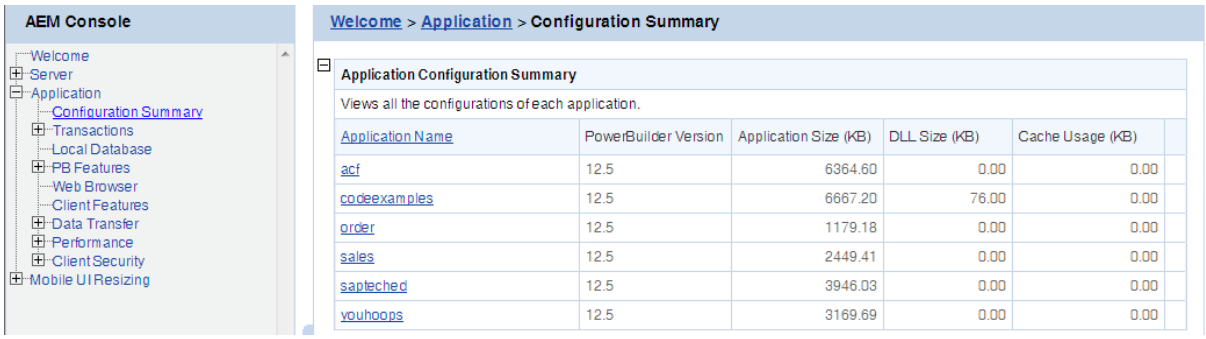
Figure 5.59: Application



5.4.1 Configuration Summary

The Configuration Summary of applications lists all the deployed applications and their configuration summaries.

Figure 5.60: Application Summary



Click **Application Name** to sort the applications.

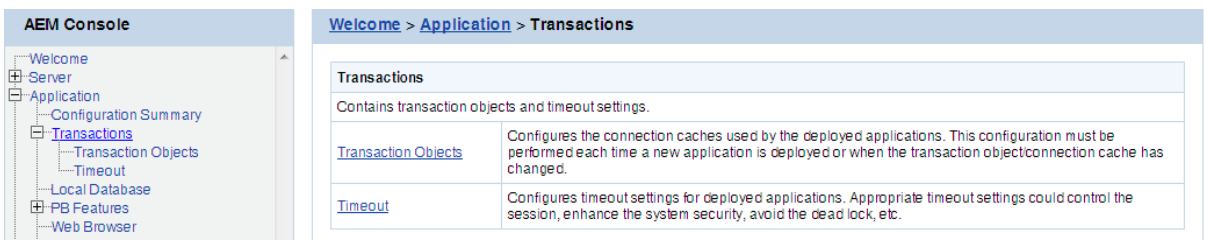
Click on an application to view the summary of the application.

Figure 5.61: Application Configuration Summary

5.4.2 Transactions

Transactions is a set of tools for viewing and modifying all the transaction objects and timeout. There are two tools: Transaction Objects and Timeout.

Figure 5.62: Transactions



5.4.2.1 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, PowerServer handles the database connection using data sources configured in PowerServer rather than transaction objects defined in the PowerBuilder application.

All transaction objects in the PowerBuilder application must be mapped to a correct PowerServer data source. "Correct" means that the data source should be created as a JDBC data source in the application server hosting PowerServer, 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 data source mapping methods:

- Dynamic Transaction object to data source mapping via PowerScript
- Static Transaction object to data source 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 Dynamic transaction object to data source mapping.

5.4.2.1.1 JDBC requirement for transaction object mappings

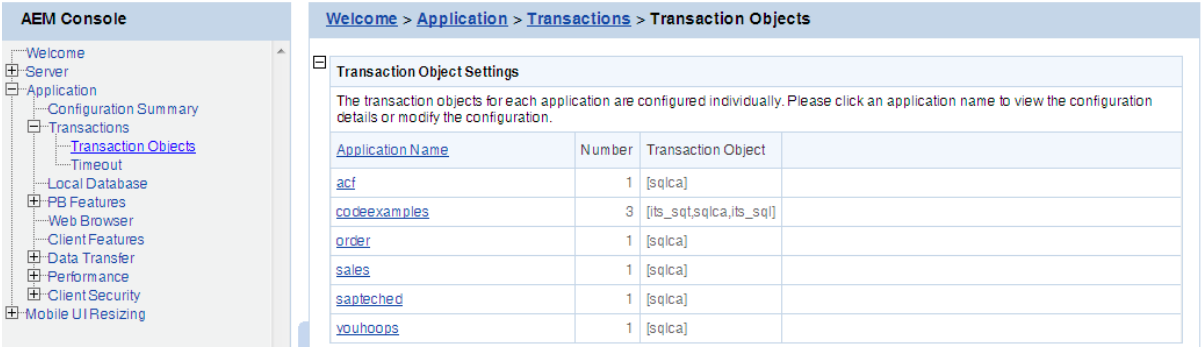
PowerServer is based on J2EE architecture and therefore requires JDBC to interface with the database. The JDBC data sources can use any of the following four types of JDBC drivers: JDBC-ODBC Bridge, Native-API/partly Java driver, Net-protocol/all-Java driver, or Native-protocol/all-Java driver.

Refer to Setting up PowerServer data sources for more information on this topic, including recommendations on which JDBC driver to use and instructions for creating data sources.

5.4.2.1.2 Configuring transaction object mappings

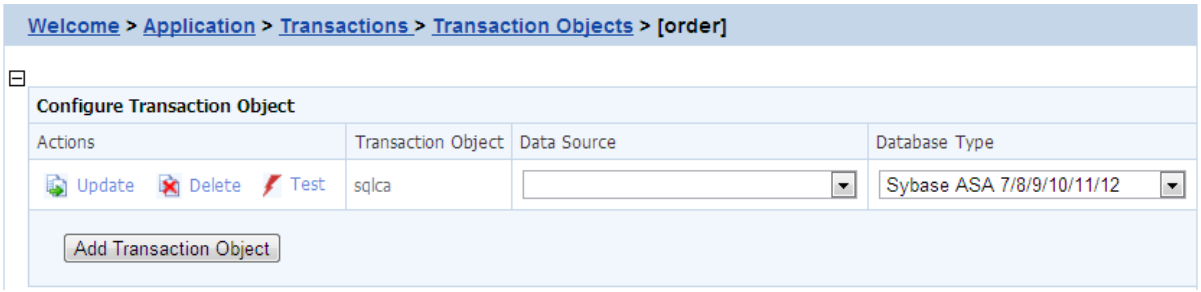
When an application is deployed to PowerServer, AEM automatically adds the application profile name into the application list of the Transaction Objects tool.

Figure 5.63: Applications with transaction objects



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.

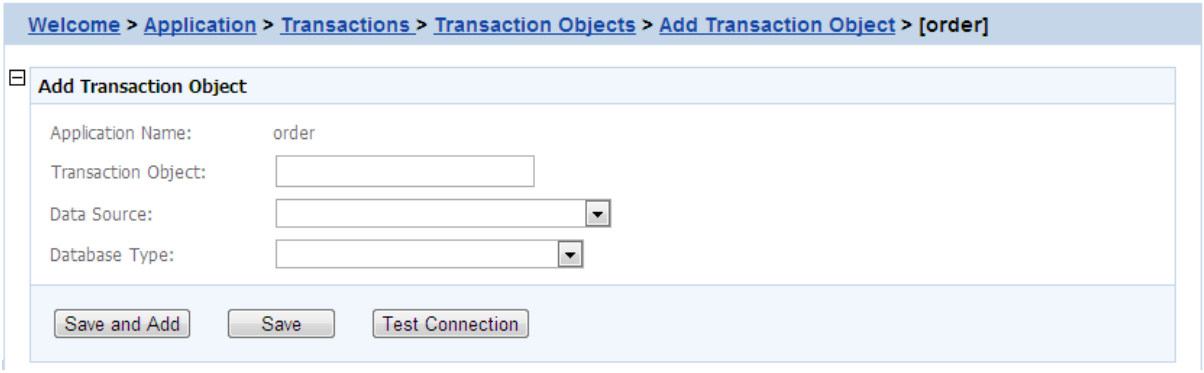
Figure 5.64: Configuring transaction object mappings for an application



Adding a transaction object mapping

Step 1: Click the **Add Transaction Object** button. The Add Transaction Object page appears.

Figure 5.65: 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 data source from the "**Data Source**" dropdown list. The list displays the data sources created in PowerServer.

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

Note: For .NET server, the data source is created in the AEM; while for Java server, the data source is created in the server console provided by the corresponding application server.

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 **Save** or **Save and Add** button if testing data source succeeded.

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

Modifying an existing transaction object mapping

1) To change the data source

For each transaction object, there is a dropdown list in the "Data Source" column. The list box lists the data sources created in PowerServer.

Make sure the selected data source connects to the same database that the transaction object connects to.

You can change the current data source 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 SAP), 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.

Deleting an existing transaction object mapping

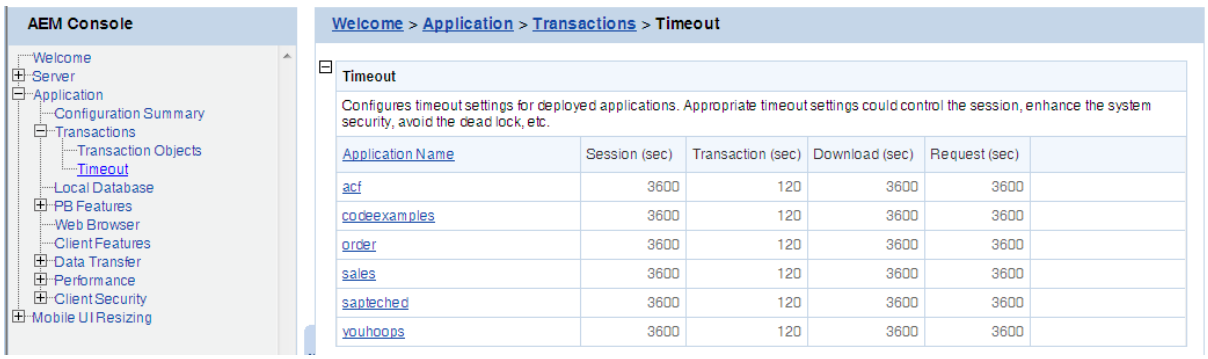
Clicking the **Delete** button will delete a transaction object mapping. A pop-up message will ask you to confirm deletion.

5.4.2.2 Timeout

The Timeout provides configuration for four important functions of PowerServer for the deployed applications:

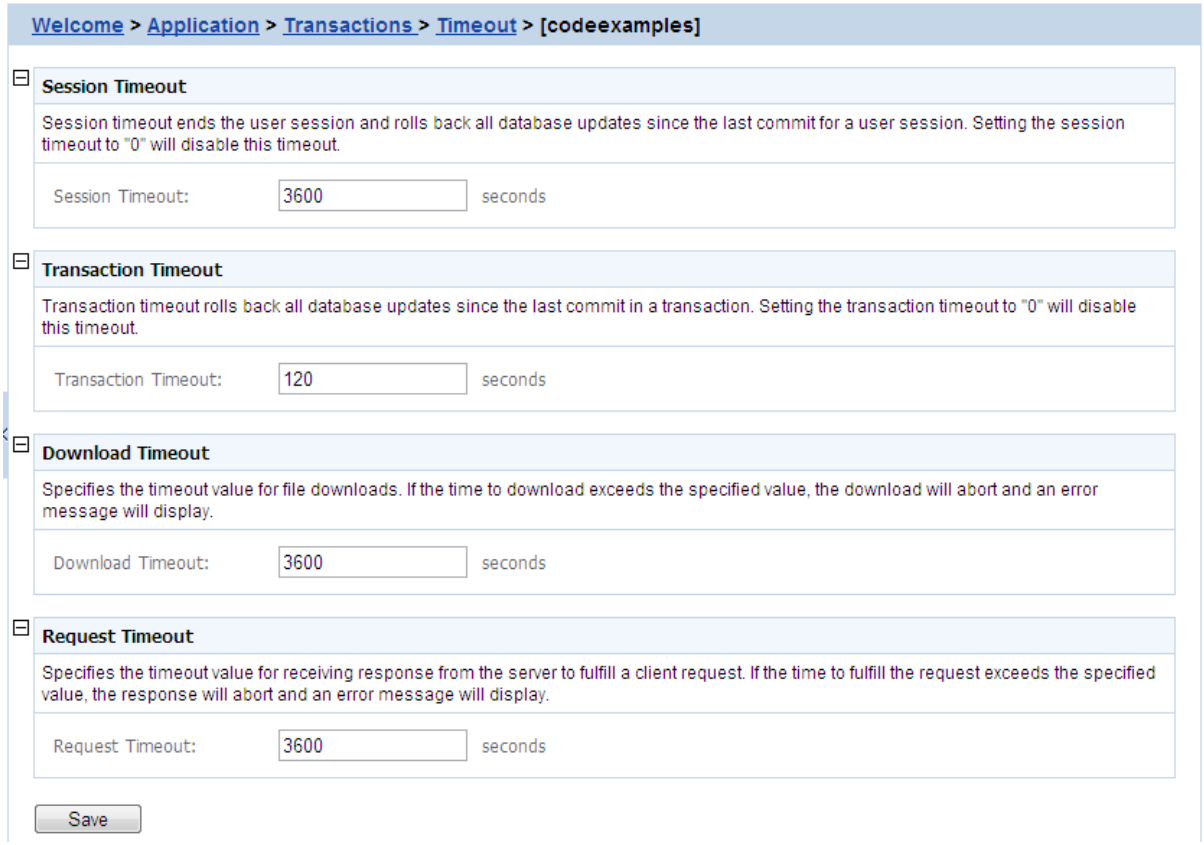
- When the session will timeout (Session Timeout)
- When the transaction will timeout (Transaction Timeout)
- When the file download will timeout (Download Timeout)
- When the message request will timeout (Request Timeout)

Figure 5.66: 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.

Figure 5.67: Timeout settings



5.4.2.2.1 Session timeout

A session starts when the user sends a request to load an Appeon 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. Session Timeout period should be greater than the Transaction Timeout period. Generally speaking, the session timeout period should not be smaller than 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.

5.4.2.2.2 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 (1 to 3600), because a small transaction timeout value can prevent:

- Database locking. When an Appeon Web or Appeon mobile application closes abnormally, the active transaction in it can neither commit nor roll back.

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

The default value is 120 seconds. Transaction Timeout should be less than Session Timeout.

If transaction timeout in the application database is set to 1800 seconds, then Transaction Timeout in AEM should be set to 1810 or larger. If transaction timeout in the application database is not set, then Transaction Timeout in AEM should be set to a number greater than the maximum time needed to execute regular database operations for the application, suppose the most time-consuming table query operation takes 3000 seconds to complete, then Transaction Timeout should be set to 3010 or larger.

5.4.2.2.3 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.

5.4.2.2.4 Request timeout

It takes time for each request to receive response from PowerServer 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.

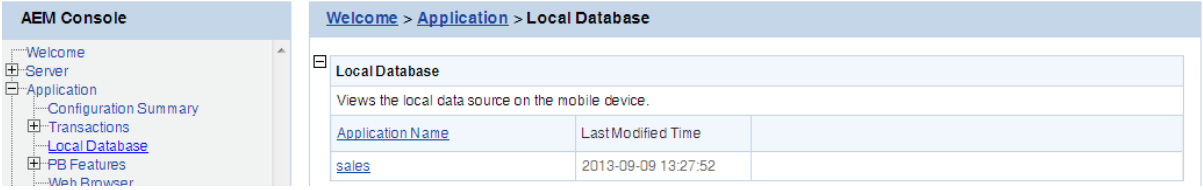
5.4.3 Local Database

Note: This tool is for Web applications only.

In the Local Database tool, you can view the local database settings configured in the Local DB Settings tab in PowerServer Toolkit after the application is deployed. For details, refer to Section 4.2.1.2.6, “Offline Settings” in *PowerServer Toolkit User Guide*.

When an offline application is deployed to the PowerServer, AEM automatically adds the application profile name into the application list of the Local Database tool.

Figure 5.68: Local database

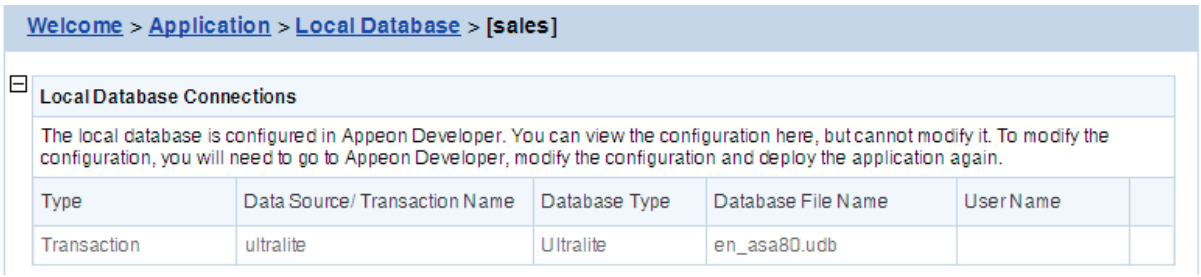


5.4.3.1 Viewing local database connections for an application

To view the local database connections for an application, click the application name in the **Local Database** table, and the **Local Database Connections** table appears.

You can only view the local database connections. To modify the local database connections for an application, you need to modify them in Local DB Settings in *PowerServer Toolkit User Guide* (in PowerServer Toolkit), and deploy the application again to make the changes take effect.

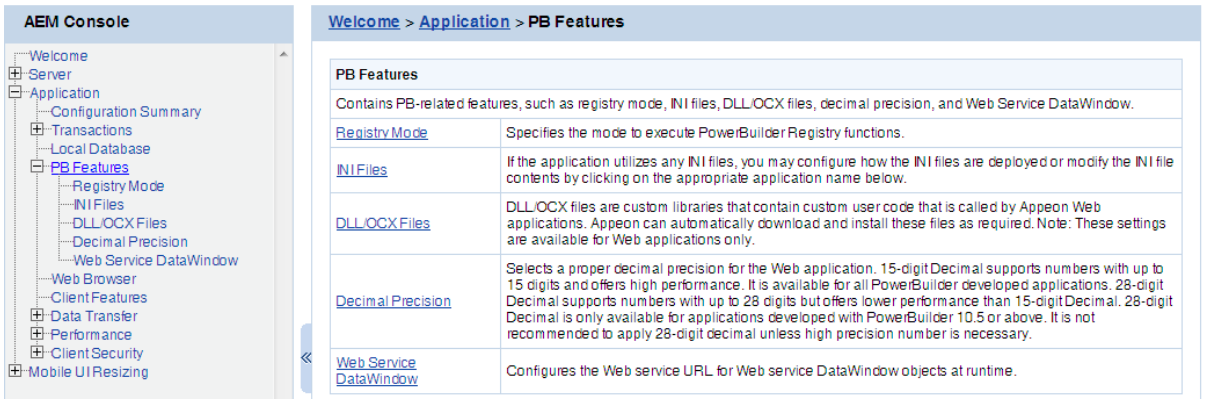
Figure 5.69: Local database connections for an application



5.4.4 PB Features

PB Features is a set of tools for viewing and modifying Registry Mode, INI Files, DLL/OCX Files, Decimal Precision, and Web Service DataWindow.

Figure 5.70: PB Features



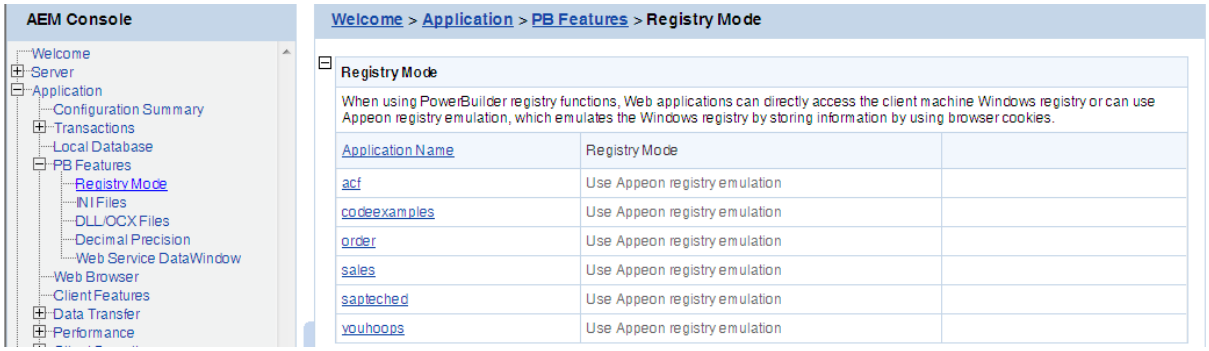
5.4.4.1 Registry Mode

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

Note: Mobile applications can only read Appeon emulation registry.

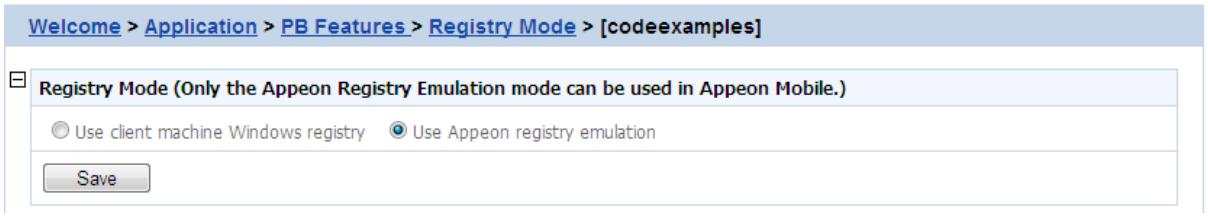
Appeon emulation registry refers to the mock registry file stored in the PowerServer database. It keeps the registry settings users specify when executing RegistrySet. Because it initially has no values, with the Appeon emulation registry method, users must first set values using RegistrySet before reading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

Figure 5.71: Registry Mode



Click the application name listed in **Registry Mode** table, and then select one registry mode on the page that appears, and then click **Save**.

Figure 5.72: Registry Functions Execution Mode



By default, all the Appeon applications are set to "Use Appeon registry emulation".

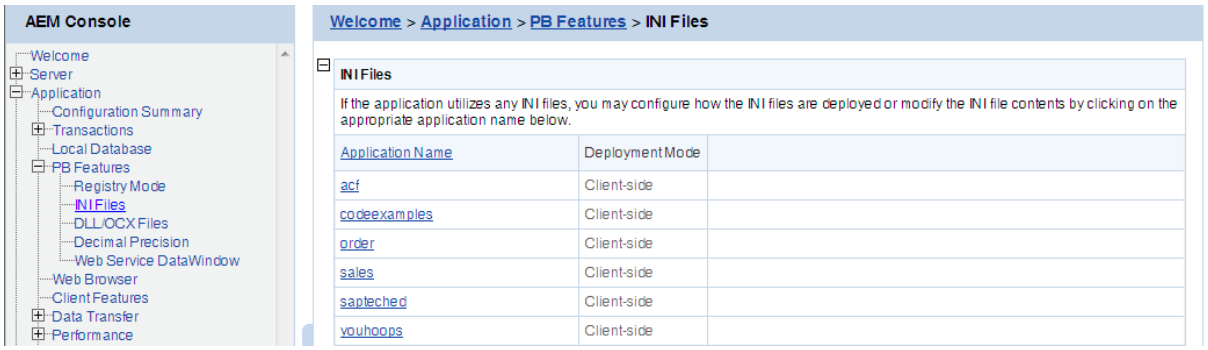
Appeon recommends you change the default value to “Use client machine Windows registry” if the application is deployed as a Web application. This option is recommended because it enables the application to directly interact with the client registry, the same as that in PowerBuilder.

Note: for "Client machine Windows registry", 32-bit IE browser and 64-bit IE browser use different registries, even they are on the same machine, which means, if the application runs in a 32-bit IE and a 64-bit IE separately on the same machine, it reads different registries, thus uses different registry settings to execute registry functions.

5.4.4.2 INI Files

The INI Files tool determines whether the Appeon deployed applications would download XML files that emulate INI files to the clients for profile functions, or directly use the XML files stored in PowerServer database, and it also provides the function to allow you to view and modify the INI file contents of the application.

Figure 5.73: INI files

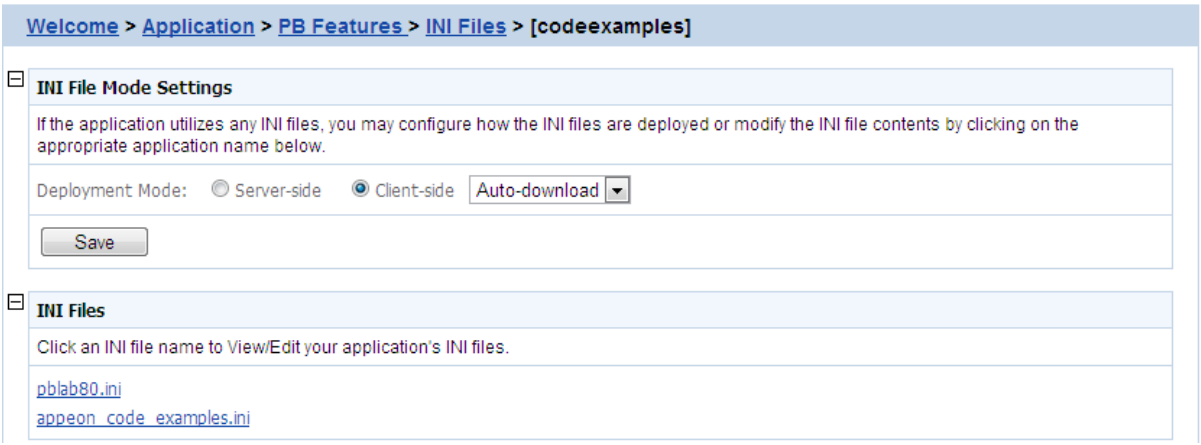


5.4.4.2.1 INI File Mode

Note: This part is for Web applications only.

Click the application name in the "Application Name" column of the table to select the deployment mode for the application and view or modify the contents of the INI Files.

Figure 5.74: INI file mode settings



In the server-side manipulations mode, the PowerServer 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:

1. in the %Windows%\system32\AppeonINI\ directory at the client side, if you have selected the **Default User Profile Location** or the **Browser Cache Folder** option in Client Storage Location.

2. in the specified directory, if you have selected **Customized Location** in Client Storage Location.

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

A. The "Server-side" mode is supported by the Web application only, while the "Client-side" mode is supported by both the Web application and the mobile application.

B. The "Server-side" mode requires that the Internet Explorer cookie is enabled at each client, while the "Client-side" mode does not. No matter in which Web browser (IE, Edge, Chrome, Firefox, or Opera) you run the application, you will need to enable the Internet Explorer cookie if you want to support the server-side mode.

C. The "Server-side" mode does not work with PowerServer 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 PowerServer cluster.

D. The "Server-side" mode keeps the confidential profile information in PowerServer 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 Web browser would prompt for the user's validation before it downloads the XML file for executing relevant profile function.

Notes:

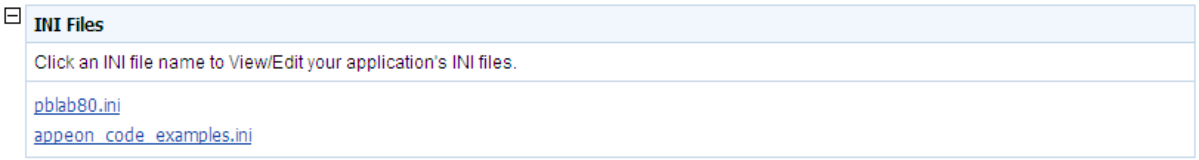
1. AEM does not allow the user to dynamically create an INI file on the local machine. Instead, AEM transfers the INI file from PowerBuilder into an XML file and allows the user to manipulate the XML file on the local machine. The INI file is transferred by PowerServer Toolkit during the parsing process and deployed to PowerServer (for how to deploy INI files, see Deploy INI Files in *PowerServer Toolkit User Guide*).
2. When the "Client-side" mode is selected, the XML file will be downloaded to the local machine at the first time that the user manipulates the INI file. However, note that the INI file after downloaded to the local machine will be named differently and placed in a folder different than the application folder, therefore, it is not recommended to use the FileExists PowerScript function to determine whether the INI file exists. You should remove the FileExists function that checks any INI file to avoid errors when running the Web application.

Click the **Save** button to save changes.

5.4.4.2.2 INI Files

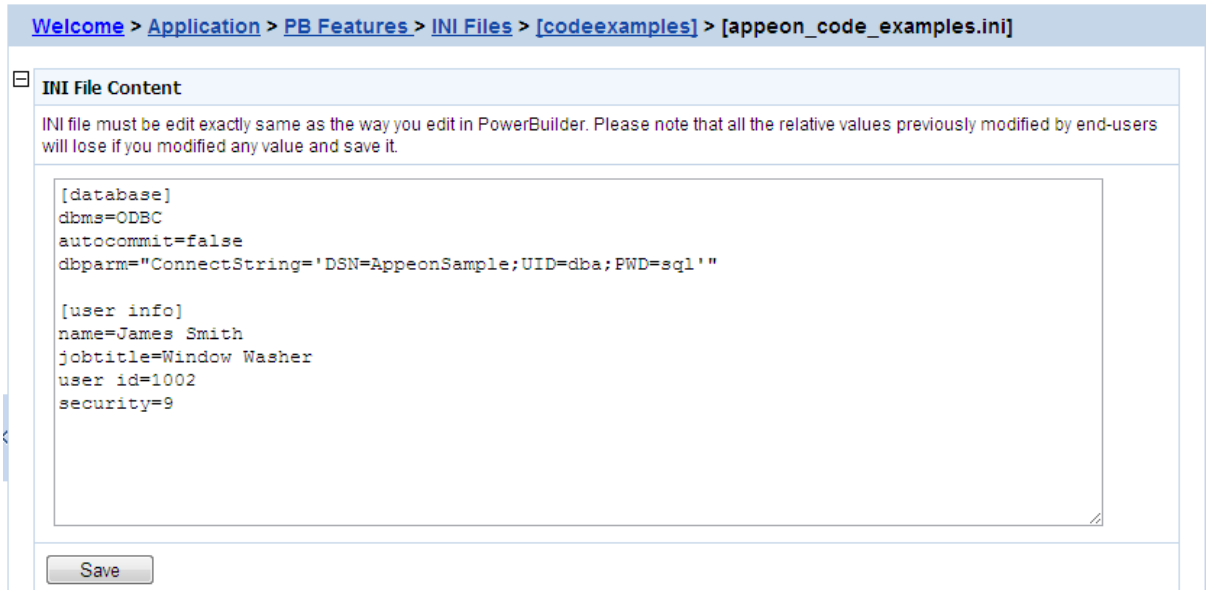
The INI file content tool allows you to view and edit the INI files after the deployment by clicking the name of INI file that you need to view or edit. You need to keep the INI content format here consistent with that in the PowerBuilder.

Figure 5.75: INI files



Click a file name of INI file to view or edit its content.

Figure 5.76: INI file content



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.

Note

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 manipulation 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.

5.4.4.3 DLL/OCX Files

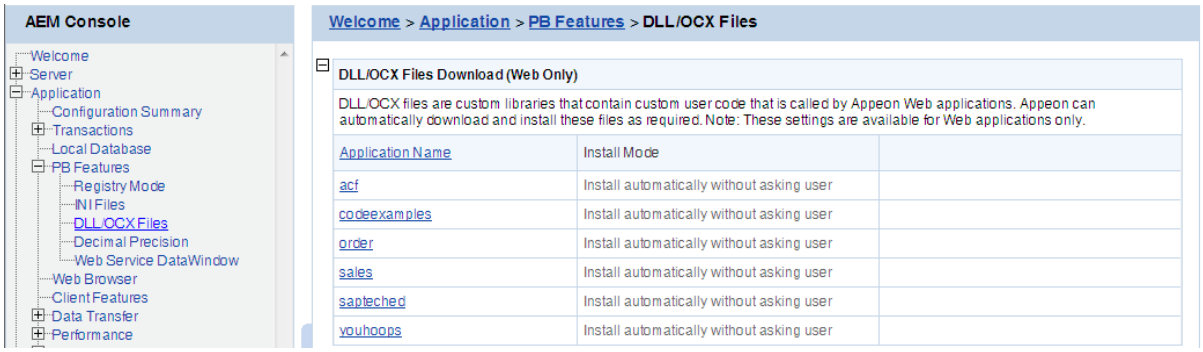
Note: This tool is for Web applications only.

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 Deploy External Files in *PowerServer Toolkit 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 tool.

Figure 5.77: DLL/OCX Files

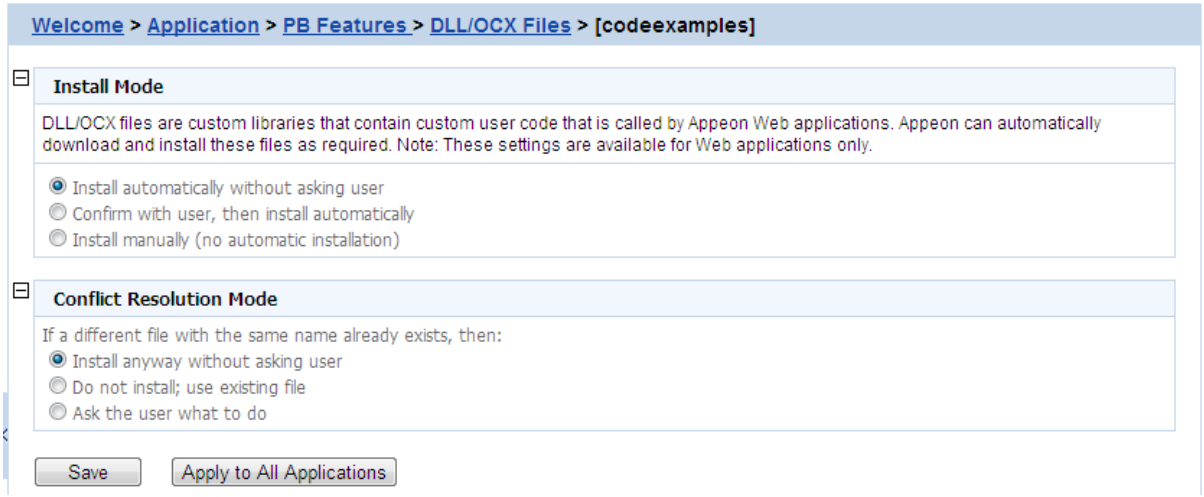


5.4.4.3.1 Install mode

"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, it will be saved to the "plugin" folder under the application directory.

Click the application name listed in the **DLL/OCX files** table, and then select a mode from the **Install Mode** table on the page that appears, and then click **Save**.

Figure 5.78: DLL/OCX Files settings



You can select the install mode that is most suitable for the application according to the description in the following table.

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

Install Mode	Description
	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.

5.4.4.3.2 Conflict Resolution Mode

"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

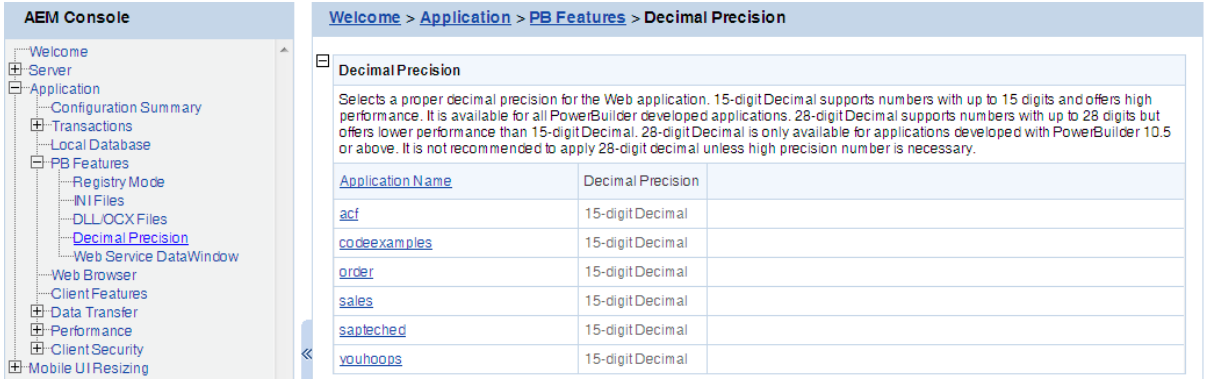
Conflict Resolution Mode	Description
Install anyway without asking user	Default. Directly replaces the file of the same name without notifying you.
Do not install; use existing file	Continues using the existing file.
Ask the user what to do	Displays a message box for the user to select whether to replace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

5.4.4.4 Decimal Precision

The Decimal Precision Settings specifies the decimal precision for the Web or mobile application, you can select a proper one according to your actual needs.

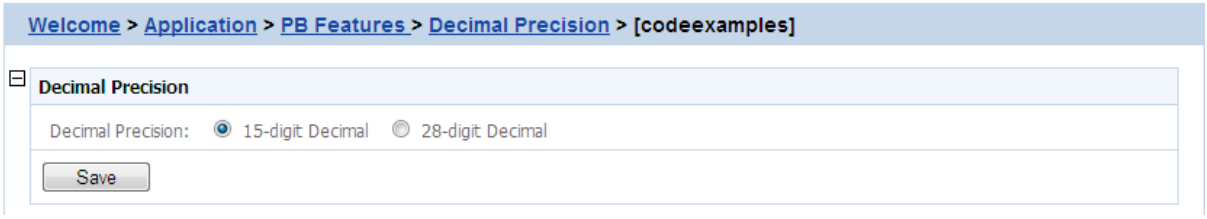
- 15-digit Decimal supports numbers with up to 15 digits and offers high performance. It is available for all PowerBuilder developed applications.
- 28-digit Decimal supports numbers with up to 28 digits but offers lower performance than 15-digit Decimal. 28-digit Decimal is only available for applications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

Figure 5.79: Decimal Precision



Step 1: Click the application name listed in the **Decimal Precision** table, and then select a decimal mode on the page that appears.

Figure 5.80: Decimal Precision Settings

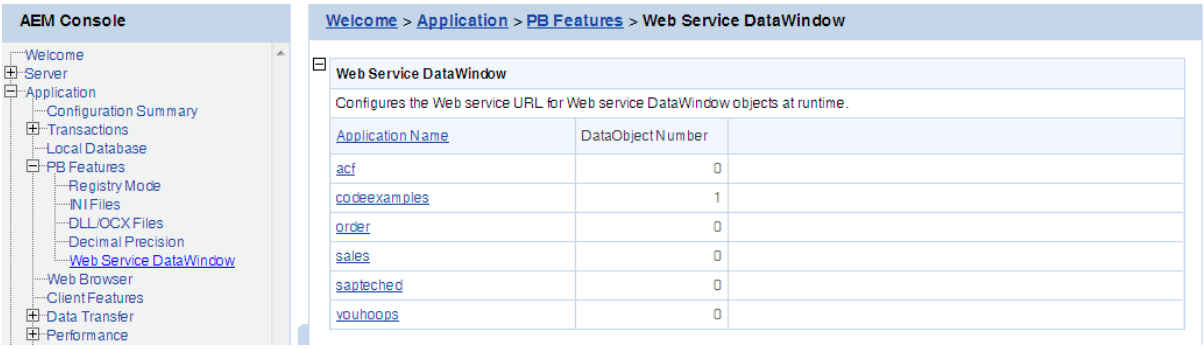


Step 2: Click the **Save** button to save changes.

5.4.4.5 Web service DataWindow

You select the Web service DataWindow object and then configure the Web service URL.

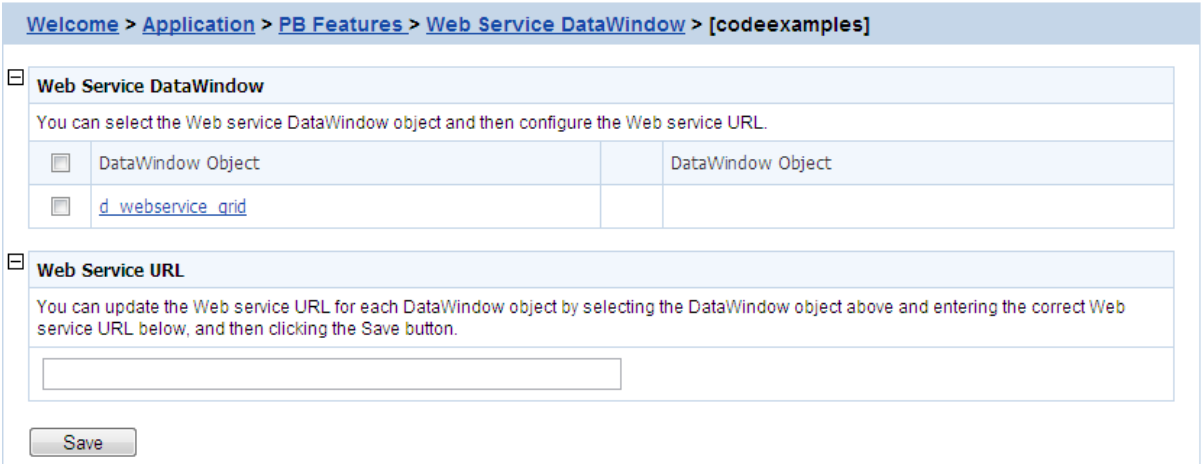
Figure 5.81: Web service DataWindow



This section takes the appeon_code_examples as an example to show how to configure the Web service URL in AEM.

Step 1: Choose **Application** > **PB Features** > **Web Service DataWindow** on the left pane of the AEM Console, and then click the application name listed in the **Web Service DataWindow** table.

Figure 5.82: Web service DataWindow for appeon_code_examples



Step 2: Select the DataWindow Object to configure or modify the Web Service URL(s).

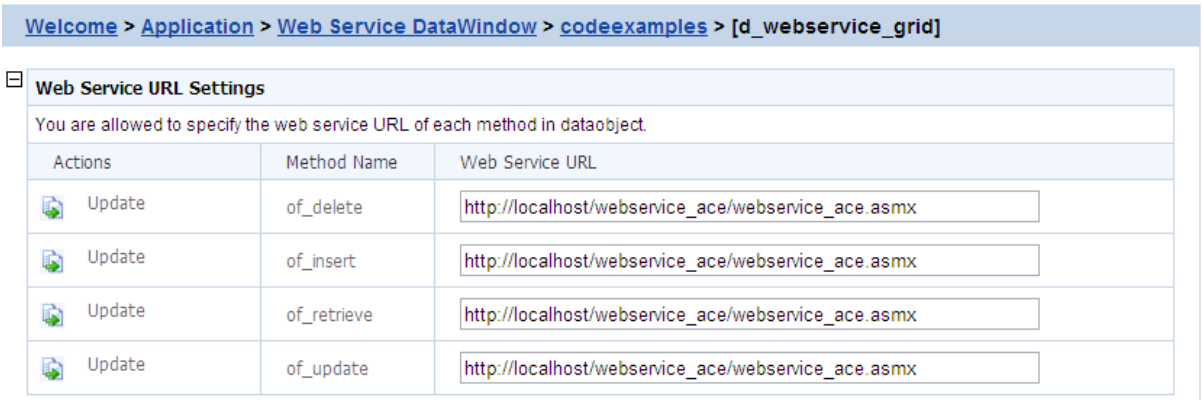
To configure the Web Service URL for all methods of the selected DataWindow object(s):

1. In the **Web Service DataWindow** table, check the DataWindow object(s) for which you want to modify the Web Service URL.
2. In the **Web Service URL** table, input the Web Service URL.
3. Click **Save**. The input Web Service URL will be set to all methods of the selected DataWindow object(s).

To modify the Web Service URLs for a method of a DataWindow object:

1. In the **Web Service DataWindow** table, click the name of the DataWindow.
2. On the Web Service URL Settings page that displays, modify the Web Service URL for a method.

Figure 5.83: Modify URL for DataWindow methods



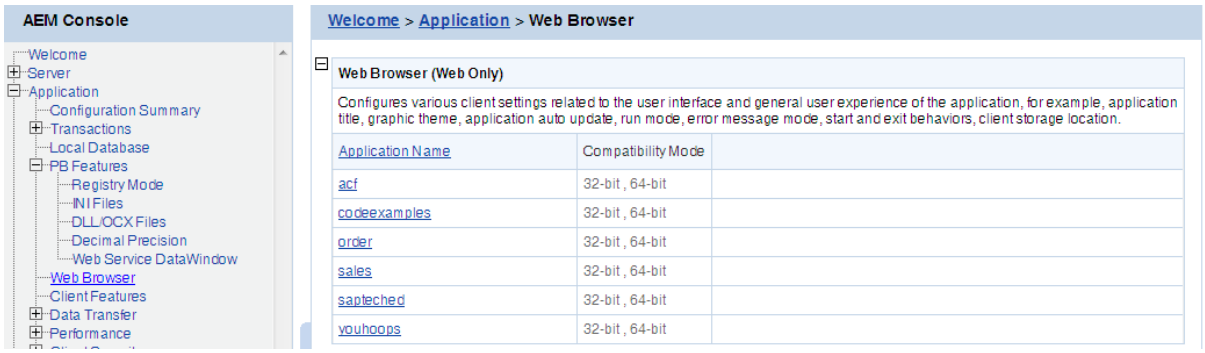
3. Click **Update**.

5.4.5 Web Browser

Note: This tool is for Web applications running in Internet Explorer only.

The Web Browser tool helps you manage and configure IE compatibilities and views.

Figure 5.84: Web Browser



5.4.5.1 IE Compatibility

Appeon Web applications can be run in both 32-bit and 64-bit Internet Explorer; and it will automatically call the compatible PowerServer Web Component. But if the application calls OCX/DLL/OLE files, and depending how you compile the OCX/DLL/OLE files (in 32-bit

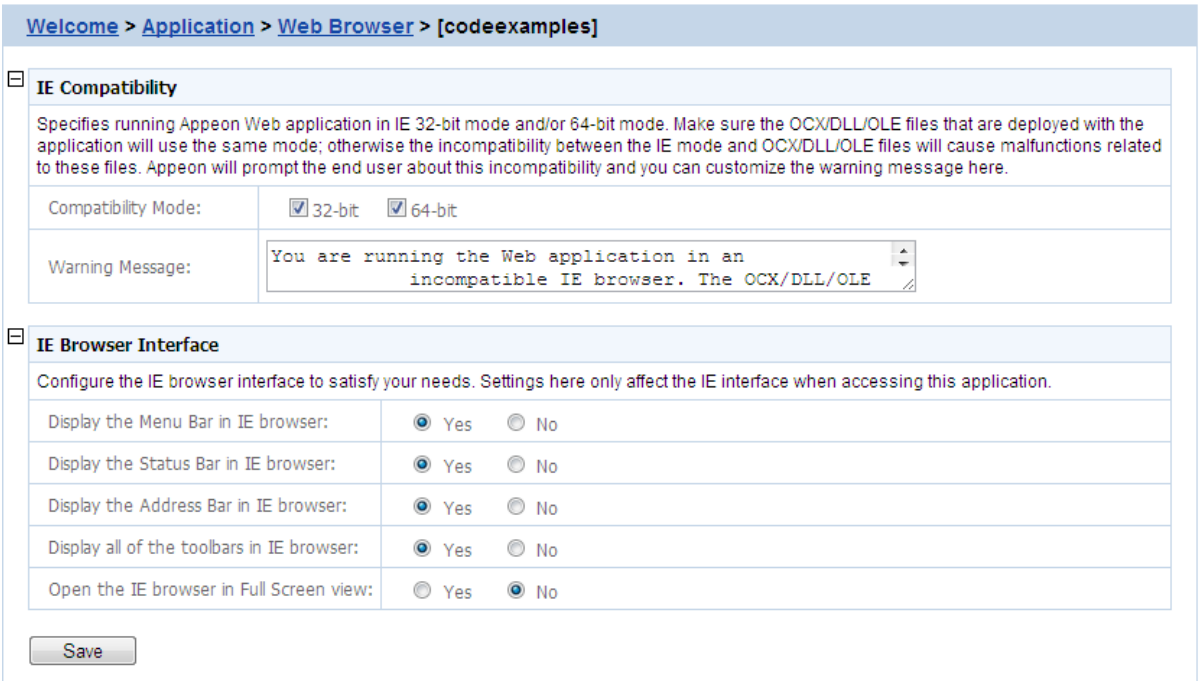
and/or 64-bit), you may want to specify the compatibility mode (32-bit and/or 64-bit) of the OCX/DLL/OLE files in this **IE Compatibility** tool, so if the OCX/DLL/OLE files run in an incompatible browser, the customized warning message will be displayed to the end user.

The other browsers such as Edge, Chrome, Firefox, or Opera only support 32-bit mode, therefore, if you have de-selected the 32-bit compatibility mode here, the warning message will be displayed at runtime when OCX/DLL/OLE files are executed.

Note: 32-bit DLLs can only work with 32-bit Internet Explorer, and cannot work with 64-bit Internet Explorer. As a workaround, you can modify the Windows system registry to start the Internet Explorer in 32-bit mode instead of 64-bit mode. To do this,

1. Run "**regedit**" command to open the **Registry Editor**.
2. Find the registry entry **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\TabProcGrowth**, and set it to a value greater than 0.
3. Close **Registry Editor** so changes will be saved, and restart Internet Explorer so it will be run in 32-bit mode.

Figure 5.85: IE compatibility settings



Step 1: Specify the compatibility mode (32-bit or 64-bit or both) of the OCX/DLL/OLE files called by the Web application.

If the OCX/DLL/OLE files called by the Web application are compiled under 32-bit compatibility mode, then select 32-bit compatibility mode, if the OCX/DLL/OLE files are compiled under 64-bit compatibility mode, then select 64-bit compatibility mode; if there are two sets of OCX/DLL/OLE files: one complied under 32-bit compatibility mode for running in 32-bit IE browsers, the other complied under 64-bit compatibility mode for running in 64-bit IE browsers; then select both 32-bit and 64-bit compatibility modes. (To call the two sets of OCX/DLL/OLE files for different IE browsers in your source code, you may need to use the of_is64browser function in the Appeon Workarounds PBL to determine if the IE browser is 64-bit. Refer to Section 2.3.1, “AppeonExtFuncs Object” in *Workarounds & API Guide*.

Step 2: In the Warning Message field, customize the warning message that will be displayed to end users when the OCX/DLL/OLE files run in an incompatible IE browser.

For example, if the OCX/DLL/OLE files called by the Web application are compiled under 32-bit compatibility mode (thus can only be run in a 32-bit IE browser), you may want to select 32-bit as Compatibility Mode, and then specify the following message in the Warning Message field so that it will be displayed if the user runs the Web application in a 64-bit IE browser: "You are running on a 64-bit IE browser now. Please notice that the Web application (mainly the OCX/DLL/OLE files) is compatible with 32-bit only, if you run on a 64-bit IE browser, the OCX/DLL/OLE related function may not work correctly. Do you want to continue running the 64-bit IE browser?".

5.4.5.2 IE Browser Interface

You can control the IE behavior by customizing the IE views in the IE Browser Interface tool in AEM. You can select to display or hide the menu bar, status bar, address bar, or all of the toolbars of IE browser, and open IE in full screen mode or normal mode, when a Web application runs in IE.

Figure 5.86: IE Browser Interface

Notes:

1. For IE 6, though the menu bar, status bar, address bar and all of the toolbars are set to display, they will be hidden if **Open the IE browser in Full Screen view** is set to **Yes**.

2. Address bar in IE 7/8/9/10/11 cannot be hidden, due to the new protection mechanism in Microsoft. You may want to see Microsoft help for details.

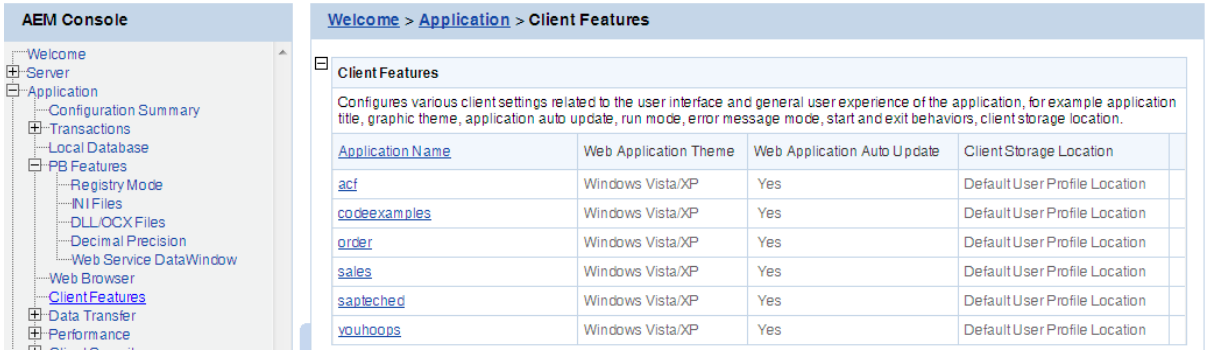
3. IE 7/8/9/10/11 toolbars include the Tab bar, the Menu bar, the Favorites or Links bar, and the Command bar, while IE 6 toolbars include the Menu bar, and the Address bar. Due to this difference, when **Display all of the toolbars in IE browser** is turned on or off, you will find different behaviours between IE 6 and IE 7/8/9/10/11.

   For example, tabs in IE 7/8/9/10/11 will be shown, if both **Display all of the toolbars in IE browser** and **Display the Address bar in IE browser** are set to **Yes**, and will be hidden if either is set to **No**.

5.4.6 Client Features

The Client Features helps you configure various clients settings related to the user interface and general user experience of applications, for example, graphics theme, start and exit behaviors, and client deployment locations.

Figure 5.87: Client Features

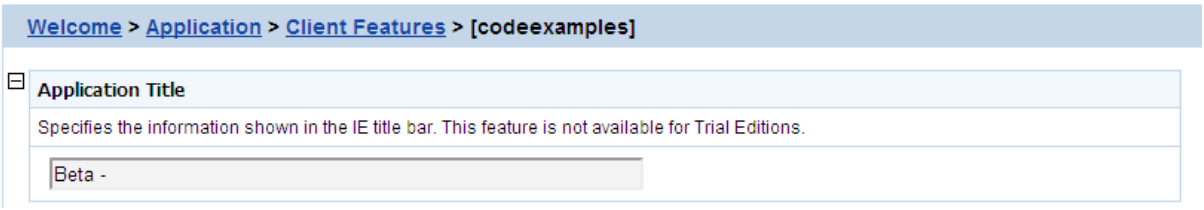


5.4.6.1 Application Title

You can configure the text shown in the title bar when the Web or mobile application is run. The default text is what defined in the Appeon license file.

This setting is effective only when you are using a Developer, Workgroup, or Enterprise Edition of PowerServer.

Figure 5.88: Application Title



5.4.6.2 Web Application Theme

Note: This tool is for the browser-based Web application running in Internet Explorer only.

The Web Application Theme specifies the theme of the browser-based Web application that will be used on the client side. The IWA Web app will not take this theme setting, instead they will directly use the theme of OS.

Figure 5.89: Web Application Theme

There are two options for Web Application Theme:

- **Windows Vista**: Applying this theme enables Appeon Web applications to show in Windows Vista style. The Windows Vista style also requires the end user set the Windows desktop Theme to Windows Vista.
- **Windows Classic**: Applying this theme makes Appeon Web application presented in traditional Windows 2000 style.

5.4.6.3 Web Application Auto Update

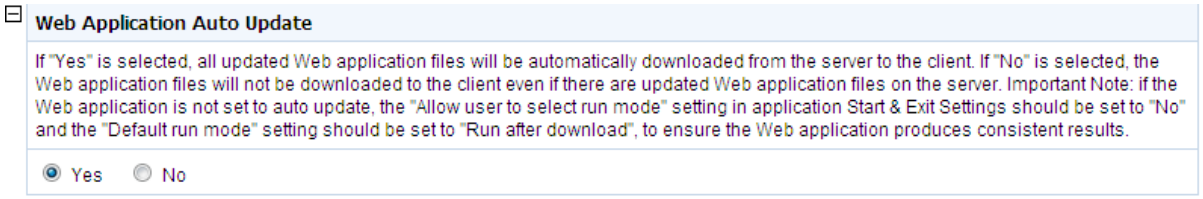
When an Appeon Web application or Appeon mobile application is re-deployed and run, it will compare the application files on the client with the files on the server, if there are

updated files on the server, it will download the files to the client if "Auto Update Web Files" is set to Yes, and will not download the files but directly use the cached files on the client if set to No. However, if there are new files on the server that do not exist on the client, then the new files will be downloaded regardless auto update is Yes or No.

If auto update is set to No, then the "Allow user to select run mode" setting in application Start & Exit Settings should be set to "No" and the "Default run mode" setting should be set to "Run after download", this will download all files to the client when the application is run for the first time, thus can avoid the following problems:

- If "Run now" rather than "Run after download" is selected, the files will be downloaded only when needed, which may cause the updated files (or part of them) to be downloaded unexpectedly, as they may not be used and downloaded already (thus do not exist on the client).
- If you switch the file generation mode (from release mode to debug mode, or vice versa, on PowerServer Toolkit | Configure button | Application Profiles tab page) and re-deploy the application, and if you select "Run now" rather than "Run after download", then you will see Web page errors when launching the Web application, as the application re-deployed under release mode (or debug mode) cannot directly use the cached files which were generated under debug mode (or release mode).

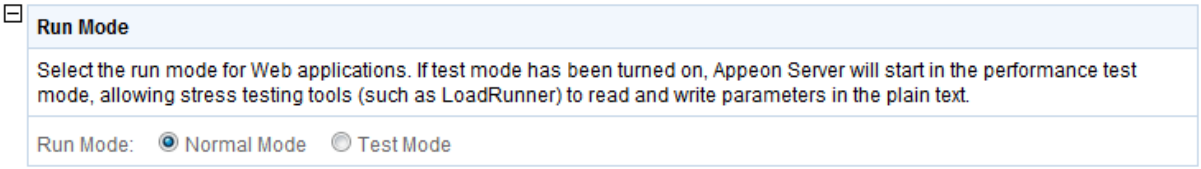
Figure 5.90: Auto Update



5.4.6.4 Run Mode

The Run Mode sets whether the parameters transferred between the application and the server can be read and analyzed by stress-testing tools such as LoadRunner, UFT (Unified Functional Testing).

Figure 5.91: Run mode



There are two Run Mode options:

- Normal mode: This is the default and recommended mode for running the Appeon Web application or the Appeon mobile application.
- 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:

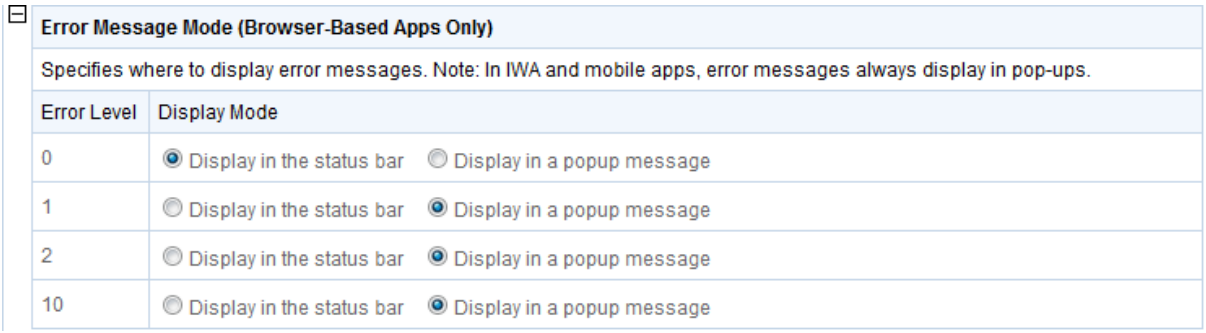
1. If the Test mode is selected, be sure to disable the data cache in the DataWindow Data Cache page before the application is run.
2. If the settings in the Test Mode have been changed, restart the Web browser to begin a new session. The changes will not take effect if you only click the **Refresh** button of the Web browser.

5.4.6.5 Error Message Mode

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

Click an application in the **Application Name** column of the table. The Error Message Mode settings page displays.

Figure 5.92: Error mode configuration



- **Display in the status bar** mode means that the error displays in the Web browser 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.

  Note: Appeon mobile apps, IWA apps, as well as Web apps running in non-IE browser (such as Edge, Chrome, Firefox, or Opera) can only support this mode.

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

- Level 0 - Not severe. The error has little impact to the functions of the application and displays in the status bar.
- Level 1 - Quite severe. The error is caused by incorrect configuration, and affects the running of the application. For example, no data source is set for the application. It displays in a popup message.
- Level 2 - Very severe. The error is caused by incompatibility with Appeon product. For example, the specification of invalid Web URL. The error displays in a popup message.

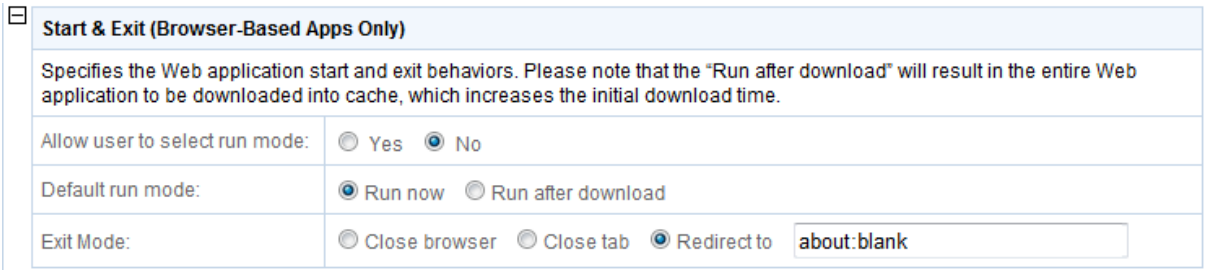
- Level 10 - Most severe. The error reflects a bug in the Appeon product and displays in a popup message.

5.4.6.6 Start & Exit

Note: These settings are available for Web apps running in the browser only, and not available for mobile and IWA apps.

The Start & Exit settings determine 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 **Exit Mode** when exiting the Web application.

Figure 5.93: Start & Exit Settings



5.4.6.6.1 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 modes: **Run Now** or **Run After Download**. Note: These two modes are not related with that are set in **Default run mode**, even you set the value of **Default run mode**, you can still 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 under the mode selected in **Default run mode**.

5.4.6.6.2 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.

5.4.6.6.3 Exit Mode

You can control the behavior of the Web browser when you exit the Web application.

- **Close browser**: Select this option if you want the Web browser to automatically close when you exit the Web application.

- **Close tab**: Select this option if you want the Web browser to stay opened and only the tab page running the Web application to be closed when you exit the Web application. This option is effective to Internet Explorer 7.0 or above.
- **Redirect to**: Select this option if you want the current browser or tab page which runs the Web application to be redirected to run the specified URL.

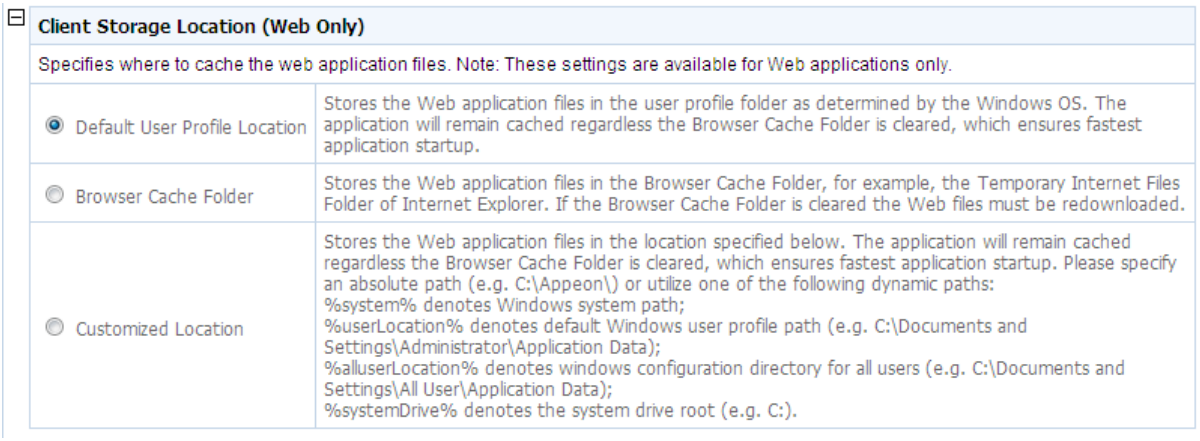
5.4.6.7 Client Storage Location

Note: This setting is available for Web applications only.

Specify a location to store the Web application files on the client side.

No matter which location is specified, you can call AppeonGetCacheDir function in *Workarounds & API Guide* to get the current directory for the application.

Figure 5.94: Client storage location



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

- Default User Profile Location: The Web application files will be stored permanently in the %appdata%\appeon folder allocated by the Windows system, unless you remove them manually. The %appdata%\appeon folder in Windows 7/8 is: %SYSTEMDRIVE%\users\{username}\AppData\Roaming\appeon
- Browser Cache Folder: The Web application files will be stored in the IE cache (no matter the application is run in IE, Edge, Chrome, Firefox, or Opera). If the IE cache is cleared, the files will be downloaded again the next time the application runs. The IE cache directory varies depending on the Windows OS:

  Windows 7: %SYSTEMDRIVE%\Users\{username}\AppData\Local\Microsoft\Windows\Temporary Internet Files\

  Windows 8/8.1: %SYSTEMDRIVE%\Users\{username}\AppData\Local\Microsoft\Windows\INetCache\
- Customized Location: The Web application files will be stored in the location specified here. You must specify absolute path here (e.g. C:\Appeon\) or use one of the following dynamic paths:

  %SYSTEMDRIVE% which stands for system drive root, e.g. C:\.

%SYSTEM% which stands for the Windows system directory. In Windows 7 and later, C:\Windows.

%USERPROFILE% which stands for the Windows user profile folder. In Windows 7 and later, C:\Users\{username}.

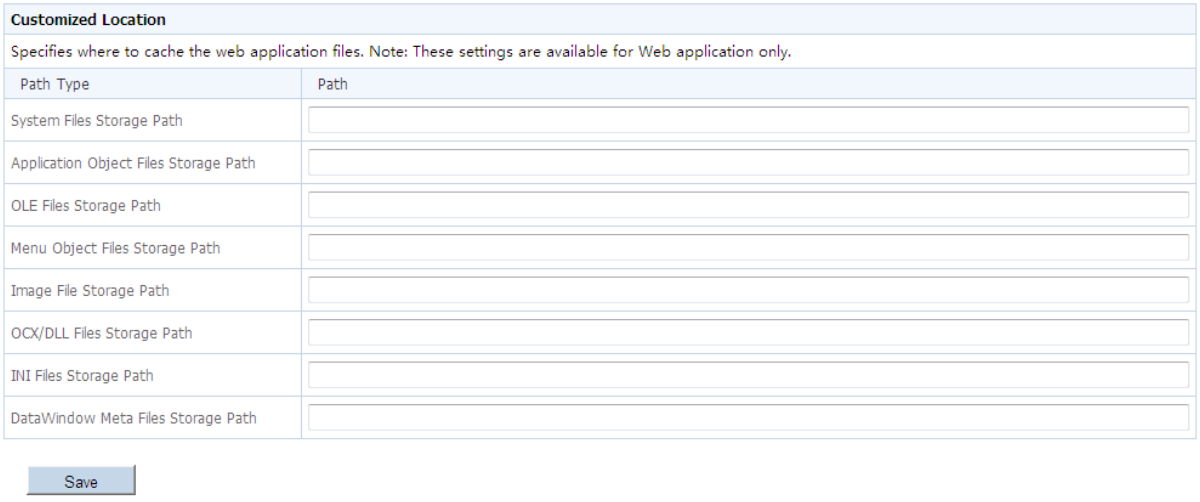
%HOMEPATH% which stands for the home folder for the Windows user. In Windows 7 and later, C:\Users\{username}.

%USERLOCATION% which stands for the Windows user profile folder. In Windows 7 and later, C:\Users\{username}\AppData\Roaming.

%ALLUSERLOCATION% which stands for the Windows user profile folder for all users. In Windows 7 and later, C:\ProgramData.

When this option is selected, the following table will display for you to specify the storage location for the Web files of different types. Note that the first path **System Files Storage Path** cannot be empty or null, and it should be specified first, because the value specified here will be used automatically as the root path for the following items by default. You can change the path for each file type according to the actual needs.

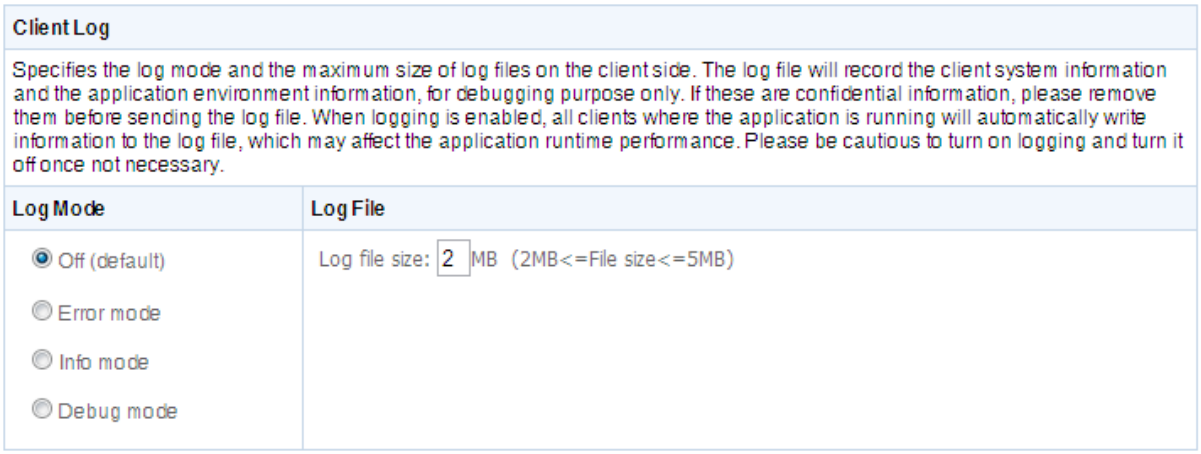
Figure 5.95: Customized location



5.4.6.8 Client Logs

Select one of the following modes for the logs generated on the client side, and specify the maximum size for the log files.

Figure 5.96: Client Logs



See the following table for details on the mode options.

Table 5.6: Client Log Mode

Client Log Mode	Description
OFF	Does not generate any log file.
ERROR	Only generates error log files.
INFO	Generates log files that are informative to users.
DEBUG	Generates detailed log files that are sufficient for routine checking and troubleshooting.

Log File: Enter a number between 2 to 5 here to specify the log size to be generated. If the log generated reaches the specified number, the generated logs will be automatically removed from the client.

Log path:

- For Web applications:

  1. If you select **Default User Profile Location** as the client storage location in Client Storage Location, the log is saved in C:\Users\{username}\AppData\Roaming\appeon\%appname%\log\appeonclient.log. {username} is the Windows login name you are using, for example, *administrator*.

  2. If you select **Browser Cache Folder** as the client storage location in Client Storage Location, the log is saved in C:\Users\{username}\AppData\Local\Microsoft\Windows\Temporary Internet Files\{systemfolder1}\{subsystemfolder1}\appeonclient.log.

     {username} is the Windows login name you are using, for example, *administrator*.

     {systemfolder1} is a system-hidden directory (not the general hidden files) that cannot be displayed even by enabling the **Show hidden files, folders, and drivers** option (**Computer** > **Organize** > **Folder and search options** > **View** > **Show hidden files, folders, and drivers**), and the name for the {systemfolder1} is usually *content.IE5* or similar, so you just can open the {systemfolder1} by typing C:\Users\{username}\AppData\Local\Microsoft\Windows\Temporary Internet Files\content.IE5\ into the **Address** bar.

The name for {subsystemfolder1} is random.

An automatic way to determine the browser cache directory for the current application is by calling an API Appeon provides. See AppeonGetCacheDir function in *Workarounds & API Guide*.

3. If you select **Customized Location** as the client storage location in Client Storage Location, the log is saved in %System Files Storage Path%\log\appeonclient.log. For example, if you type *e:\App* in the **System Files Storage Path** text box in **Client Storage Location**, the log will be saved in e:\App\log\appeonclient.log.

- For mobile applications (that run in Appeon Workspace): The log file is saved in the **Log** folder under the application folder on your mobile device. You cannot view the log file on mobile device as how you view the Web application log on PCs; but you can view the log or send the log via email in Appeon Workspace. For details on how to view the log or send the log via email, refer to Section 5.9, “Configuring logs” in *Appeon Workspace User Guide*.

- For native mobile applications: You can call the **of_sendmail** function of **eon_mobile_awsex** object to send the log as attachment, and the log file path and name is: AppeonGetCacheDir()+"/Log/EonMob.log".

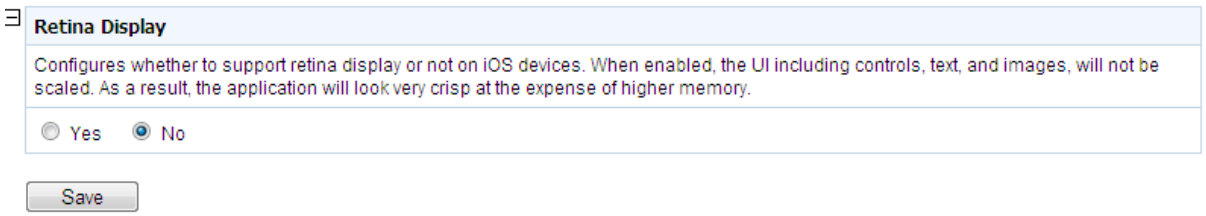
  Refer to the section called “of_sendmail” in *Workarounds & API Guide* for details.

5.4.6.9 Retina Display

Note: This tool is for iOS mobile apps only.

Configures whether to support retina display or not on retina-supported iOS devices using this **Retina Display** tool. When enabled, the UI including controls, text, and images will not be scaled. As a result, the application will look very crisp at the expense of higher memory.

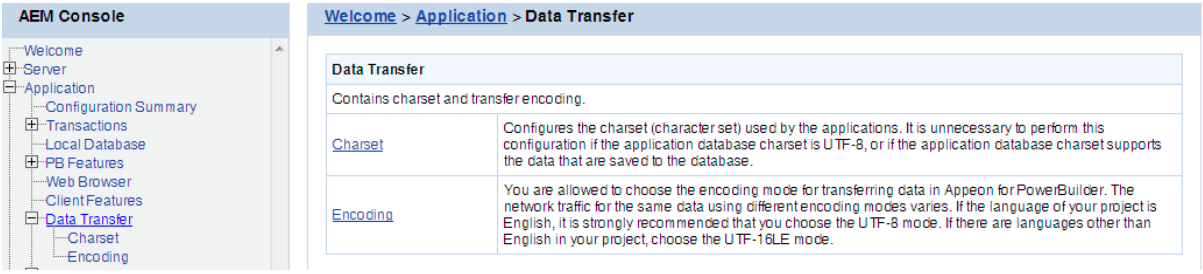
Figure 5.97: Retina Display Supported



5.4.7 Data Transfer

Data Transfer is a set of tools for viewing and modifying Charset and Encoding.

Figure 5.98: Data Transfer



5.4.7.1 Charset

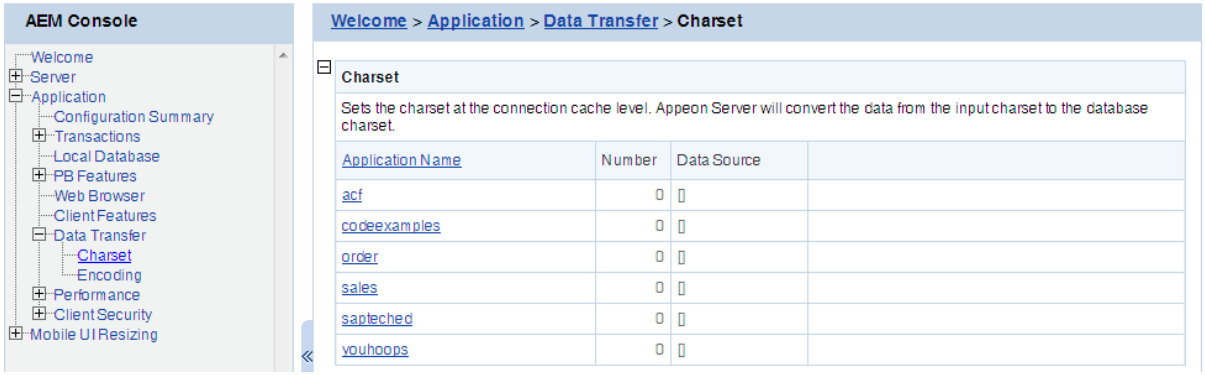
The character set conversion can be enabled at the data source level for each application if you specify the input Charset and database Charset for the cache in AEM.

You will find the Charset tool useful when:

- The database uses non-UTF-8 character set, and
- The language display of the application has error code in it

Otherwise, it is unnecessary to use this tool.

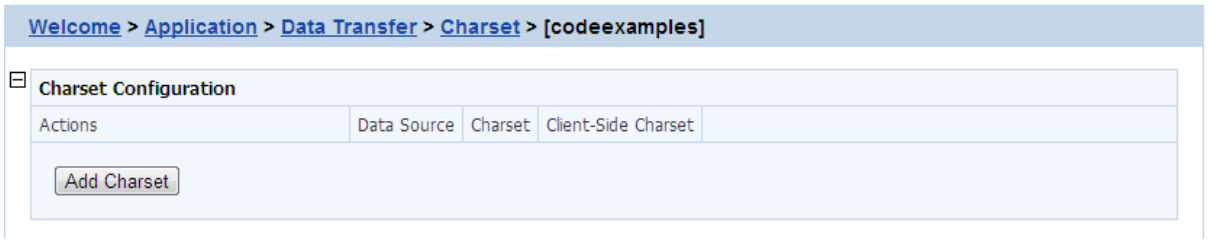
Figure 5.99: Charset settings



5.4.7.1.1 Configuring database Charset for a data source

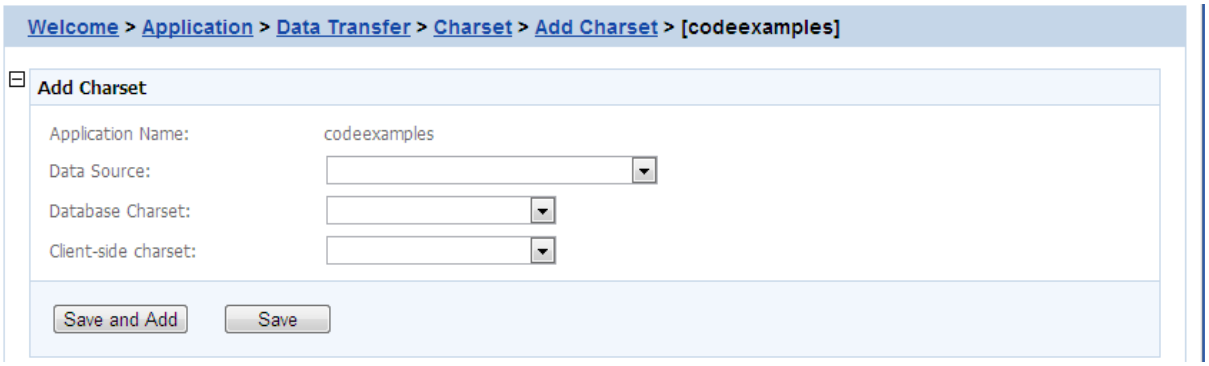
Step 1: Click an application in the Application Name column. The Configure Charset window opens.

Figure 5.100: Configure charset settings



Step 2: Click the **Add Charset** button. The Add Charset window opens.

Figure 5.101: Add charset settings



Step 3: Select the data source from the **Data Source** dropdown list.

Step 4: Select the database charset type from the **Database Charset** dropdown list. 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 **Client-side Charset** dropdown list. This setting should match the input Charset type at the client side.

Step 6: Click the **Save** button to confirm the configuration or **Save and Add** to add another one.

5.4.7.1.2 Updating a Charset

On the Charset page, click **Update** under Actions to update a Charset for a data source.

5.4.7.1.3 Deleting a Charset

On the Charset page, click **Delete** under Actions to delete an unwanted Charset for a data source.

5.4.7.1.4 Charset options given in the Charset fields

The following table 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 constant.config in the directory %powerserver%\AEM\config\.

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 <charset name="gbk" value="gbk"></charset> in the file.

Step 3: Restart PowerServer and the "gbk" Charset will be added to the Charset lists.

The following table lists the character sets and code pages. The asterisk (*) at the last column indicates that Microsoft .NET Framework supports the code page, regardless of the platform.

Table 5.7: Charset and code pages

Page	Charset	Description	Asterisk
37	IBM037	IBM EBCDIC (US - Canada)	
437	IBM437	OEM US	
500	IBM500	IBM EBCDIC (International)	
708	ASMO-708	Arabic (ASMO 708)	
720	DOS-720	Arabic (DOS)	
737	ibm737	Greek (DOS)	
775	ibm775	Baltic (DOS)	
850	ibm850	Western European (DOS)	
852	ibm852	Central European (DOS)	
855	IBM855	OEM Cyrillic	
857	ibm857	Turkish (DOS)	

Page	Charset	Description	Asterisk
858	IBM00858	OEM Multi-Language Latin I	
860	IBM860	Portuguese (DOS)	
861	ibm861	Iceland (DOS)	
862	DOS-862	Hebrew (DOS)	
863	IBM863	Canadian French (DOS)	
864	IBM864	Arabic (864)	
865	IBM865	Northern European (DOS)	
866	cp866	Cyrillic (DOS)	
869	ibm869	Modern Greek (DOS)	
870	IBM870	IBM EBCDIC (Multi-Language Latin 2)	
874	windows-874	Thai (Windows)	
875	cp875	IBM EBCDIC (Modern Greek)	
932	shift_jis	Japanese (Shift-JIS)	
936	gb2312	Simplified Chinese (GB2312)	*
949	ks_c_5601-1987	Korean	
950	big5	Traditional Chinese (Big5)	
1026	IBM1026	IBM EBCDIC (TurkishLatin 5)	
1047	IBM01047	IBM Latin 1	
1140	IBM01140	IBM EBCDIC (US - Canada - Europe)	
1141	IBM01141	IBM EBCDIC (German - Europe)	
1142	IBM01142	IBM EBCDIC (Denmark - Norway - Europe)	
1143	IBM01143	IBM EBCDIC (Finland - Sweden - Europe)	
1144	IBM01144	IBM EBCDIC (Italy - Europe)	
1145	IBM01145	IBM EBCDIC (Spain- Europe)	
1146	IBM01146	IBM EBCDIC (U.K. - Europe)	
1147	IBM01147	IBM EBCDIC (France - Europe)	
1148	IBM01148	IBM EBCDIC (International - Europe)	
1149	IBM01149	IBM EBCDIC (Iceland - Europe)	
1200	utf-16	Unicode	*
1201	UnicodeFFFE	Unicode (Big-Endian)	*
1250	windows-1250	Central Europe (Windows)	
1251	windows-1251	Cyrillic (Windows)	

Page	Charset	Description	Asterisk
1252	Windows-1252	Central Europe (Windows)	*
1253	windows-1253	Greek (Windows)	
1254	windows-1254	Turkish (Windows)	
1255	windows-1255	Hebrew (Windows)	
1256	windows-1256	Arabic (Windows)	
1257	windows-1257	Baltic (Windows)	
1258	windows-1258	Vietnamese (Windows)	
1361	Johab	Korean (Johab)	
10000	macintosh	Central Europe (Mac)	
10001	x-mac-japanese	Japanese (Mac)	
10002	x-mac-chinesetrad	Traditional Chinese (Mac)	
10003	x-mac-korean	Korean (Mac)	*
10004	x-mac-arabic	Arabic (Mac)	
10005	x-mac-hebrew	Hebrew (Mac)	
10006	x-mac-greek	Greek (Mac)	
10007	x-mac-cyrillic	Cyrillic (Mac)	
10008	x-mac-chinesesimp	Simplified Chinese (Mac)	*
10010	x-mac-romanian	Romanian (Mac)	
10017	x-mac-ukrainian	Ukrainian (Mac)	
10021	x-mac-thai	Thai (Mac)	
10029	x-mac-ce	Central Europe (Mac)	
10079	x-mac-icelandic	Iceland (Mac)	
10081	x-mac-turkish	Turkish (Mac)	
10082	x-mac-croatian	Croatian (Mac)	
20000	x-Chinese-CNS	Traditional Chinese (CNS)	
20001	x-cp20001	TCA Taiwan	
20002	x-Chinese-Eten	Traditional Chinese (Eten)	
20003	x-cp20003	IBM5550 Taiwan	
20004	x-cp20004	TeleText Taiwan	
20005	x-cp20005	Wang Taiwan	
20105	x-IA5	Central Europe (IA5)	
20106	x-IA5-German	Germany (IA5)	
20107	x-IA5-Swedish	Swedish (IA5)	
20108	x-IA5-Norwegian	Norwegian (IA5)	
20127	us-ascii	US-ASCII	*

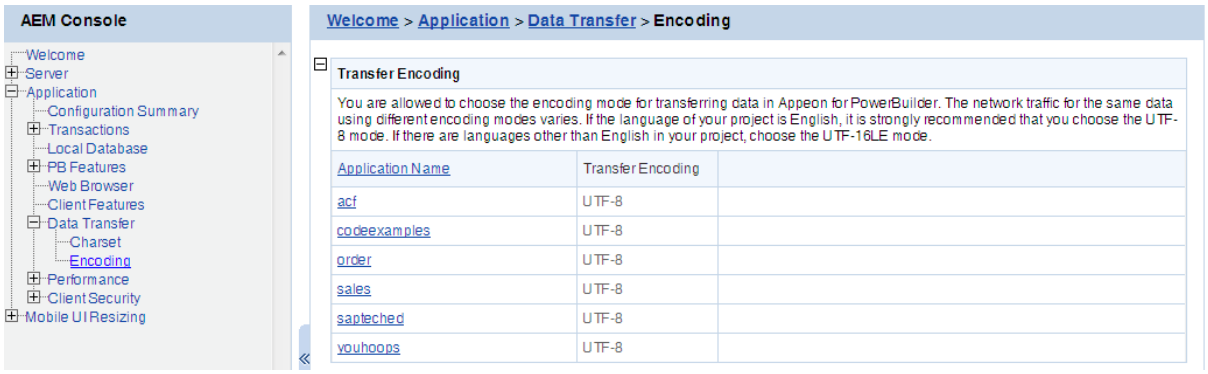
Page	Charset	Description	Asterisk
20261	x-cp20261	T.61	
20269	x-cp20269	ISO-6937	
20273	IBM273	IBM EBCDIC (Germany)	
20277	IBM277	IBM EBCDIC (Denmark - Norwegian)	
20278	IBM278	IBM EBCDIC (Finland- Swedish)	
20280	IBM280	IBM EBCDIC (Italy)	
20284	IBM284	IBM EBCDIC (Spanish)	
20285	IBM285	IBM EBCDIC (U.K.)	
20290	IBM290	IBM EBCDIC (Japanese Katakana)	
20297	IBM297	IBM EBCDIC (France)	
20420	IBM420	IBM EBCDIC (Arabic)	
20423	IBM423	IBM EBCDIC (Greek)	
20424	IBM424	IBM EBCDIC (Hebrew)	
20833	x-EBCDIC-KoreanExtended	IBM EBCDIC (Korean Extension)	
20838	IBM-Thai	IBM EBCDIC (Thai)	
20866	koi8-r	Cyrillic (KOI8-R)	
20871	IBM871	IBM EBCDIC (Iceland)	
20880	IBM880	IBM EBCDIC (Cyrillic Russian)	
20905	IBM905	IBM EBCDIC (Turkish)	
20924	IBM00924	IBM Latin 1	
20932	EUC-JP	Japanese (JIS 0208-1990 and 0212-1990)	
20936	x-cp20936	Simplified Chinese (GB2312-80)	*
20949	x-cp20949	Korean Wansung	*
21025	cp1025	IBM EBCDIC (Cyrillic Serbian - Bulgarian)	
21866	koi8-u	Cyrillic (KOI8-U)	
28591	iso-8859-1	Central Europe (ISO)	*
28592	iso-8859-2	Central Europe (ISO)	
28593	iso-8859-3	Latin 3 (ISO)	
28594	iso-8859-4	Baltic (ISO)	
28595	iso-8859-5	Cyrillic (ISO)	
28596	iso-8859-6	Arabic (ISO)	
28597	iso-8859-7	Greek (ISO)	

Page	Charset	Description	Asterisk
28598	iso-8859-8	Hebrew (ISO-Visual)	*
28599	iso-8859-9	Turkish (ISO)	
28603	iso-8859-13	Estonian (ISO)	
28605	iso-8859-15	Latin 9 (ISO)	
29001	x-Europa	Europa	
38598	iso-8859-8-i	Hebrew (ISO-Logical)	*
50220	iso-2022-jp	Japanese (JIS)	*
50221	csISO2022JP	Japanese (JIS- 1 byte Kana)	*
50222	iso-2022-jp	Japanese (JIS- 1 byte Kana - SO/SI)	*
50225	iso-2022-kr	Korean (ISO)	*
50227	x-cp50227	Simplified Chinese (ISO-2022)	*
51932	euc-jp	Japanese (EUC)	*
51936	EUC-CN	Simplified Chinese (EUC)	*
51949	euc-kr	Korean (EUC)	*
52936	hz-gb-2312	Simplified Chinese (HZ)	*
54936	GB18030	Simplified Chinese (GB18030)	*
57002	x-iscii-de	ISCII Sanskrit	*
57003	x-iscii-be	ISCII Bengalese	*
57004	x-iscii-ta	ISCII Tamil	*
57005	x-iscii-te	ISCII Telugu	*
57006	x-iscii-as	ISCII Assamese	*
57007	x-iscii-or	ISCII Oriya	*
57008	x-iscii-ka	ISCII Kannada	*
57009	x-iscii-ma	ISCII Malayalam	*
57010	x-iscii-gu	ISCII Gujarat	*
57011	x-iscii-pa	ISCII Punjab	*
65000	utf-7	Unicode (UTF-7)	*
65001	utf-8	Unicode (UTF-8)	*
65005	utf-32	Unicode (UTF-32)	*
65006	utf-32BE	Unicode (UTF-32 Big-Endian)	*

5.4.7.2 Encoding

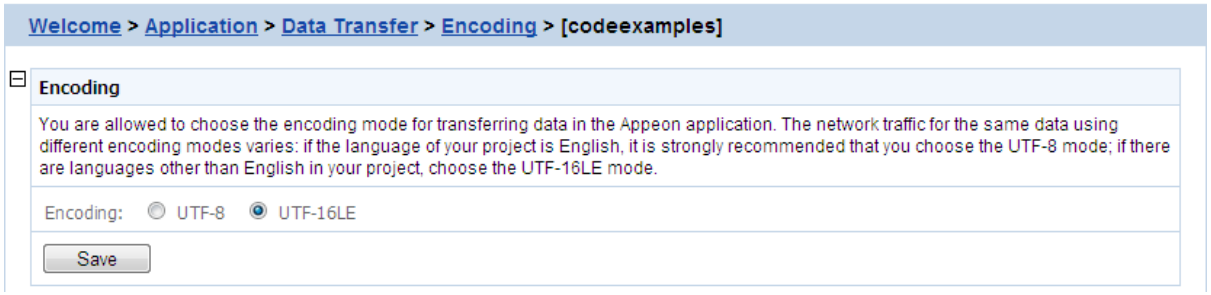
Encoding specifies the encoding format for data transferred between the clients and the server. The transfer speed varies when the encoding format changes.

Figure 5.102: Encoding



If the language of the application is pure English, select UTF-8; otherwise, select UTF-16LE.

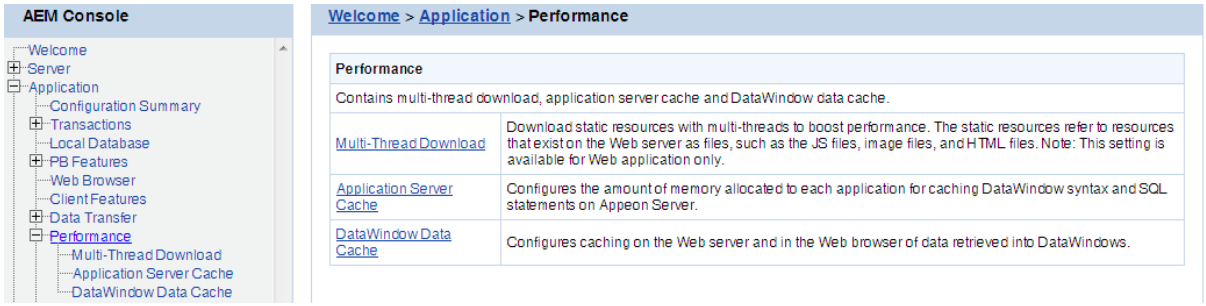
Figure 5.103: Encoding settings



5.4.8 Performance

Performance is a set of tools for viewing and modifying Multi-thread Download, application Server Cache and DataWindow Data Cache.

Figure 5.104: Performance

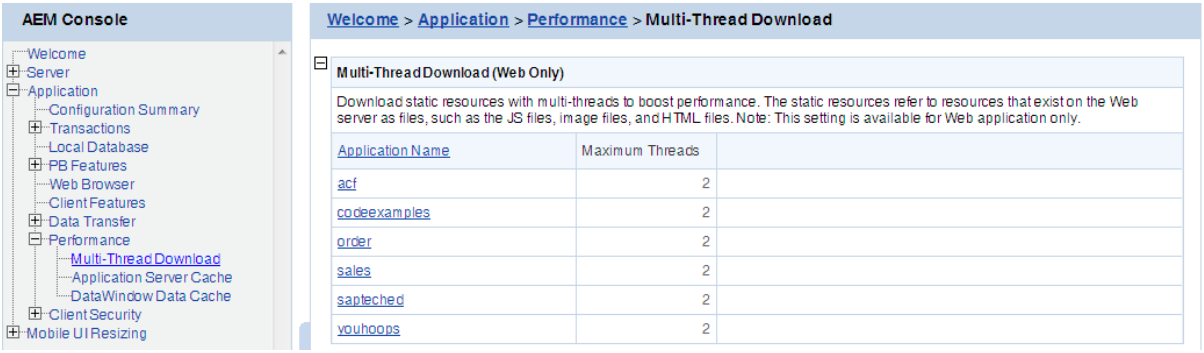


5.4.8.1 Multi-Thread Download

Note: This option is available for Web applications only.

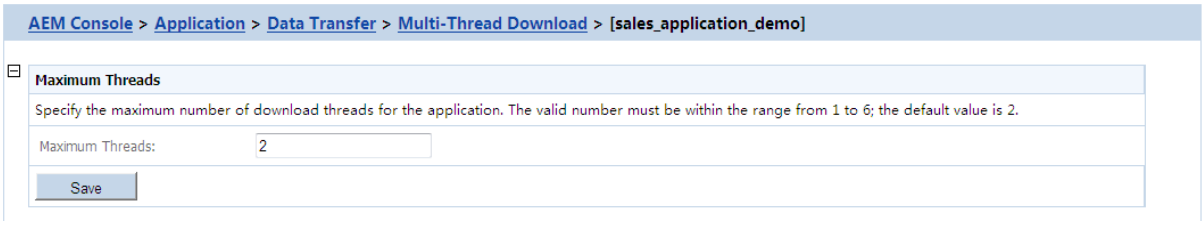
The Multi-Thread Download setting specifies how many threads a client will take for simultaneously downloading application Web files (such as JavaScript files, image files, and HTML files) from the Web server. This option makes full use of the network bandwidth between clients and Web server, and shortens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

Figure 5.105: Multi-thread Download



Click the application name in the **Multi-thread Download** table, and then enter a number in the **Maximum Threads** text box, and then click **Save**.

Figure 5.106: Maximum Threads



Before setting the thread number, you should take full consideration of the network condition where the application will be running, 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 your choice to set the thread number from 1 to 6 based on the available network condition.

5.4.8.2 Application Server Cache

Note: This tool is available for Web applications only.

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

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

5.4.8.2.1 What is Application Server cache?

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

Depending on the cache size specified for an application, PowerServer loads part or all of the application DataWindow syntax and embedded SQLs when the application

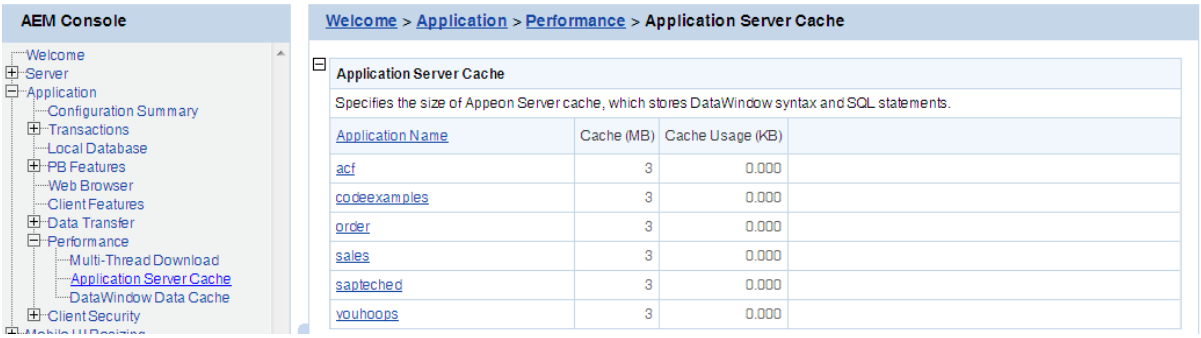
starts. If PowerServer only loads part of the DataWindow syntax and embedded SQLs of an application to the cache, the application runtime performance is affected because PowerServer needs to read certain DataWindow syntax and embedded SQLs from the database instead of reading from the memory.

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

5.4.8.2.2 Modifying the PowerServer cache settings for an application

In the **Application Server Cache** table, the **Cache** column shows the PowerServer cache size allocated for the corresponding application, while the **Cache Usage** column shows how much cache the application currently occupies in the PowerServer memory.

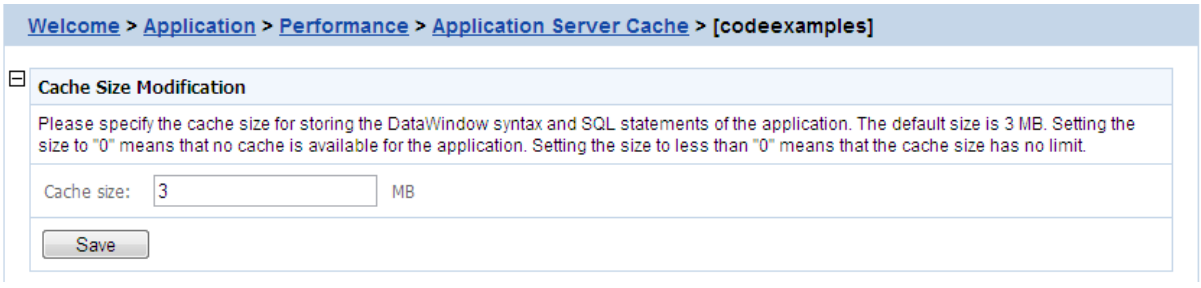
Figure 5.107: Application Server Cache



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

Step 1: Click an application listed in the **Application Server Cache** table. A new page opens and displays the current cache setting for the application.

Figure 5.108: Modify Cache Setting



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, PowerServer loads a maximum of 3MB syntax and SQL into its memory; if the client runs appB, PowerServer 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. PowerServer 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. PowerServer will load all the DataWindow syntax, DataWindow SQLs, and Embedded SQLs of the application into the cache.

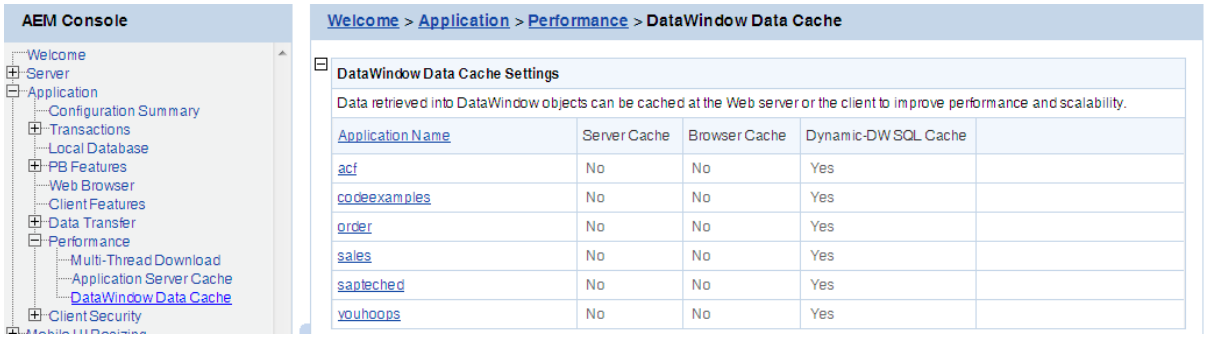
  Setting the size to "0" is not recommended because it will result in slow performance. If the server has enough memory and the number of the deployed applications is less than 10, it is recommended that you set the size for all applications to less than "0". If the server does not have enough memory, 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** button to save changes.

5.4.8.3 DataWindow Data Cache

You can configure the **Dynamic-DW SQL Cache** settings and the **DataWindow Object Cache** settings for a particular application under this the **DataWindow Data Cache** tool.

Figure 5.109: DataWindow Data Cache



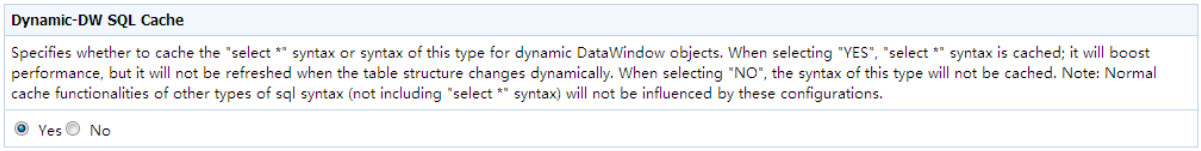
5.4.8.3.1 Dynamic-DW SQL Cache

Dynamic-DW SQL Cache tool specifies whether to cache the "select *" syntax or and syntax of this type for dynamic DataWindow objects. If the "select *" syntax is cached, it will boost performance, but it will not be refreshed when the table structure changes dynamically.

Step 1: Click on the application you intend to configure on the **DataWindow Data Cache** page.

Step 2: In the **Dynamic-DW SQL Cache** table, configure whether to cache the "select*" syntax or syntax of this type or not, as shown in the following figure.

Figure 5.110: Dynamic-DW SQL Cache



5.4.8.3.2 DataWindow Object Cache Settings

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

- DataWindow Data Cache at the PowerServer stores the data in the memory. The cached data will be available unless the server memory is cleared (for example, by restarting the 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, 10g, and 11g) databases.

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

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

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

5) DataWindow Data Cache at the PowerServer 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).

Configuration required for database servers

Appeon specially provides SQL files 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, MySQL, Teradata, HANA, and PostgreSQL.

The following table lists the SQL file that should be executed for the supported database server. The SQL files reside in the %powerserver%\sql\cache\ folder, where %powerserver% indicates the PowerServer installation directory, for example, C:\Inetpub\wwwroot\appeon.

Table 5.8: SQL files for each database server

Database Type	SQL File
Oracle	To enable this feature, execute install_appeon_cache_ORACLE.sql. To disable this feature, execute uninstall_appeon_cache_ORACLE.sql.
Microsoft SQL Server	To enable this feature, execute install_appeon_cache_MSSQL.sql. To disable this feature, execute uninstall_appeon_cache_MSSQL.sql.
ASE	To enable this feature, execute install_appeon_cache_ASE.sql. To disable this feature, execute uninstall_appeon_cache_ASE.sql.
SQL Anywhere	To enable this feature, execute install_appeon_cache_ASA.sql. To disable this feature, execute uninstall_appeon_cache_ASA.sql.
SAP IQ	To enable this feature, execute install_appeon_cache_IQ.sql. To disable this feature, execute uninstall_appeon_cache_IQ.sql.
DB2	To enable this feature, execute install_appeon_cache_DB2.sql. To disable this feature, execute 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, 10g, and 11g 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 SAP ASE server installed.

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 in PowerServer Help.

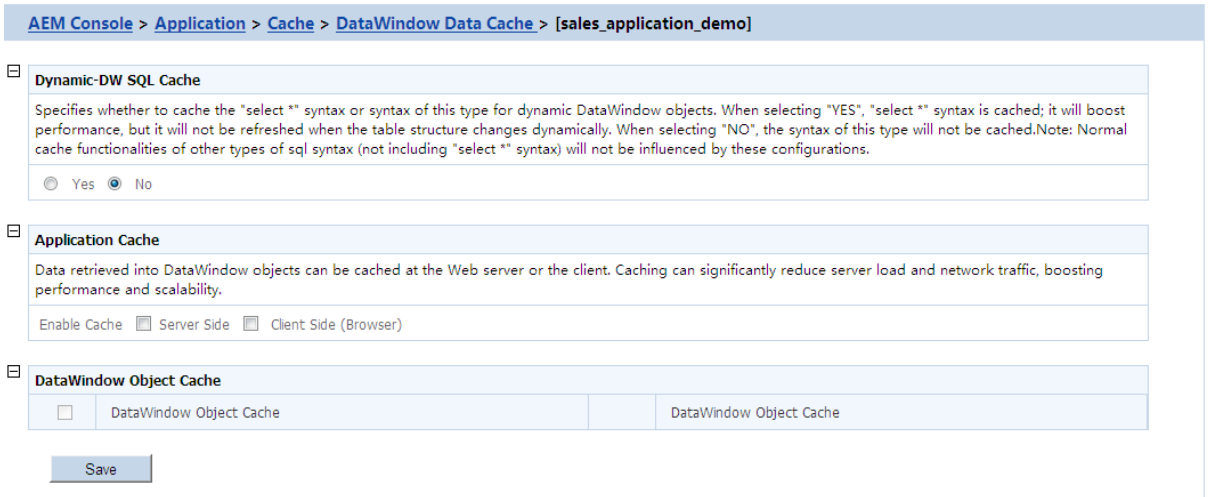
Configuration required for AEM

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

Step 1: Select **Application** > **Performance** > **DataWindow Data Cache** on the left pane of the AEM Console. The DataWindow Data Cache page displays on the right pane of the Console.

Step 2: Click "sales_application_demo" listed in the "Application Name" column of the table. The sales_application_demo page displays.

Figure 5.111: DataWindow Data Cache for sale_application_demo



Step 3: In the **Application Cache** table, select the **Server Side** option or **Client Side (Browser)** option to enable the cache setting for the application DataWindows.

Step 4: In the **DataWindow Object Cache** table 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.

5.4.9 Client Security

The Client Security tool in AEM is used to configure the User Authentication and Appeon Workspace securities. This tool is only effective when the Security Toggle is on in System Security.

Figure 5.112: Client Security

5.4.9.1 User Authentication

User Authentication is a tool to configure the security of the Appeon deployed applications. All the deployed applications are listed in the tool and are configured individually.

Figure 5.113: Application Security

5.4.9.1.1 Viewing the current settings

1) View the current application security settings for all applications available in the User Authentication page.

- Application Name -- Lists the names of all the deployed applications. The names are automatically registered with AEM when an application is deployed by PowerServer Toolkit to the PowerServer.

- Configured Groups -- The number of groups with access rights to the Appeon Web application or the Appeon mobile application.

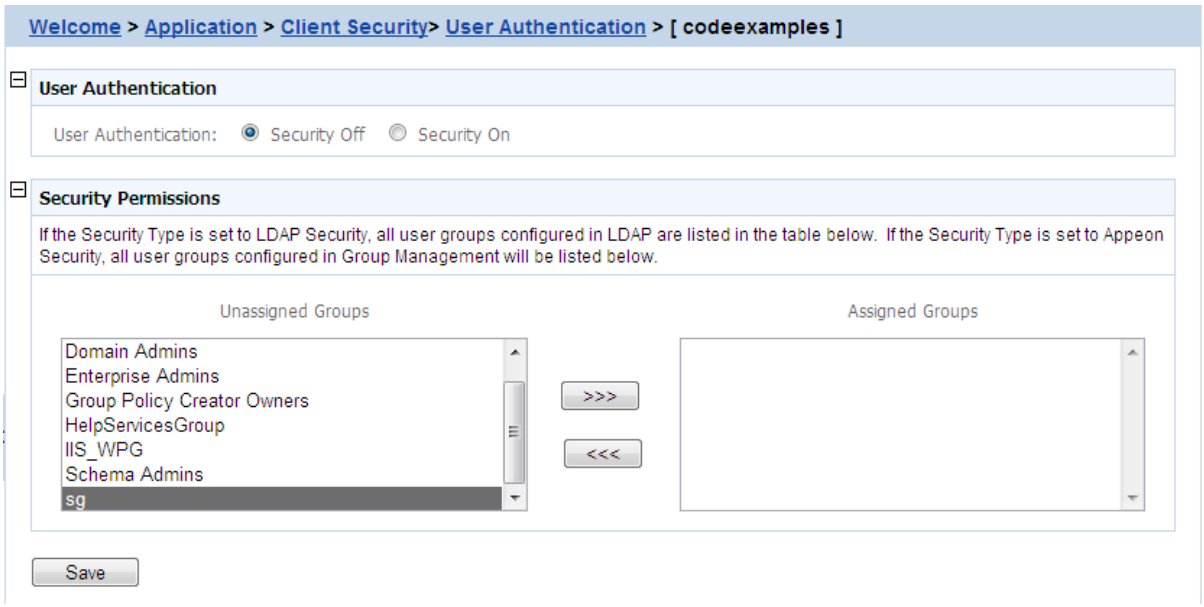
  To view the names of the groups, click the link at the application name. To view details of the groups, go to the Group Management page.

- User Authentication -- Shows the security mode for the user authentication. This is only effective when the Security Toggle is on in System Security.

  "Security on" explicates that the user will be prompted to enter the user name and password when accessing the selected application, while "Security off" requires no user name and password for the application access. You can click the link of an application name listed in the User Authentication 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.

Figure 5.114: Detailed security settings for an application



As the following table shows, different application security settings determine different security behaviors in an Appeon application.

Table 5.9: Application security settings and security behaviors in an Appeon application

User Authentication	A Given Group	Security behaviors in an Appeon application
Off	Assigned	All users can access to an Appeon application without being prompted for a user name or password.
	Unassigned	
On	Assigned	Users of an assigned group have access rights to a Appeon application and they are prompted for

User Authentication	A Given Group	Security behaviors in an Appeon application
		user names and passwords when loading an Appeon application. For offline applications, you are only prompted for user names and passwords when connecting to the database.
	Unassigned	Users of an unassigned group do not have access rights to the Appeon application.

5.4.9.1.2 Modifying the security settings of an application

The user can enter the security-setting page of the application by clicking an application name link on the User Authentication 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 Web browser 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 system 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 the system 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, refer to Section 2.3.2.16, “AppeonLDAPLogon function” in *Workarounds & API 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 PowerServer (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** button to apply changes.

5.4.9.2 Appeon Workspace

Figure 5.115: Appeon Workspace application security

5.4.9.2.1 Introduction to Appeon Workspace

Appeon Workspace is a free native mobile application which is publicly available on the online app store. As its name suggests, it is a workspace provided by Appeon to simplify distributing, running and managing the Appeon native mobile applications. In Appeon Workspace, you can download and run the Appeon native mobile applications conveniently, and can configure a number of settings for the application, such as log, title bar, etc. For detailed information on Appeon Workspace, please refer to the Appeon Workspace User Guide.

Since Appeon Workspace can install the native mobile application from PowerServer, you may want different applications on the same PowerServer to be installed by different mobile devices, for example, you may probably want application A to be installed by the mobile device from company A only, and application B by the device from company B only, etc. In such cases, you can take advantage of the Appeon Workspace security tools in AEM to control each application's access rights. You can follow these procedures to configure the tools:

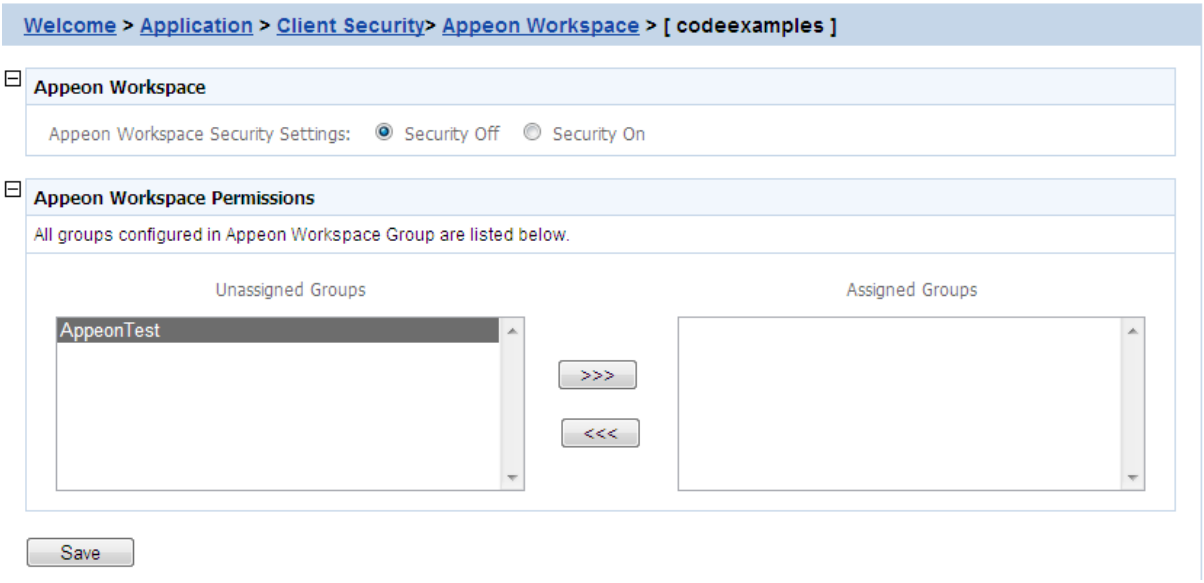
1. Adding an Appeon Workspace client: see Adding an Appeon Workspace client for details.
2. Adding an Appeon Workspace group and assigning the client to the group: see Adding an Appeon Workspace group for details.
3. Enabling the Appeon Workspace security and assigning the app accessibility rights to the group: see Setting Appeon Workspace security and Assigning access permissions for details.

5.4.9.2.2 Setting Appeon Workspace Security

Appeon Workspace security settings for each application are configured individually.

Step 1: Click on an application name, and the Appeon Workspace page appears.

Figure 5.116: Configuring Appeon Workspace



Step 2: Select the **Security Off** radio button to set the security off, or select the **Security On** radio button to set the security on. This is only effective when the Security Toggle is on in System Security.

If the security is set to On, only assigned users have rights to access the application.

5.4.9.2.3 Assigning access permissions

To assign access right of an application to a specific user group, click on the application. In the **Appeon Workspace Permissions** table, move the group you intend to assign access right to in the **Unassigned Group** list box to the **Assigned Group** list box.

If you want to deprive access right from a specific group, just move it from the **Assigned Group** list box to the **Unassigned Group** list box.

Note: For offline applications that start up offline (the startup mode is Offline), if the Apppeon Workspace Security Settings option is set to **Security On**, and if the application runs on an unassigned device, all operations that need to access the PowerServer are forbidden.

5.4.10 Mobile App Distribution

5.4.10.1 Requirements

5.4.10.1.1 iOS IPA file requires to be installed through HTTPS

Staring from iOS 7.1, Apple requires the enterprise apps manifest file (.plist) to be served over HTTPS. Install through HTTP will fail. Therefore you would need to follow documentations from the Web server vendor to configure the Web server to support HTTPS.

5.4.10.1.2 File size requirement

This section is required for IIS (7.5 thru 10) and WildFly 10.0. Skip this section if you are using the other Web server (such as JBoss EAP 6.1, JEUS, WebLogic, WebSphere, etc).

Before uploading the app package to the PowerServer Web Server, please be beware that the server has limitations on the file size to be uploaded, therefore you would need to follow the instructions below to configure a proper file size.

To change the default file size in WildFly 10.0:

Open the standalone.xml file (in %jboss home%/standalone/configuration/) with a text file editor, find the settings according to the protocol for accessing AEM and uploading file:

- If using HTTPS to access AEM and upload file, locate the following line and configure "max-post-size" for the maximum file size to be uploaded, for example, 104857600 (which indicates 100 MB).

```
<https-listener name="default1" max-post-size="104857600" security-
realm="ManagementRealm" socket-binding="https"/>
```

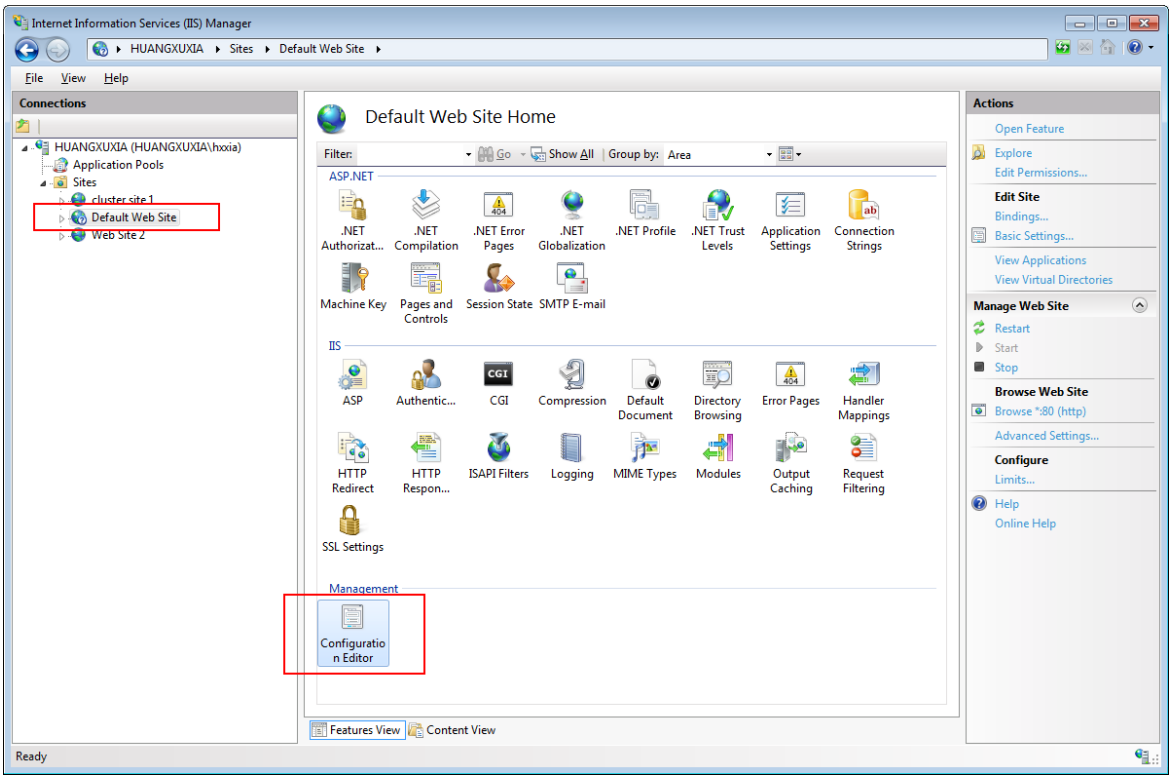
- If using HTTP to access AEM and upload file, locate the following line and configure "max-post-size" for the maximum file size to be uploaded, for example, 104857600 (which indicates 100 MB).

```
<http-listener name="default" max-post-size="104857600" socket-binding="http"
 redirect-socket="https"/>
```

To change the default file size in IIS (7.5 thru 10):

1. In the **IIS Manager**, select the Web site where PowerServer is installed, and then select the **Configuration Editor** feature.

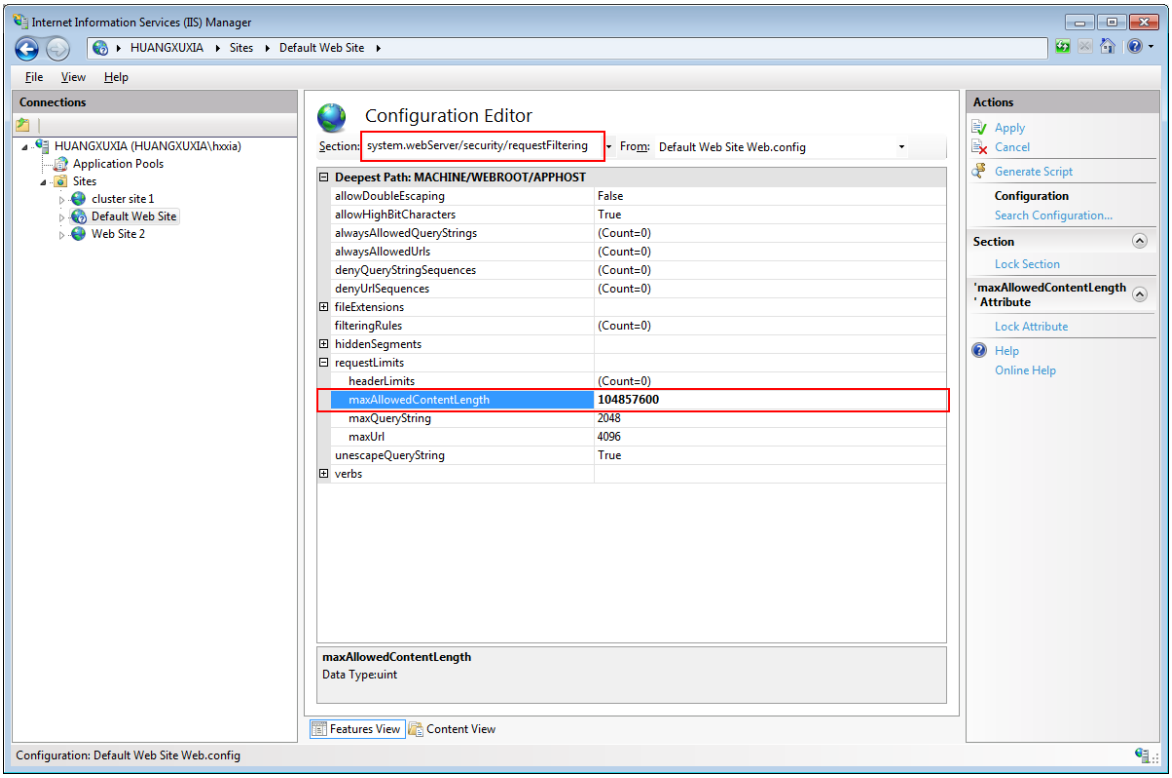
Figure 5.117: IIS -> Configuration Editor



2. Open the **Configuration Editor** feature, select or input *system.webServer/security/requestFiltering* in the **Section** field, and then modify the value of the

maxAllowedContentLength attribute under **requestFiltering** to a proper value, for example, 104857600 (which indicates 100 MB). Click **Apply** to save changes.

Figure 5.118: requestFiltering -> maxAllowedContentLength



5.4.10.2 Upload standalone mobile apps and Appeon Workspace

After you package a standalone mobile app or Appeon Workspace, you can upload the file to the PowerServer and then send the download URL to your users. If you have uploaded an updated file to overwrite the existing file, your users will get automatically updated, as Appeon Workspace and the standalone mobile app will check for the updates and compare the version/build number once it connects with PowerServer.

For how to package a standalone mobile app or Appeon Workspace, refer to Section 10.3, “Packaging a stand-alone mobile project” in *PowerServer Toolkit User Guide* and Section 10.4, “Customizing and packaging Appeon Workspace” in *PowerServer Toolkit User Guide*.

For how to make the auto-upgrade feature of Appeon Workspace and standalone mobile app to work, refer to Section 3.2.1, “Enabling auto-upgrade of Appeon Workspace” in *Appeon Workspace User Guide*.

To upload the standalone mobile app and Appeon Workspace to the server:

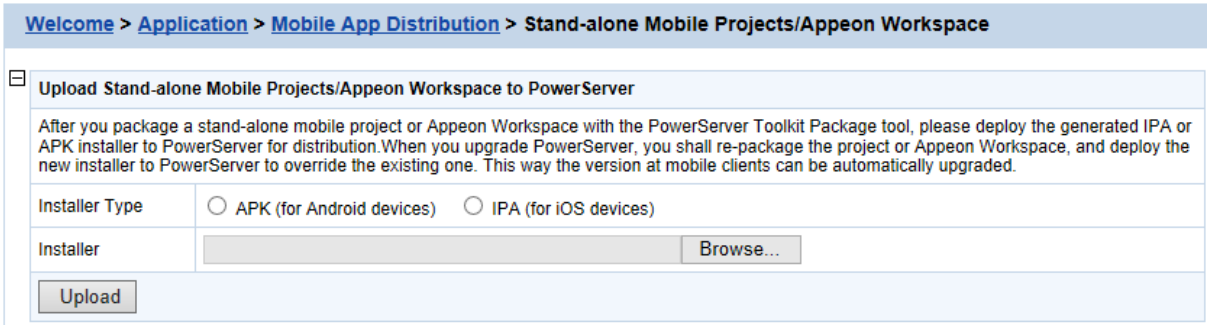
Step 1: Select the installer type for the standalone mobile app or Appeon Workspace: APK (.apk) for the Android device, or IPA (.ipa) for the iOS device.

Step 2: Click **Browse** to select the installer file.

File name

If you create the installer file by using the PowerServer ToolKit Package tool, you should keep the file name by default. A valid file name should look like this: *App Name-App Identifier-BuildNumber*.apk or *App Name-Bundle ID-BuildNumber*.ipa, for example, sales-appeon-9_0_1681_00.ipa. Note that any dot (.) in *App Name* (or *Display Name*) or *App Identifier* (or *Bundle ID*) shall be replaced by an underscore(_). For more about the file name, refer to Section 10.3, "Packaging a stand-alone mobile project" in *PowerServer Toolkit User Guide* and Section 10.4, "Customizing and packaging Appeon Workspace" in *PowerServer Toolkit User Guide*.

Figure 5.119: Upload the installer



Step 3: Click **Upload** to upload the selected file to the PowerServer.

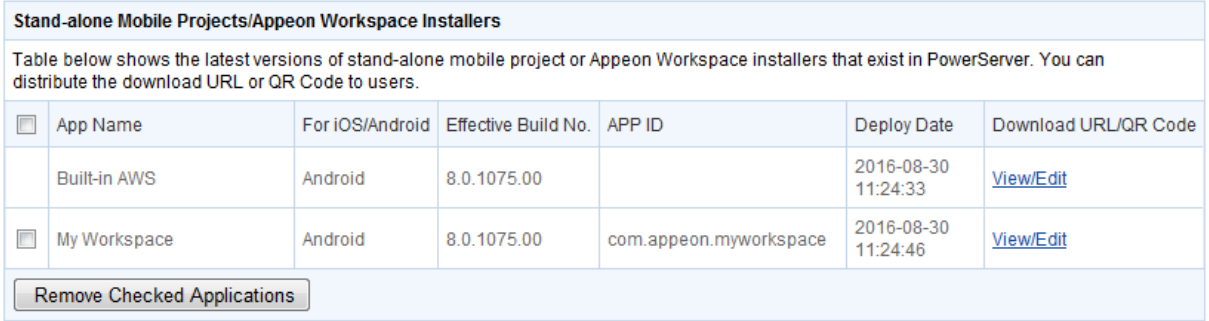
During this process, the file will be uploaded to the PowerServer Web server, and will be deployed as a WAR file if PowerServer is installed on top of JBoss, WebLogic, and WebSphere. The deployment process is automatic for JBoss, WebLogic (development mode), and JEUS, but **not** automatic for WebLogic (production mode) and WebSphere, in this case you will need to manually deploy it just as how you deploy the other applications.

If any error occurs due to the file size, please resolve the error by following instructions in the File size requirement.

Once the installer file is uploaded successfully, the download URL and QR code of the installer will be available from the table below.

A built-in Appeon Workspace for the Android device (App Name: Built-in AWS) is provided by Appeon by default. You can view and change the download URL of this built-in Appeon Workspace but cannot remove it.

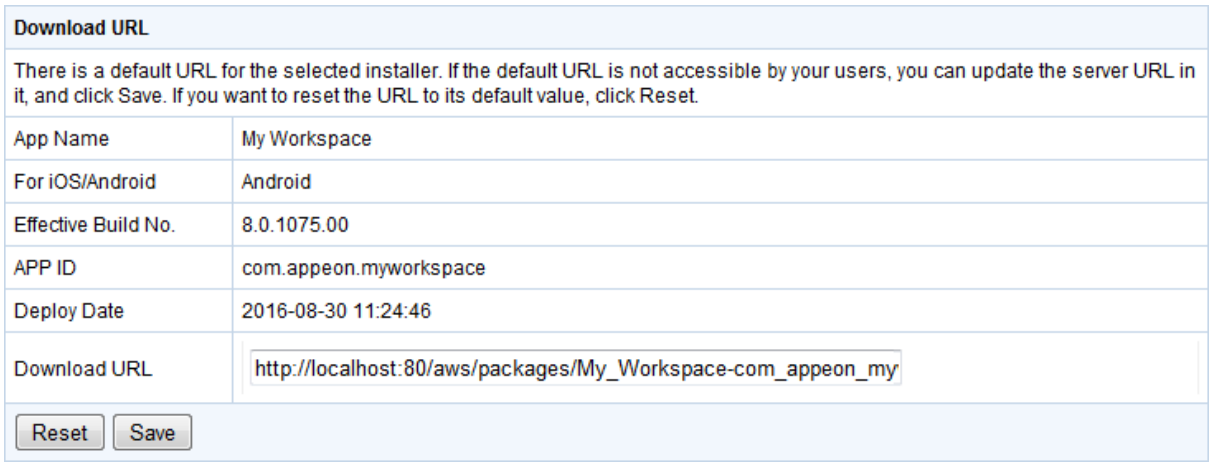
Figure 5.120: View and edit the installer information



To get the download URL and the QR code of the installer:

Step 1: Click the **View/Edit** link of the installer in the table. You will be directed to the **Download URL or QR Code** page.

Figure 5.121: Download URL of the installer



Step 2: Make sure the download URL is accessible to your users. By default the IP address/ domain name and port number of PowerServer will be used in the download URL of the installer.

You can change the download URL if the server IP or port number cannot be accessed by your users (for example, a "localhost" URL is not accessible to users); or if you have set up another Web site to host the installer, you will need to manually copy the installer over and change the download URL to point to the correct location.

For the Android installer, you should set the download URL of the APK file.

For the iOS installers, you should set the download URLs pointing to different files for different client types: for the installer to be downloaded and installed on the mobile device, you should set the download URL of the **PLIST** file in the **For Download on Mobile Devices** field; while for the installer to be downloaded to the Windows PC or Mac (and later synchronized to the mobile device via iTunes), you should set the download URL of the **IPA** file in the **For Download to iTunes on Desktops** field.

For the built-in Appeon Workspace, the download URL is bound to the Appeon Workspace download center by default; you can de-select the **Bind the above URL to Download Center** box to unbind them.

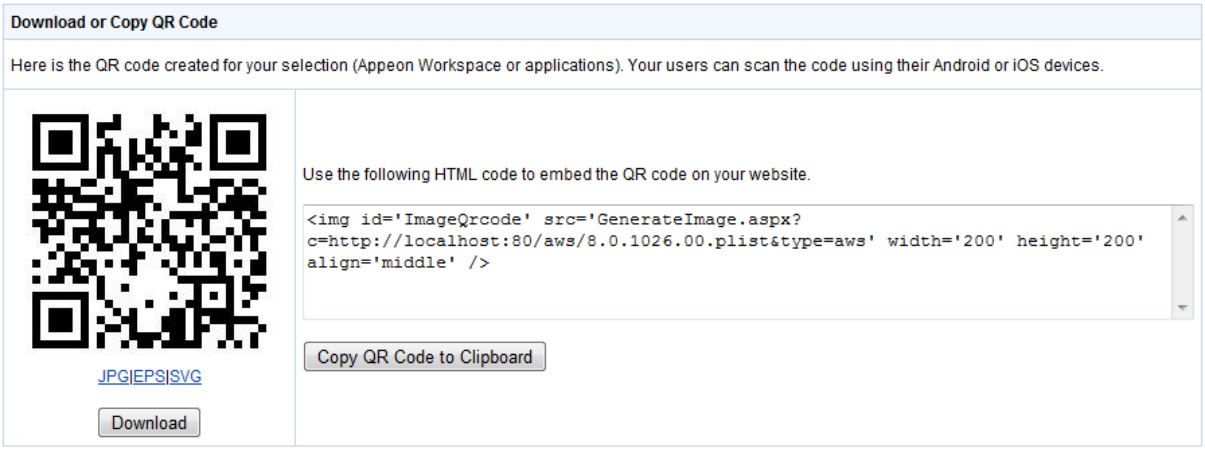
Figure 5.122: Download URL of the installer

Once you change the URL, click **Save** to save the change and refresh the QR code.

Step 3: Click the **Download** button to download the image file of the QR code in JPG/EPS/ SVG format and send the image file to your users, or click the **Copy QR Code to Clipboard** button to copy and embed the image of QR code in your download web page.

The end user can use a scanning tool to scan the QR code to directly download and install Appeon Workspace on their mobile devices.

Figure 5.123: QR code of the installer



5.4.10.3 QR code generation for mobile application(s)

You can also generate the QR code for those mobile apps that you deployed to PowerServer using the Appeon Deployment Wizard. For how to deploy the mobile app using the Appeon Deployment Wizard, refer to Chapter 6, *Deploying PowerBuilder Applications* in *PowerServer Toolkit User Guide*.

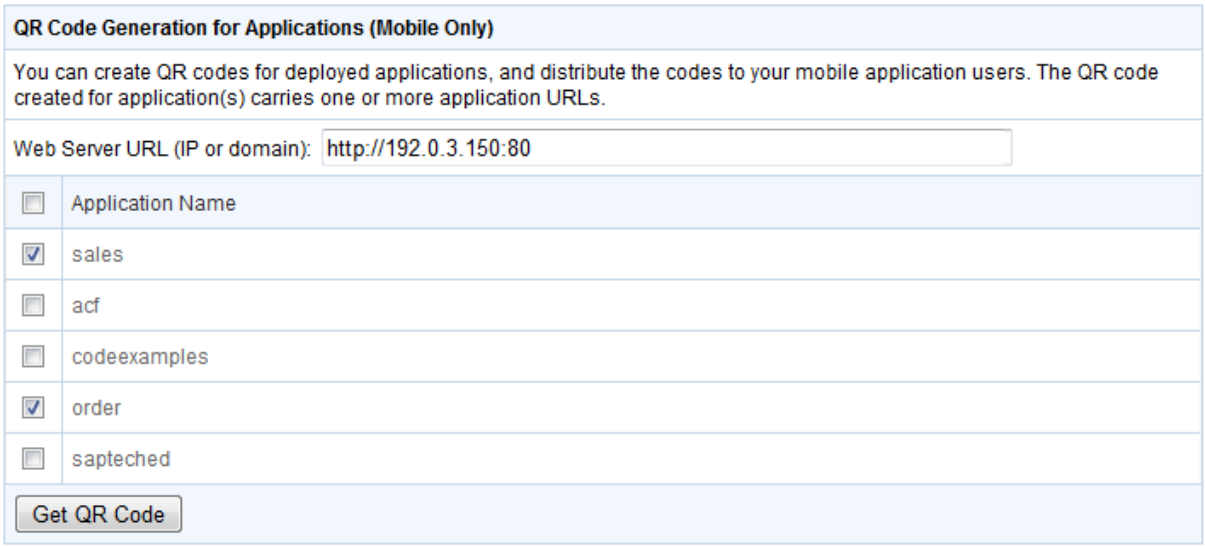
To generate the QR code for mobile application(s):

Step 1: In the **Web Server URL** field, input the IP address or domain name of the Web server where mobile apps are deployed.

Step 2: From the application list, select one or more mobile apps to be included in the QR code.

Step 3: Click the **Get QR Code** button to download or copy the QR code generated for the selected app(s).

Figure 5.124: QR code generation for apps (mobile only)

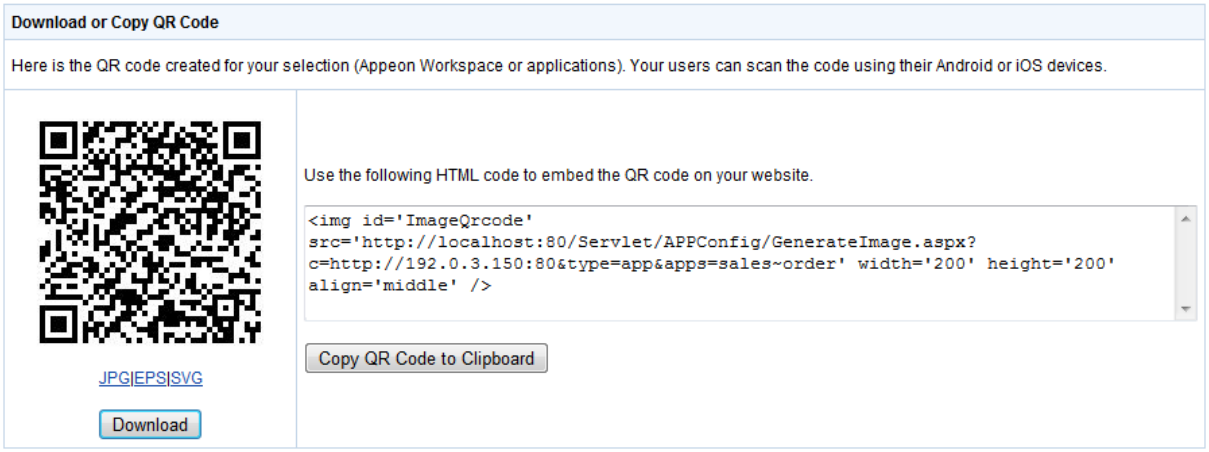


To download or copy the QR code:

You can click the **Download** button to download the image file of the generated QR code in JPG/EPS/SVG format and send the image file to end users, or click the **Copy QR Code to Clipboard** button to copy and embed the image of QR code in your download web page.

The end user can open Appeon Workspace and use the scan tool in Appeon Workspace to directly download and install mobile application(s). For more about the scan tool in Appeon Workspace, refer to Section 4.1, “Adding applications” in *Appeon Workspace User Guide*.

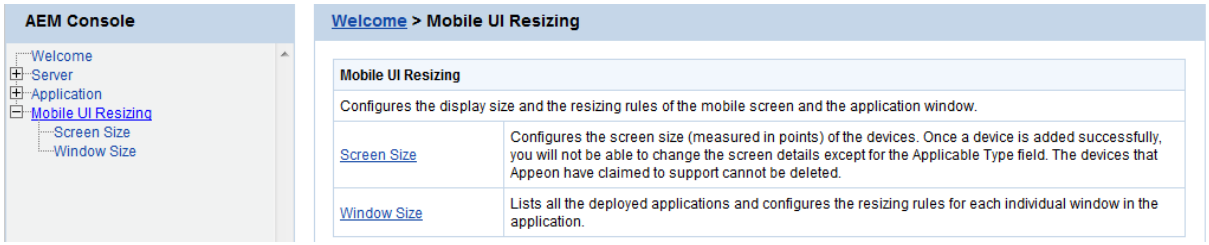
Figure 5.125: Download or copy QR code of the installer



5.5 Mobile UI Resizing

Mobile UI Resizing is a set of tools for configuring mobile devices and resizing application windows. There are two sets of tools: Screen Size and Window Size.

Figure 5.126: Mobile UI Resizing



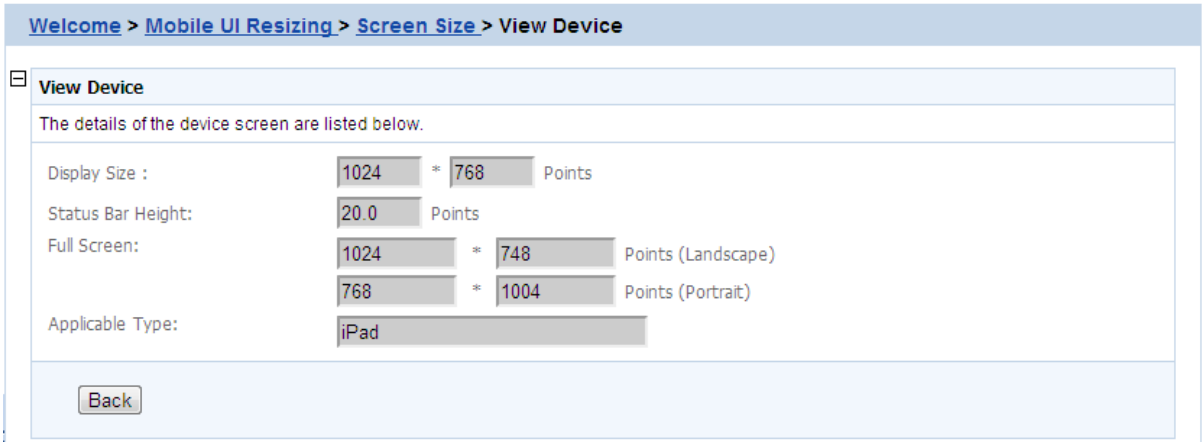
5.5.1 Screen Size

Screen Size is a tool for managing the Appeon-supported mobile devices. It allows adding, editing and removing devices. But those devices which PowerServer Mobile claims to support cannot be modified or deleted. All the supported device screen size (measured in points) added are listed below.

Figure 5.127: Screen Size

Click the **Edit** button to view the details of the device screen size.

Figure 5.128: Screen details



5.5.1.1 Adding a device

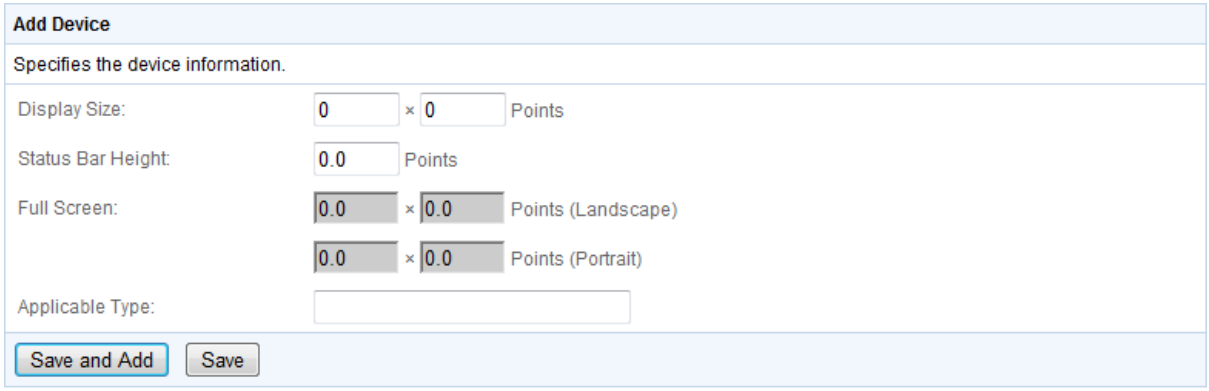
On the **Screen Size** page, the supported devices (measured in points) are configured by default, such as iPad 2/3/4/Mini/Air, iPhone 4/4S/5/5C/5S/6/6 Plus, iPod touch 4/5 etc. You can view the settings by clicking the associated **Edit** button, but cannot edit or delete these default devices.

You can also add a device which is not listed by default.

To add a new device, follow the following steps:

Step 1: Click **Add Device**, and the **Add Device** page appears.

Figure 5.129: Add a device



Step 2: On the **Add Device** page, enter the following values:

Settings	Descriptions
Display Size	The size of the device screen. You should be able to get this information from the device specification provided by the manufacturers. Or you can use the device to access a deployed application and use the screen size that is automatically loaded. Refer to Automatically adding a device to an application for details.

Status Bar Height	Height of the system status bar. a. **iOS devices**: The status bar is 20 points high. b. **Android devices**: The status bar height is subject to the devices. Developers may need to write scripts to get the height first. The height of the system status bar will be automatically deducted when calculating the available screen space for the application window.
Full Screen	The full screen size will be calculated automatically once you input the above values.
Applicable Type	Enter the device types that the specified size support.

Step 3: Click the **Save** button to add the device or click **Save and Add** to save the device and begin to add another one.

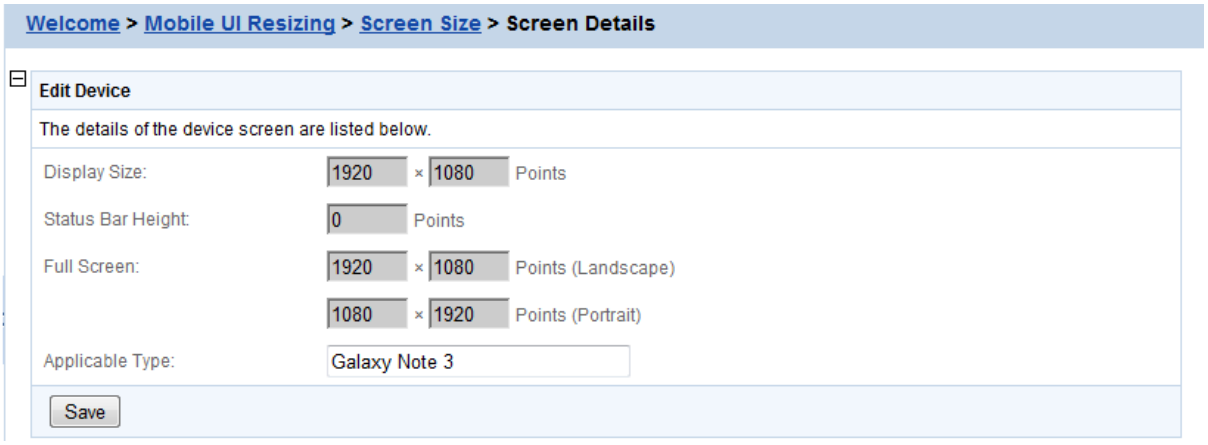
5.5.1.2 Editing a device

You can always edit the applicable type of devices of an added device on the Edit Device page in AEM.

To edit an added device:

Step 1: click **Edit**, and make the changes you intend to on the **Edit Device** page.

Figure 5.130: Edit a device



Step 2: Click **Save** to save the changes.

5.5.1.3 Deleting a device

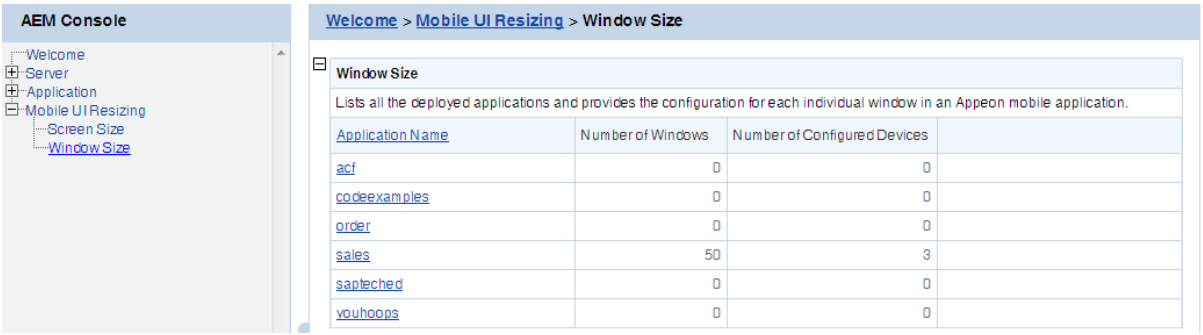
To delete a device, click **Delete**, and then click **OK** to confirm the deletion in the popup dialog box.

5.5.2 Window Size

When you are developing an application for mobile device, you probably want to make it universal and run on various mobile devices, such as iPad, Android tablets etc. There are basically two ways to achieve this:

- Method 1: Resize the windows and controls at runtime to fit with the various screen sizes. You will be required to remember all these screen sizes, and write code to resize the windows and controls.
- Method 2: Use this Window Resizing tool to automatically scale the windows and its UI controls (except for controls in DataWindow objects) to fit with a wide range of mobile devices. This tool works especially well if the mobile devices have similar screen sizes, such as iPad and the Android tablets, or iPhone and the Android smart phones. See this section for details.

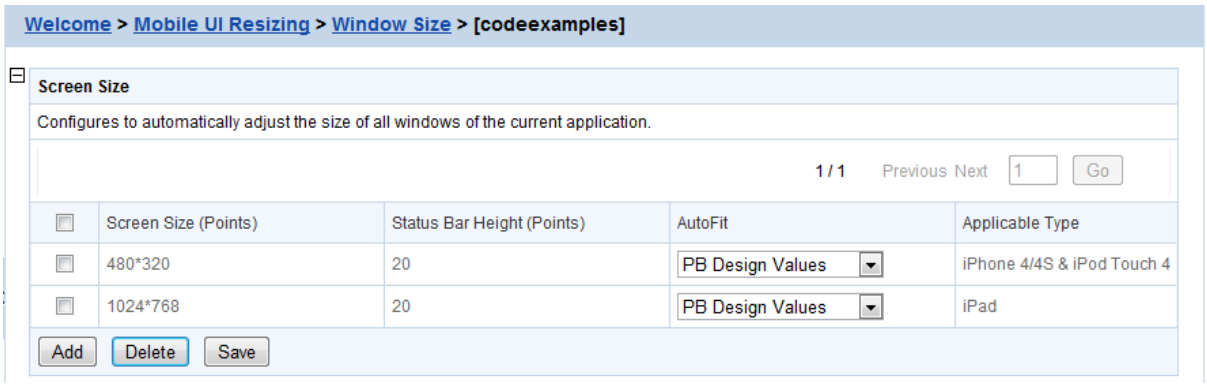
Figure 5.131: Window size



5.5.2.1 Configuring size for all windows

Click on the application name you want to configure, and the Screen Size table appears.

Figure 5.132: Screen size list



In the **Screen Size** table, you can:

1. **Add a device**: Click the Add button and select a device from the dropdown list box that appears.

   The devices that Appeon claims to support and that you specified in Screen Size are listed for choices.

   Automatically adding a device for an application

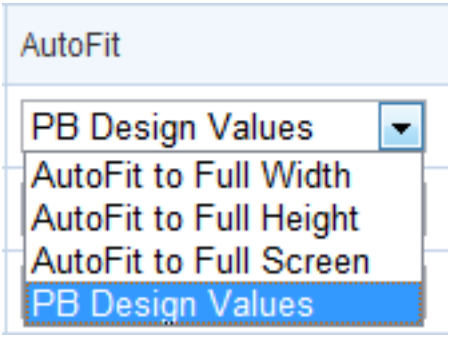
   When a mobile device accesses the deployed application, the device will be automatically registered and the device screen size will be saved into the **Screen Size** table for the application if it is not registered. If the application UI is not properly

displayed on a particular device, you can configure the window size for this particular device.

2. **Delete devices**: Check the checkboxes associated to the device(s) you want to delete and click **Delete**.

3. **Configure size for all windows**: You can specify one of the autofit modes which will automatically adjust all windows of the application from the AutoFit dropdown list box associated with the device, as shown in the following figure.

Figure 5.133: Autofit mode



The modes and the corresponding descriptions are listed in the following table.

Table 5.10: Autofit mode

Mode	Descriptions
PB Design Values	Windows will be displayed in the original size on the target device. This means windows will not be scaled, if the window is wider and/or longer than the screen, you would need to scroll to view the remaining part.
AutoFit to Full Width (X axis)	Windows will be displayed in full screen in the X direction only. This means, windows will be scaled up or down in both the X and Y direction, until they reach the same width as the device screen, but probably not the same height, therefore, if the window is higher than the screen, you will need to scroll vertically to view the remaining part of the window.
AutoFit to Full Height (Y axis)	Windows will be displayed in full screen in the Y direction only. This means windows will be scaled up or down in both the X and Y direction, until they reach the same height as the device screen, but probably not the same width, therefore, if the window is wider than the screen, you will need to scroll horizontally to view the remaining part of the window.
AutoFit to Full Screen (X & Y axis)	Windows will be displayed in full screen in both the X and Y directions. This means windows will be scaled up or down to have the same height and the same width as the device screen, therefore, you can view the

Mode	Descriptions
	entire window and all of its controls in the device screen without needing to scroll.

Select one mode from the **AutoFit** options, and then click **Save**.

Once you have clicked **Save**, all windows of the application will be adjusted automatically by the selected mode.

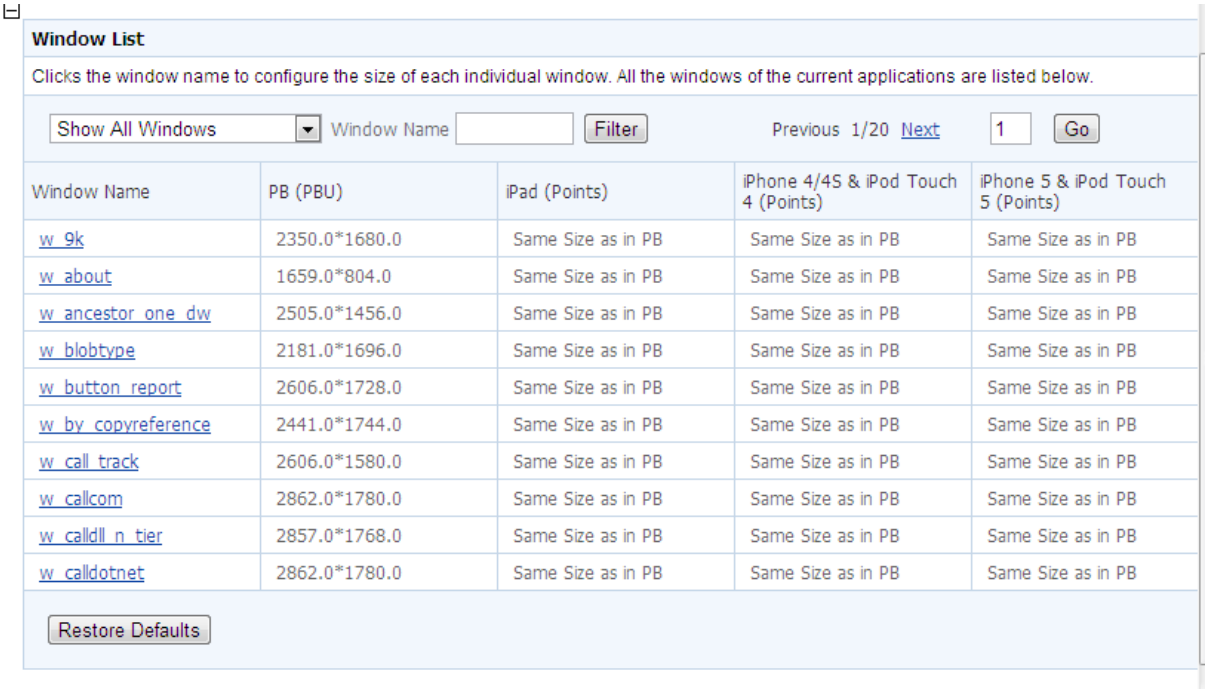
Note: if new windows are added to the application, you will need to click **Save** again to manually apply the selected autofit mode to the new windows, otherwise, the new windows will be displayed in the original size (the PB design values), not in the selected autofit mode.

5.5.2.2 Configuring size for an individual window

After you set the autofit mode for the application, all windows of the application will be adjusted by the selected mode, if any window needs to be adjusted differently, you can proceed to configure the size of each individual window in the **Windows List** table.

In the **Windows List** table (**AEM** > **Mobile UI Resizing > Window Size** > *Application Name*), all windows of the application is listed by default, including its original size in PB and the size in the selected device(s).

Figure 5.134: Windows List



The size in the selected device(s) is determined by the selected autofit mode by default. When the autofit mode is changed, the size in the selected device(s) changes accordingly. For example, if you set the autofit mode to "Design value in PB" for iPad in the Device List table, then "Same size as in PB" will be displayed in the iPad column in the Window List table. If you configure the size of the individual window, then the new size for that window will be displayed.

View windows: You can select a search criteria from search field dropdown list box to narrow down your search area or/and input a keyword in the **Window Name** text box, and then click **Filter** to view windows that meet your request. You can also use page navigator on the top right of the Window List table to view the windows.

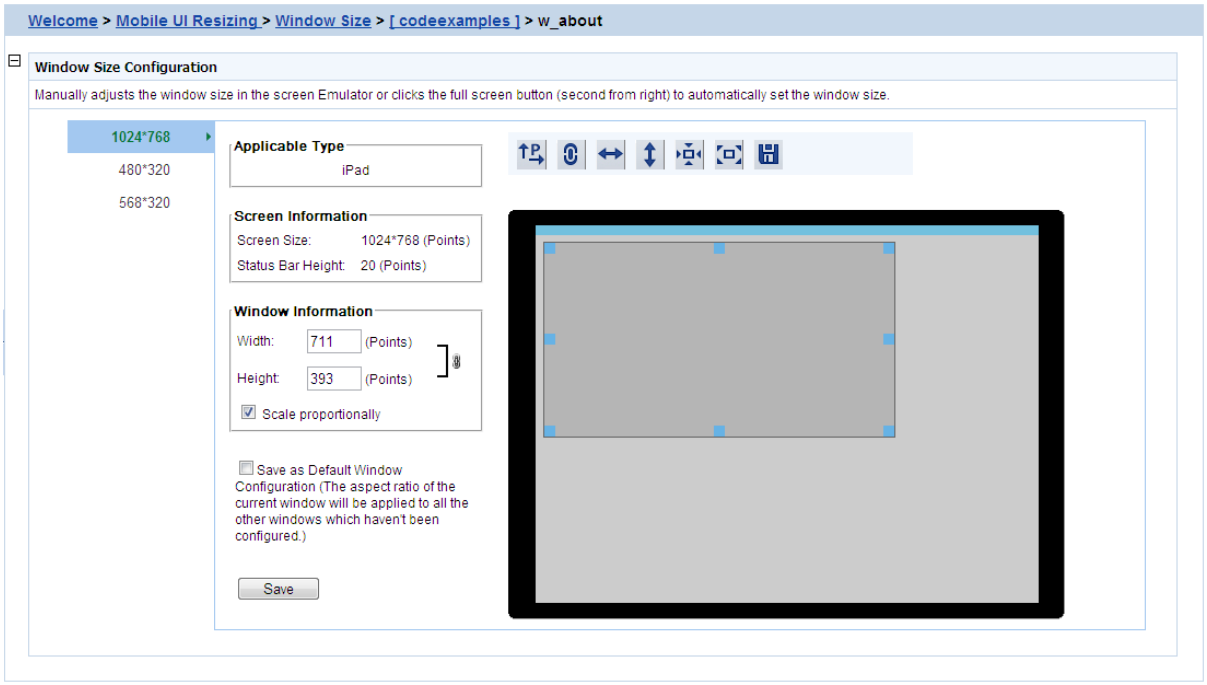
Restore defaults: You can revert all the windows to default by clicking the **Restore Defaults** button at the bottom.

To configure an individual window of the application, do the following:

Step 1: In the **Window List** table, click on the window you intend to configure.

In the **Window Size Configuration** table that displays, you will see a device screen simulator in which you can preview how the window will be displayed and adjust its size. Now you are ready to resize the window in the screen emulator:

Figure 5.135: Screen emulator



Step 2: Select a device name from the left column. The device(s) added to the Screen Size table are displayed. You need to configure the window size for each device separately.

Step 3: Select a displaying orientation (in landscape or in portrait) by clicking the orientation icon (). You need to configure the window size for each orientation separately.

Step 4: (Optional) enable the proportional scale by either clicking the proportional icon () or check the **Scale proportionally** checkbox. We kindly recommend that you keep this enabled to avoid window deformations.

Step 5: Use one of the following to resize the window:

- Drag the corner of the window in the screen emulator; or

- Click the full width icon (), the full height icon (), the original screen icon (), or the full screen icon () above the screen simulator; or
- Input the desired numbers in the **Width** and the **Height** text box under **Window Information** respectively.

The new size and the window coordinates (X & Y axis) will be displayed simultaneously.

Step 6: (Optional) if you want to apply the new size to the remaining windows, check the **Save as default window configuration** check box.

Step 7: Either click the save icon () above the screen simulator or the **Save** button at the bottom to save all the settings.

You will not be able to save the window size, if AEM prompted "Current aspect ratio will lead to window deformation!". AEM performed detection immediately after the window is resized, to help prevent the window and control being stretched or shrunk unreasonably.

Notes: Dragging the screen emulator to change a window coordinates does not work on windows that are opened using OpenSheet().

Index

T

U

V

W