PowerServer Configuration Guide for .NET

Appeon® PowerServer® 2020

FOR WINDOWS

Contents

1 Server Configuration Tasks

Server configuration for Web architecture is usually a daunting task that requires a wide range of server knowledge. The same rule applies to Appeon architecture. Appeon architecture resides in at least three types of servers: Web server, application server, and database server. Each server involves a third-party server product: for example, PowerServer is installed to IIS. A number of configuration tasks must be performed before a PowerServer 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.

1.1 Scope of configurations discussed in this book

PowerServer architecture is a typical n-tier architecture that can provide development and runtime environments for both PowerServer and non-PowerServer applications. This book focuses on the configurations for supporting PowerServer 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 therefore, will not be addressed in this guide.

Configurations specific to the functioning and performance of third-party servers in PowerServer architecture may still impact the architecture. For example, indexing database tables has nothing to do with PowerServer knowledge but can greatly improve the performance of a PowerServer 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 PowerServer architecture.

1.2 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 1.1: 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.
Performance Management	Improving server performance.
Server Information Management	Managing server-related information.

Configuration During...	For the Purpose of ...
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.

1.2.1 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 1.2: 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 PowerServer 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 PowerServer Web application or the PowerServer mobile application 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 PowerServer Web application or the PowerServer mobile application 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

1.2.2 Configuration during debugging

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

Table 1.3: 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

1.2.3 Configuration during security management

The following table lists the server configuration tasks for managing the security of applications and servers in PowerServer architecture.

Table 1.4: 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 a PowerServer Web or PowerServer 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

1.2.4 Configuration during performance management

The following table lists the server configuration tasks for improving server performance.

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

Table 1.5: Configuration tasks during performance management

Task	Description	See section
(In AEM) Active Sessions	Monitor all active sessions and mobile devices 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.	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

1.2.5 Configuration during server information management

The following table lists the server configuration tasks for managing server-related information.

Table 1.6: 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 a PowerServer.	Licensing
(In AEM) Support	View the valid product support period and renew the support.	Support

1.2.6 Configuration for emergency control

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

Table 1.7: Configuration for emergency control

Task	Description	See section
Status Monitor	Configure the PowerServer Status Monitor so it can be used for restarting PowerServer automatically.	[PowerServer Monitor](#)

2 PowerServer Monitor

2.1 Overview

PowerServer Monitor is a small program installed along with PowerServer, which contains four monitors: server state monitor, CPU usage monitor, memory usage monitor, and recycle monitor.

- Server state monitor automatically backs up PowerServer session information, monitors if PowerServer is in "running" status, and in the event that PowerServer shuts down it automatically restarts PowerServer and recovers the runtime information.

- CPU usage monitor and memory usage monitor detect the server resource usage, if the usage reaches the peak, they automatically back up PowerServer session information, restart PowerServer, and restore the session information.

- Recycle monitor automatically restarts PowerServer periodically.

The monitor backs up PowerServer session information that includes:

- User authentication information

- References to PowerServer transaction components

The monitor does not back up:

- Information being processed in active transaction

Important note: to ensure the monitor runs successfully:

1. The version of PowerServer Monitor must be the same as the version of PowerServer.

2. PowerServer's license must be Enterprise Edition.

2.2 Launching PowerServer Monitor

You can launch PowerServer Monitor using either of the following methods:

Method 1: Launch PowerServer Monitor from **Windows Start** > **Programs** > **Appeon PowerServer 2020** > **PowerServer for .NET** > **Instances** > **%websitename%** > **Status Monitor**.

Method 2: Launch PowerServer Monitor by running %appeon%\Toolkit\status monitor \AppeonMonitor.exe.

The PowerServer Monitor main window is shown in the figure below. The status information of the four monitors would be displayed on the left, and the event log information would be displayed on the right. But before the information can display correctly, you would need to configure and run the monitors. See the following sections for details.

Figure 2.1: PowerServer Monitor main window
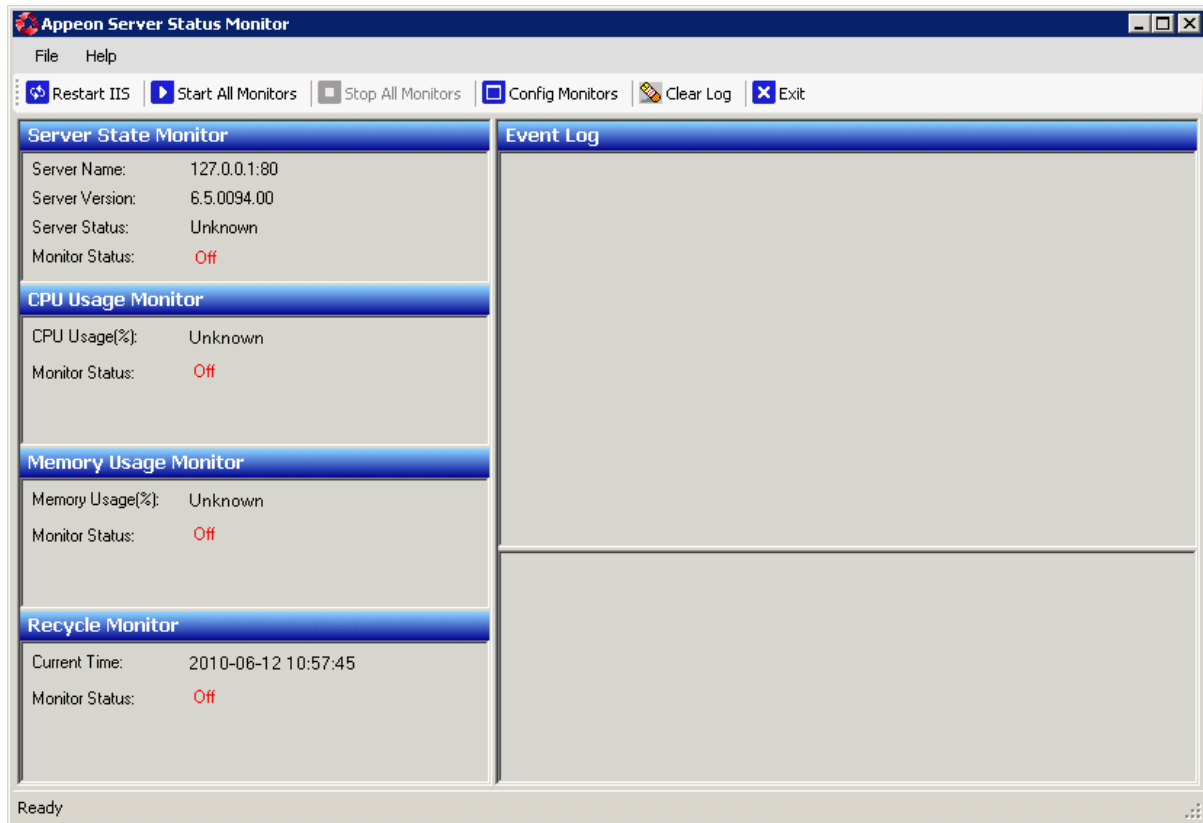
2.3 Configuring Monitors

In the monitor's main window, click the **Config Monitors** button on the toolbar to open the Monitor Configuration window. The Monitor Configuration window provides five tab pages for you to configure the monitor settings.

Figure 2.2: Monitor Configuration window
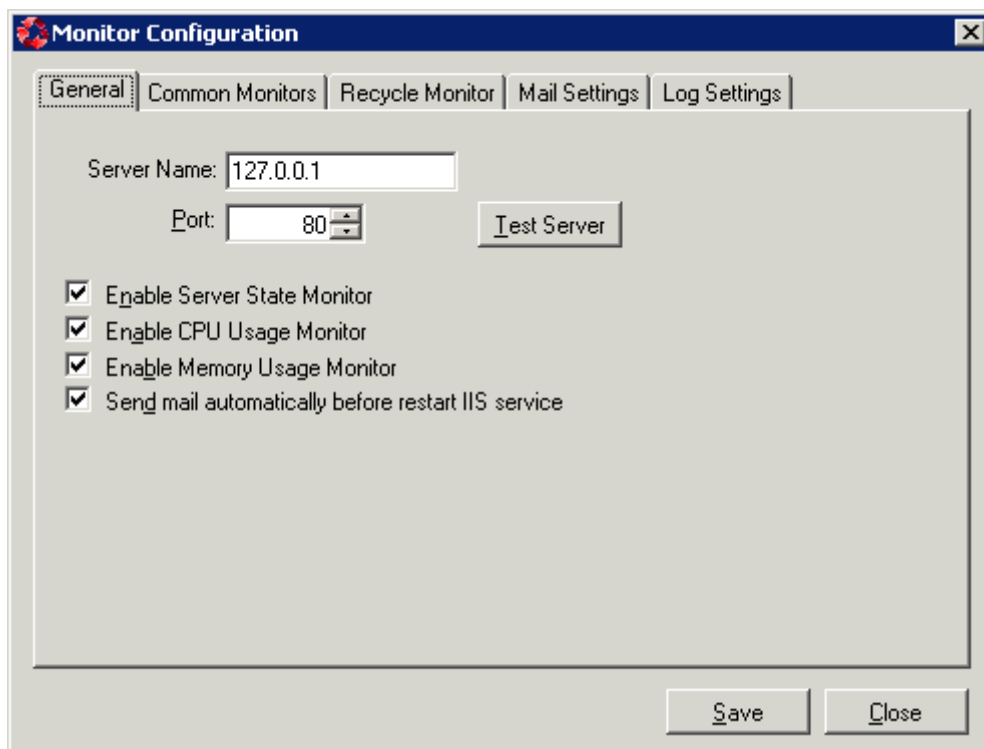
2.3.1 General tab

In the **General** tab, you can configure the server IP and port, enable the server state monitor, CPU usage monitor, and memory usage monitor, and enable email notification.

Figure 2.3: General tab
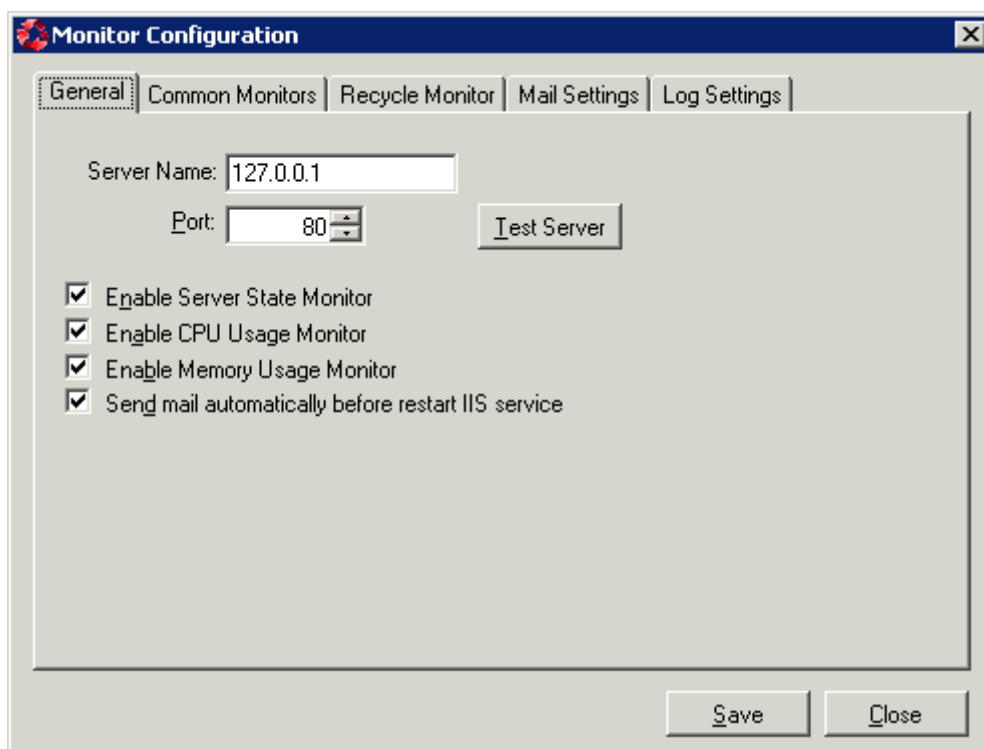
Table 2.1: Instructions

To...	Do this...
To specify the IP address and port of PowerServer...	Specify the IP address in the Server Name group box, and the port of IIS Web site where PowerServer is installed, then click the **Test Server** button to test whether PowerServer can be connected successfully.
	PowerServer Monitor and PowerServer must be installed to the same machine.
To enable the server state monitor, CPU usage monitor, and memory usage monitor...	Select the corresponding option: • Enable PowerServer Status Monitor • Enable CPU Usage monitor • Enable Memory Usage Monitor If the option is enabled, you can configure the monitor in the **Common Monitors** tab (see Common Monitors tab for details); and you can then run the monitor from menu **File** > **Monitor** > **Start** ..., or by clicking the **Start All Monitors** button on the toolbar to run all of the monitors that have been enabled and configured properly.
	Recycle monitor is enabled and configured in the **Recycle Monitor** tab (see Recycle Monitor tab for detailed instructions).
To send email notifying users that the IIS service is to be restarted...	Select the **Send mail automatically before restart IIS service** option.
	If this option is enabled, and if email settings are configured properly in the **Mail Settings** tab (see Mail Settings tab for detailed instructions), notification emails will be sent to receivers automatically each time before IIS service is restarted.

2.3.2 Common Monitors tab

The **Common Monitors** tab allows you to configure the server state monitor, CPU usage monitor and memory usage monitor, as shown in the following figure.

Only when the monitor is enabled in the **General** tab, you will be able to configure the settings in the **Common Monitors** tab, otherwise, the settings will be grayed out (not configurable).

Figure 2.4: Common Monitors tab
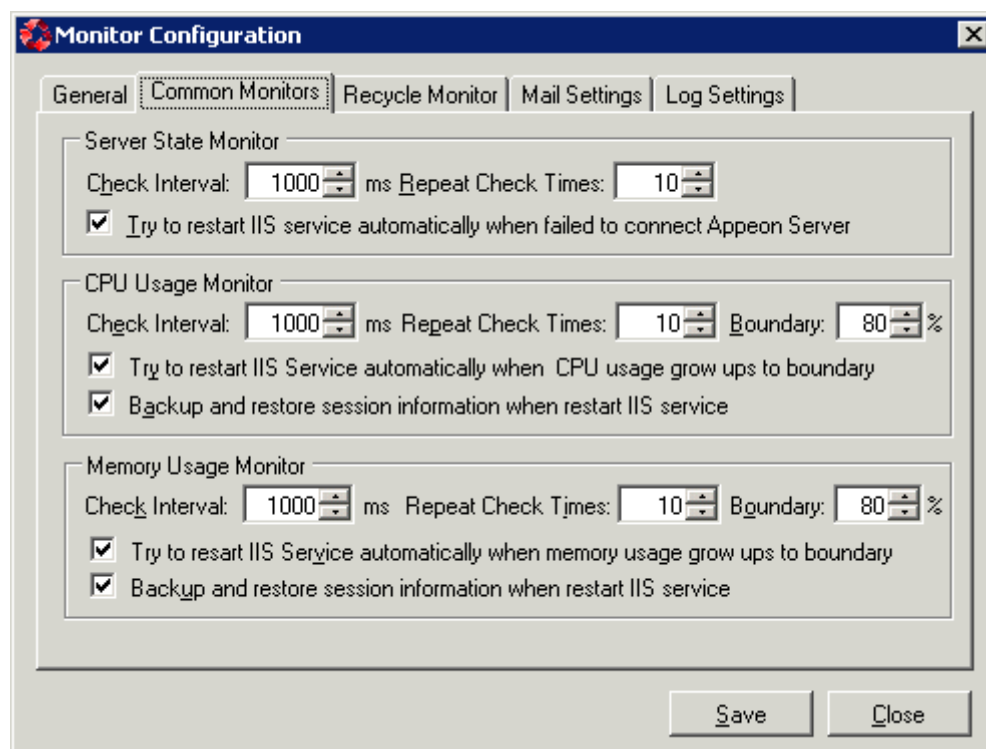
To configure the server state monitor:

Step 1: Specify the time interval that the monitor checks the server.

• Check Interval: The value represents the time interval the monitor detects the server. By default, the check time interval is 1000 milliseconds. The smaller the value is, the more precise the result is, but the more impact it has to the system performance.

Step 2: Specify the times that the monitor should successively detect that the condition to restart IIS service is met before it restarts the IIS service.

• Repeat Check Times: The value represents the times that the monitor successively detects that the condition to restart IIS service is met. When the value is reached, the IIS service will be restarted. For example, if the server state monitor detects for 10 times (default value) in succession that PowerServer cannot be connected, it will restart IIS service.

   This setting is to avoid the incorrect detection result due to accidental events.

Step 3: Select whether to restart IIS Service automatically when PowerServer cannot be connected for the specified times in succession.

• Try to restart IIS Service automatically when failed to connect PowerServer: If this option is enabled, IIS Service will be restarted automatically if server state monitor detects that PowerServer cannot be connected for the specified times in succession.

To configure the CPU usage monitor and memory usage monitor, the steps are similar:

Step 1: Specify the time interval that the monitor checks the server.

- Check Interval: The value represents the time interval the monitor detects the server. By default, the check time interval is 1000 milliseconds. The smaller the value is, the more precise the result is, but the more impact it has to the system performance.

Step 2: Specify the times that the monitor should successively detect that the condition to restart IIS service is met before it restarts the IIS service.

- Repeat Check Times: The value represents the times that the monitor successively detects that the condition to restart IIS service is met. For example, if CPU usage monitor detects for 10 times (default value) in succession that the CPU usage has reached the boundary that is set, it will restart IIS service.

  This setting is to avoid the incorrect detection result due to accidental events.

Step 3: Specify the maximum percentage of CPU usage or memory usage.

- Boundary: The value represents the maximum percentage of CPU usage or memory usage. By default, the boundary is 80%.

Step 4: Select whether to restart IIS Service automatically when CPU usage or memory usage grows up to the boundary that is specified.

- Try to restart IIS Service automatically when CPU usage grows up to boundary: If this option is enabled, IIS Service will be restarted automatically when the CPU usage monitor detects that the CPU usage has reached the boundary for the specified times in succession.

- Try to restart IIS Service automatically when Memory usage grows up to boundary: If this option is enabled, IIS Service will be restarted automatically when the memory usage monitor detects that the memory usage has reached the boundary for the specified times in succession.

Step 5: Select to back up and restore session information when restarting IIS service.

- Backup and restore session information when restart IIS service: If this option is enabled, the monitor will back up the session information before restarting IIS service, and then restore the information after PowerServer is successfully restarted.

2.3.3 Recycle Monitor tab

The **Recycle Monitor** tab allows you to configure how Recycle Monitor should work, as shown in the following figure.

Figure 2.5: Recycle Monitor tab
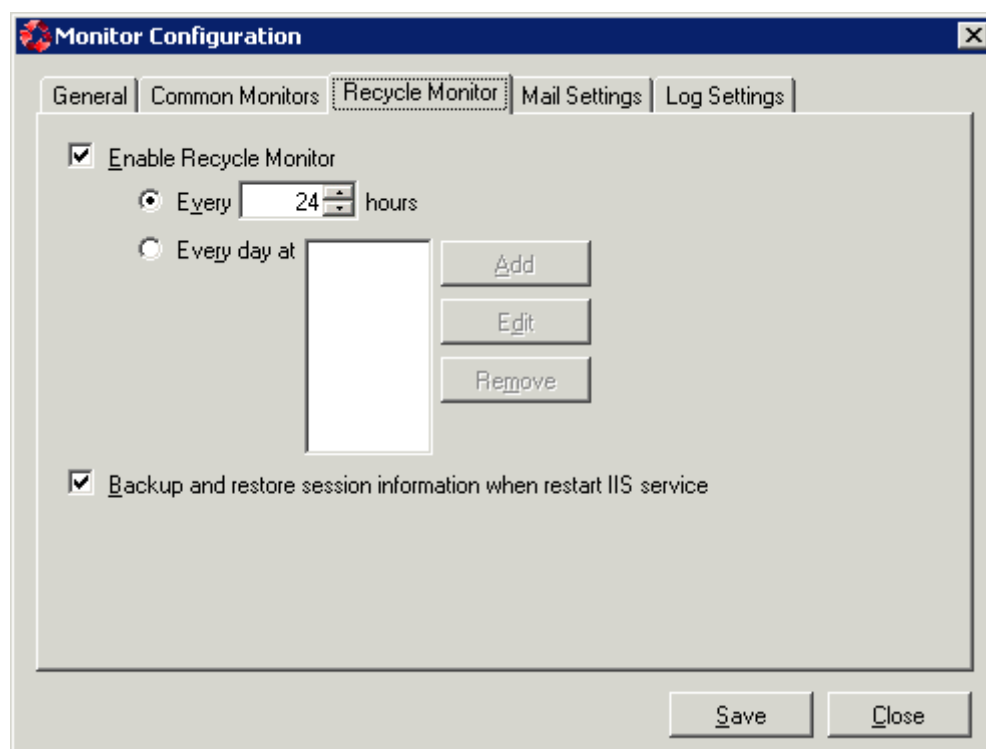
Step 1: Decide whether to enable recycle monitor.

• Enable recycle monitor: If this option is selected, the recycle monitor is enabled. You can then configure the cycle to restart IIS service automatically.

Step 2: Configure the time setting to restart IIS service automatically: by every _ hours, or every day at a fixed time.

Step 3: Select to back up and restore session information when restarting IIS service.

• Backup and restore session information when restart IIS service: If this option is enabled, the monitor will back up the session information before restarting IIS service, and then restore the information after PowerServer is successfully restarted.

2.3.4 Mail Settings tab

The **Mail Settings** tab allows you to configure the mail settings of sender and receiver(s) if you want the monitor to automatically send notification emails to users each time before the IIS service is restarted.

Figure 2.6: Mail Settings tab

Step 1: Make sure email notification is enabled, that is, make sure the **Send mail automatically before restart IIS service** option is selected in the **General** tab.

Step 2: Configure the email settings in the **Mail Settings** tab.

The following table describes how to configure the settings.

Table 2.2: Mail settings

Setting	Description
SMTP Server	Type the IP address of the mail server.
Port	Type the port of the mail server.
Sender	Type the mail address of the sender.
Password	Type the password used to log in to the sender's mailbox. If no password has been set, leave this field blank.
Receiver(s)	Type the mail address of the receiver. If there are more than one address, split them by semicolon.
Message	Type contents of the mail. This field can be left blank.

Step 3: Click the **Send Test Email** button to send a test email using the specified settings.

2.3.5 Log Settings tab

The **Log Settings** tab allows you to configure how the monitor should generate the log information.

Figure 2.7: Log Settings tab
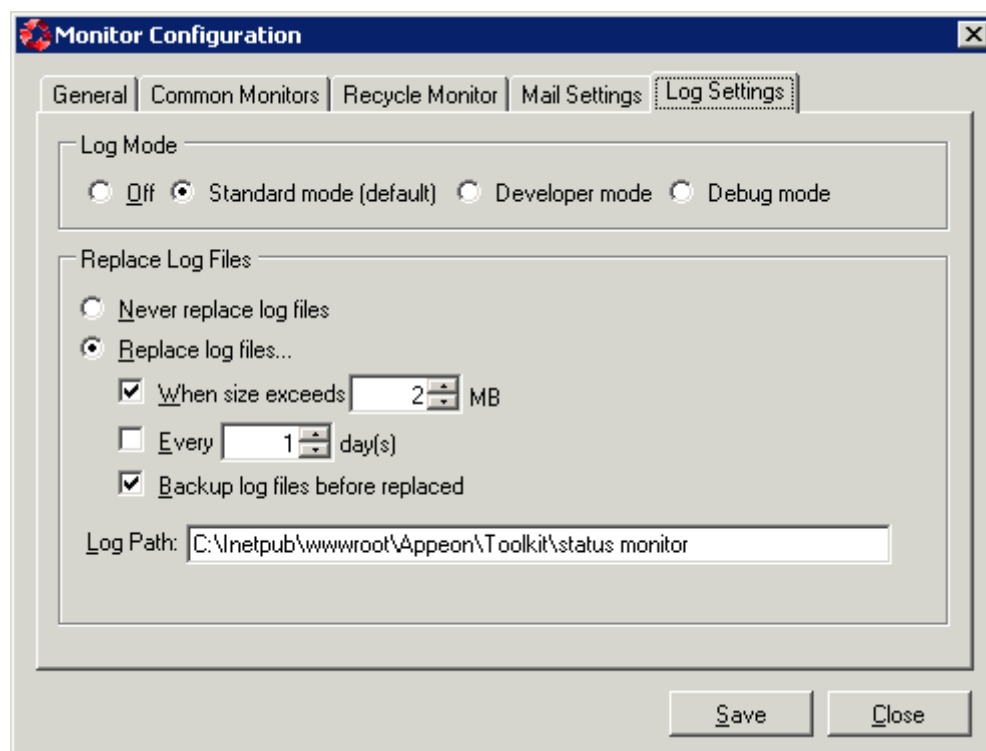
Log mode

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

- Off: Off mode does not generate any log files.

- Standard mode: Standard mode is the default mode. It generates standard log files that are sufficient for providing basic information. This mode may be inadequate for detailed troubleshooting.

- Developer mode: Developer mode generates detailed log files that are sufficient for troubleshooting.

- Debug mode: Debug mode generates log files that record every 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.

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.

To configure log file settings:

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

- Never replace log files: If you select this option, the log files will never be replaced.

- Replace log files...: If you select this option, the log files will be replaced according to conditions configured in Step 2. 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.

- Replace log files when size exceeds ___ MB: The system automatically replaces the log files when the file size exceeds the value set here.

- 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.

- Backup log files before replacing: This setting allows the monitor 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.

Step 4: Type the log path.

It can help you find log files easily when you need.

2.4 Understanding the information in monitor window

After enabling and configuring the monitor, click the menu **File** > **Monitor** > **Start** ... to run the monitor, or by clicking the **Start All Monitors** button on the toolbar to run all monitors.

Figure 2.8: PowerServer Monitor main window
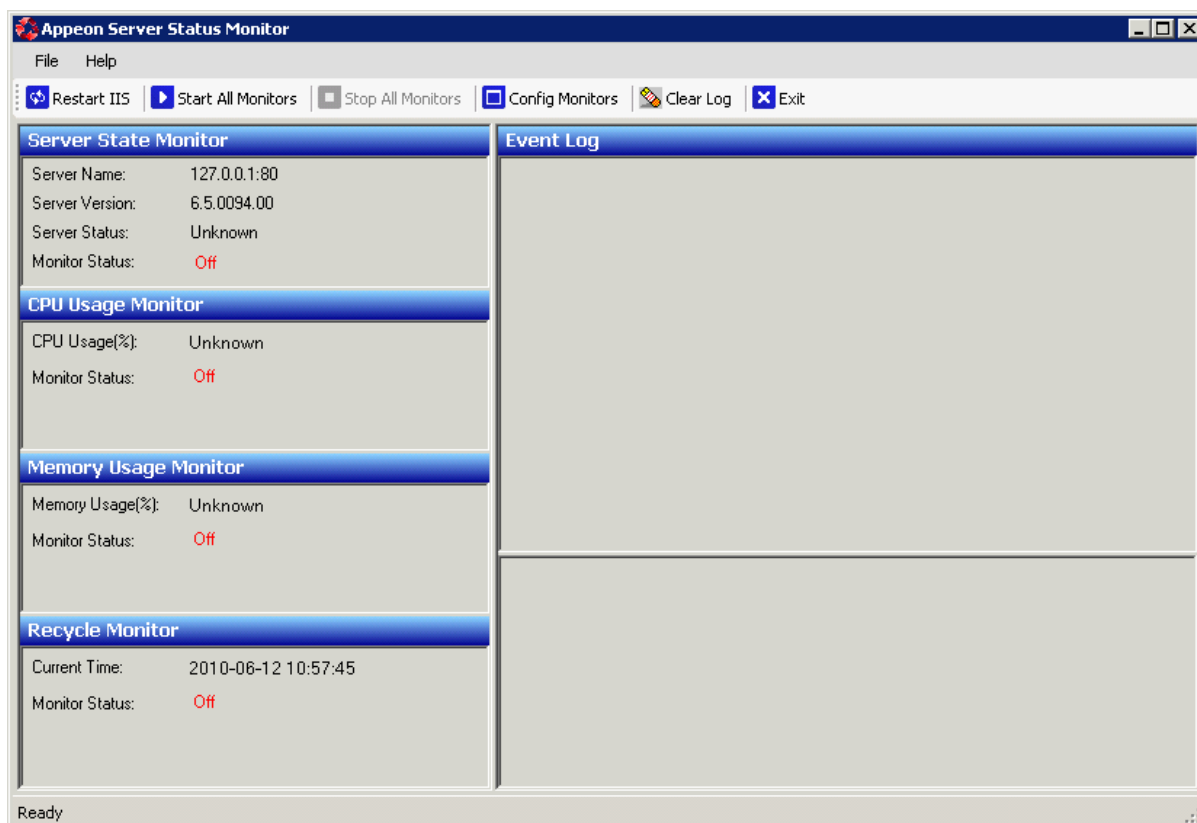
The monitor status information is displayed on the left of the main window, the log information is displayed on the right.

Server Status

Server Status in Server State Monitor window can be "unknown", "running" or null value.

- Running: If server state monitor detects that PowerServer is running, the value is Running.

- Unknown: If server state monitor detects that IIS service or PowerServer fails to run, the value is Unknown.

- Null value: If server state monitor is not started, it is null value.

Monitor Status

Monitor Status is "On" or "Off", which represents whether the monitor is started or not.

Event Log

Event Log is on the right of the PowerServer Monitor window. It reports the following types of information depending on the log mode:

1. Actions that the user has taken on the monitor, for example, stopping and running the monitor.

2. Actions that the monitor has taken, such as restarting IIS service, backing up session information etc.

3. Email notifications that the monitor has sent.

4. Warnings that the monitor has failed to execute a task.

3 Database Connection Setup

3.1 Overview

The steps for configuring the database for a PowerServer-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 a PowerServer-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 PowerServer environment.

3.2 What is PowerServer data source?

PowerServer data source is the same terminology as data source in Microsoft .NET Framework or other application servers.

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 PowerServer Web application and the PowerServer mobile application relies on PowerServer data sources to interact with the database servers.

3.3 Supported Database Drivers

Appeon .NET version supports the following database drivers for different database types and versions:

Table 3.1: Supported Drivers

Supported Driver	Supported Database Type and Version
SQL Anywhere native driver	SAP SQL Anywhere 16.0/17.0
Oracle native driver	Oracle 11g/12c/18c/19c
SQL Server native driver	Microsoft SQL Server 2012/2014/2016/2017/2019
Informix native driver	Informix 7.x/8.x/9.x/10.x/11.x
MySQL native driver	MySQL 5.5.x/5.6.x

Supported Driver	Supported Database Type and Version
ASE native driver ODBC driver	SAP ASE 12.5.x/15.x
PostgreSQL native driver	PostgreSQL 9.2 or 12.x
IBM DB2 native driver	IBM DB2 UDB 9.7

3.4 Setting up PowerServer data sources

The following sections give a general description of the data source settings. For step-by-step instructions on how to set up PowerServer data sources, refer to Data Source.

3.4.1 Data source settings for ODBC driver

PowerServer supports using ODBC driver to connect with SAP SQL Anywhere (8.x/9.x/10.0.1 only), or ASE databases. Before you start creating a data source with ODBC driver, you must install the corresponding ODBC driver and create the ODBC data source by following the instructions in the documents provided by the database vendor.

Figure 3.1: Settings for ODBC driver

Table 3.2: Settings for ODBC driver

Data Source Name	Type the name of the data source.
Data Source Type	Select "ODBC" to connect with SAP SQL Anywhere, or SAP ASE databases.
ODBC Data Source	Select a system DSN that was created in the ODBC administrator.
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 database is a SQL Anywhere database, be aware of the following:

- If the SQL Anywhere database resides in an NTFS folder, make sure the Windows "Network Service" or "Everyone" user has full controls over that folder, otherwise, testing of the data source may fail.

3.4.2 Data source settings for SQL Anywhere .NET Data Provider

PowerServer supports using SQL Anywhere .NET Data Provider driver to connect with SQL Anywhere 11.0/12.0/16.0/17.0/Web databases. Before you start creating a data source with SQL Anywhere .NET Data Provider driver, you must install the corresponding SQL Anywhere .NET Data Provider driver and create the ODBC data source by following the instructions in the documents provided by the database vendor.

Figure 3.2: Settings for SQL Anywhere .NET Data Provider driver

Table 3.3: Settings for SQL Anywhere .NET Data Provider driver

Data Source Name	Type the name of the data source.
Data Source Type	Select "SQL Anywhere Native Driver" (or "SQL Anywhere 17 Native Driver" for SQL Anywhere 17) to connect with the SAP SQL Anywhere database.
ODBC Data Source	Select a system DSN that was created in the ODBC administrator.
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.

When using the SQL Anywhere database, be aware of the following points:

- If the SQL Anywhere database resides in an NTFS folder, make sure the Windows "Network Service" or "Everyone" user has full controls over that folder, otherwise, testing of the data source may fail.

- If you want to switch SQL Anywhere drivers between different versions, you would need to go to the %powerserver%\AEM\ServerDll folder and copy the files (Server.dll, code.key, and iAnywhere.Data.SQLAnywhere.dll) from the sub-folder named after the SQL Anywhere version (such as **ASA11**, **ASA12**, **ASA16**, or **ASA17**), and then paste them to the %powerserver%\AEM\bin folder.

- Enable the connection pooling setting in ODBC driver, otherwise, the data source pools settings in AEM will not take effect, and the runtime performance of the deployed applications may dramatically slow down. Detailed steps are as below:
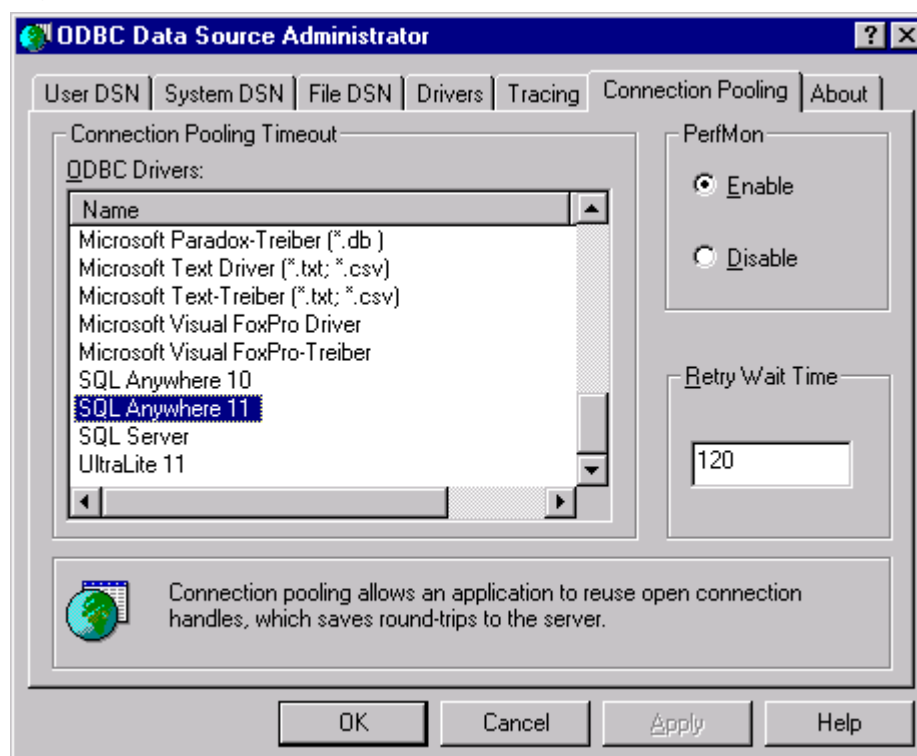
(1) Open ODBC Administrator.

(2) Switch to the **Connection Pooling** tab, as shown in the following figure.

(3) Select the **Enable** option in the **PerfMon** group box, as shown in the following figure.

(4) Select **SQL Anywhere 11** from the **ODBC Drivers** list box, or any other driver you want, and double click it.

Figure 3.3: Select SQL Anywhere from the ODBC Drivers list box

(5) Select the second option **Pool Connections to this Driver**, as shown in the following figure.

Figure 3.4: Select Connection Pooling Attributes
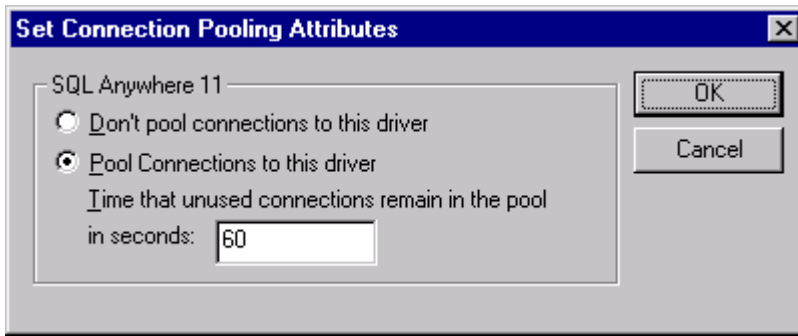
3.4.3 Data source settings for Oracle native driver

PowerServer supports using Oracle native driver to connect with Oracle databases. Before you start creating a data source with Oracle native driver, you must install Oracle full client. Note Appeon does not support Oracle instant client. If you have Oracle instant client installed, you will need to uninstall it first and then install Oracle full client. For installation instructions, refer to the Oracle documents.
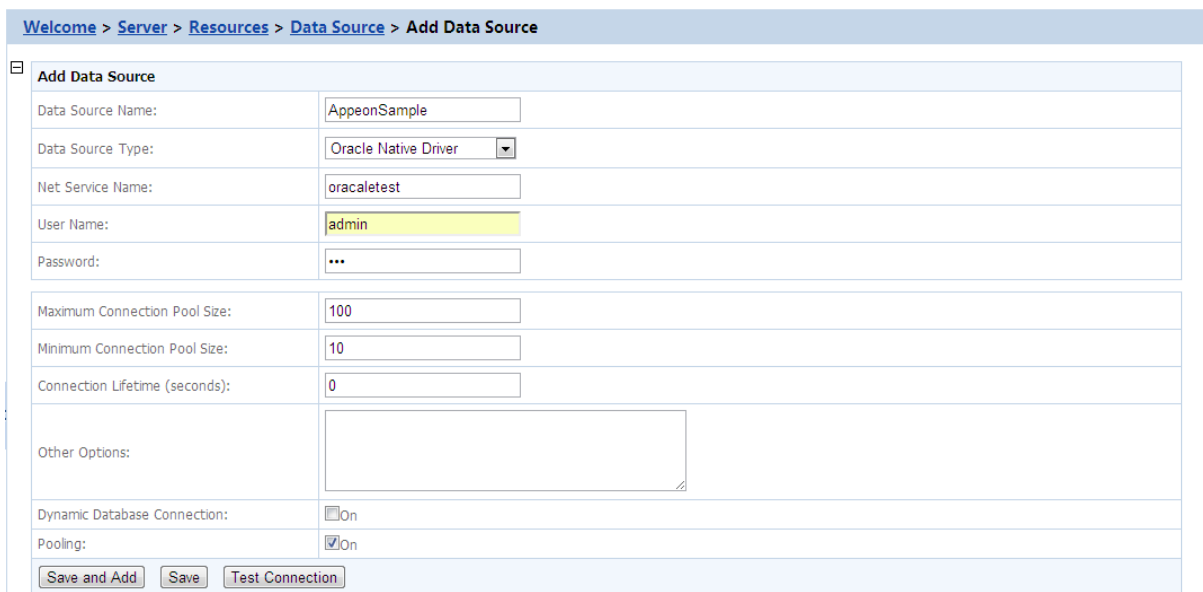
Figure 3.5: Settings for Oracle native driver

Table 3.4: Settings for Oracle native driver

Data Source Name	Type the name of the data source.
Data Source Type	Select "Oracle Native" to connect with Oracle databases.
NET Service Name	Select a service name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.

Note: if the database is an Oracle database and it resides in an NTFS folder, make sure the Windows "Network Service" or Everyone" user has full controls over that folder, otherwise, testing of the data source may fail.

3.4.4 Data source settings for SQL Server native driver

PowerServer supports using SQL Server native driver to connect with SQL Server databases.

Note

If you have difficulties in connecting with the SQL Server database, try with the solutions in this article.

Figure 3.6: Settings for SQL Server native driver

Table 3.5: Settings for SQL Server native driver

| Data Source Name	Type the name of the data source.
Data Source Type	Select "SQL Server Native" to connect with Microsoft SQL Server databases.
Database Host	Specify the machine name or IP address of the database server.
Database Port	Specify the port number of the database server.
Database Name	Specify the database name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.

3.4.5 Data source settings for Informix native driver

PowerServer supports using IBM Informix .NET Provider driver to connect with Informix databases. Before you start creating a data source with Informix .NET Provider driver, you must install Informix Client (SDK 2.90 or above) and then use the installed client to configure Informix Server. For detailed instructions, refer to the Informix documents.
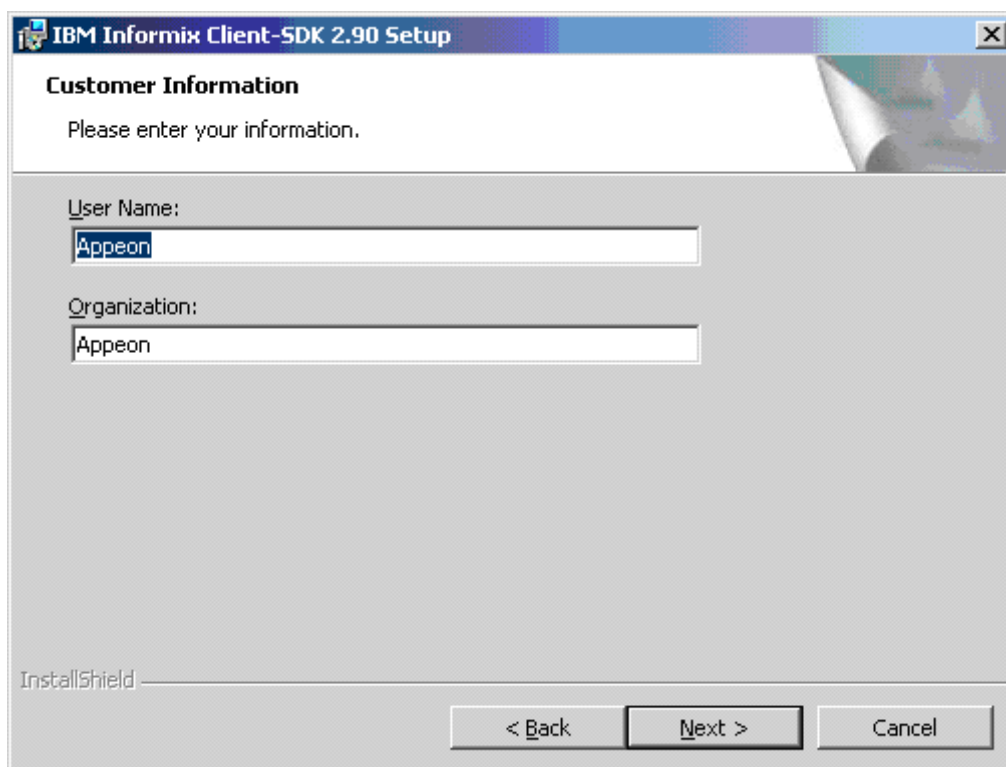
Following are important installation steps that are worth mentioning here:

1) Accept the license agreement and click **Next**.
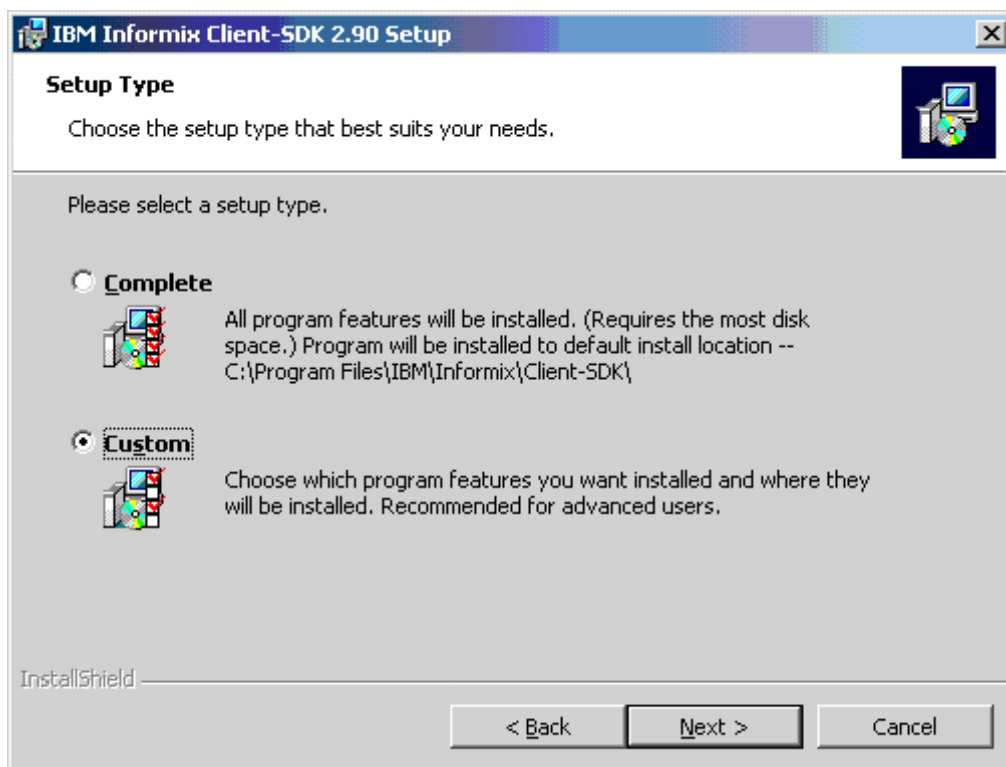
Figure 3.7: Accept the license agreement
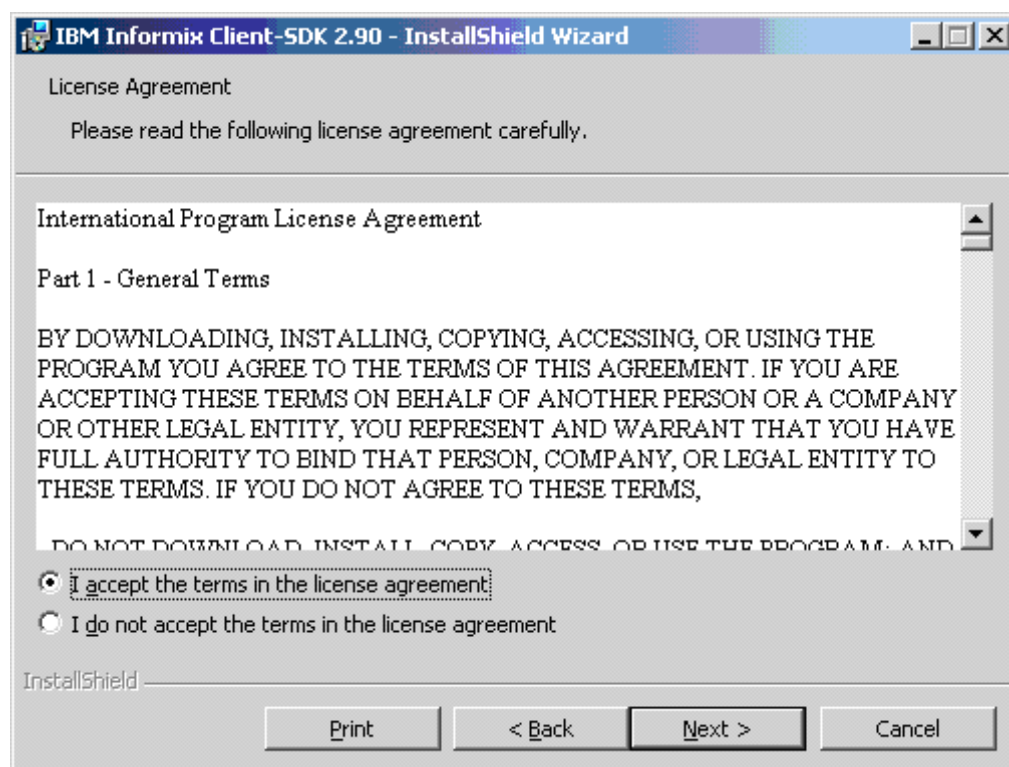
2) Input user name and organization name and click **Next**.

Figure 3.8: Enter customer information

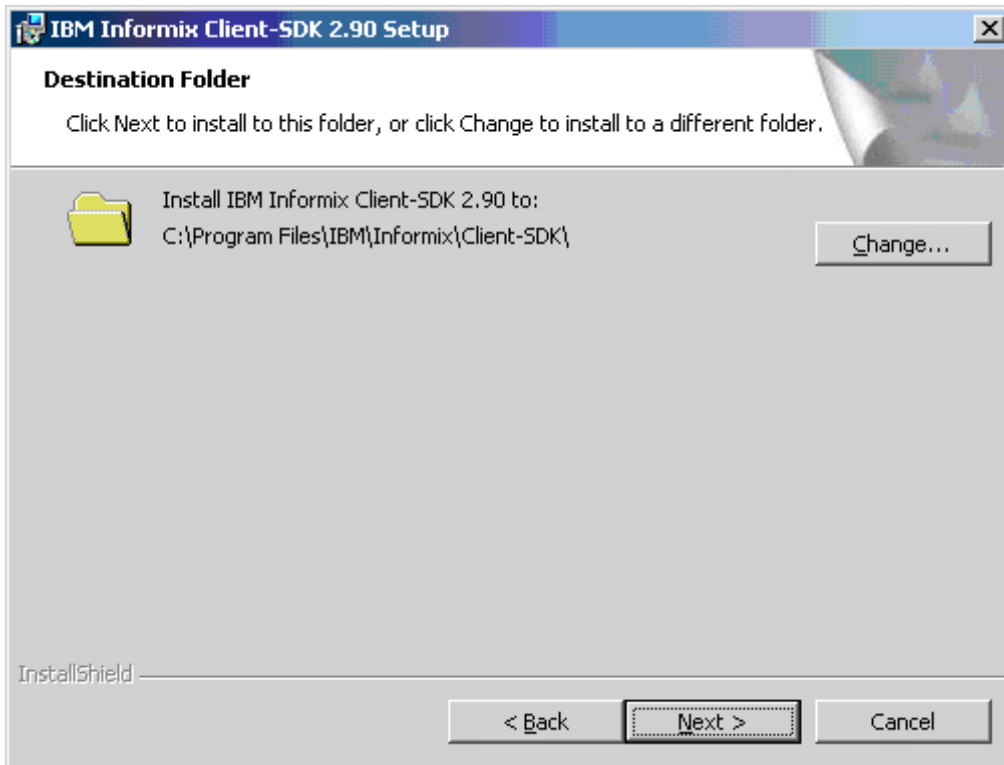
3) Select the **Custom** installation type and click **Next**.

Figure 3.9: Select Custom installation type

4) Select the installation directory for the driver and click **Next**.

Figure 3.10: Select the installation directory for the driver

5) (**VERY IMPORTANT**) Make sure that **IBM Informix .NET Provider** is selected to install and click **Next**.

Figure 3.11: Select "IBM Informix .NET Provider"
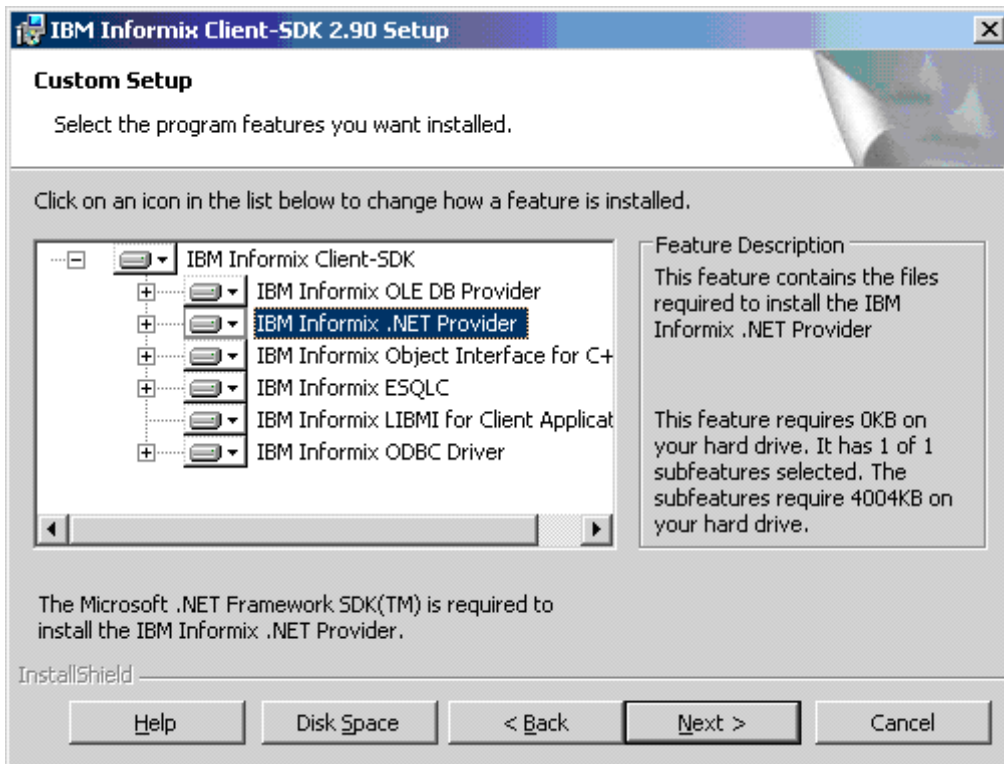
6) Click **Install** to start the installation.

Figure 3.12: Ready to install the program
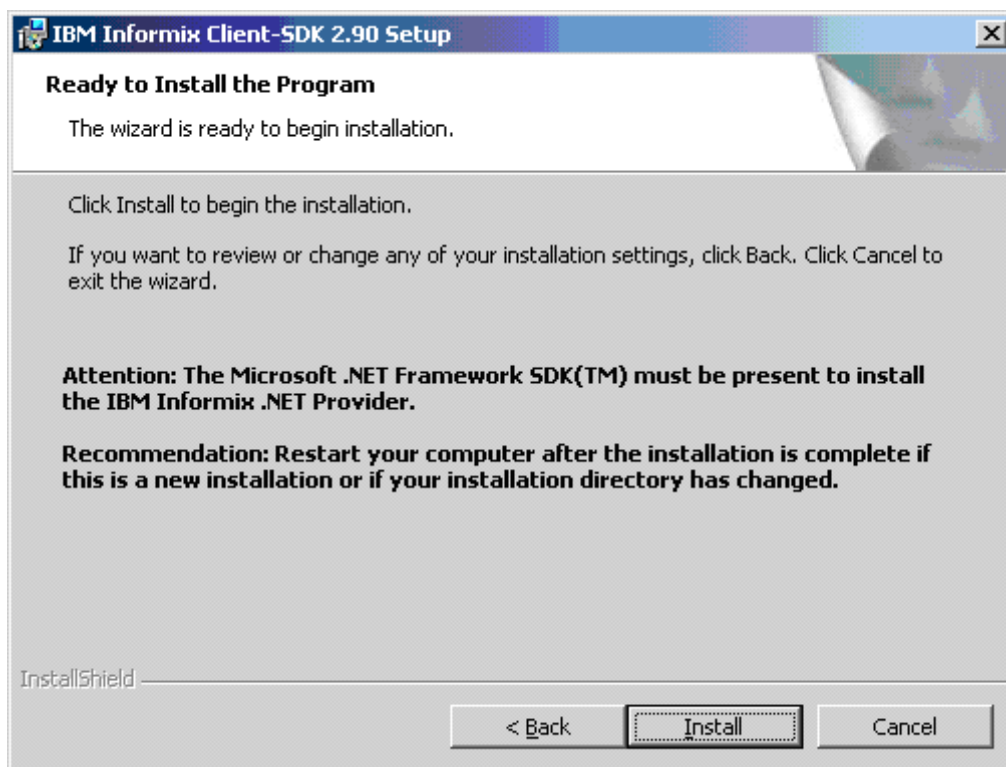
Following are important configuration steps that we think are worth mentioning:

1) Select **Start** > **Programs** > **IBM Informix Client-SDK 2.90** > **Setnet32**.

2) Configure the Informix server information, as shown in the following figure. Remember that the "IBM Informix Server" name will be used in AEM.

Figure 3.13: Configure the Informix server information
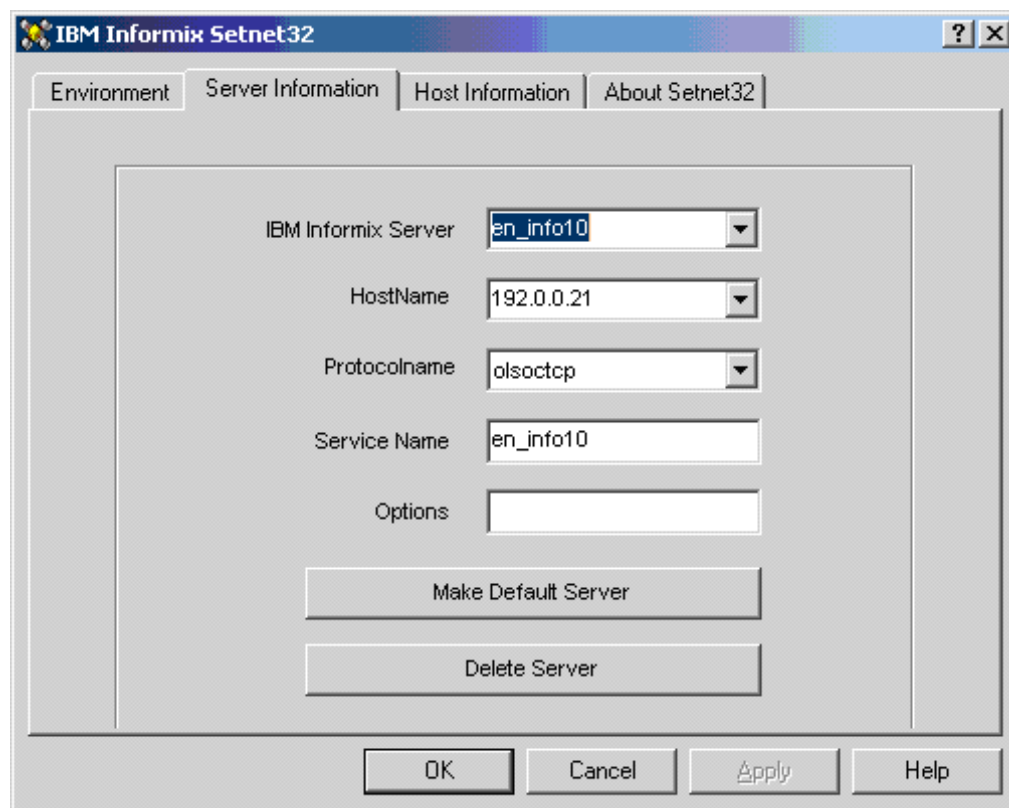
Note:

It is recommended that you test the connection with the specified server name in other programs such as PowerBuilder. You may need to manually add the following text to the %system32%/drivers/etc/Service file:

```
en_info10 1526/tcp #en_info10
```

en_info10 should be the name of IBM Informix Server you specified above; 1526 is the port number of Informix server; #en_info10 is the comment text.

Following are configurations in AEM:

Figure 3.14: Data source settings in AEM

Table 3.6: Data source settings in AEM

Data Source Name	Type the name of the data source.
Data Source Type	Select "IBM Informix Native Driver".
IBM Informix Server	Specify the Informix Server name. This must be the same name that is used to configure the Informix Server above.
Database Name	Specify the database name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.

3.4.6 Data source settings for MySQL native driver

PowerServer supports using MySQL native driver to connect with MySQL Server databases.

Figure 3.15: Settings for MySQL native driver

Table 3.7: Settings for MySQL native driver

Data Source Name	Type the name of the data source.
Data Source Type	Select "MySQL Native Driver" to connect with MySQL Server databases.
Database Host	Specify the machine name or IP address of the database server.
Database Port	Specify the port number of the database server.
Database Name	Specify the database name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.

3.4.7 Data source settings for ASE native driver

PowerServer supports using ASE native driver to connect with SAP ASE (15.x only) databases.

Figure 3.16: Settings for ASE native driver

Table 3.8: Settings for ASE native driver

Data Source Name	Type the name of the data source.
Data Source Type	Select "ASE Native Driver" to connect with SAP ASE 15.x databases.
Database Host	Specify the machine name or IP address of the database server.
Database Port	Specify the port number of the database server.
Database Name	Specify the database name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.

3.4.8 Data source settings for Teradata native driver

PowerServer supports using Teradata native driver to connect with Teradata databases. Before you start creating a data source with Teradata native driver, you must install Teradata .NET Data Provider 13.1 or later. For detailed instructions, refer to the Teradata documents.

Figure 3.17: Settings for Teradata driver

Table 3.9: Settings for Teradata driver

Data Source Name	Type the name of the data source.
Data Source Type	Select "Teradata Native Driver" to connect with Teradata databases.
Data Source	Type the name of the Teradata server, or equivalently the DBC Name or TDPID.
Database Port	Specify the TCP/IP port number that the .NET Data Provider for Teradata uses for connection to the Teradata Gateway. Default port number is 1025.
Database Name	Specify the database name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.
Character Set	Select the character set according to mapping characters bidirectionally from the client application and teradata databases.
Session Mode	Select the session mode according to the duration of the session. The session mode is used on a Teradata Database V2R2.0 or later system.

3.4.9 Data source settings for IBM DB2 native driver

PowerServer supports using IBM DB2 native driver to connect with IBM DB2 databases. Before you start creating a data source with IBM DB2 native driver, you must install IBM DB2 client (32-bit or 64-bit). For detailed instructions, refer to the IBM DB2 documents.

Figure 3.18: Settings for IBM DB2 native driver

Table 3.10: Settings for IBM DB2 native driver

Data Source Name	Type the name of the data source.
Data Source Type	Select "IBM DB2 Driver" to connect with IBM DB2 databases.
Database Host	Specify the machine name or IP address of the database server.
Database Port	Specify the port number of the database server.
Database Name	Specify the database name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.

3.4.10 Data source settings for PostgreSQL native driver

PowerServer supports using PostgreSQL native driver to connect with PostgreSQL databases.

Figure 3.19: Settings for PostgreSQL native driver

Table 3.11: Settings for PostgreSQL native driver

Data Source Name	Type the name of the data source.
Data Source Type	Select "PostgreSQL Native Driver" to connect with PostgreSQL databases.
Database Host	Specify the machine name or IP address of the database server.
Database Port	Specify the port number of the database server.
Database Name	Specify the database name.
User Name	Type the database login username. The username is set on the database server.
Password	Type the database login password. The password is set on the database server.

3.5 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 PowerServer Web or mobile application as the replacement of the transaction object in the PowerBuilder application.

Figure 3.20: Map transaction to data source
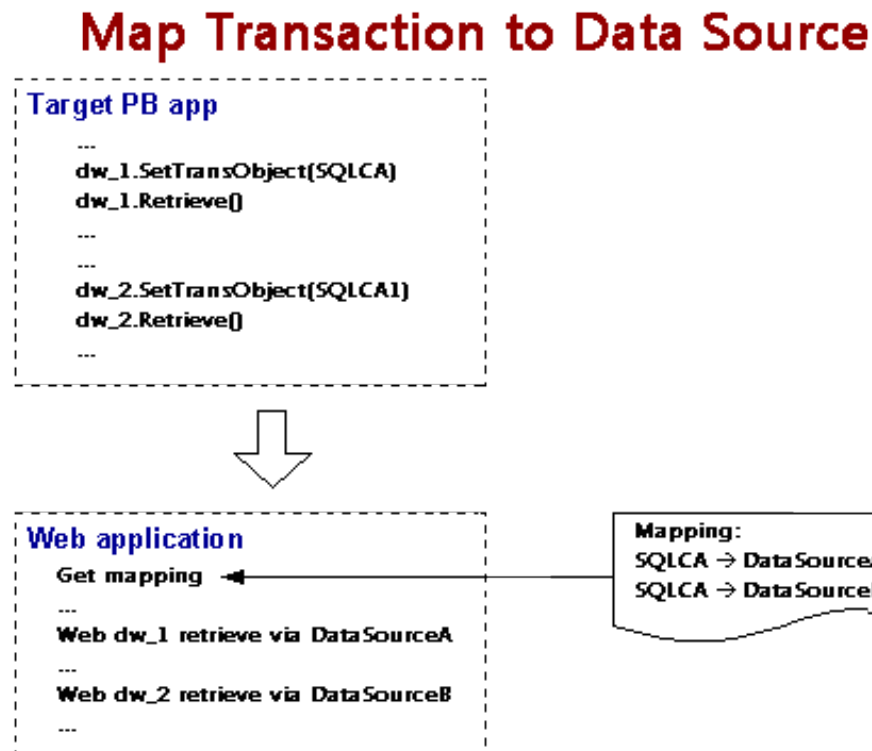
Once PowerServer data sources are configured, you can set up the transaction object to data source mapping in two different ways:

• 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.

3.5.1 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='ASADataSource1'"
```

"ASADataSource1" 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-ASA"
```

The value of the DBMS property should be set based on the database type; refer to the table below.

Table 3.12: 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 11g/12c	ODB-O10	JDB-O10	OLE-O10	O10
Oracle 18c/19c	-	-	-	ORA
SAP ASE	ODB-SYC	JDB-SYC	OLE-SYC	SYC
SAP SQL Anywhere	ODB-ASA	JDB-ASA	OLE-ASA	-
IBM DB2 UDB	ODB-DB2	JDB-DB2	OLE-DB2	DB2
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

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, PowerServer will regard the database type as SAP 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.

3.5.2 Static transaction object to data source mapping

For a PowerServer 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.

3.6 Advanced configurations related with database connection

3.6.1 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 PowerServer 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.

3.6.1.1 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.

PowerServer Web applications and PowerServer 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.

3.6.1.1.1 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.

3.6.1.2 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 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", "")
...
```

3.6.2 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 PowerServer system database. If the user name or password is not correct, the user is not allowed to access the PowerServer application.

For more information on using the Appeon security features for the PowerServer Web application or the PowerServer mobile application, refer to the [Server Security](#) section.

3.6.2.1 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 1.3.1, "AppeonExtFuncs Object" in *Workarounds & APIs Guide*.

3.6.2.2 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.

PowerServer Web applications and PowerServer 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.

3.6.2.2.1 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.

4 AEM User Guide

4.1 Introduction

4.1.1 Overview

AEM is a Web-based application that is automatically installed with PowerServer to manage the PowerServer and the PowerServer 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 the settings configured in AEM are saved as XML files in the %powerserver%\AEM \config folder, where %powerserver% stands for the PowerServer installation directory, for example, C:\Inetpub\wwwroot\appeon\AEM\config.

4.1.2 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 4.1: AEM Console

4.1.3 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.

4.2 Getting started

4.2.1 Running PowerServer

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

Since PowerServer is installed to the IIS server, starting IIS server will automatically start PowerServer. Open IIS Manager and verify that the Web site hosting PowerServer is running.

Figure 4.2: IIS Web site hosting PowerServer
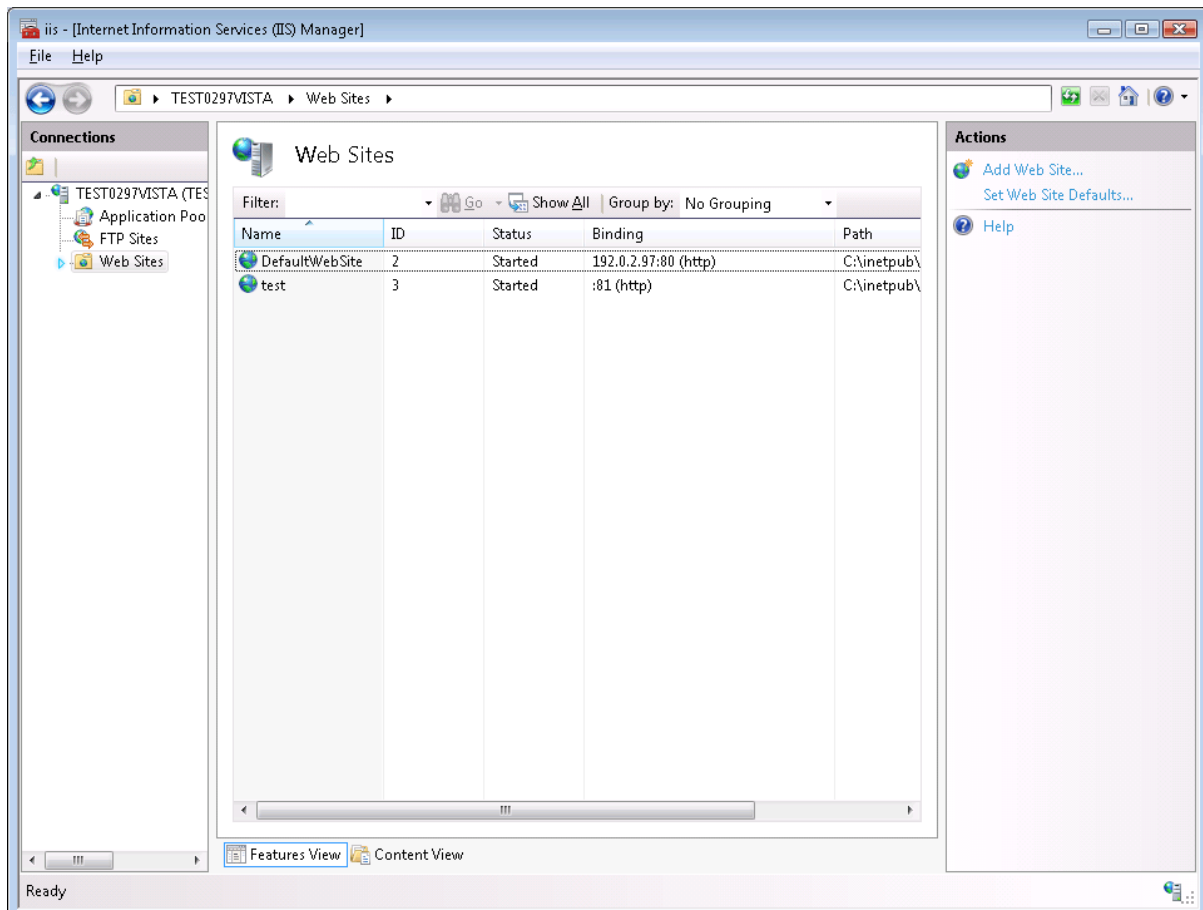
4.2.2 Starting AEM

4.2.2.1 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.

During installation, you can specify the name and port for PowerServer. If you want to start AEM from the computer that hosts the PowerServer, you can use the specified server name and port to access AEM, for example, http://localhost:80/AEM. However, you should not use a "localhost" listener in a production environment.

4.2.2.2 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.

4.2.2.3 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, it is recommended 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.

4.2.2.4 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 the "404 Not Found" error occurs, please use the same solution for the error Section 5.2.1, ""java.io.IOException: Cannot run program 'jar': ..." error" in *PowerServer Troubleshooting Guide*.

If you are a server administrator, it is highly recommended that you read through Chapter 2, *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 4.3: AEM login

4.2.2.5 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 4.4: Language settings
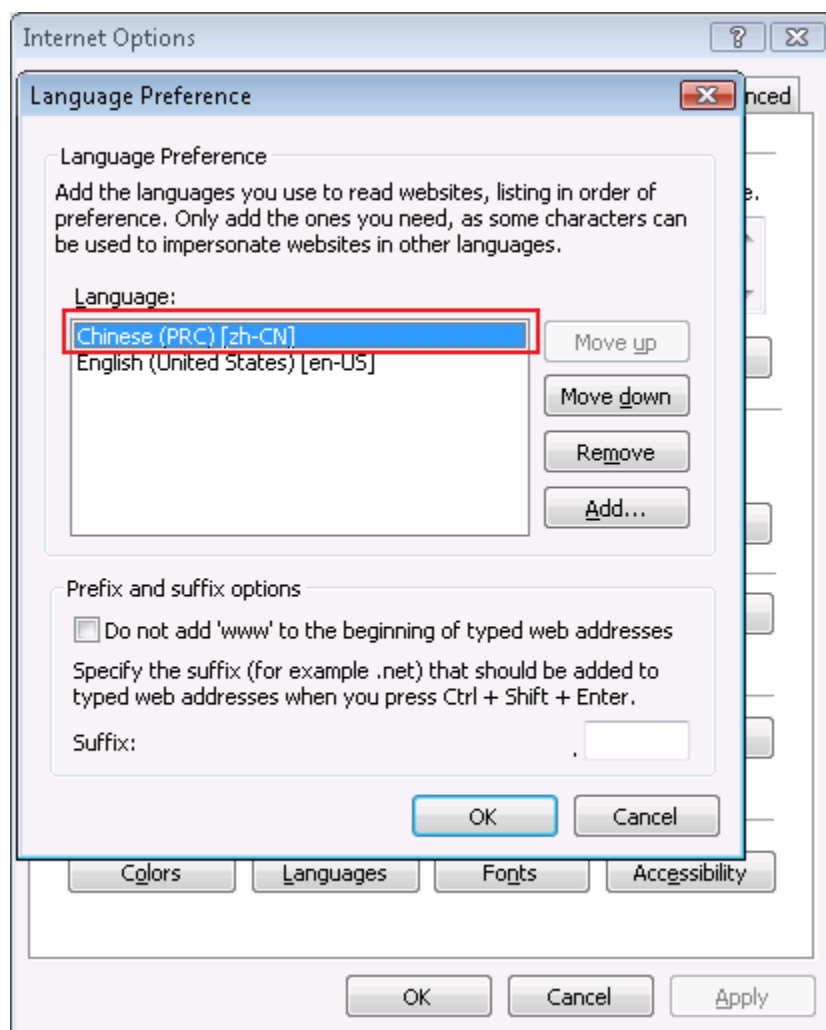
4.2.3 AEM Help

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

Figure 4.5: Help button

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

Figure 4.6: PowerServer Help
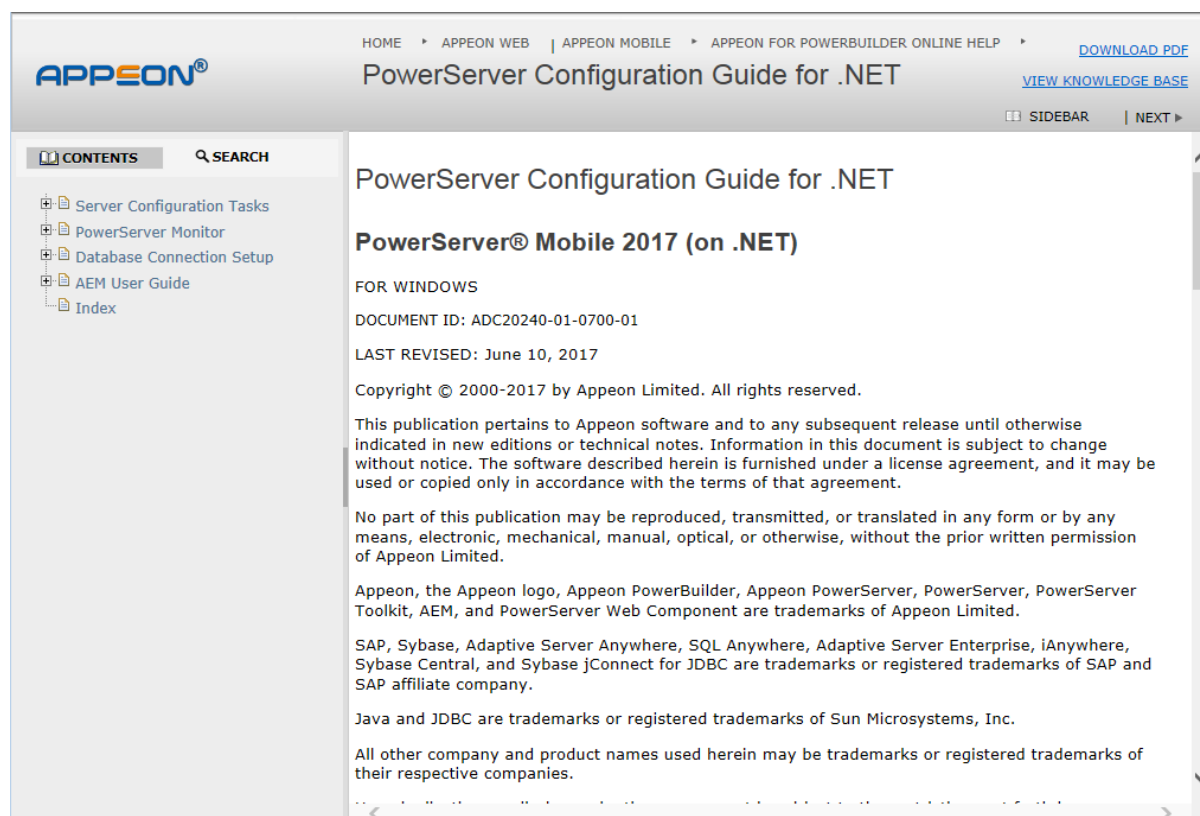
4.3 Server

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

Figure 4.7: Server
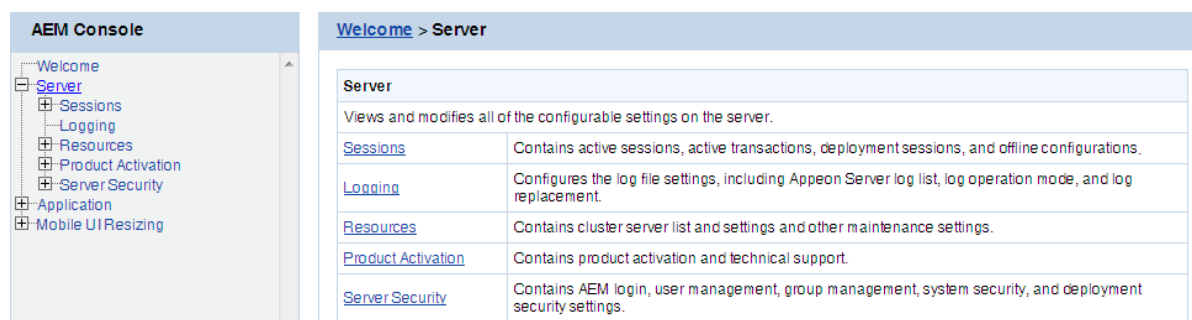
4.3.1 Sessions

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 4.8: Sessions

4.3.1.1 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 4.9: Active Sessions

4.3.1.1.1 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.

4.3.1.1.2 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.

4.3.1.2 Active Transactions

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

Figure 4.10: Active Transactions
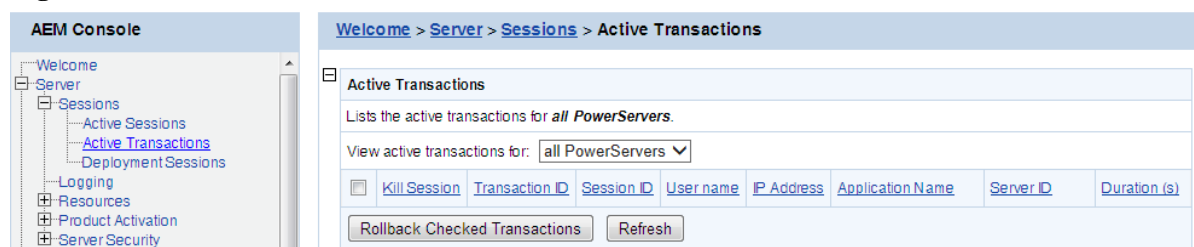
4.3.1.2.1 Viewing active transactions

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.

4.3.1.2.2 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.

4.3.1.3 Deployment Sessions

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

Figure 4.11: Deployment Sessions
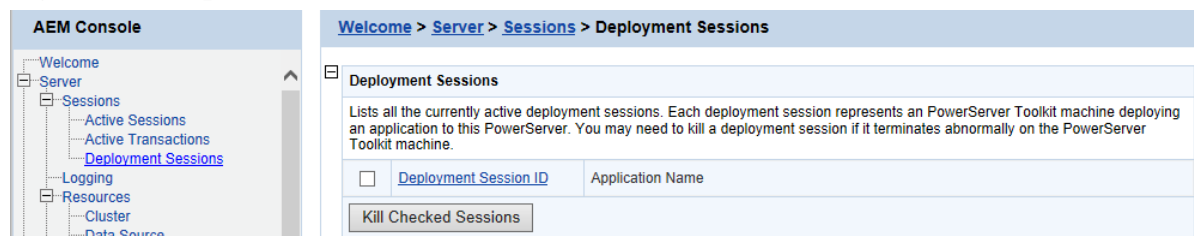
An active deployment session automatically starts and displays in the Deployment Sessions table when PowerServer Toolkit starts to upload the embedded SQL statements, DataWindow SQLs, and INI files of an application to PowerServer. It ends and disappears automatically from the table when the upload process 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.

4.3.2 Logging

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

Figure 4.12: Logging

4.3.2.1 Viewing logs

PowerServer creates three different log files for troubleshooting usage. The viewer provides the direct access to all the three log files. You could also find the log files in the directory %powerserver%\AEM\Log.

PowerServer logs include the following log files:

• Server Log: Records messages logged from services and the core PowerServer runtime.

• Error Log: Records errors occurred on PowerServer.

• Deployment Log: Records interactions between PowerServer and PowerServer Toolkit during application deployments.

The PowerServer Logs 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 4.13: Deployment Log
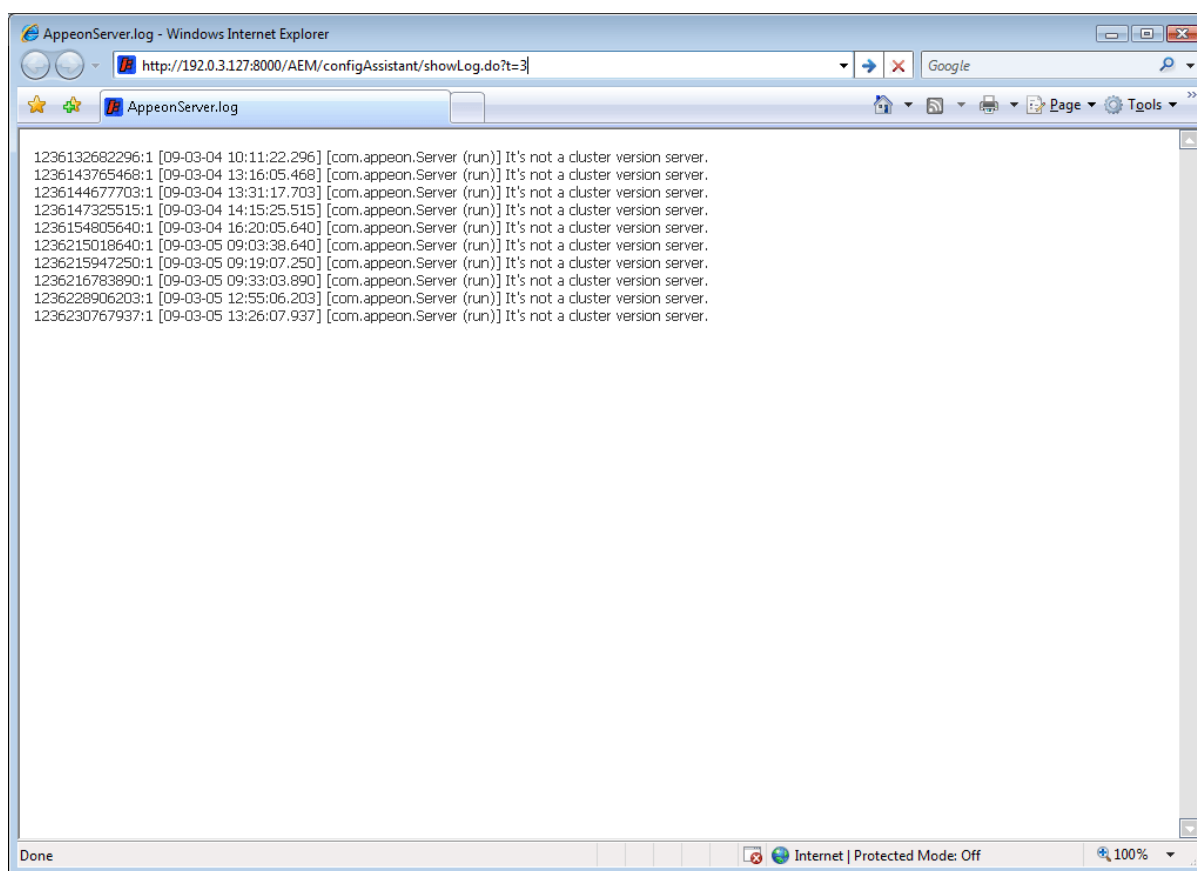
- To download a log file

  Click **Download** and then click **Save** in the dialog box that appears.

- To clear a log file

  Click **Clear** to remove the contents in the PowerServer log files.

4.3.2.2 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.

4.3.2.3 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.

4.3.3 Resources

Resources is a set of tools for viewing and configuring server cluster, data sources, temporary files and configuration backups. There are three tools: Cluster, Data Source, and Maintenance.

Figure 4.14: Resources
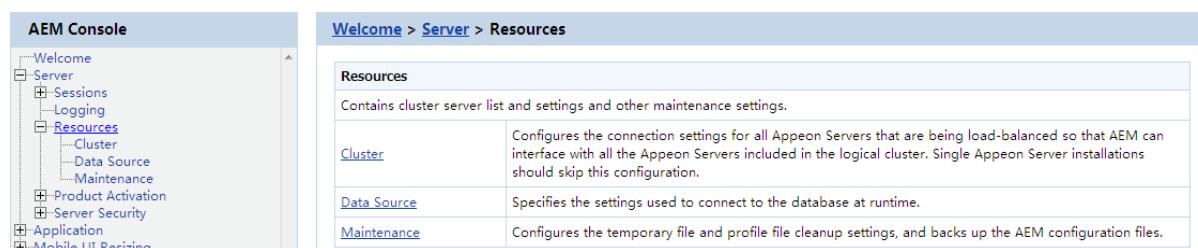
4.3.3.1 Cluster

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 5, *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 4.15: Cluster
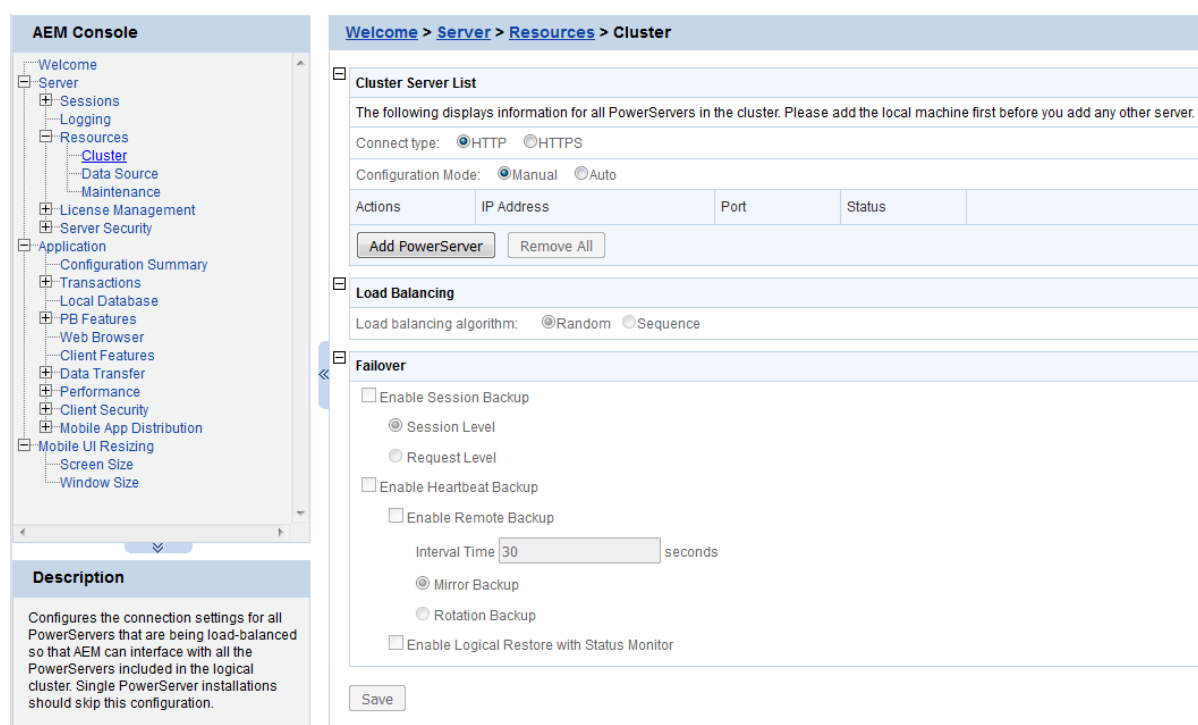
4.3.3.1.1 Cluster Server List

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 PowerServer Application Deployment Wizard to perform the application deployment. For detailed instructions, refer to the Chapter 5, *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 connect type (HTTP or HTTPS) for the PowerServer cluster.

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

Step 2: If using the Amazon Web Service cloud server, select the configuration mode for auto scaling.

- Manual - does not support auto scaling (so the developer needs to manually update the PowerServer list in the cluster).

- Auto - supports auto scaling by automatically detecting PowerServers and updating the PowerServer list in the cluster.

For more about configuration for auto scaling in Amazon Web Service, see Section 5.4.4, "Special instructions for Auto Scaling in Amazon Web Service" in *PowerServer Mobile Tutorials*.

Step 3: Click the **Add PowerServer** button in the **Cluster Server List** table. The Add PowerServer page opens.

Figure 4.16: Add PowerServer

Step 4: 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 5: 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.

4.3.3.1.2 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.

4.3.3.1.3 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.

4.3.3.1.4 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.

4.3.3.2 Data Source

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

Figure 4.17: Data source
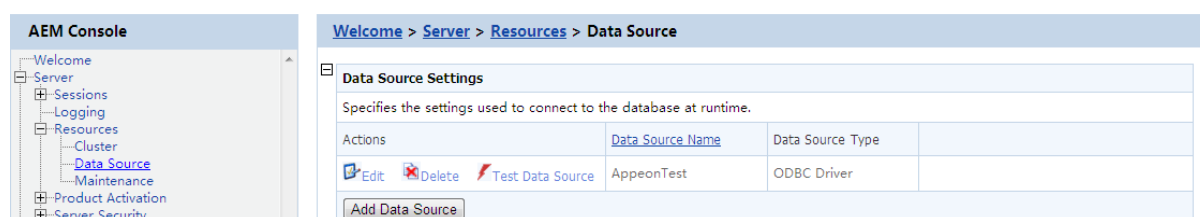
4.3.3.2.1 Adding a data source

Click **Add Data Source** below the data source list and specify the data source settings according to the following table.

Figure 4.18: Add data source

Data source properties vary with different database types. For detailed description for each database type, refer to the Setting up PowerServer data sources.

Table 4.1: Data Source Properties

Data Source Name	Type the name of the data source.
Data Source Type	Select the data source type. The data source options will change according to the selected data source type. • Use "ODBC Driver" to connect with SAP SQL Anywhere 8.x/9.x/10.0.1 and SAP ASE databases; • Use "Oracle Native Driver" to connect with Oracle databases; • Use "MS SQL Server Native Driver" to connect with Microsoft SQL Server databases; • Use "IBM Informix Native Driver" to connect with IBM Informix databases; • Use "SQL Anywhere Native Driver" to connect with SAP SQL Anywhere 11.0/12.0/16.0/Web databases;

	• Use "SQL Anywhere 17 Native Driver" to connect with SAP SQL Anywhere 17.0 databases;
	• Use "Teradata Native Driver" to connect with Teradata databases;
	• Use "MySQL Native Driver" to connect with MySQL databases;
	• Use "ASE Native Driver" to connect with SAP ASE (15.x only) databases;
	• Use "PostgreSQL Native Driver" to connect with PostgreSQL databases;
	• Use "IBM DB2 Driver" to connect with IBM DB2 databases.
ODBC Data Source	Select a system DSN. PowerServer supports system DSN only, so only system DSN will be listed here. This option becomes visible when you select **ODBC Driver** or **SQL Anywhere Native Driver** from the **Data Source Type** drop-down list.
NET Service Name	Select a service name. This option becomes visible when you select **Oracle Native Driver** from the **Data Source Type** drop-down list.
IBM Informix Server	Specify the machine name or IP address of the Informix database server. This option becomes visible when you select **IBM Informix Native Driver** from the **Data Source Type** drop-down list.
Database Host	Specify the machine name or IP address of the database server. This option becomes visible when you select **MS SQL Server Native Driver**, **Teradata Native Driver**, **MySQL Native Driver**, **ASE Native Driver**, **PostgreSQL Native Driver**, or **IBM DB2 Driver** from the **Data Source Type** drop-down list.
Database Port	Specify the port number of the database server. This option becomes visible when you select **MS SQL Server Native Driver**, **Teradata Native Driver**, **MySQL Native Driver**, **ASE Native Driver**, **PostgreSQL Native Driver**, or **IBM DB2 Driver** from the **Data Source Type** drop-down list.
Database Name	Specify the database name. This option becomes visible when you select **MS SQL Server Native Driver**, **IBM Informix Native Driver**, **Teradata Native Driver**, **MySQL Native Driver**, **ASE Native Driver**, **PostgreSQL Native Driver**, or **IBM DB2 Driver** from the **Data Source Type** drop-down list.
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.
Character Set	Select the character set according to mapping characters bidirectionally from the client application and Teradata databases.
	This option becomes visible when you select **Teradata Native Driver** from the **Data Source Type** drop-down list.
Session Mode	Select the session mode according to the duration of the session. The session mode is used on a Teradata Database V2R2.0 or later system.
	This option becomes visible when you select **Teradata Native Driver** from the **Data Source Type** drop-down list.
Maximum Connection Pool Size	Specify the maximum number of connections PowerServer opens and pools on startup.
Minimum Connection Pool Size	Specify the minimum number of connections PowerServer opens and pools on startup.
Connection Timeout	Specify the timeout period (in seconds) for the connection.
Command Timeout	Specify the timeout period (in seconds) for the commands.
Connection Lifetime	Specify the lifetime period (in seconds) for the pooled connection.
	To be specific, you can specify the timeout period from the time a connection is created to the time when the connection returns to the pool. If the actual lifetime of a connection exceeds that specified in Connection Lifetime, the connection will be terminated. It is recommended to be used in cluster configuration when forcing the load balancing between a running server and a server just brought online.
	If the value is set to 0, the pooled connection allows the maximum connection timeout.
Other Options	Currently, this setting is effective to SQL Anywhere databases only.
	Specify the connection_authentication property for SQL Anywhere databases.
	The value should be in this format: "authentic_code=###" where "authentic_code" is the key word, text after "=" should be the authorization code.
	PowerServer will automatically set the connection_authentication property when connecting with the SQL Anywhere database.
Dynamic Database Connection	Select whether to enable dynamic database connection.
	When it is on, the LogID and LogPass of the Transaction object will be used to connect to the database; when it is off, the user name and password specified in the data source will be used to connect to the database.

Pooling	Select whether to use the connection pool. This option must be turned on, if **Dynamic Database Connection** is on.
	When setting to "true", the connection with database does not release; when setting to "false", the connection with database fully releases.
	This setting is supported in all the driving types except for ODBC driver.
Extended Options	Specify the connection parameters that are not listed above. The value should be in this format: "parameter_name=###" where "parameter_name" is the name of the connection parameter, for example, TextSize=64000, this sets the maximum size of text or binary data sent or received from ASE to 64 KB. If there are more than one parameter, separate them by semicolon (";").
	Appeon PowerServer provides the ability to specify more connection parameters than those listed above, however, different database types require different connection parameters, and the use of parameters may also depend on the environment, therefore, PowerServer cannot guarantee every single parameter specified here would work as expected and thus would highly recommend you test them out thoroughly before adding any parameter into the production use.
Remark	Specify the comment or description (if any) for the data source.
	This option becomes visible if PowerServer is installed on the .NET IIS server.

4.3.3.2.2 Editing a data source

Click **Edit** and change the settings on the **Edit Data Source** page. The settings are specified the same way as on the **Add Data Source** page.

Figure 4.19: Edit data source

4.3.3.2.3 Deleting a data source

Click **Delete** and you will be prompted whether to delete the specified data source. Click **OK** to proceed.

4.3.3.2.4 Testing a data source

Click **Test Data Source** to test if the specified data source is successful. If the data source fails, click **Edit** to modify the settings until it succeeds.

4.3.3.3 Maintenance

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

Figure 4.20: Maintenance
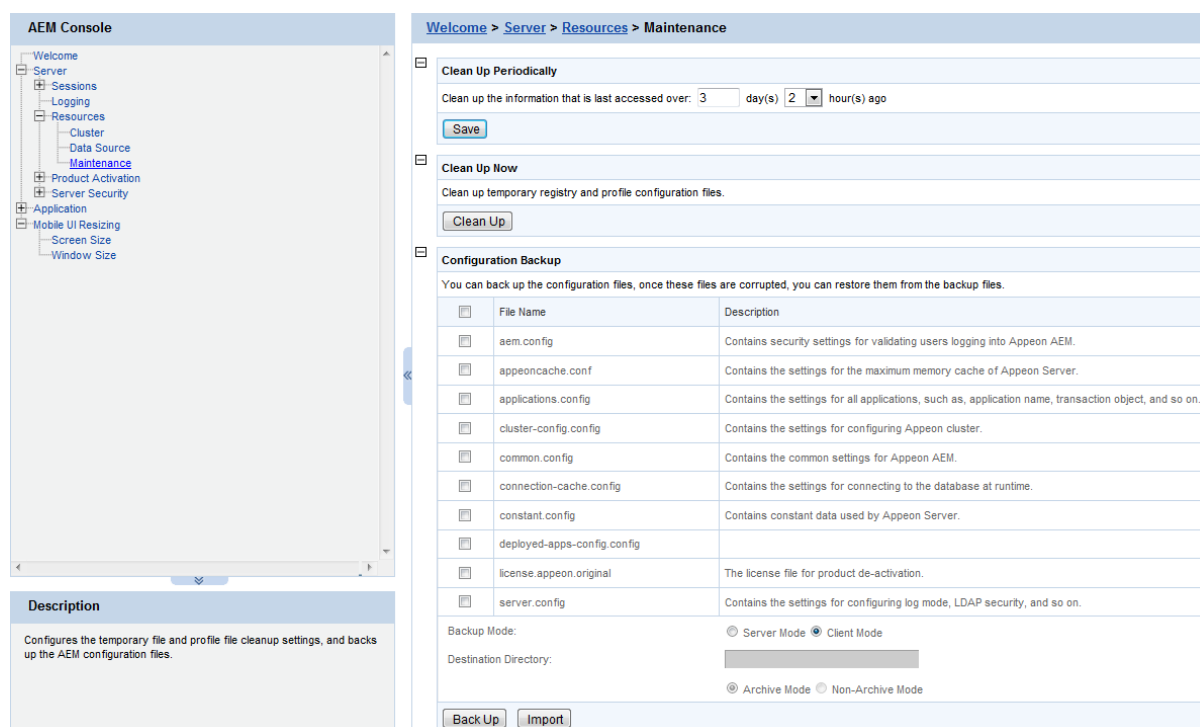
4.3.3.3.1 Auto cleanup

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 all temporary register and profile configuration files that were accessed over 2 days and 4 hours ago will be cleaned up everyday.

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

4.3.3.3.2 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, click the **Clean Up** button in the "Clean Up Now" group box to commit the cleanup.

The temporary registry and profile configuration files will be deleted immediately from all the PowerServer that are configured in the Cluster tool.

4.3.3.3.3 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.

4.3.4 Product Activation

Product Activation is a set of tools for viewing product license information and activating products. There are two tools: Licensing and Support.
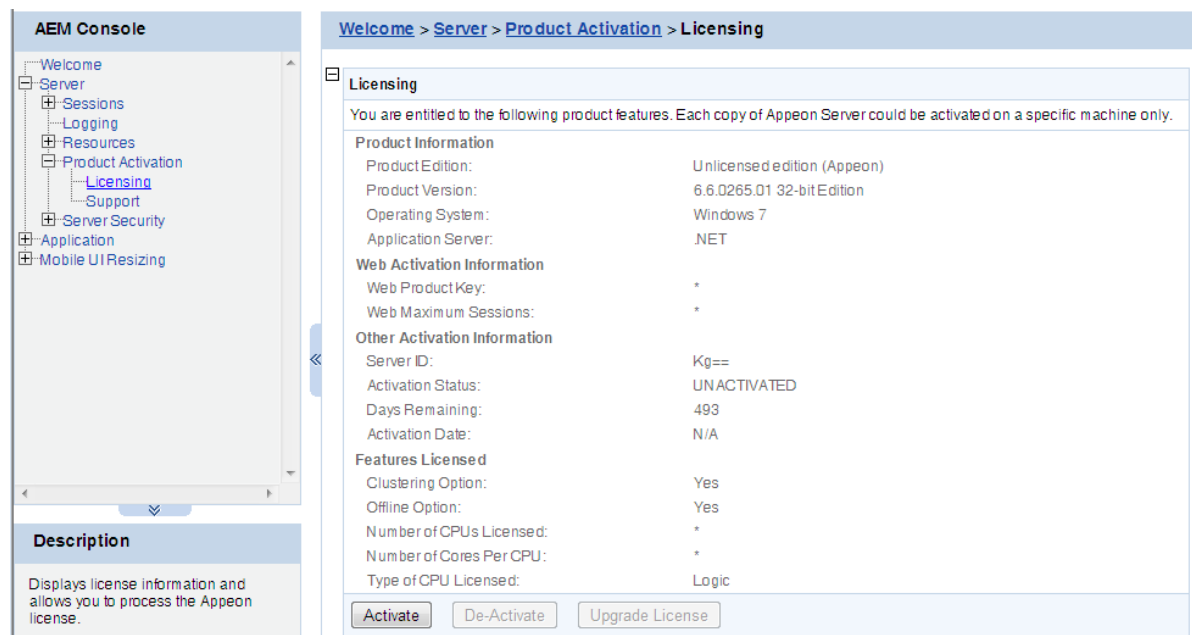
Figure 4.21: Product Activation

4.3.4.1 Licensing

The Licensing tool enables you to view the detailed license information, activate or de-activate a PowerServer, and update the license.
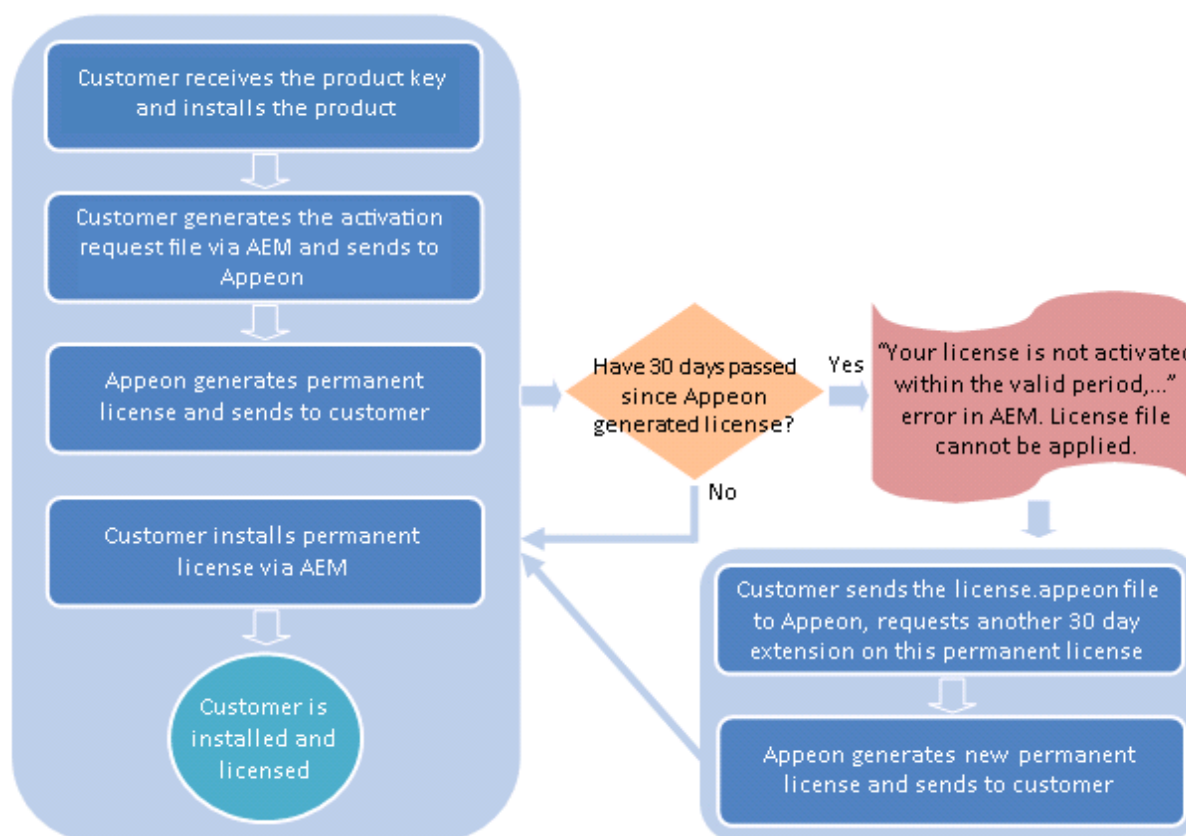
Figure 4.22: Licensing

4.3.4.1.1 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 4.23: 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 PowerServer mobile app will need to get the device ID when running on the mobile device, so that the app as well as other PowerServer 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 PowerServer 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 4.2.3.1, "Task 3.1: Set 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 4.24: 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 PowerServer and an activated permanent license (license.appeon) will be sent to you later.

Figure 4.25: 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 4.26: 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 4.27: Apply license

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

Figure 4.28: Licensing

Licensing

You are entitled to the following product features. Each copy of Appeon Server could be activated on a specific machine only.

Product Information

Product Edition:	DEVELOPER (Appeon)
Product Version:	6.6.0077.00 32-bit Edition
Operating System:	Windows 7
Application Server:	.NET

Mobile Activation Information

Mobile Product Key:	*
Maximum Mobile Devices:	10

Other Activation Information

Server ID:	MCNGMC00RC1BMi0yQS0wQi1GOXwwMC01MC01Ni1DMC0wMC0wMXwwMC01MC01Ni1DMC0wMC0wOA==
Activation Status:	ACTIVATED
Days Remaining:	*
Activation Date:	12/01/2012

Features Licensed

Clustering Option:	No
Offline Option:	Yes
Number of CPUs Licensed:	1
Number of Cores Per CPU:	*
Type of CPU Licensed:	Physics

[Activate] [De-Activate] [Upgrade License]

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 4.29: Users area
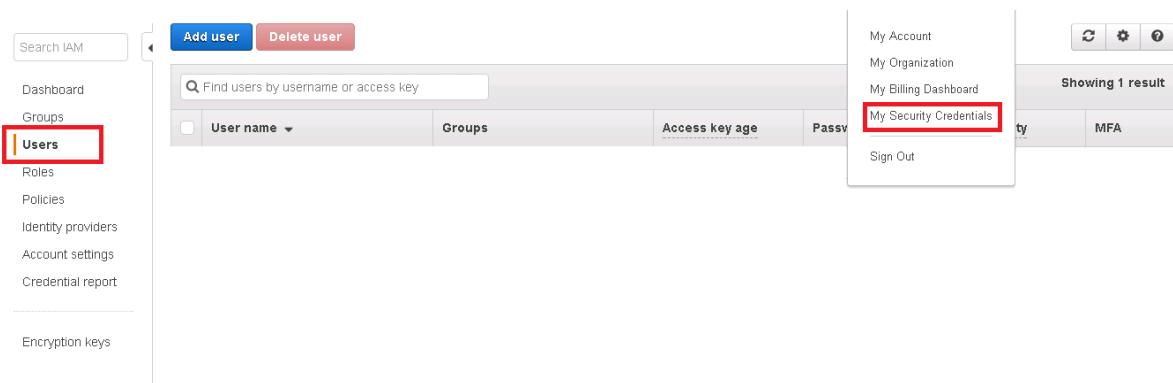
When you add a new user, be sure to select the **Programmatic access** type, and assign the user to the group with **AmazonEC2ReadOnlyAccess** permissions.
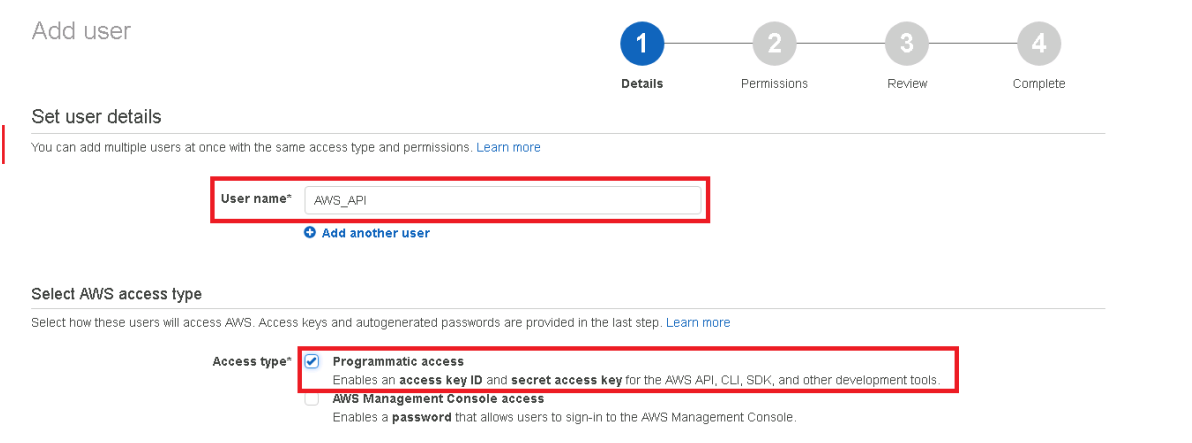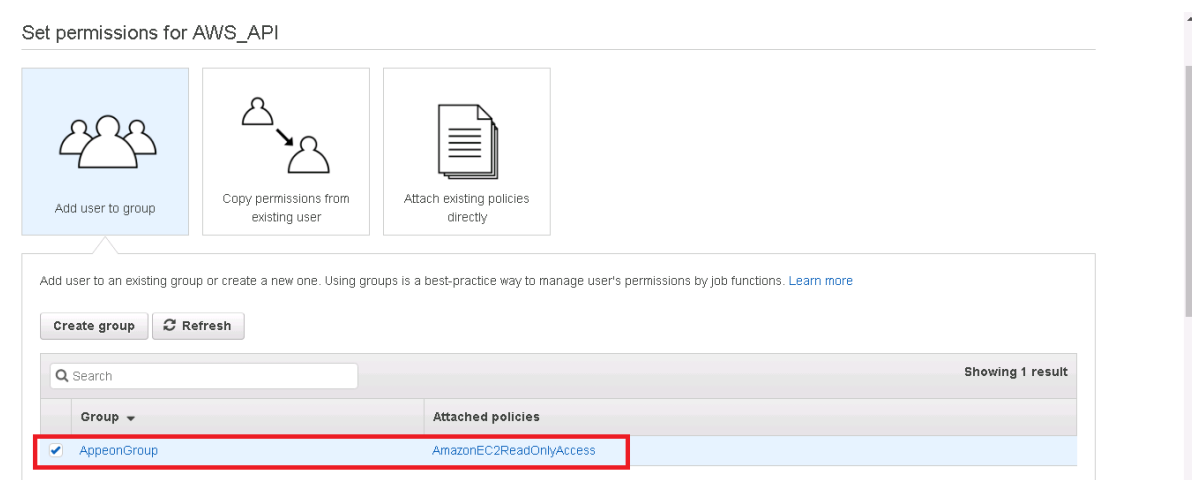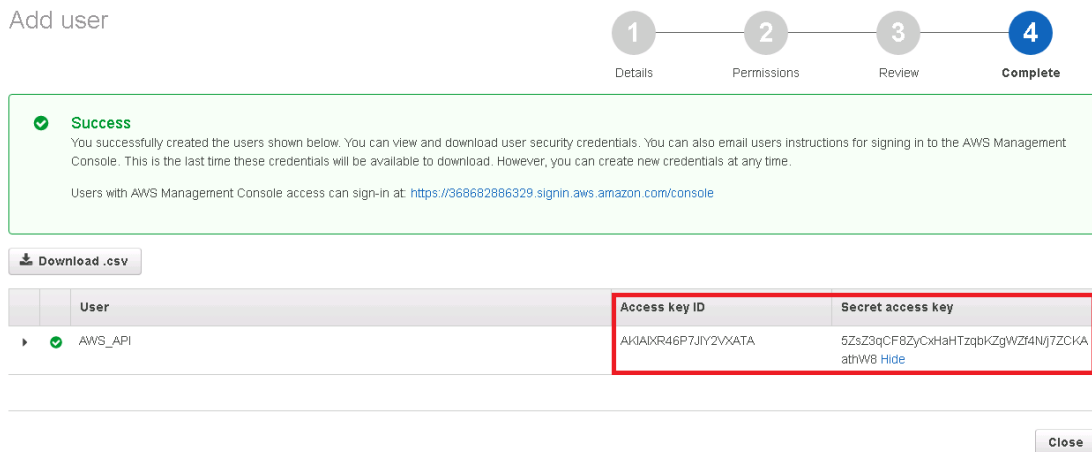
Figure 4.30: Access type

Figure 4.31: User group

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

Figure 4.32: 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 4.33: Environment name**
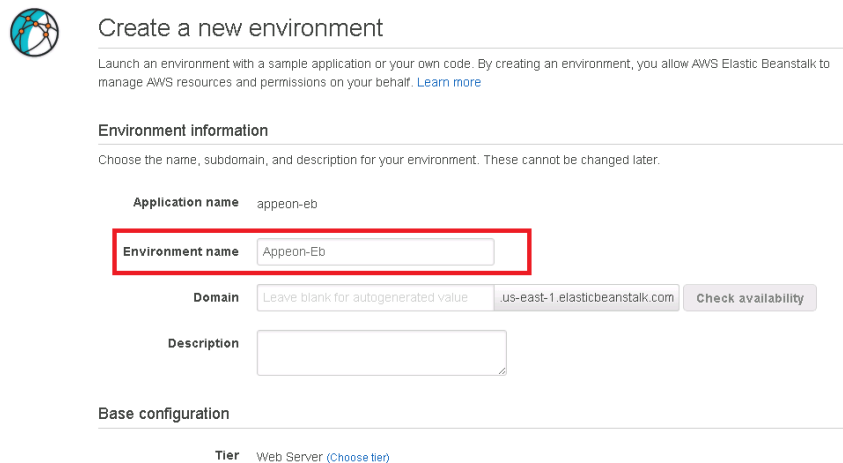
When creating an instance of **Amazon Elastic Compute Cloud(EC2)**, the key pair must start with the keyword prefix specified for the PowerServer license activation. For example, "appeon" is the keyword prefix.

Figure 4.34: Key pair
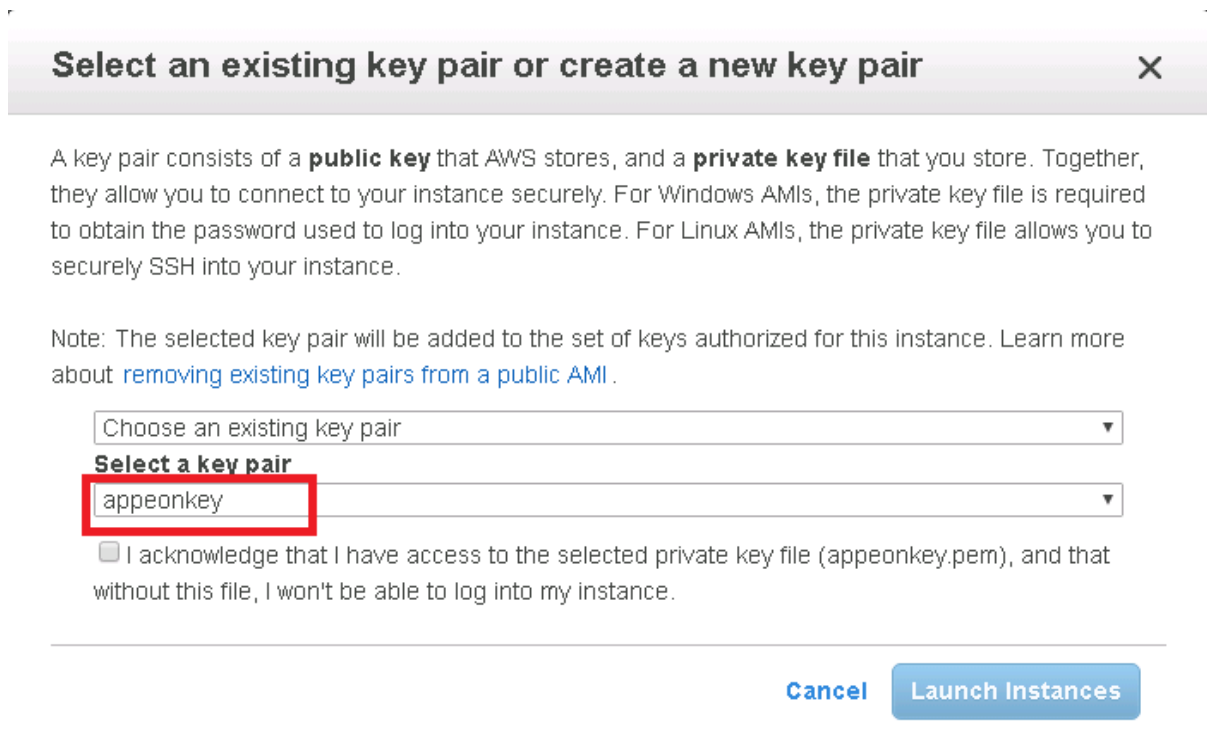
After you create an instance (either **Elastic Beanstalk(EB)** or **Amazon Elastic Compute Cloud(EC2)**), you can modify the instance name. Make sure the prefix of the instance name matches with the keyword prefix specified for the PowerServer license activation.

Figure 4.35: Instance name
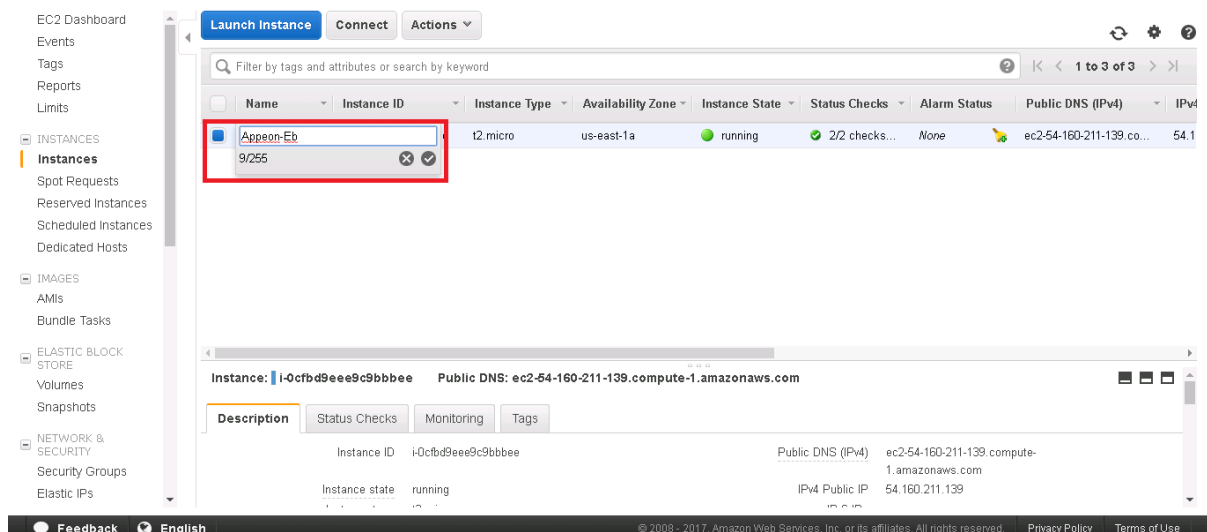
- **Numbers of Services**: The maximum number of service instances allowed for deploying PowerServer under the current AWS account. Simply specify a number in the AEM page.

4.3.4.1.2 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 4.36: License deactivation

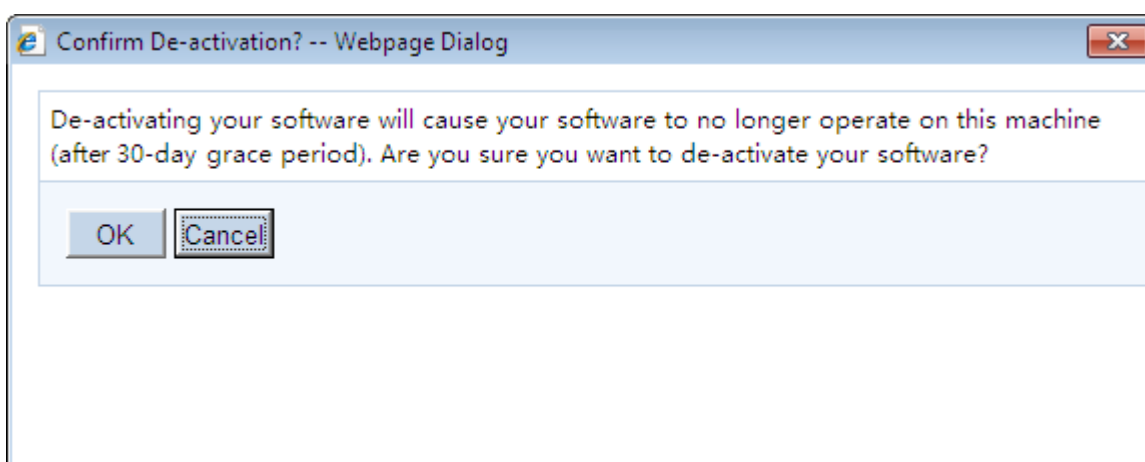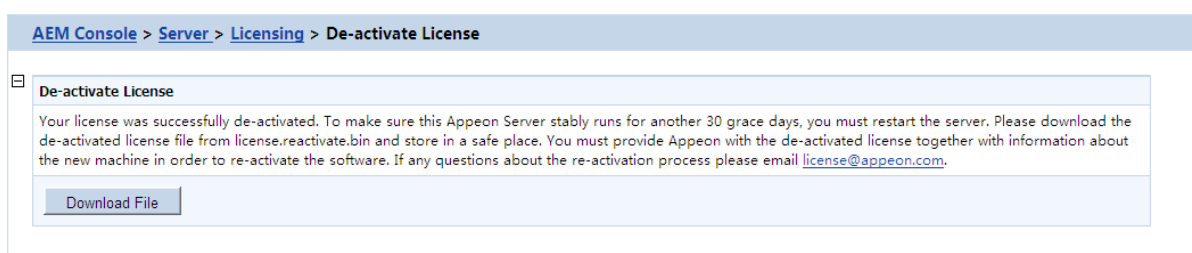| Licensing	
You are entitled to the following product features. Each copy of Appeon Server could be activated on a specific machine only.	
Product Information	
Product Edition:	DEVELOPER (Appeon)
Product Version:	6.6.0077.00 32-bit Edition
Operating System:	Windows 7
Application Server:	.NET
Mobile Activation Information	
Mobile Product Key:	*
Maximum Mobile Devices:	10
Other Activation Information	
Server ID:	MCNGMC00RC1BMi0yQS0wQi1GOXwwMC01MC01Ni1DMC0wMC0wMXwwMC01MC01Ni1DMC0wMC0wOA==
Activation Status:	ACTIVATED
Days Remaining:	*
Activation Date:	12/01/2012
Features Licensed	
Clustering Option:	No
Offline Option:	Yes
Number of CPUs Licensed:	1
Number of Cores Per CPU:	*
Type of CPU Licensed:	Physics

[Activate] [De-Activate] [Upgrade License]

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 4.37: Product De-activate
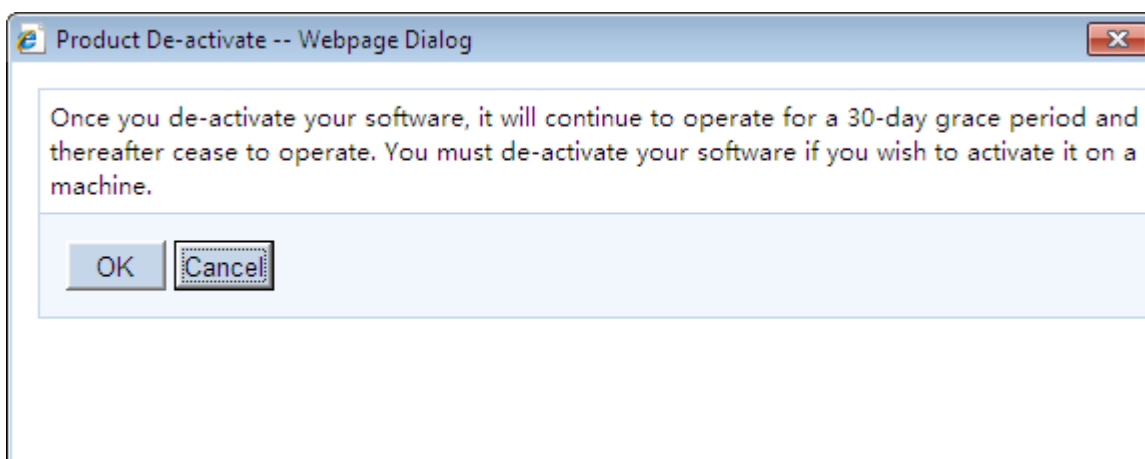
Figure 4.38: Confirm De-activation

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

Figure 4.39: 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.

PowerServer 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.

4.3.4.1.3 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 4.40: 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 PowerServer and an upgraded license will be sent to you later.

Figure 4.41: 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 4.42: Apply license
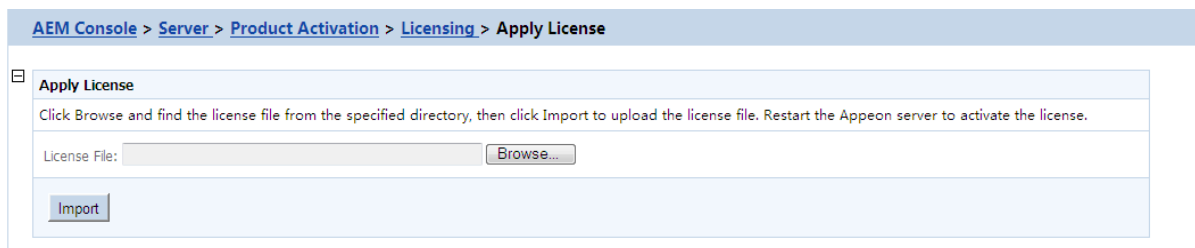
Step 7: After you restart PowerServer, go back to the **Licensing** page, and verify that the license information is updated, and the **Activation Status** is shown as **Activated**.

4.3.4.2 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 4.43: Support

4.3.4.2.1 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 4.44: 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 PowerServer and a new license with extended support period will be sent to you later.
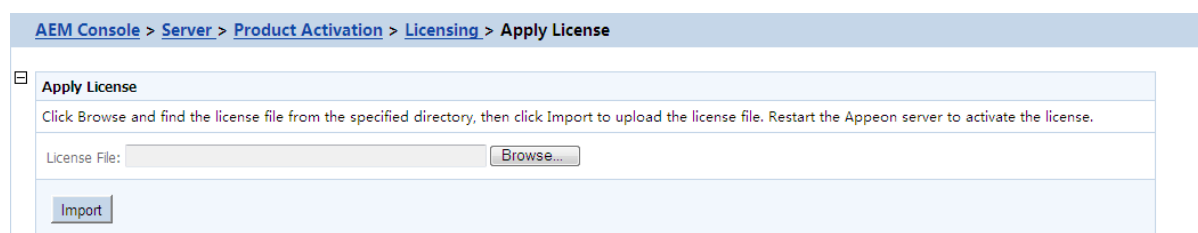
Figure 4.45: Generate renew request
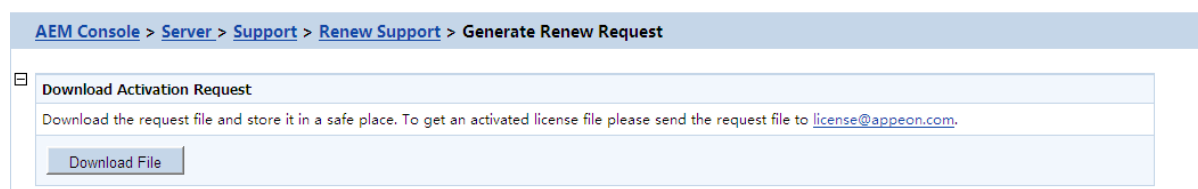
Step 3 - When you get the new license named license.appeon, click the **Apply License** button.

Figure 4.46: Product support
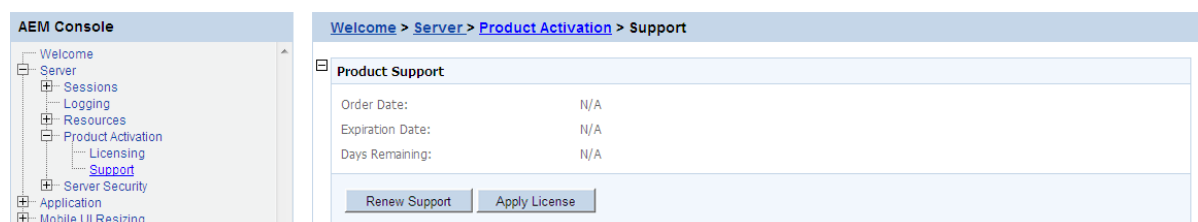
Step 4 - In the **Apply License** window, click the **Browse...** button to select the license.appeon file delivered by Appeon. Click the **Import** button to import your license file.

Figure 4.47: 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.

4.3.5 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 PowerServer Web application or the PowerServer 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 4.48: Server Security
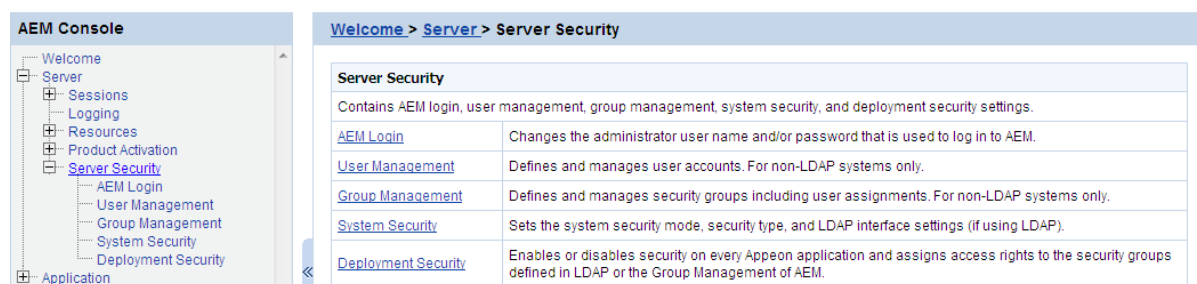
4.3.5.1 AEM login

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

Figure 4.49: AEM Login
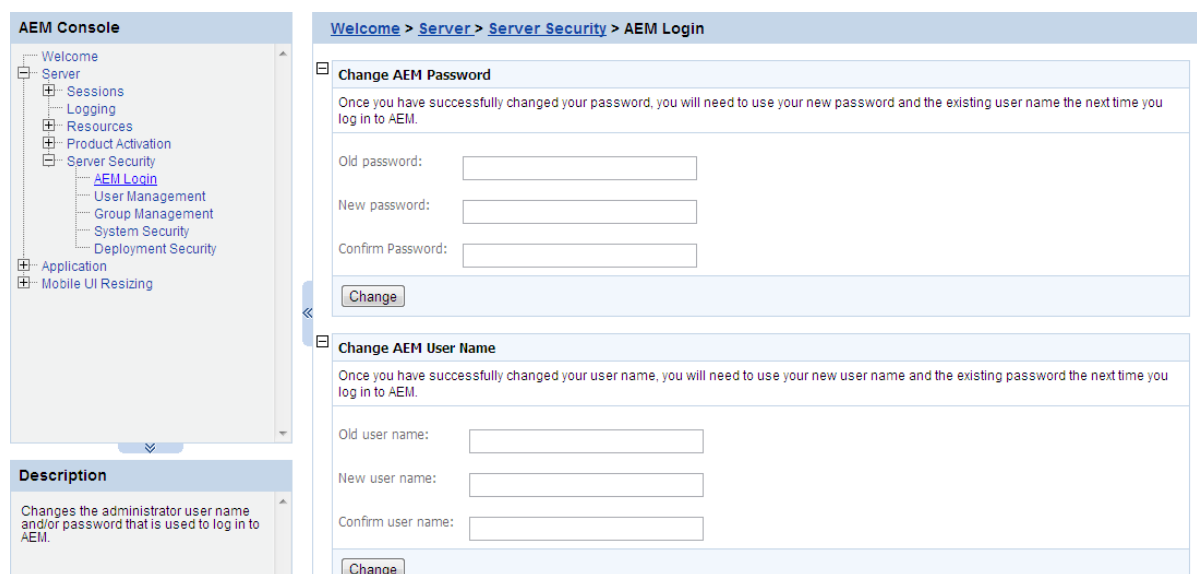
1) Change AEM Password

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, it is recommended that you change the username and password after the initial login.
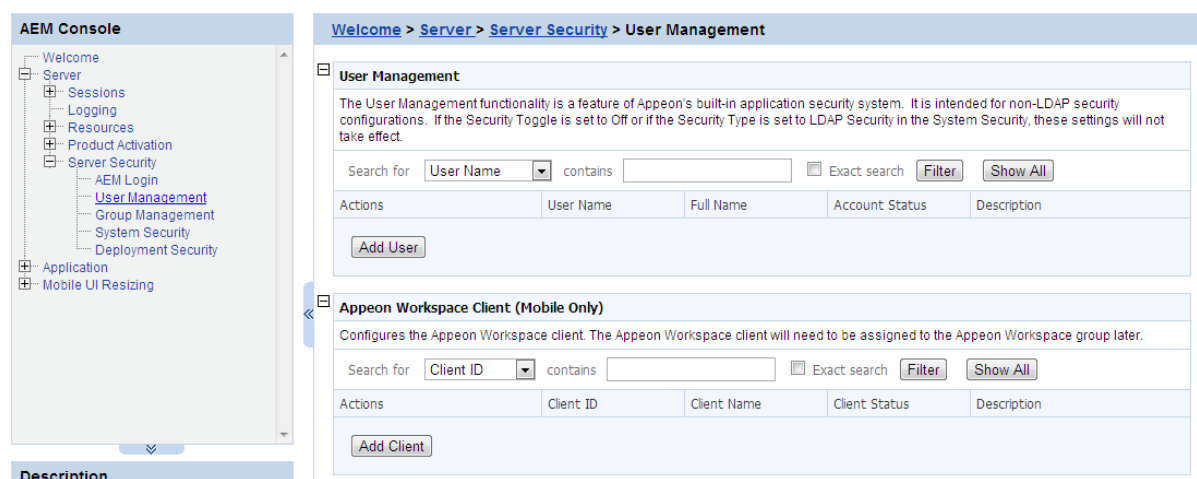
4.3.5.2 User Management

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

1. user accounts for all PowerServer applications including Web apps and mobile apps

2. Appeon Workspace clients for the PowerServer 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 4.50: User Management

4.3.5.2.1 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 4.51: 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 4.52: 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.

4.3.5.2.2 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 4.53: Add Appeon Workspace Client

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

Detailed configuration descriptions are shown in the following table.

Table 4.2: 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 PowerServer 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 4.54: 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.

4.3.5.3 Group Management

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

Figure 4.55: Group Management
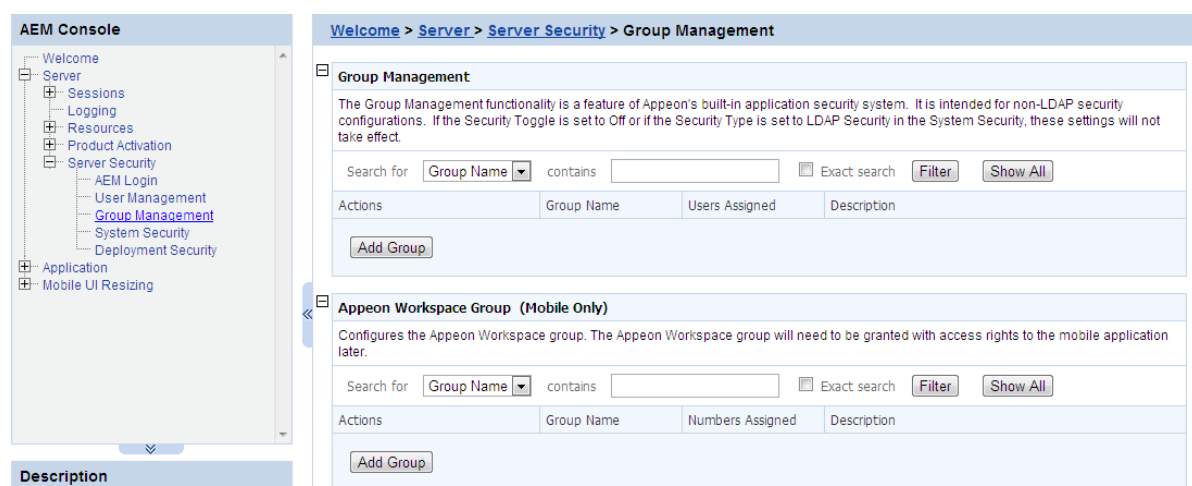
4.3.5.3.1 Group Management

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 4.56: 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.

4.3.5.3.2 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:

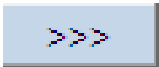Step 1: In the **Appeon Workspace Group** table, click **Add Group**.

Figure 4.57: 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 4.58: 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 4.59: 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.

4.3.5.4 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 PowerServer Web application or the PowerServer mobile application.

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

4.3.5.5 System Security

Figure 4.60: 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 <u>Client Security</u> 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. Appeon .NET version only supports Microsoft LDAP server, which requires Windows 2003 & 2008 Active Directory.

4.3.5.5.1 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 4.3: 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.

4.3.5.5.2 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 domain name of the LDAP Server.

- LDAP port -- The network port (by default 389) of the LDAP server. The default port for LDAP over SSL (LDAPS) is 636.

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

  For Microsoft LDAP server, the LDAP DN should be "CN=*Common Name*, DC=*AAA*, DC=*BBB, (DC=CCC)*", where CN denotes common name of the entry, DC denotes domain component, in this example, *AAA* stands for the domain component (DC) that contains all the groups, and *BBB* stands for the domain component that contains the *AAA* component.

- 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 -- A common alternate method of securing LDAP communication. The default port for LDAP over SSL is 636. If Yes is selected, the communication between PowerServer and LDAP Server will use LDAPS protocol. You need to import the Certificate Authenticated file of LDAPS (see the section called "Importing certificate file of LDAPS" for details). If No is selected, the communication between PowerServer and LDAP server will use LDAP protocol.

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.

Importing certificate file of LDAPS

In order to use LDAP over SSL (LDAPS), every PowerServer needs to import the certificate authenticated file of LDAPS in the following way:

1. Add the PowerServer machine to the domain. Please consult the network administrator if you do not know how to do this.

2. On the PowerServer machine, import the certificate file of the domain server.

   Here are detailed steps:

   a. Choose from **Start** > **Run**, then type *MMC*, and then click **OK**.

   b. On the **Console** menu, click **Add/Remove Snap-in**. The **Add/Remove Snap-in** dialog box opens.

   c. Click **Add** to display the **Add Standalone Snap-in** dialog box that lists the snap-ins installed on your computer.

   d. From the list of snap-ins, double-click **Certificates** to open the **Certificates snap-in** wizard.

   e. Select **Computer account**, then click **Next**, and then click **Finish**. Click **Close** and then **OK** to return to the Console.

   f. Choose from **Console Root > Certificates (local computer) > Trusted Root Certification Authorities**, then right-click **Certificates**, and then select from **All Tasks > Import…** in the **Certificate Import Wizard**, and then select and import the certificate file.

When the certificate file is imported successfully, you will be able to see the certificate listed, as shown below.

**Figure 4.61: Imported Certificates**
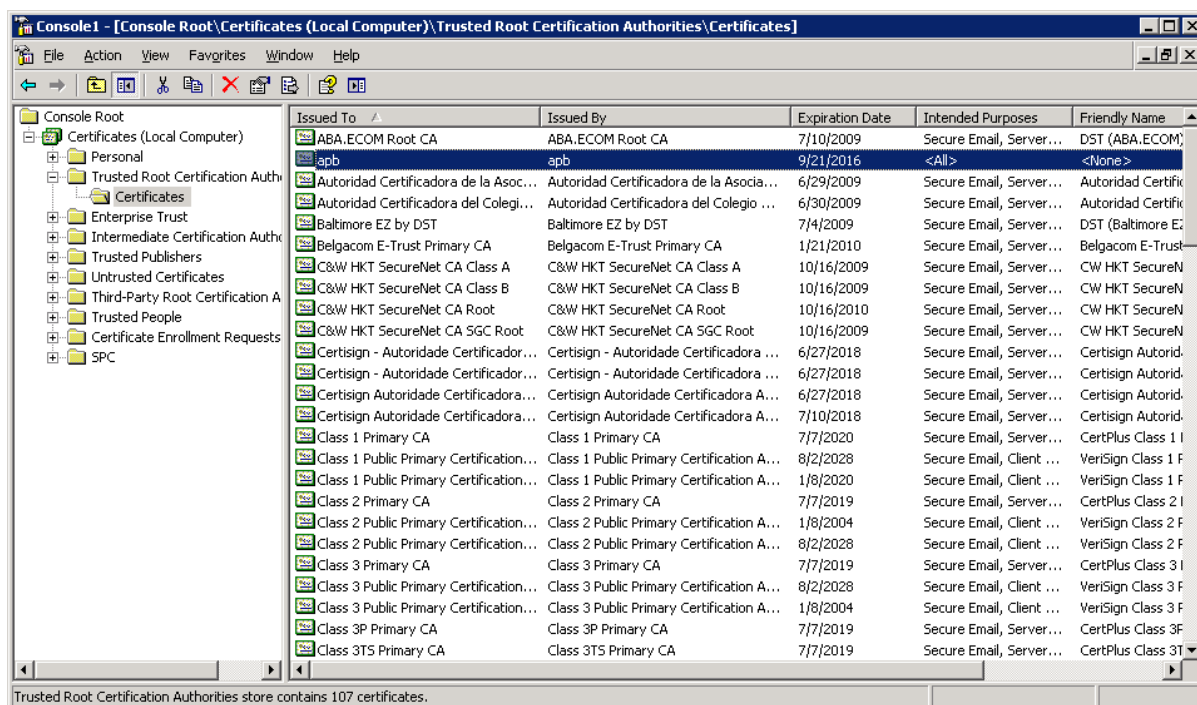
4.3.5.6 Deployment Security

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 4.62: Deployment Security
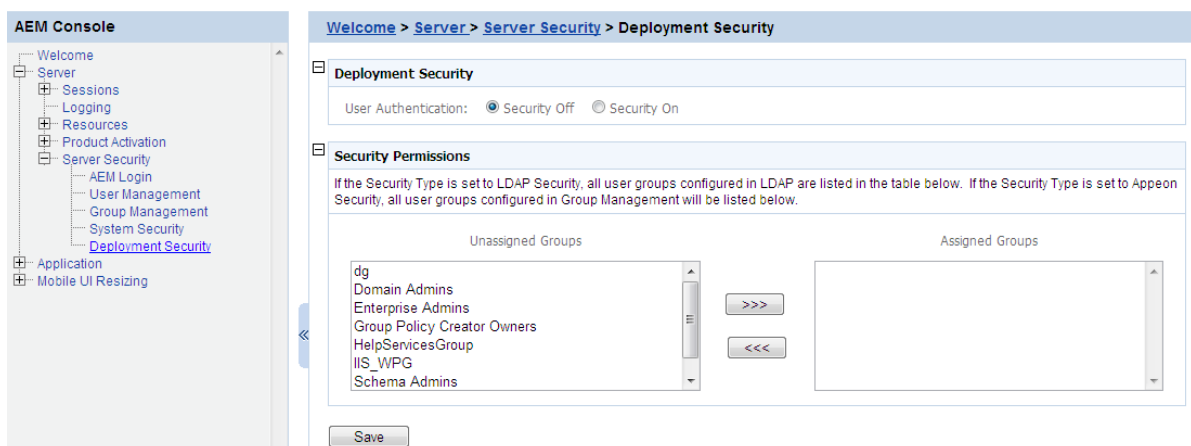
The Deployment Security tool enables you to do the following:

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.

4.4 Application

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

The **Application** node contains a set of tools for setting the server-related properties for the deployed applications. The settings for each application profile affect application(s) deployed from the application profile.
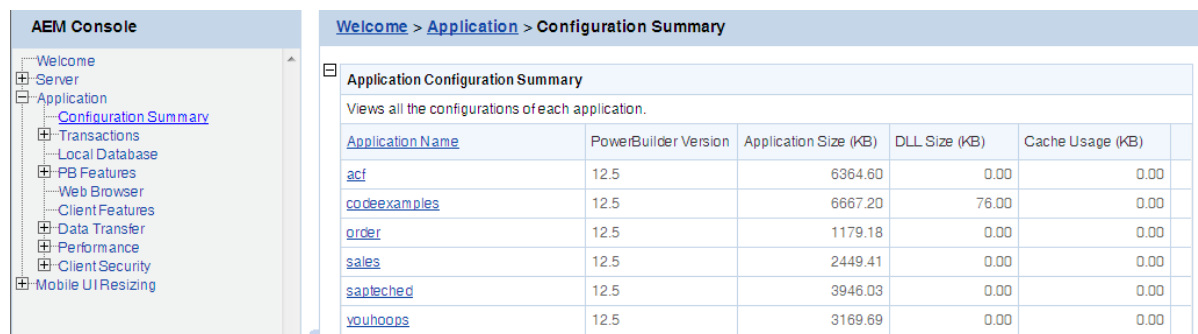
Figure 4.63: Application
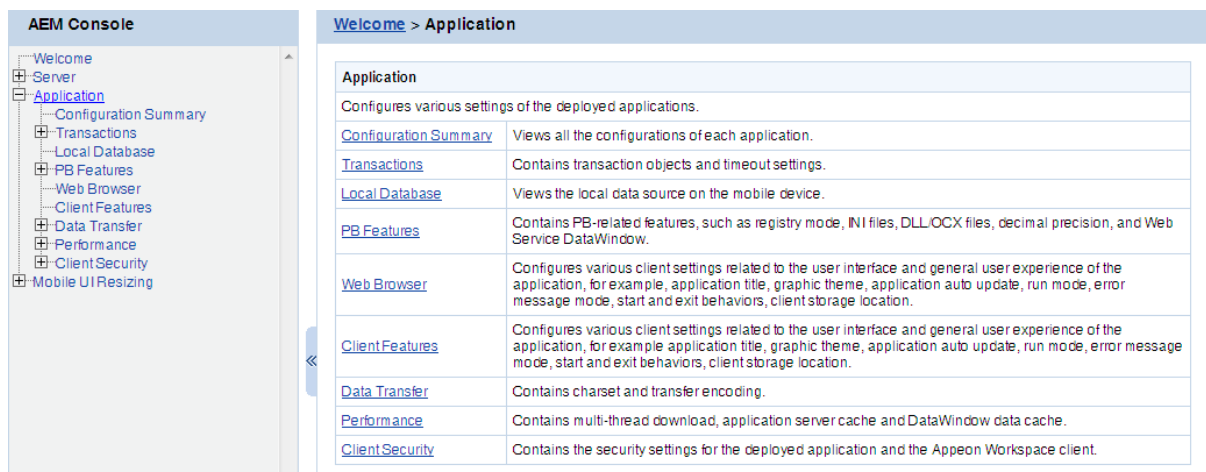
4.4.1 Configuration Summary

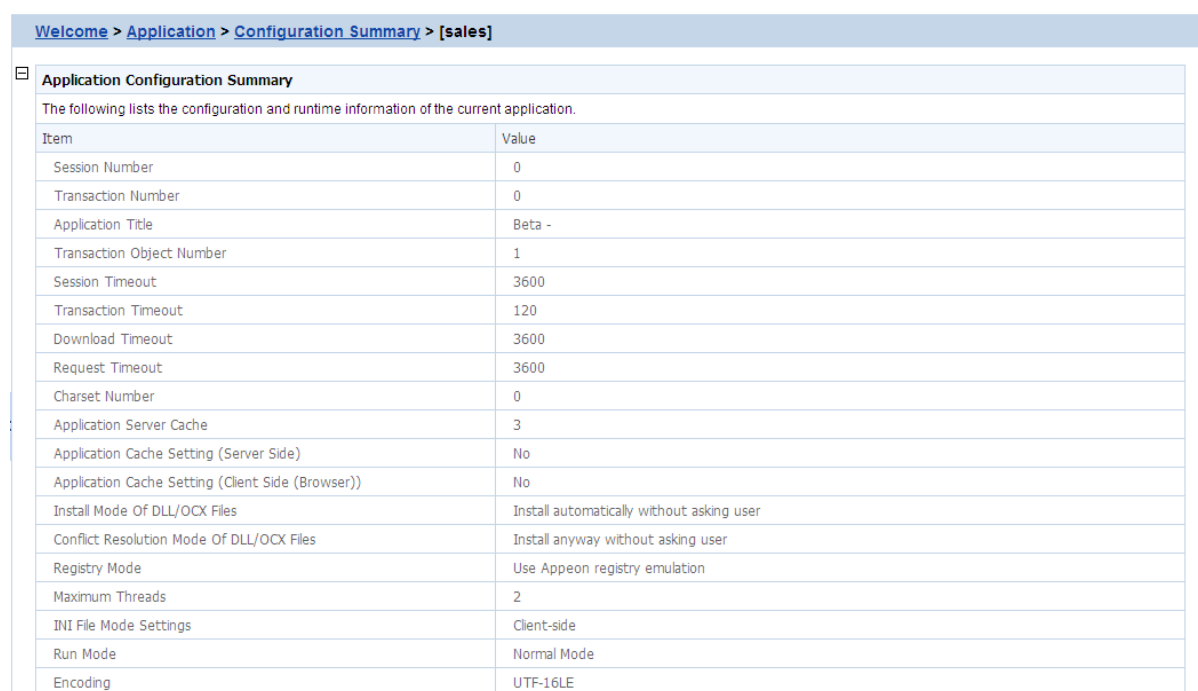The Configuration Summary of applications lists all the deployed applications and their configuration summaries.

Figure 4.64: Application Summary

AEM Console	Welcome > Application > Configuration Summary				
Welcome	**Application Configuration Summary**				
Server	Views all the configurations of each application.				
Application	Application Name	PowerBuilder Version	Application Size (KB)	DLL Size (KB)	Cache Usage (KB)
— Configuration Summary	acf	12.5	6364.60	0.00	0.00
Transactions	codeexamples	12.5	6667.20	76.00	0.00
Local Database	order	12.5	1179.18	0.00	0.00
PB Features	sales	12.5	2449.41	0.00	0.00
Web Browser	sapteched	12.5	3946.03	0.00	0.00
Client Features	youhoops	12.5	3169.69	0.00	0.00
Data Transfer					
Performance					
Client Security					
Mobile UI Resizing					

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

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

Figure 4.65: Application Configuration Summary

Welcome > Application > Configuration Summary > [sales]	
Application Configuration Summary	
The following lists the configuration and runtime information of the current application.	
Item	Value
Session Number	0
Transaction Number	0
Application Title	Beta -
Transaction Object Number	1
Session Timeout	3600
Transaction Timeout	120
Download Timeout	3600
Request Timeout	3600
Charset Number	0
Application Server Cache	3
Application Cache Setting (Server Side)	No
Application Cache Setting (Client Side (Browser))	No
Install Mode Of DLL/OCX Files	Install automatically without asking user
Conflict Resolution Mode Of DLL/OCX Files	Install anyway without asking user
Registry Mode	Use Appeon registry emulation
Maximum Threads	2
INI File Mode Settings	Client-side
Run Mode	Normal Mode
Encoding	UTF-16LE

4.4.2 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 4.66: Transactions

AEM Console	Welcome > Application > Transactions	
Welcome	**Transactions**	
Server	Contains transaction objects and timeout settings.	
Application	Transaction Objects	Configures the connection caches used by the deployed applications. This configuration must be performed each time a new application is deployed or when the transaction object/connection cache has changed.
— Configuration Summary		
Transactions	Timeout	Configures timeout settings for deployed applications. Appropriate timeout settings could control the session, enhance the system security, avoid the dead lock, etc.
— Transaction Objects		
— Timeout		
Local Database		
PB Features		
Web Browser		

4.4.2.1 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 to the Web, 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 correctly in 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.

4.4.2.1.1 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 4.67: 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 4.68: 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 4.69: 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.

4.4.2.2 Timeout

The Timeout provides configuration for six important functions of PowerServer for the PowerServer Web application or the PowerServer mobile application:

- 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)

- When the rollback of transactions will complete (Rollback Completion Time)

- The maximum times to retry the rollback of transactions (Maximum Rollback Retries)

Figure 4.70: Timeout

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 4.71: Timeout settings

4.4.2.2.1 Session timeout

A session starts when the user sends a request to load a PowerServer 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.

4.4.2.2.2 Transaction timeout

PowerServer 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 a PowerServer Web or PowerServer 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.

4.4.2.2.3 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.

4.4.2.2.4 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.

4.4.2.2.5 Rollback Completion time

The Rollback Completion time setting is to specify the maximum time (in seconds) to complete a rollback of a transaction. If the time to roll back transaction exceeds the specified value, the transaction rollback will be terminated. You can use this setting to prevent the deadlock from causing the application to hang for a long time.

The default value is 3 seconds. It is recommended that it is set to a number between 3 seconds and Transaction Timeout *0.1.

4.4.2.2.6 Maximum Rollback Retries

The Maximum Rollback Retries setting is to specify the maximum times to retry a rollback of a transaction. PowerServer executes a rollback if a transaction times out. If the rollback fails, PowerServer will keep retrying until this maximum value is reached. Setting this value to 0 will disable this feature.

The default value is 3. It is recommended that it is set to a number smaller than 10.

4.4.3 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 3.2.1.2.6, "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 4.72: Local database
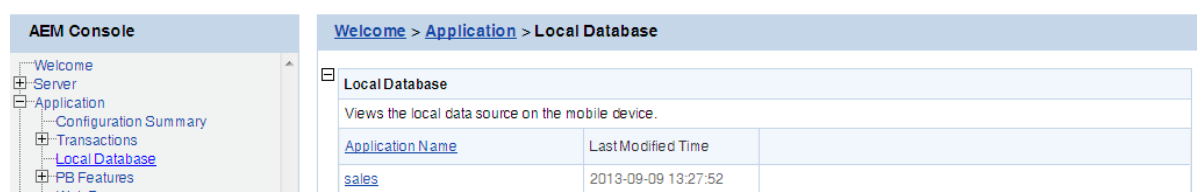
4.4.3.1 Viewing local database connections for an application

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 4.73: Local database connections for an application
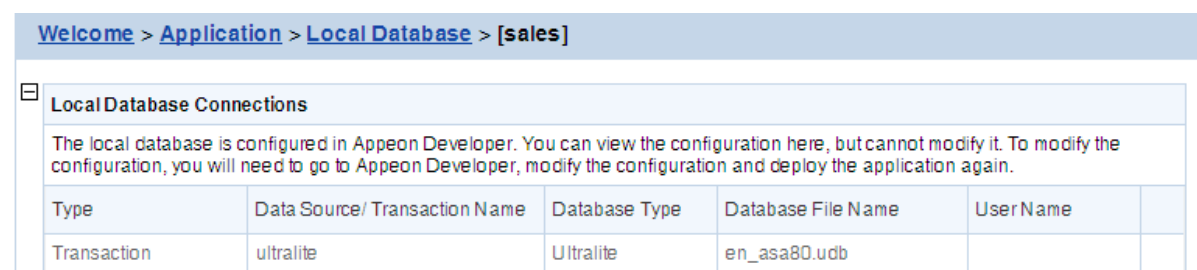
4.4.4 PB Features

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 4.74: PB Features

4.4.4.1 Registry Mode

The Registry Mode tool determines whether the PowerServer 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 4.75: Registry Mode
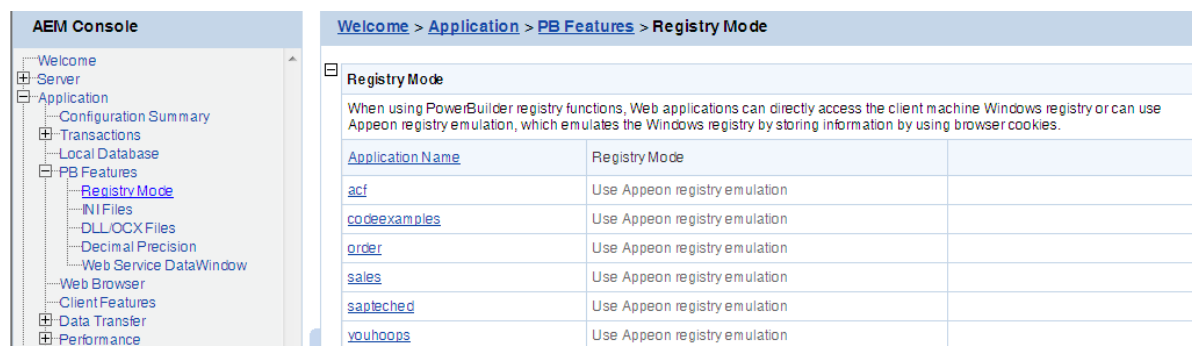
Click the application name listed in **Registry Mode** table, and then select one registry mode on the page that appears, and then click **Save**.

Figure 4.76: Registry Functions Execution Mode
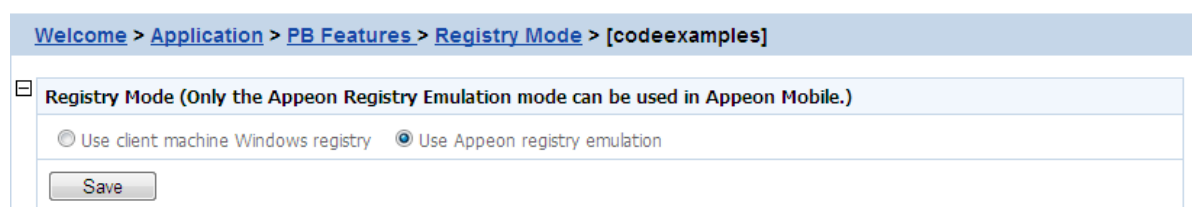
By default, all the PowerServer applications are set to "Use Appeon registry emulation".

We recommend 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.

4.4.4.2 INI Files

The INI Files tool determines whether the PowerServer 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 4.77: INI files
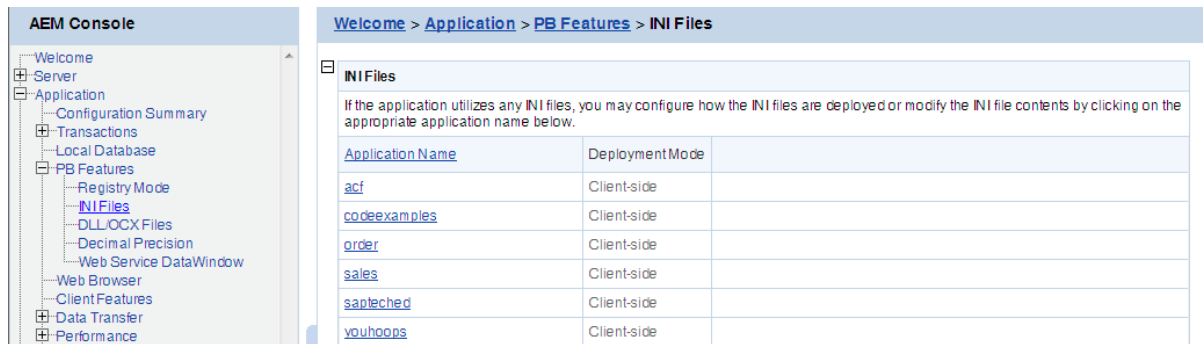
4.4.4.2.1 INI File Mode

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 4.78: INI file mode settings
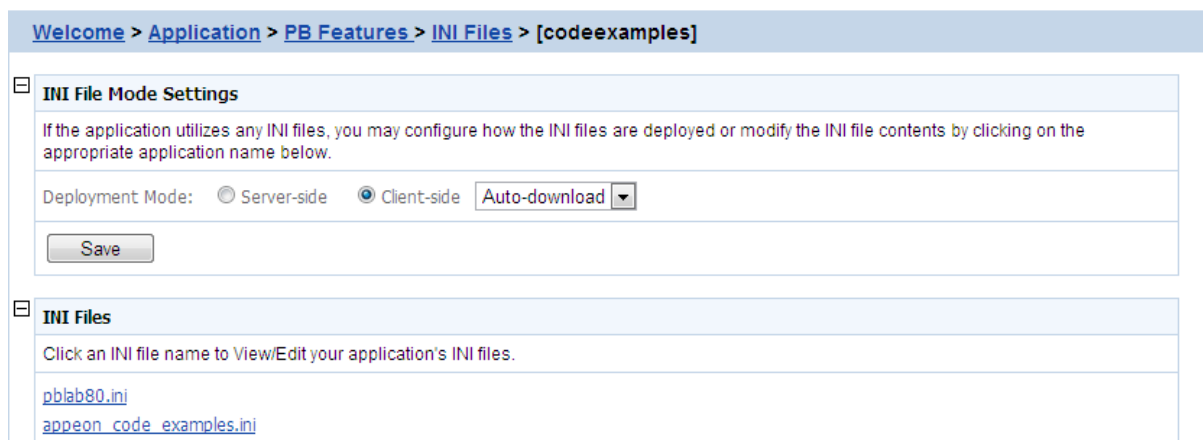
In the server-side manipulations mode, the PowerServer database creates an XML file for each application client, and differentiates the XML files for different clients with the client cookie information.

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.

4.4.4.2.2 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 4.79: INI files

```
⊟  INI Files

    Click an INI file name to View/Edit your application's INI files.

    pblab80.ini
    appeon_code_examples.ini
```
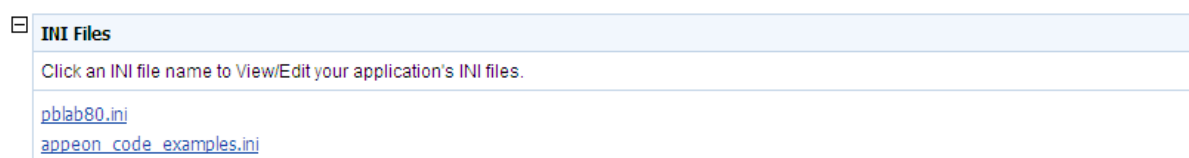
Click a file name of INI file to view or edit its content.

Figure 4.80: INI file content

```
Welcome > Application > PB Features > INI Files > [codeexamples] > [appeon_code_examples.ini]

⊟  INI File Content

    INI file must be edit exactly same as the way you edit in PowerBuilder. Please note that all the relative values previously modified by end-users
    will lose if you modified any value and save it.

    ┌────────────────────────────────────────────────────────────────────┐
    │ [database]                                                           │
    │ dbms=ODBC                                                            │
    │ autocommit=false                                                     │
    │ dbparm="ConnectString='DSN=AppeonSample;UID=dba;PWD=sql'"            │
    │                                                                      │
    │ [user info]                                                          │
    │ name=James Smith                                                     │
    │ jobtitle=Window Washer                                               │
    │ user id=1002                                                         │
    │ security=9                                                           │
    │                                                                      │
    │                                                                      │
    └────────────────────────────────────────────────────────────────────┘

    [ Save ]
```

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.

4.4.4.3 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 4.81: DLL/OCX Files
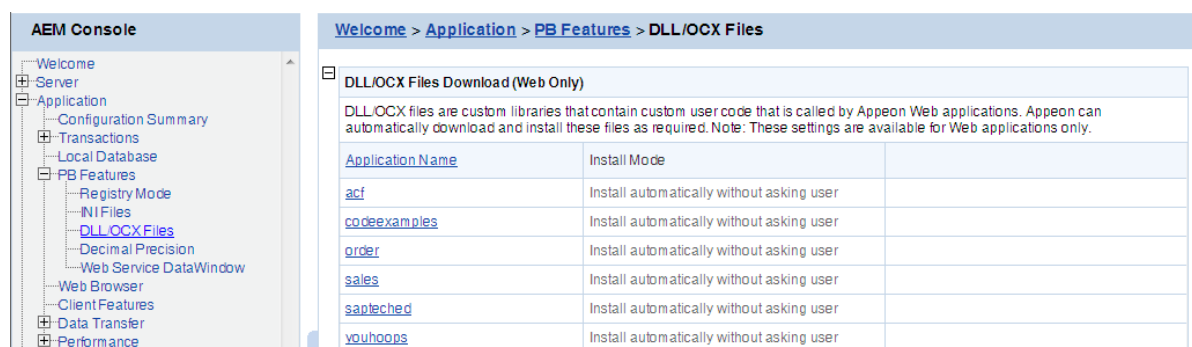
4.4.4.3.1 Install mode

"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 4.82: DLL/OCX Files settings
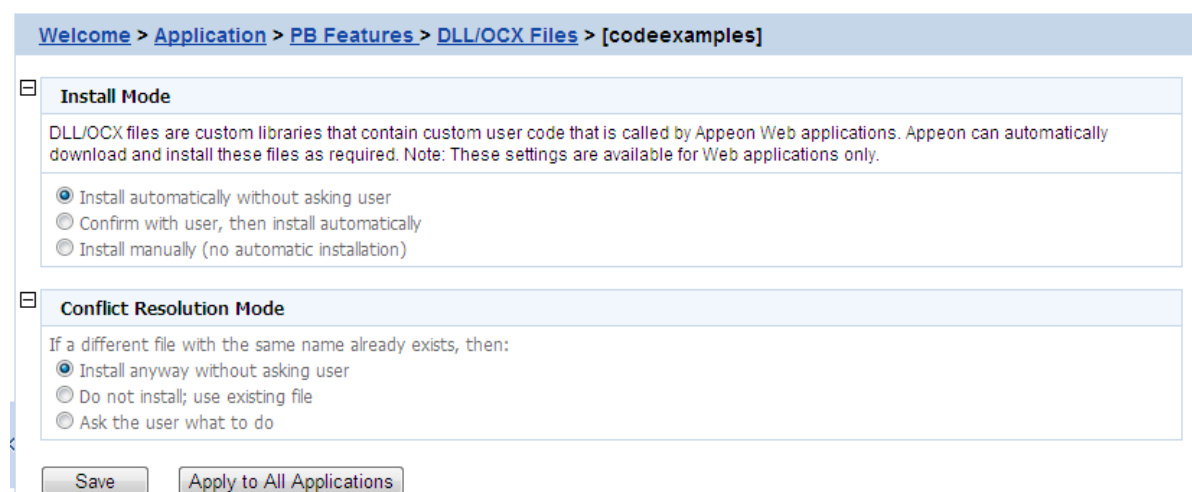
You can select the install mode that is most suitable for the application according to the description in the following table.

Table 4.4: 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, PowerServer does not handle the DLL and OCX files installation for the application. Users must manually install the DLL and OCX files of the application before accessing the application. This option is recommended if the DLL and OCX files used by the application are large size and take a long time to be downloaded over the network.

4.4.4.3.2 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 4.5: 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.

4.4.4.4 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, and is only supported in DataWindow. It is not recommended to apply 28-digit decimal unless high precision number is necessary.

Figure 4.83: Decimal Precision
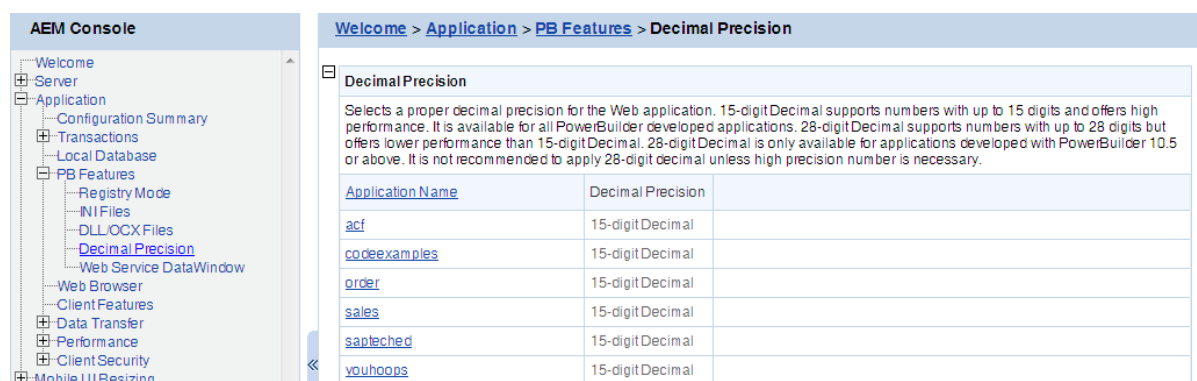
Step 1: Click the application name listed in the **Decimal Precision** table, and then select a decimal mode on the page that appears.

Figure 4.84: Decimal Precision Settings
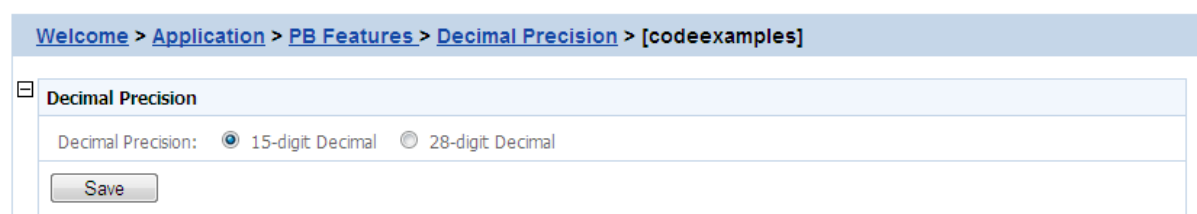
Step 2: Click the **Save** button to save changes.

4.4.4.5 Web service DataWindow

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

Figure 4.85: Web service DataWindow
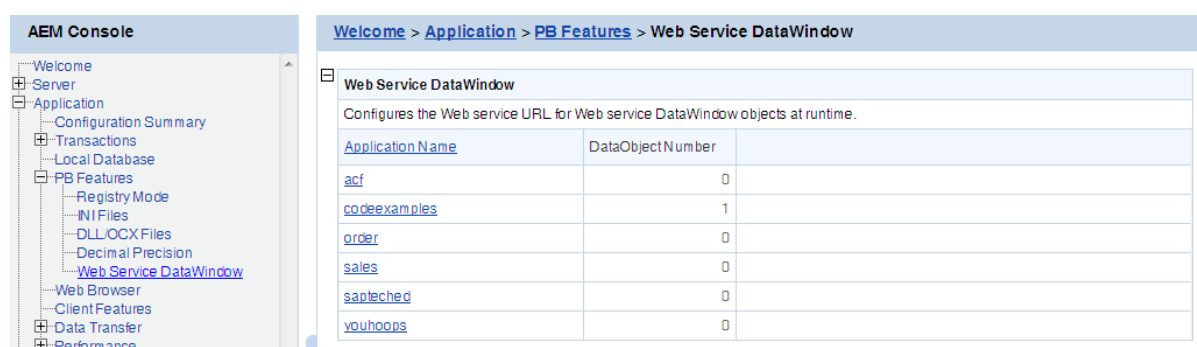
This section takes the appeon_code_examples as an example to show how to configure the Web service URL in AEM.

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 4.86: 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 4.87: Modify URL for DataWindow methods

3. Click **Update**.

4.4.5 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 4.88: Web Browser
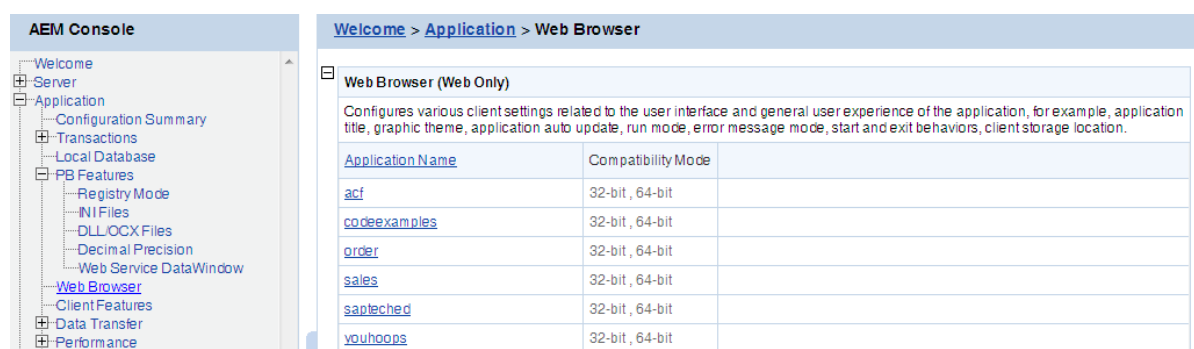
4.4.5.1 IE Compatibility

PowerServer 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 4.89: 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 1.3.1, "AppeonExtFuncs Object" in *Workarounds & APIs 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?".

4.4.5.2 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 4.90: 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**.

4.4.6 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 4.91: Client Features

4.4.6.1 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 4.92: Application Title

4.4.6.2 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 4.93: Web Application Theme

There are two options for Web Application Theme:

- **Windows Vista**: Applying this theme enables PowerServer 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 PowerServer Web application presented in traditional Windows 2000 style.

4.4.6.3 Web Application Auto Update

When a PowerServer Web application or PowerServer 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 4.94: Auto Update

4.4.6.4 Run Mode

Note: This tool is for Web applications only.

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 4.95: Run mode

There are two Run Mode options:

- **Normal Mode**: This is the default and recommended mode for running the PowerServer Web or PowerServer mobile applications.

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

Note:

1. If **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 setting of **Test Mode** has 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.

3. Mobile applications cannot run in **Test Mode**.

4.4.6.5 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 4.96: 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: PowerServer 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 PowerServer. 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 PowerServer and displays in a popup message.

4.4.6.6 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 4.97: Start & Exit Settings

4.4.6.6.1 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**.

4.4.6.6.2 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.

4.4.6.6.3 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.

  This option is only effective to Internet Explorer 7.0 or above.

- **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 only 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.

4.4.6.7 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 & APIs Guide* to get the current directory for the application.

Figure 4.98: 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, or run as IWA. 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 4.99: Customized location

Customized Location	
Specifies where to cache the web application files. Note: These settings are available for Web application only.	
Path Type	Path
System Files Storage Path	
Application Object Files Storage Path	
OLE Files Storage Path	
Menu Object Files Storage Path	
Image File Storage Path	
OCX/DLL Files Storage Path	
INI Files Storage Path	
DataWindow Meta Files Storage Path	

Save

4.4.6.8 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 4.100: Client Logs

Client Log	
Specifies the log mode and the maximum size of log files on the client side. The log file will record the client system information and the application environment information, for debugging purpose only. If these are confidential information, please remove them before sending the log file. When logging is enabled, all clients where the application is running will automatically write information to the log file, which may affect the application runtime performance. Please be cautious to turn on logging and turn it off once not necessary.	
Log Mode	**Log File**
○ Off (default)	Log file size: 2 MB (2MB<=File size<=5MB)
○ Error mode	
○ Info mode	
○ Debug mode	

See the following table for details on the mode options.

Table 4.6: 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 PowerServer provides. See AppeonGetCacheDir function in *Workarounds & APIs 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 4.9, "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 & APIs Guide* for details.

4.4.6.9 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 4.101: Retina Display Supported
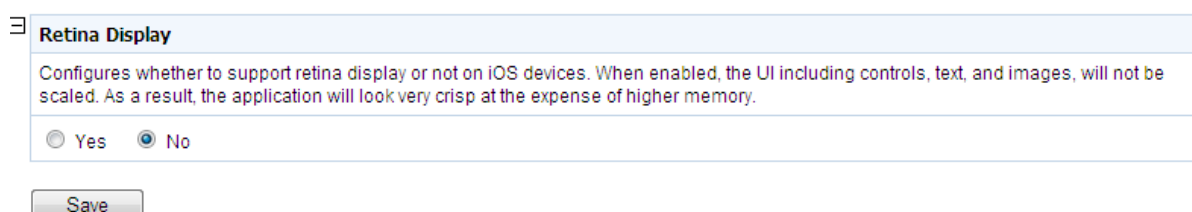
4.4.7 Data Transfer

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

Figure 4.102: Data Transfer
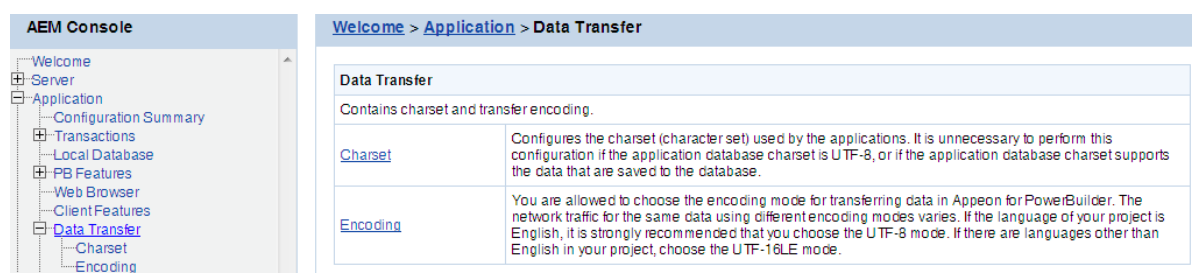
4.4.7.1 Charset

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 4.103: Charset settings
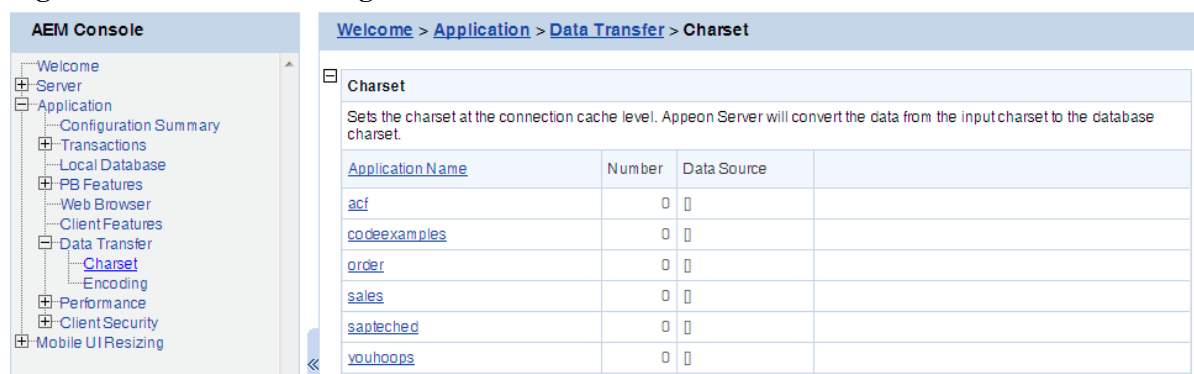
4.4.7.1.1 Configuring database Charset for a data source

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

Figure 4.104: Configure charset settings
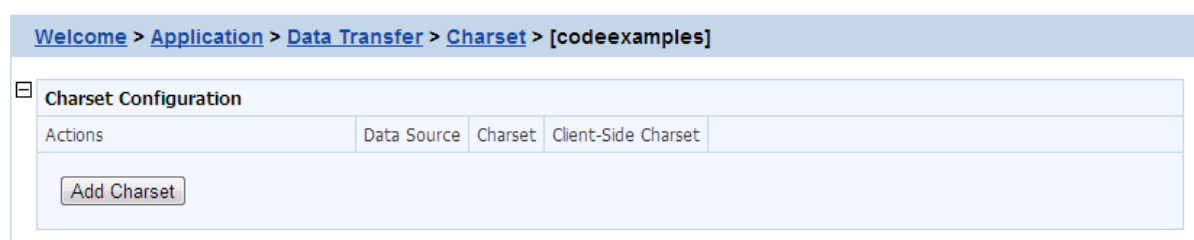
Step 2: Click the **Add Charset** button. The Add Charset window opens.

Figure 4.105: Add charset settings
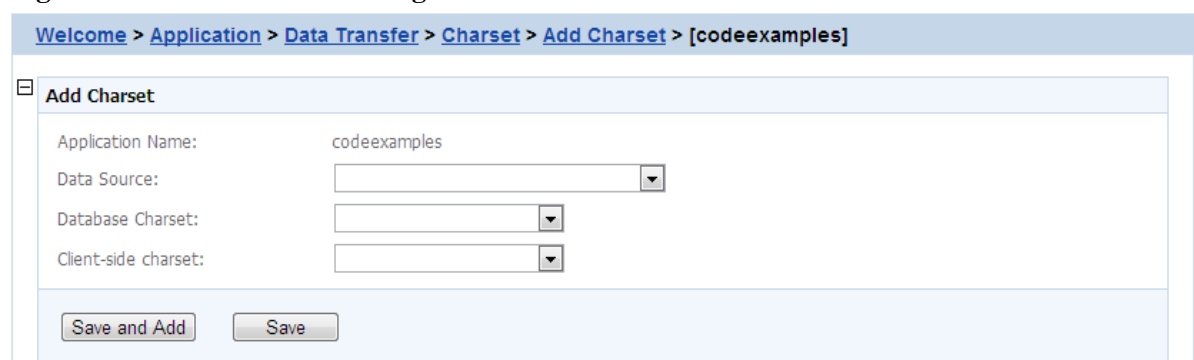
Step 3: Select the data source from the **Data Source** dropdown list.

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.

4.4.7.1.2 Updating a Charset

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

4.4.7.1.3 Deleting a Charset

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

4.4.7.1.4 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 4.7: 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)	
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)	

Page	Charset	Description	Asterisk
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)	
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)	

Page	Charset	Description	Asterisk
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	*
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.)	

Page	Charset	Description	Asterisk
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)	
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)	*

Page	Charset	Description	Asterisk
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)	*

4.4.7.2 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 4.106: Encoding
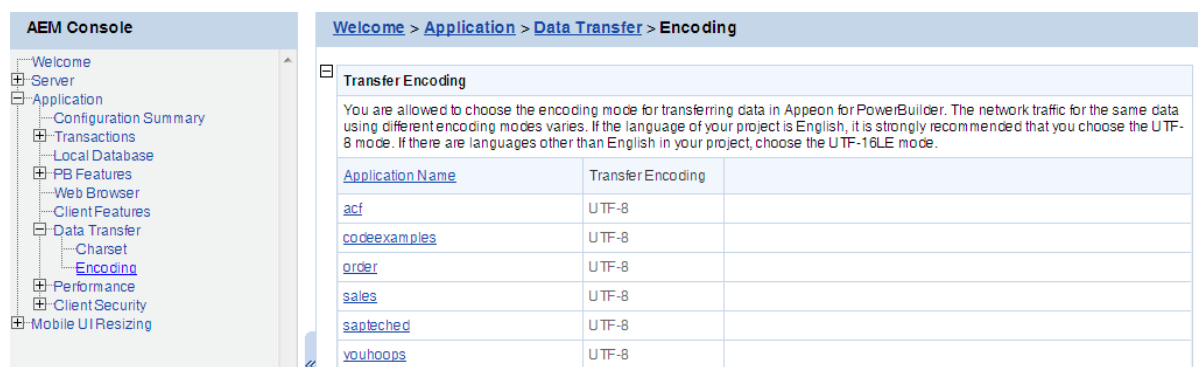
If the language of the application is pure English, select UTF-8; otherwise, select UTF-16LE.

Figure 4.107: Encoding settings
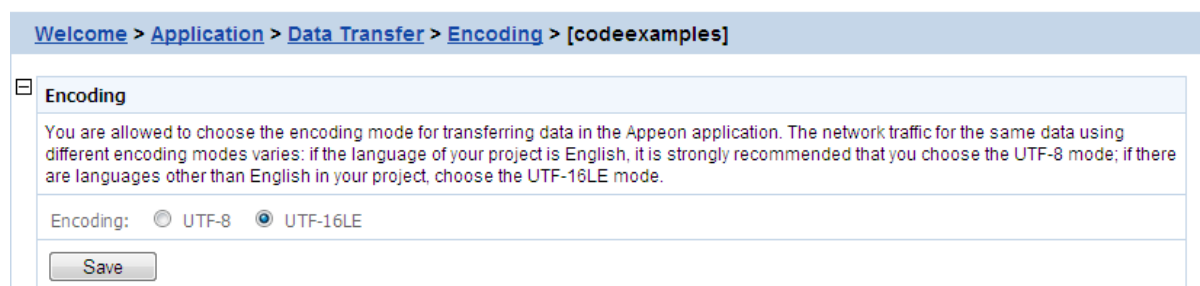
4.4.8 Performance

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

Figure 4.108: Performance
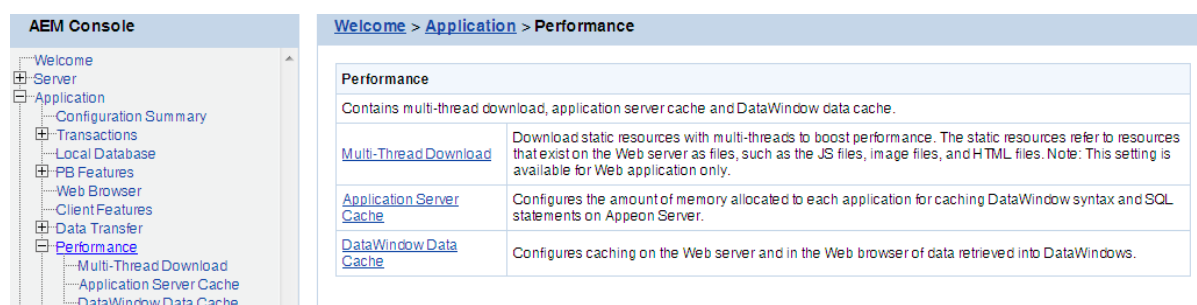
4.4.8.1 Multi-Thread Download

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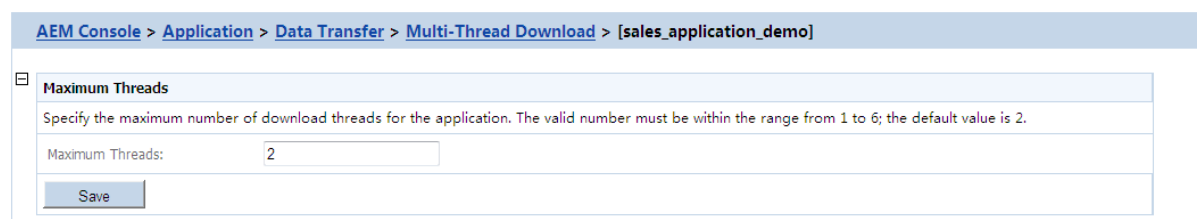
The Multi-Thread Download setting specifies how many threads a client will take for simultaneously downloading application Web files (such as JavaScript files, image files, and HTML files) from the Web server. This option makes full use of the network bandwidth between clients and Web server, and shortens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

Figure 4.109: Multi-thread Download
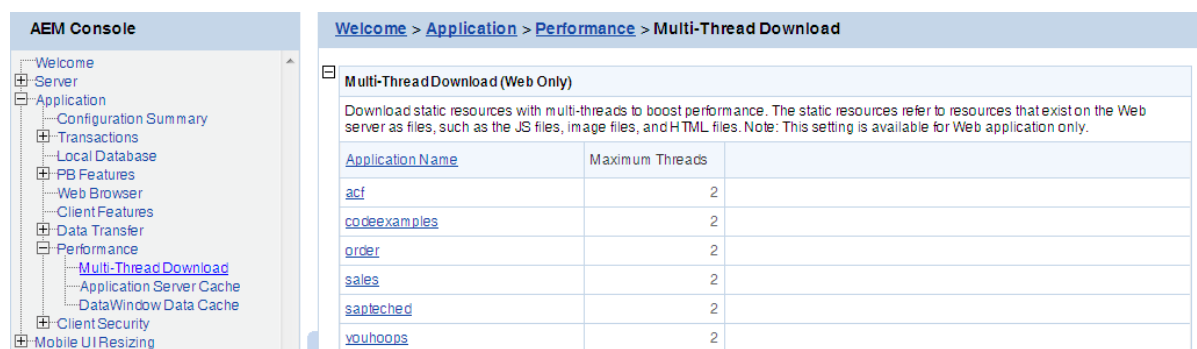
Click the application name in the **Multi-thread Download** table, and then enter a number in the **Maximum Threads** text box, and then click **Save**.

Figure 4.110: 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.

4.4.8.2 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.

4.4.8.2.1 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.

4.4.8.2.2 Modifying the Application Server cache settings for an application

In the **Application Server Cache** table, the **Cache** column shows the Application Server 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 4.111: 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 4.112: 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.

4.4.8.3 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 4.113: DataWindow Data Cache

4.4.8.3.1 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 4.114: Dynamic-DW SQL Cache

4.4.8.3.2 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 database.

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 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.

Configuration required for database servers

PowerServer 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, 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 4.8: 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.

Database Type	SQL File
DB2	To enable this feature, execute install_appeon_cache_DB2.sql.
	To disable this feature, execute uninstall_appeon_cache_DB2.sql.

Important notes:

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 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 4.115: 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.

4.4.9 Client Security

The Client Security tool in AEM is used to configure the User Authentication and Appeon Workspace securities.

Figure 4.116: Client Security

4.4.9.1 User Authentication

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

Figure 4.117: Application Security

4.4.9.1.1 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 PowerServer Web application or the PowerServer 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 4.118: Detailed security settings for an application
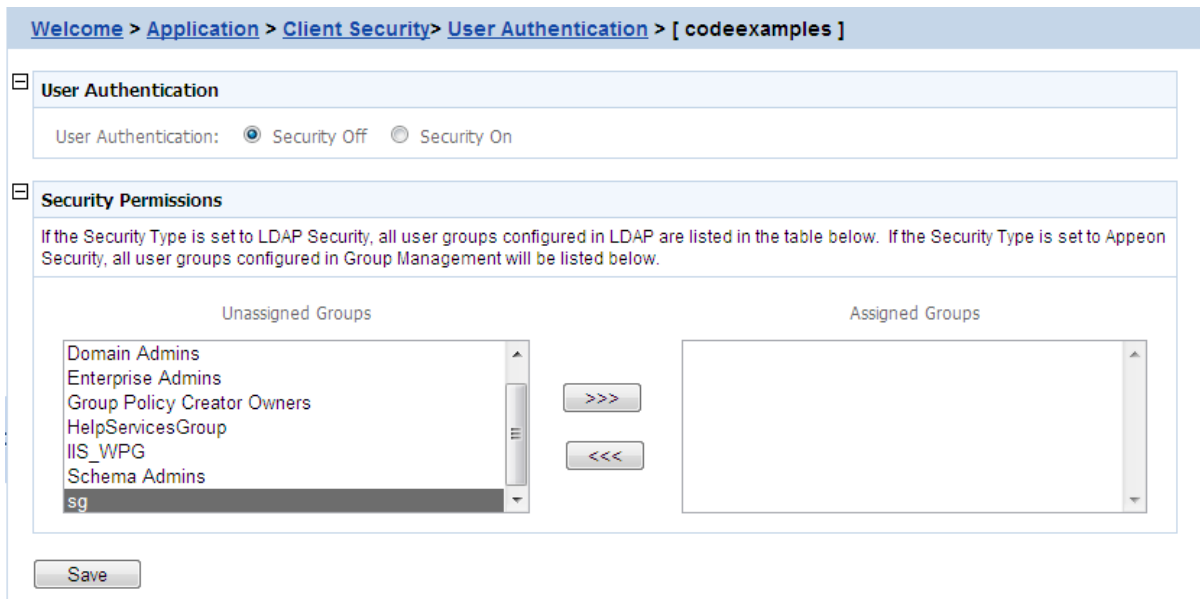
As the following table shows, different application security settings determine different security behaviors in a PowerServer application.

Table 4.9: Application security settings and security behaviors in a PowerServer application

User Authentication	A Given Group	Security behaviors in a PowerServer application
Off	Assigned	All users can access to a PowerServer application without being prompted for a user name or password.
	Unassigned	

User Authentication	A Given Group	Security behaviors in a PowerServer application
On	Assigned	Users of an assigned group have access rights to a PowerServer application and they are prompted for user names and passwords when loading a PowerServer 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 PowerServer application.

4.4.9.1.2 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 1.3.2.16, "AppeonLDAPLogon function" in *Workarounds & APIs 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.

4.4.9.2 Appeon Workspace

Figure 4.119: Appeon Workspace application security

4.4.9.2.1 Introduction to Appeon Workspace

Appeon Workspace is a free native mobile application which can only be distributed internally or privately. As its name suggests, it is a workspace provided by Appeon to simplify distributing, running and managing the PowerServer native mobile applications. In Appeon Workspace, you can download and run the PowerServer 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.

4.4.9.2.2 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 4.120: 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.

4.4.9.2.3 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 Setting Appeon Workspace security 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.

4.4.10 Mobile App Distribution

4.4.10.1 Requirements

4.4.10.1.1 iOS IPA file requires to be installed through HTTPS

Starting 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.

4.4.10.1.2 File size requirement

This section is required for IIS and WildFly. Skip this section if you are using the other Web server (such as JBoss EAP, 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:

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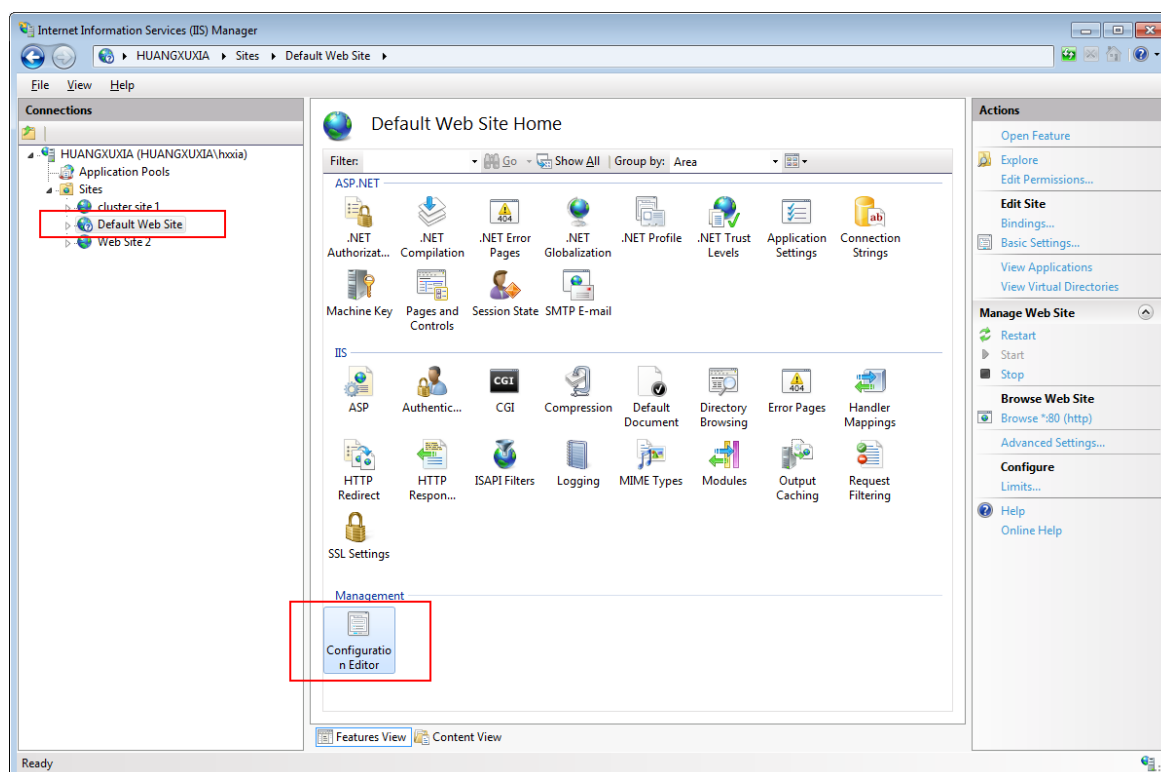
2. Open the **Configuration Editor** feature, select or input *system.webServer/ security/requestFiltering* in the **Section** field, and then modify the value of the

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

Figure 4.122: requestFiltering -> maxAllowedContentLength
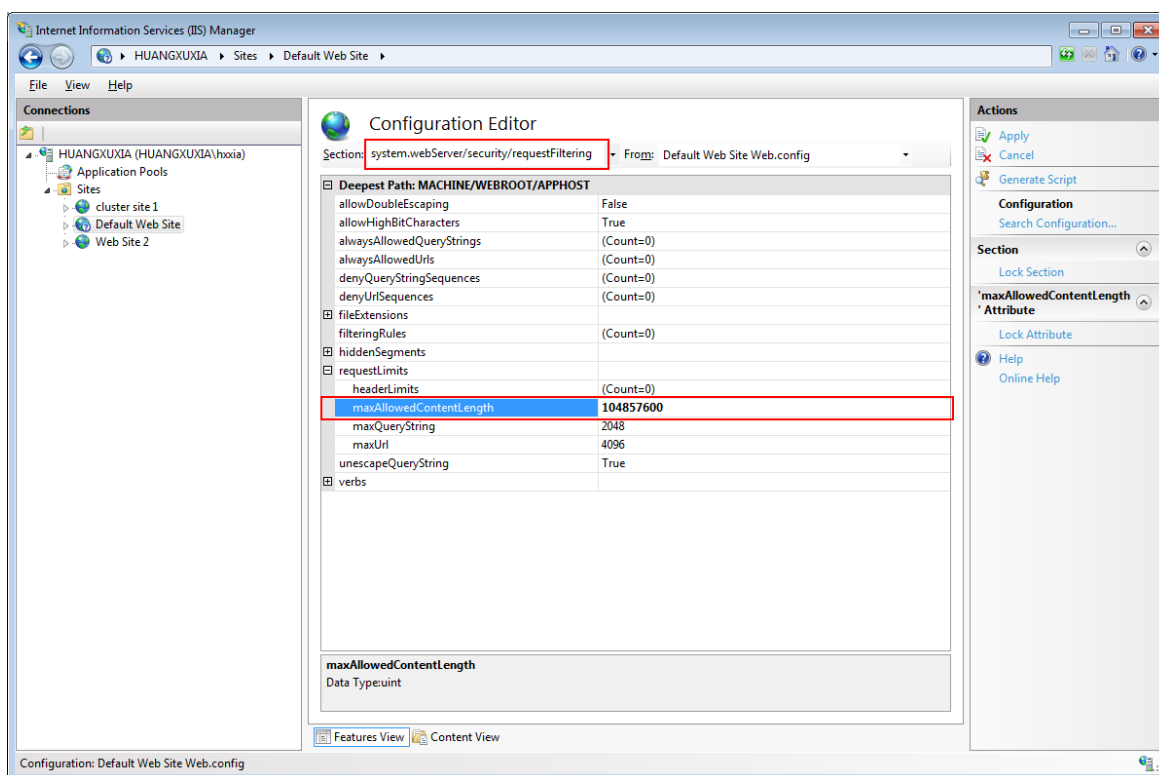
4.4.10.2 Upload standalone mobile apps and Appeon Workspace

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 9.2, "Packaging a stand-alone mobile project" in *PowerServer Toolkit User Guide* and Section 9.3, "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 2.2.2, "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\archive name

If you compile the installer file from the project file created by the PowerServer Toolkit Package tool, you should keep the file \archive name by default. A valid file\archive name should look like this: *AppName-AppIdentifier-BuildNumber-32bit/64bit*.apk or *DisplayName-BundleIdentifier-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 Identifier*) shall be replaced by an underscore(_). For more about the file name, refer to Section 9.2, "Packaging a stand-alone mobile project" in *PowerServer Toolkit User Guide* and Section 9.3, "Customizing and packaging Appeon Workspace" in *PowerServer Toolkit User Guide*.

Figure 4.123: 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 4.124: 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 4.125: Download URL of the installer

Download URL	
There is a default URL for the selected installer. If the default URL is not accessible by your users, you can update the server URL in it, and click Save. If you want to reset the URL to its default value, click Reset.	
App Name	My Workspace
For iOS/Android	Android
Effective Build No.	8.0.1075.00
APP ID	com.appeon.myworkspace
Deploy Date	2016-08-30 11:24:46
Download URL	http://localhost:80/aws/packages/My_Workspace-com_appeon_my

Reset   Save

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 4.126: Download URL of the installer

Download URL	For Download on Mobile Devices:	http://localhost:80/aws/8.0.1062.00.plist
	For Download to iTunes on Desktops:	http://localhost:80/aws/8.0.1062.00.ipa

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 4.127: QR code of the installer

4.4.10.3 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 PowerServer Application Deployment Wizard. For how to deploy the mobile app using the PowerServer Application Deployment Wizard, refer to Chapter 5, *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 4.128: 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 3.1, "Adding applications" in *Appeon Workspace User Guide*.

Figure 4.129: Download or copy QR code of the installer

4.5 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 4.130: Mobile UI Resizing

4.5.1 Screen Size

Screen Size is a tool for managing the PowerServer-supported mobile devices. It allows adding, editing and removing devices. But the sample device types which are added by default cannot be modified or deleted. All of the supported device screen size (measured in points) added are listed below.

Figure 4.131: Screen Size
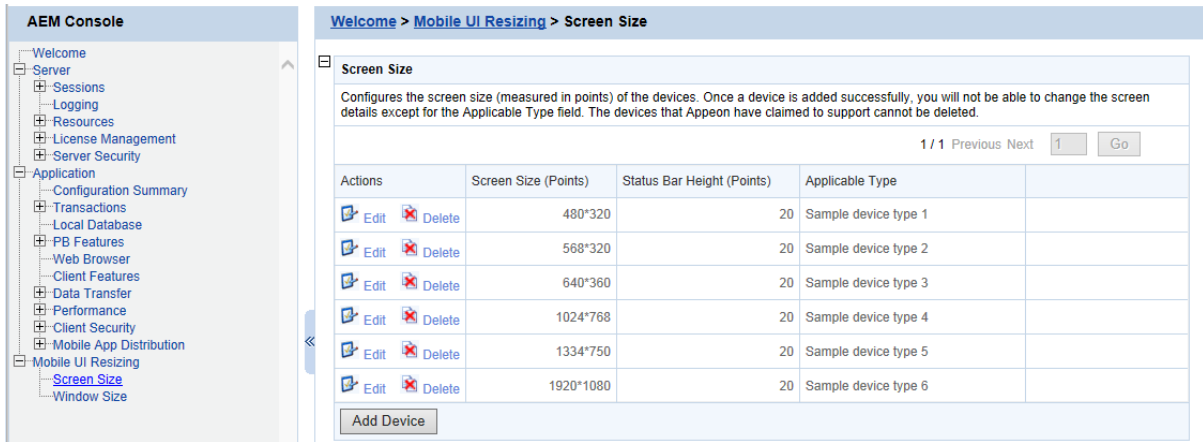
Click the **Edit** button to view the details of the device screen size.

Figure 4.132: Screen details
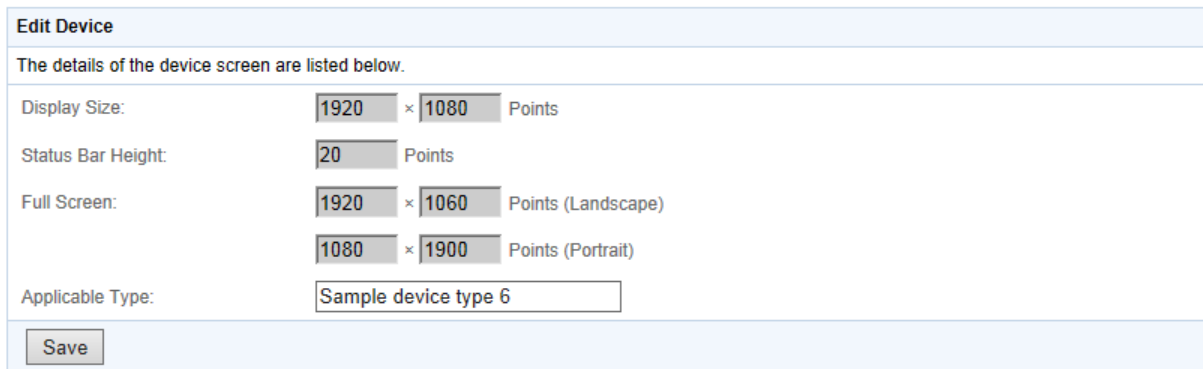
4.5.1.1 Adding a device

On the **Screen Size** page, some of the supported devices (measured in points) are configured by default. 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 4.133: Add a device
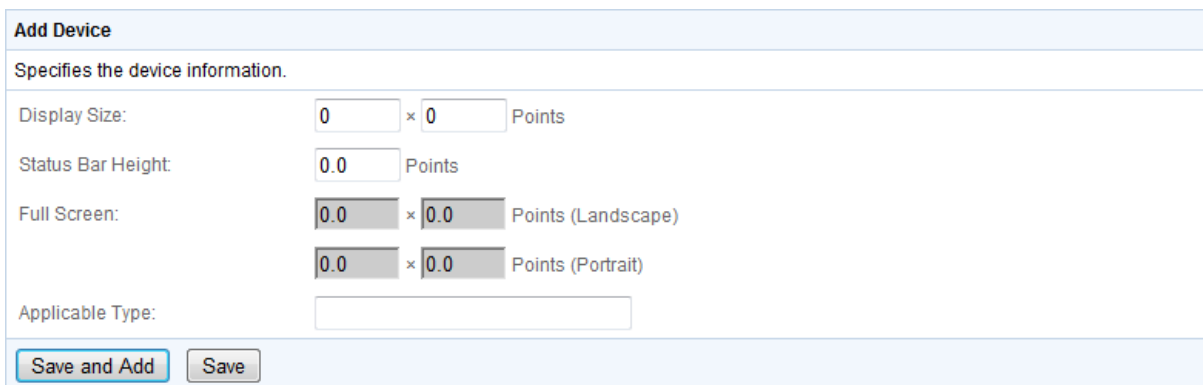
Step 2: On the **Add Device** page, enter the following values:

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 <u>Automatically adding a device to an application</u> 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.

4.5.1.2 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 4.134: Edit a device

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

4.5.1.3 Deleting a device

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

4.5.2 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 4.135: Window size

4.5.2.1 Configuring size for all windows

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

Figure 4.136: 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 4.137: Autofit mode
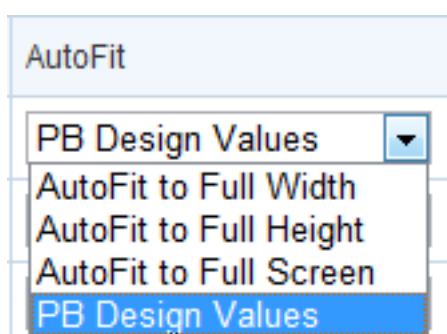
   The modes and the corresponding descriptions are listed in the following table.

   Table 4.10: 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.

Mode	Descriptions
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 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.

4.5.2.2 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 4.138: 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 4.139: Screen emulator
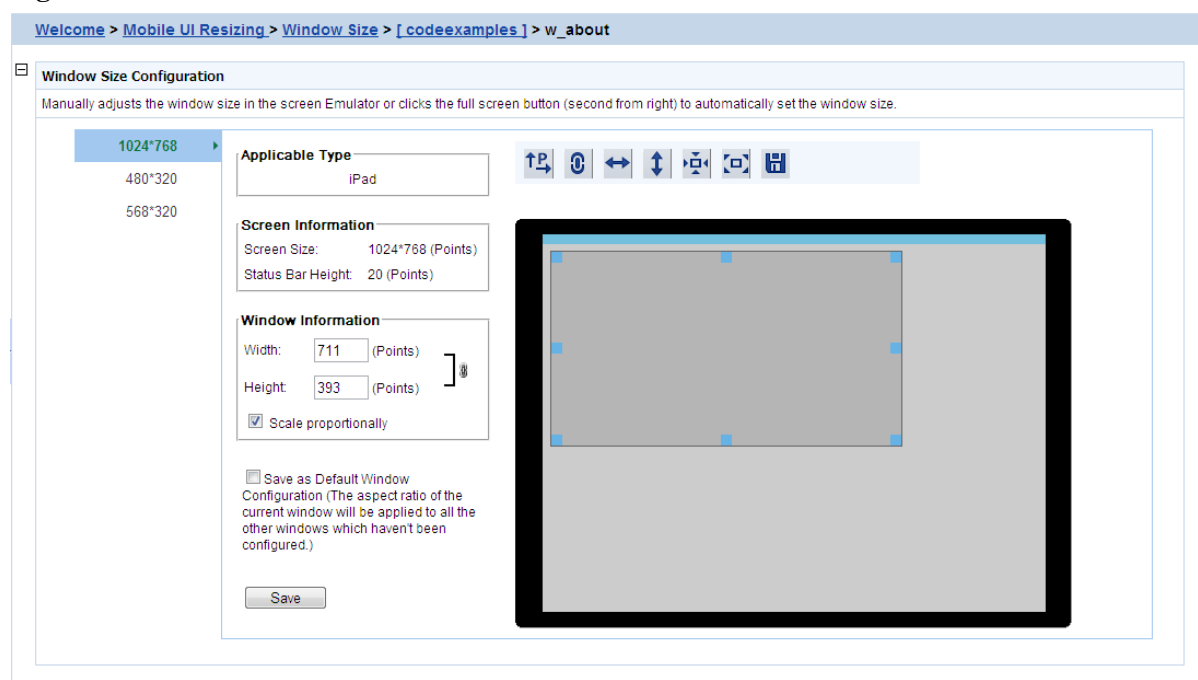
Step 2: Select a device name from the left column. The device(s) added to the Screen Size table are displayed. You need to configure the window size for each device separately.

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