

Appeon Server Configuration Guide for .NET*

Appeon® 6.0 for PowerBuilder®
WINDOWS

* Not available in Sybase Distribution. For differences of distributions, refer to the *Distributions* section in *Introduction to Appeon*.

DOCUMENT ID: DC00812-01-0600-03

LAST REVISED: July 2008

Copyright © 2008 by Appeon Corporation. All rights reserved.

This publication pertains to Appeon software and to any subsequent release until otherwise indicated in new editions or technical notes. Information in this document is subject to change without notice. The software described herein is furnished under a license agreement, and it may be used or copied only in accordance with the terms of that agreement.

No part of this publication may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without the prior written permission of Appeon Corporation.

Appeon, the Appeon logo, Appeon Developer, Appeon Enterprise Manager, AEM, Appeon Server and Appeon Server Web Component are trademarks or registered trademarks of Appeon Corporation.

Sybase, Adaptive Server Anywhere, Adaptive Server Enterprise, iAnywhere and PowerBuilder, are trademarks or registered trademarks of Sybase, Inc.

Java, JDBC and JDK are trademarks or registered trademarks of Sun, Inc.

All other company and product names used herein may be trademarks or registered trademarks of their respective companies.

Use, duplication, or disclosure by the government is subject to the restrictions set forth in subparagraph (c)(1)(ii) of DFARS 52.227-7013 for the DOD and as set forth in FAR 52.227-19(a)-(d) for civilian agencies.

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

Contents

1 About This Book	1
1.1 Audience	1
1.2 How to use this book	1
1.3 Related documents	1
1.4 If you need help	2
2 Server Configuration Tasks	3
2.1 Overview	3
2.2 Scope of configurations discussed in this book	3
2.3 Configuration stages and tasks	3
2.3.1 Configuration during application deployment	4
2.3.2 Configuration during debugging	5
2.3.3 Configuration during security management	5
2.3.4 Configuration during performance management	5
2.3.5 Configuration during server information management	6
3 Database Connection Setup	7
3.1 Overview	7
3.2 What is Apeon Server connection cache	7
3.3 Database Connection Types	7
3.4 Setting up Apeon Server connection caches	8
3.4.1 Connection cache settings for ODBC driver	8
3.4.2 Connection cache settings for Oracle Native driver	9
3.4.3 Connection cache settings for SQL Server Native driver	10
3.4.4 Connection cache settings for Informix Native driver	11
3.5 Setting up transaction object to connection cache mapping	15
3.5.1 Dynamic transaction object to connection cache mapping	16
3.5.2 Static transaction object to connection cache mapping	17
3.6 Advanced configurations related with database connection	17
3.6.1 Application security	17
3.6.2 Apeon security	19
4 Configuring Apeon Server Load Balancing	21
4.1 Overview	21
4.2 Preparing environment	21
4.3 Configuring IIS Web server	21
4.3.1 Installing Apeon plug-in	21
4.3.2 Installing Apeon Server Web Component	26
4.3.3 Restarting IIS	26
4.4 Deploying application	26
5 Configuring Windows 2003 Network Load Balancing	27
5.1 Overview	27
5.2 Introduction to Windows 2003 Network Load Balancing	27
5.2.1 How Network Load Balancing Works	27

5.2.2 Scalability	27
5.2.3 Availability	27
5.2.4 Manageability	27
5.3 Operating System.....	28
5.4 Configuring Network Load Balancing	28
5.4.1 Creating a Network Load Balancing Cluster	28
5.4.2 Adding a Host	28
5.4.3 Configuring Port Rules	28
5.5 Important Information	29
5.6 Appendix	29
6 AEM User Guide	31
6.1 Introduction	31
6.1.1 Overview	31
6.1.2 AEM tools.....	31
6.2 Getting started.....	32
6.2.1 Running Apeon Server.....	32
6.2.2 Starting AEM.....	32
6.2.3 AEM Help.....	34
6.3 Server Properties	34
6.3.1 Overview	34
6.3.2 Active Sessions.....	35
6.3.3 Active Transactions.....	36
6.3.4 Web	36
6.3.5 Log Files	38
6.3.6 Log Viewer	40
6.3.7 Temporary Files Cleanup.....	41
6.3.8 Deployment Sessions	41
6.3.9 Connection Cache	42
6.3.10 Licensing.....	44
6.4 Application Properties	45
6.4.1 Overview	45
6.4.2 Basic Information	46
6.4.3 Transaction Objects	48
6.4.4 Charset	50
6.4.5 DataWindow Data Cache.....	56
6.4.6 Error Message Mode	59
6.4.7 Decimal Precision	60
6.4.8 Misc Settings.....	61
6.5 Security	64
6.5.1 Overview	64
6.5.2 AEM login.....	65
6.5.3 System Settings.....	66
6.5.4 Application Security	69
6.5.5 Group Management.....	71
6.5.6 User Management	73
6.5.7 Deployment Security.....	75
Index.....	77

1 About This Book

1.1 Audience

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

1.2 How to use this book

There are six chapters in this book.

Chapter 1: About This Book

A general description of this book

Chapter 2: Server Configuration Tasks

Describes configuration stages and tasks related to Appeon Server.

Chapter 3: Database Connection Setup

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

Chapter 4: Configuring Appeon Server Load Balancing

Describes how to implement Appeon Server load balancing.

Chapter 5: Configuring Windows 2003 Network Load Balancing

Describes how to implement Windows 2003 Network Load Balancing with Appeon Server.

Chapter 6: AEM User Guide

Describes how to configure Appeon Enterprise Manager 6.0.

1.3 Related documents

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

- *Appeon Demo Applications Tutorial*:

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

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

Provides instructions on how to use the Appeon Developer toolbar in Appeon 6.0.

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

- *Appeon Server Configuration Guide*

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

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

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

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

- *Appeon Installation Guide*:

Provides instructions on how to install Appeon for PowerBuilder successfully.

- *Appeon Migration Guide*:

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

- *Appeon Performance Tuning Guide*:

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

- *Appeon Troubleshooting Guide*:

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

- *Introduction to Appeon*:

Guides you through all the documents included in Appeon 6.0 for PowerBuilder.

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

Introduces new features and changes in Appeon 6.0 for PowerBuilder.

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

1.4 If you need help

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

2 Server Configuration Tasks

2.1 Overview

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

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

2.2 Scope of configurations discussed in this book

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

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

- IIS server configuration: configuring IIS server to work with Appeon Server.
- Configuration for supporting dynamic DataWindows: this one-time configuration at the database server enables dynamic DataWindows for all Appeon applications.
- Configuration for patching the ASE chained mode issue: this one-time configuration at the database server can patch the ASE chained mode issue for all Appeon applications.

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

2.3 Configuration stages and tasks

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

Table 2-1: Sever configuration stages

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

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

2.3.1 Configuration during application deployment

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

Table 2-2: Configuration tasks during application deployment

Task	Description	See section
(In AEM) Connection Cache	Establish the database connection between the Apeon Server and the database server by configuring connection caches (also called data sources).	6.3.9
(In AEM) Basic Information	Display PowerBuilder version, application size, DLL/OCX file size, run mode, application server cache size, and cache usage.	6.4.2
(In AEM) Transaction Object	Set up static mapping between application transaction objects and connection caches (or data sources).	6.4.3
(In AEM) Charset	Specify the input charset and database charset to ensure characters in applications display correctly.	6.4.4
(In AEM) Decimal Precision	Select a proper decimal precision for the Web application.	6.4.7
(In AEM) DLL/OCX Files Download	Configure the mode for installing and downloading DLL and OCX files used in an application.	6.4.8.e
(In AEM) Registry Mode	Enable Web applications to directly access the client machine Windows registry or use Apeon registry emulation, so that PowerBuilder registry functions will work properly.	6.4.8.c
(In AEM) INI File Mode	Make Web applications manipulate the INI files at the client or by Apeon emulation, so that INI file function will work properly.	6.4.8.d

(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.	6.4.6
-----------------------------	--	-----------------------

2.3.2 Configuration during debugging

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

Table 2-3: Configuration tasks during debugging process

Task	Description	See section
(In AEM) Log Files	Set the log file generation mode.	6.3.5
(In AEM) Log Viewer	View the log files generated by Apeon Server.	6.3.6
(In AEM) Run Mode	Set the run mode for Web applications.	6.4.2.a

2.3.3 Configuration during security management

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

Table 2-4: Configuration tasks during security management

Task	Description	See section
Database security	Implement script-coded and database security for applications	3.6.1.a
(In AEM) AEM Login	Modify the AEM user name and password.	6.5.2
(In AEM) System Settings	Set the system security mode and type.	6.5.3
(In AEM) Application Security	Limit the accessibility of an Apeon application to selected groups.	6.5.4
(In AEM) Group Management	Create groups and grant access rights.	6.5.5
(In AEM) User Management	Create user profiles and grant access rights.	6.5.6
(In AEM) Deployment Security	Limit the number of users permitted to deploy applications to Apeon Server.	6.5.7

2.3.4 Configuration during performance management

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

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

Table 2-5: Configuration tasks during performance management

Task	Description	See section
(In AEM) Active Sessions	Monitor all active sessions in the system. Some sessions can be killed if necessary.	6.3.2
(In AEM) Active Transactions	Monitor all active transactions in the system. Some active transactions can be killed if necessary.	6.3.3
(In AEM) Temporary Files Cleanup	Set the schedule for automatically clearing temporary files, or manually deleting temporary files.	6.3.7
(In AEM) Deployment Sessions	Monitor all active deployment sessions in the system. Some active deployment sessions can be killed if necessary.	6.3.8
(In AEM) Application Server Cache	Allocate server cache between deployed applications. Ensures that important applications are cached.	6.4.2.b
(In AEM) DataWindow Data Cache	Cache DataWindow data on the server and/or client to improve data-reading performance.	6.4.5
(In AEM) Multi-Thread Download	Download static resources with multi-threads to boost performance.	6.4.8.a
(In AEM) Transfer Encoding	Choose the proper encoding mode to reduce network traffic.	6.4.8.b

2.3.5 Configuration during server information management

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

Table 2-6: Configuration tasks during server information management

Task	Description	See section
(In AEM) Web	Set session timeout, transaction timeout, download timeout and receive timeout.	6.3.4
(In AEM) Licensing	View license information.	6.3.10

3 Database Connection Setup

3.1 Overview

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

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 Apeon Server. This refers to setting up Apeon Server connection caches.
- Setting up communication between the deployed application and Apeon Server. This refers to setting up the mapping between the application transaction objects and Apeon Server connection caches.

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 Apeon environment.

3.2 What is Apeon Server connection cache

Apeon Server connection cache is also called **Apeon Server data source** which is actually the same terminology as data source in Microsoft .NET Framework or other application servers.

The connection cache\data source for a Web application is the counterpart to the transaction object in the target PowerBuilder application. The transaction properties in the target PowerBuilder application contain database connection parameters, which should be correspondingly configured in connection caches. Apeon Web applications rely on Apeon Server connection caches to interact with the database servers.

3.3 Database Connection Types

Apeon for PowerBuilder .NET supports the following database connection types:

Table 3-1: Connection type

Connection Type	Supported Database Type and Version
ODBC	Sybase ASA 7.x/8.x/9.x/10.0 Sybase ASE 12.x/15.x
Oracle Native	Oracle 8i/9i/10g
SQL Server Native	Microsoft SQL Server 2000/2005
Informix Native	IBM Informix 9.x/10.x

3.4 Setting up Appeon Server connection caches

The following sections give a general description of the connection cache settings. For step-by-step instructions on how to set up Appeon Server connection caches, refer to Section 6.3.9: [Connection Cache](#).

3.4.1 Connection cache settings for ODBC driver

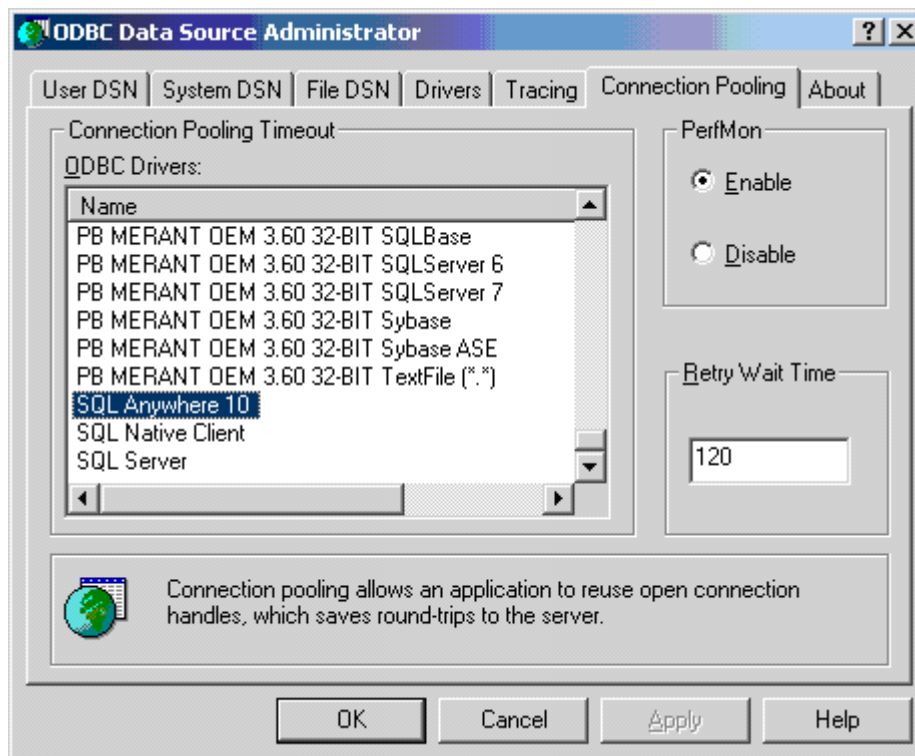
Appeon supports using ODBC driver to connect with ASA or ASE databases. Before you start creating a connection cache with ODBC driver, you must install the corresponding ODBC driver and create the ODBC data source by following the instructions in the relevant documents provided by the database vendor.

Table 3-2: Settings for ODBC driver

Connection Cache Name	Type the name of the connection cache.
Connection Type	Select “ODBC” to connect with Sybase ASA and Sybase 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.

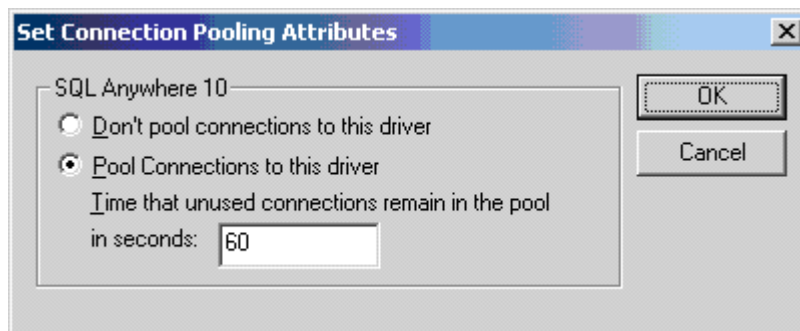
If the database is an ASA database, be aware of the following two points:

- If the ASA 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 connection cache may fail.
- Enable the connection pooling setting in ODBC driver, otherwise, the connection cache pools settings in AEM will not take effect, and the runtime performance of Web 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 10 from the ODBC Drivers list box, or any other driver you want, and double click it. Another window will pop up as following.

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



3.4.2 Connection cache settings for Oracle Native driver

Apeon supports using Oracle native driver to connect with Oracle databases. Before you start creating a connection cache with Oracle native driver, you must install Oracle Client. For detailed instructions, refer to the Oracle documents.

Table 3-3: Settings for Oracle native driver

Connection Cache Name	Type the name of the connection cache.
Connection Type	Select “Oracle Native” to connect 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 connection cache may fail.

3.4.3 Connection cache settings for SQL Server Native driver

Apeon supports using SQL server native driver to connect with SQL server databases.

Table 3-4: Settings for SQL Server native driver

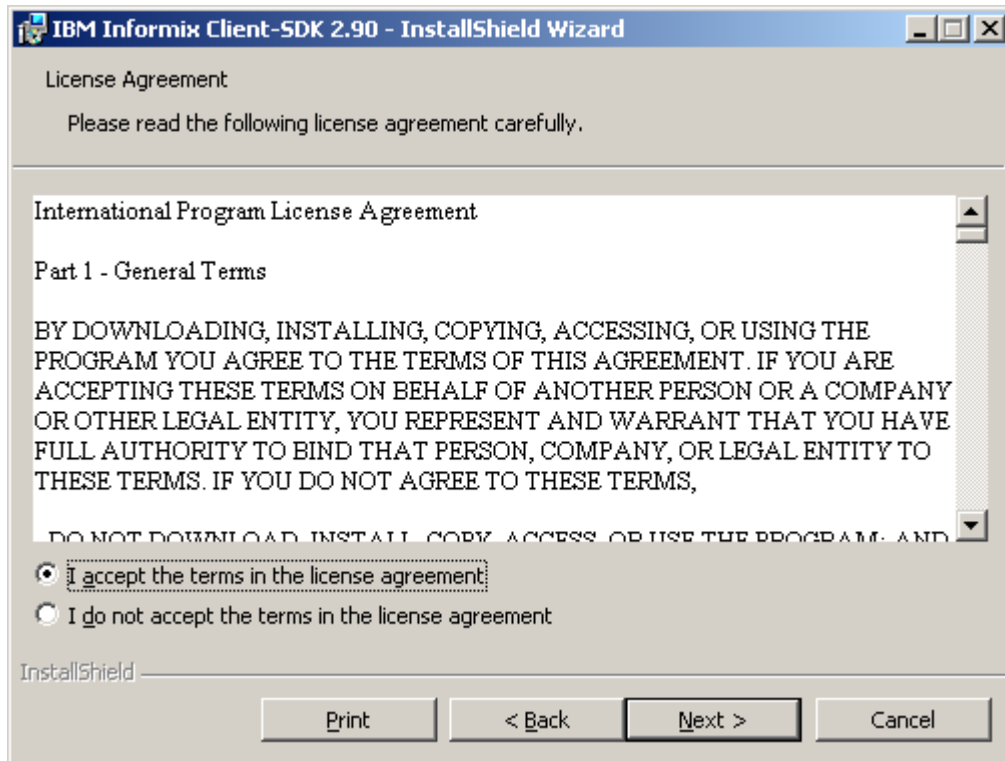
Connection Cache Name	Type the name of the connection cache.
Connection Type	Select “SQL Server Native” to connect Microsoft SQL Server databases.
Database Host	Specify the machine name or IP address of the database server.
Database Port	Specify the port number of the database server.
Database Name	Specify 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.

3.4.4 Connection cache settings for Informix Native driver

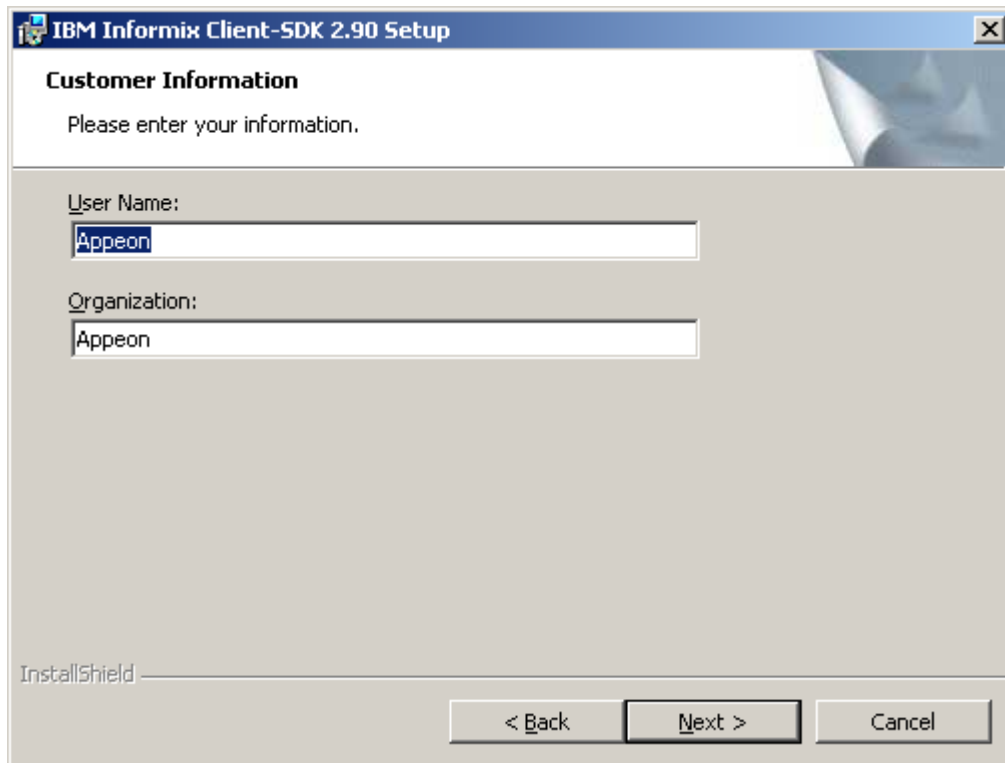
Apeon supports using IBM Informix NET Provider driver to connect with Informix databases. Before you start creating a connection cache with Informix NET Provider driver, you must install Informix Client (SDK 2.90 or above) and then use the installed client to configure Informix Server. For detailed instructions, refer to the Informix documents.

Following are important installation steps that are worth mentioning here:

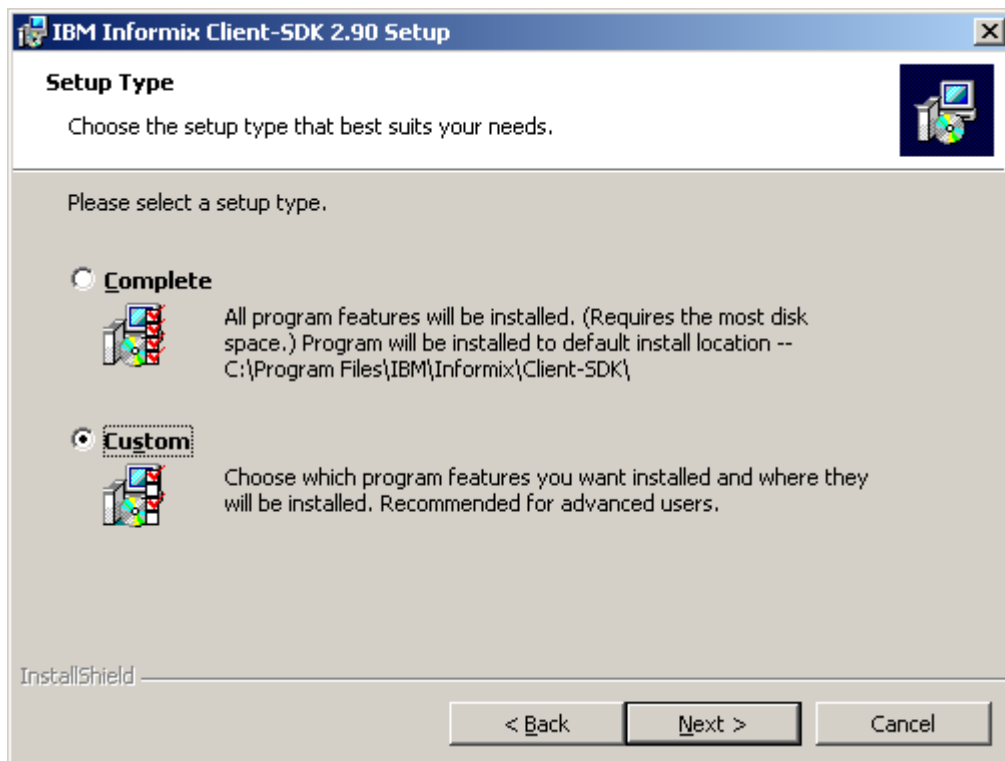
1) Accept the license agreement and click Next.



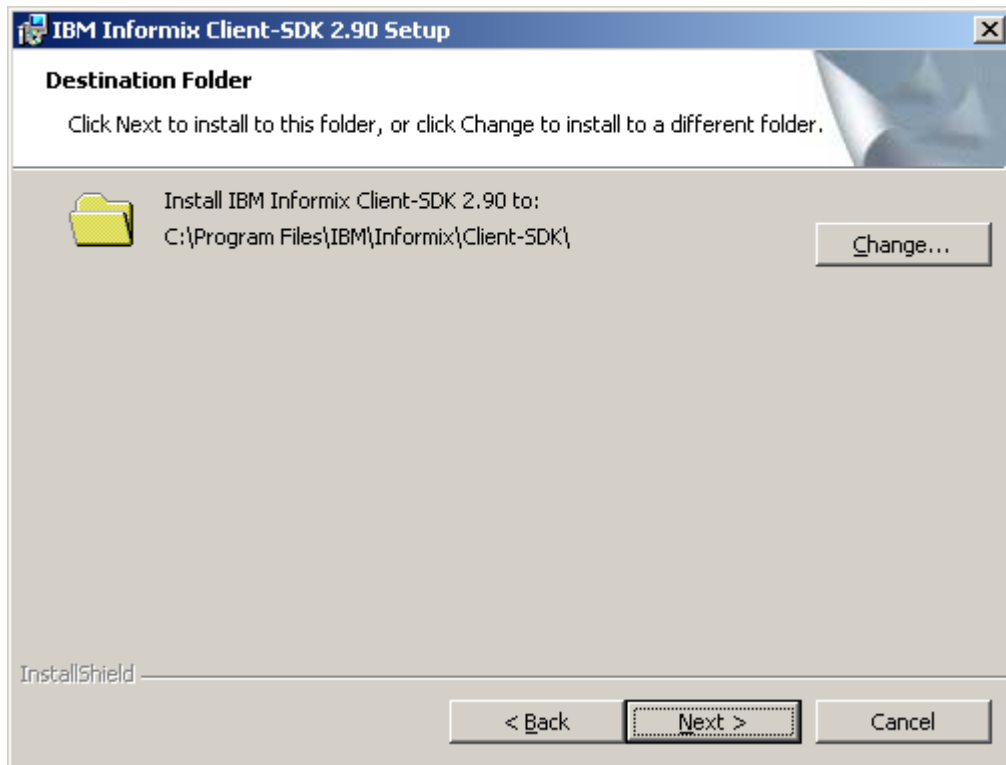
2) Input user name and organization name and click Next.



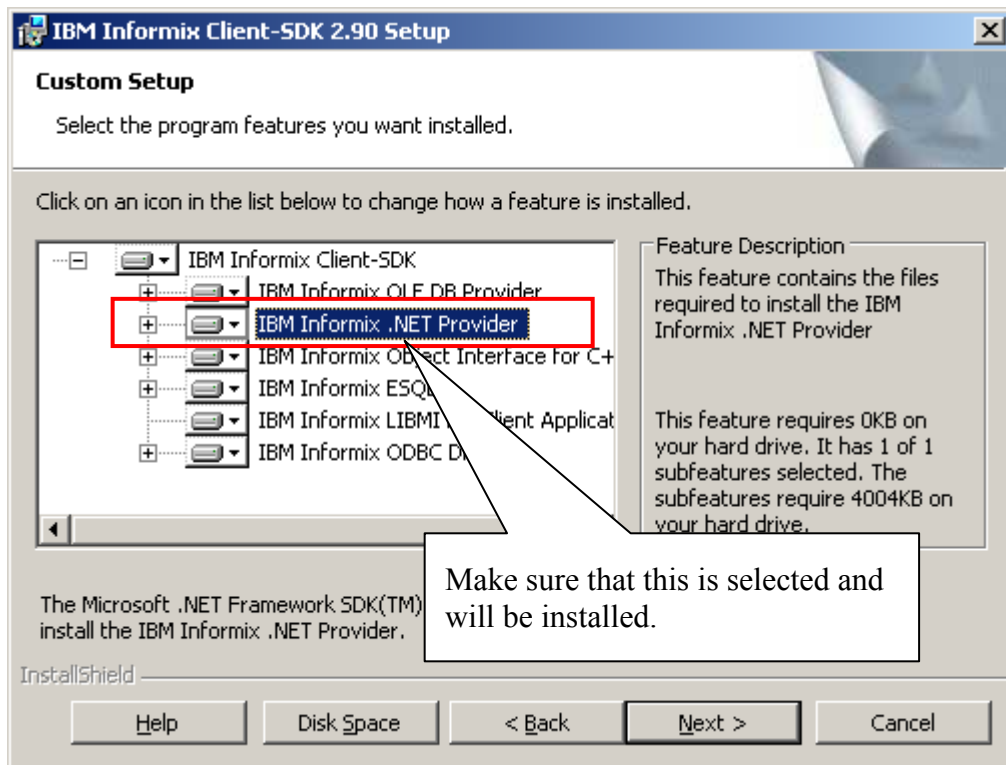
3) Select Custom installation type and click Next.



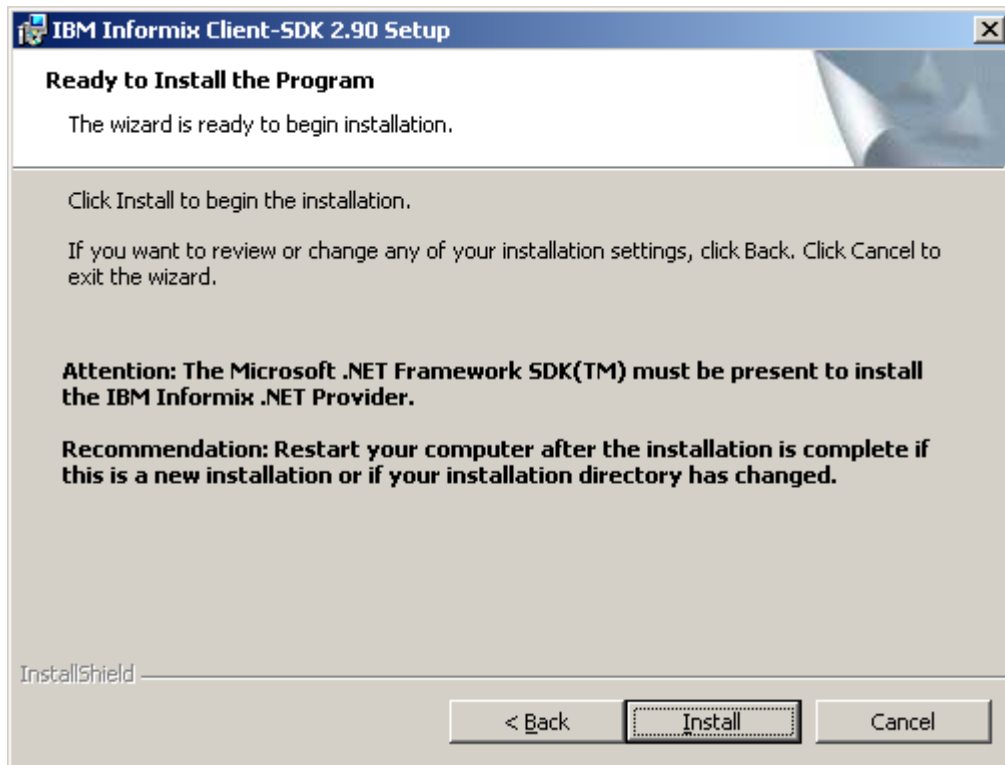
4) Select the installation directory for the driver and click Next.



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

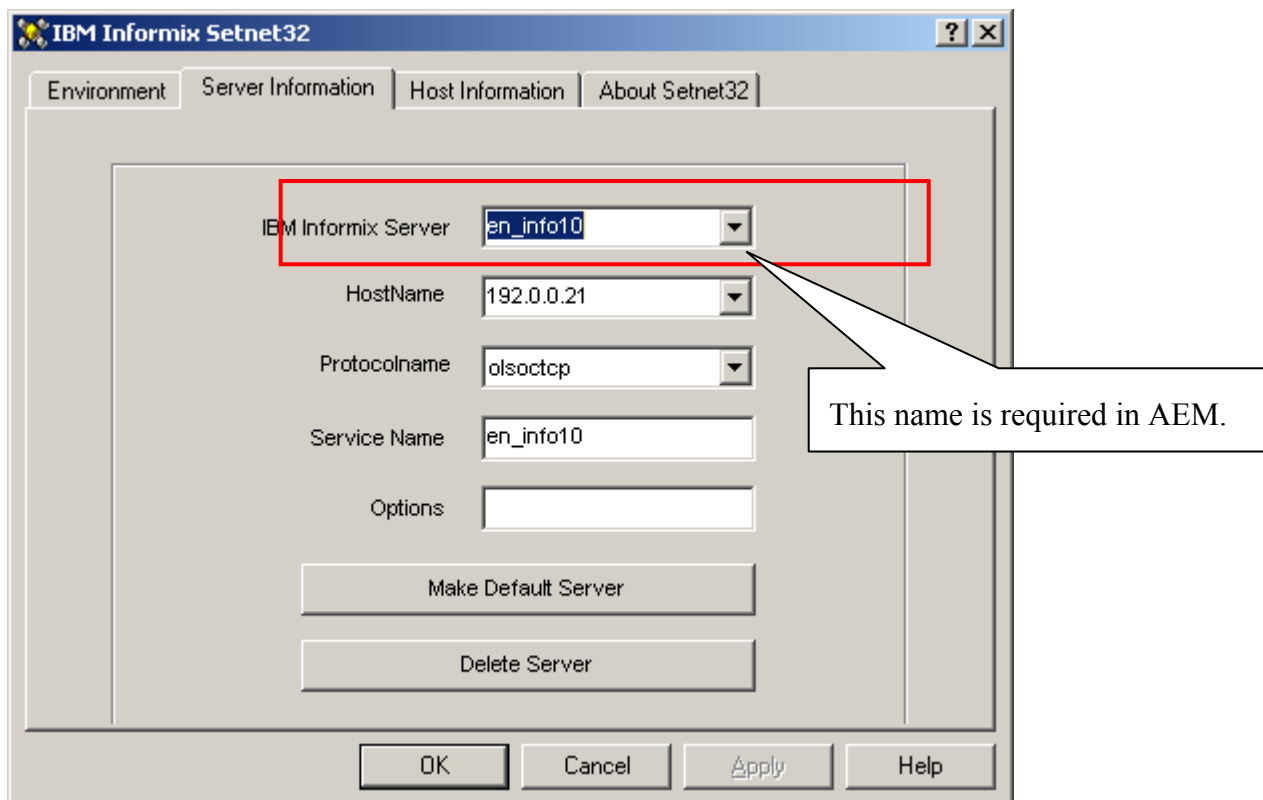


6) Click Install to start the installation.



Following are important configuration steps that are worth mentioning here:

- 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.



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:

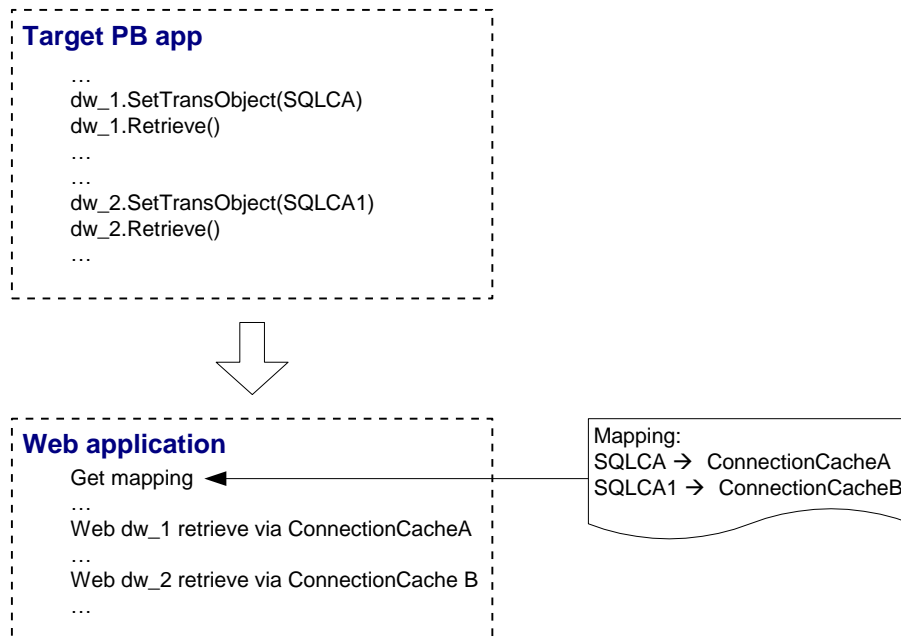
Connection Cache Name	Type the name of the connection cache.
Connection Type	Select “IBM Informix Native Driver”.
IBM Informix Server	Specify the Informix Server name. This must be the same name that is used to configure the Informix Server above.
Database Name	Specify the database name.
User Name	Type 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.

3.5 Setting up transaction object to connection cache mapping

The purpose of setting up the mapping is to make sure the configured connection cache can access the database server for the Apeon Web application as the replacement of the transaction object in the PowerBuilder application, as shown in Figure 3-1.

Figure 3-1: Map transaction to connection cache

Map Transaction to connection cache



Once Apeon Server connection caches are configured, you can set up the transaction object to connection cache mapping in two different ways:

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

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

3.5.1 Dynamic transaction object to connection cache mapping

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

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

```
SQLCA.DBParm="CacheName='ASAConnectionCache1' "
```

“ASAConnectionCache1” can be replaced by the name of the connection cache you want to use for the Transaction object.

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

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

The value of the DBMS property should be set based on the database type. Refer to Table 3-5.

Table 3-5: Setting the DBMS property based on the database type

Database Type	ODBC Interface	JDBC Interface	OLE Interface	Native Interface
MS SQL Server 2000/2005	ODB-MSS	JDB-MSS	OLE-MSS	MSS
Oracle8i	ODB-O84	JDB-O84	OLE-O84	O84
Oracle9i	ODB-O90	JDB-O90	OLE-O90	O90
Oracle10g	ODB-O10	JDB-O10	OLE-O10	O10
Sybase ASE12.X/15.x	ODB-SYC	JDB-SYC	OLE-SYC	SYC
Sybase ASA7/8/9/10	ODB-ASA	JDB-ASA	OLE-ASA	
Informix V9/V10	ODB-IN9	JDB-IN9	OLE-IN9	IN9

In Table 3-5:

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

If ODB or ODBC is set as the DBMS property, Apeon will regard the database type as Sybase ASA. The “odb-asa” and “odb-db2” are Apeon defined values. They can be recognized by Apeon 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 connection cache mapping

For an Apeon Web application, you can set up transaction object to connection cache mapping in the Application Properties settings in AEM. This is a static way for mapping the Transaction object to the connection cache. For detailed instructions, refer to Section 6.4.3: [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 Web conversion, the Apeon system provides an additional built-in layer of Web application security on top of PowerBuilder application security. Apeon security is “either-or”: the user either has or does not have access to the Web application.

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

In addition, a way to incorporate the Apeon user/group management for use with the coded security in PowerBuilder applications is discussed in Section 3.6.2.a. You can also implement your own Web security using other Web technologies.

3.6.1.a Database security

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

Apeon Web applications rely on the Apeon Server connection caches to interact with the Database Servers. In the Web application, transaction object to connection cache mapping can be dynamically set up or changed by setting or changing the DBMS and DBParm properties of the Transaction object in the application source code, or it can be statically set up in AEM database configuration. There is a limitation with connection cache configuration: the user ID and password of a connection must be pre-configured in AEM. 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.

Predefined connection caches

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

You should set up an equal number of connection caches in AEM that connect to the database with different privileges, and map the connection caches dynamically using the Transaction DBParm property to the PowerBuilder Transaction objects. Transaction object to connection cache mapping can be dynamically set up or changed by setting or changing the DBMS and DBParm properties of the Transaction object in the application source code. See Section 3.5.1: [Dynamic transaction object to connection](#) cache mapping for the details.

3.6.1.b Using INI files for connection security

You can set connection properties for a PowerBuilder application either by assigning values to the properties in the application script or using PowerScript Profile functions to read from an initialization (INI) file. It is recommended by Apeon 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: Apeon Developer deploys the INI files as XML to Apeon Server. When a Client accesses the deployed application that uses the INI file profiles, a copy of the original XML file is specially created and carries all the profile information of the Client. The cookie on the Client browser enables the Client to read the correct copy of its XML file located on Apeon Server.

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

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

If the same Windows user account profile will be used by multiple users on the Client, consider using another security method, Database security, as introduced in Section 3.6.1.a. [Database security](#).

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

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

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

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

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

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

3.6.2 Appeon security

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

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

For more information on using Appeon security features for Appeon Web applications, please refer to Section 6.5: [Security](#).

3.6.2.a Incorporate Appeon security in PowerBuilder code

If your PowerBuilder application has not coded user name/password verification at application startup that restricts access to the application, you can utilize Appeon’s built-in

user group management. When the Web application runs, the user is prompted to enter the Appeon Web user name and password in the Appeon Login Web dialog box.

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

3.6.2.b Database auditing

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

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

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 Configuring Appeon Server Load Balancing

4.1 Overview

You can install Appeon Server to a group of IIS servers and implement Appeon Server load balancing functionality using the Appeon plug-in. The Appeon plug-in distributes HTTP request to different Appeon Servers.

4.2 Preparing environment

- A group of Appeon Servers

Prepare a group of IIS 6 servers and install Appeon Server .NET to each server by following installation instructions in the *Appeon Installation Guide*.

The Appeon Servers host the AEM Web application (JSP) and the DataWindow syntax for the Web application.

Make sure that the AEM on each Appeon Server can be logged in with the same user name and password, because the Appeon Server, which hosts AEM, is selected randomly or sequentially.

- One Web server

Prepare one IIS 6 server, install Appeon Server Web Component and Appeon plug-in to the server, and configure the Web server to distribute requests to different Appeon Servers in a random or sequence order. Detailed instructions are provided in the following sections.

The Web server hosts the presentation layer of the Web application and Appeon Server Web Component; receives user requests from the Client PC; and dispatches them to the Appeon Server.

If you use an Appeon Server as the Web server, make sure the ports used by the Appeon Server and the Web server are different.

- One Appeon Developer

Prepare one machine and install Sybase PowerBuilder and Appeon Developer by following the installation instructions in the *Appeon Installation Guide*.

The Appeon Developer uploads the Web files to the Web server and the database syntax to the Appeon Servers.

4.3 Configuring IIS Web server

The following sections will focus on configuring the Web server and Appeon plug-in to implement load balancing. All mentions of "IIS", if not distinguished explicitly, indicate the Web server.

4.3.1 Installing Appeon plug-in

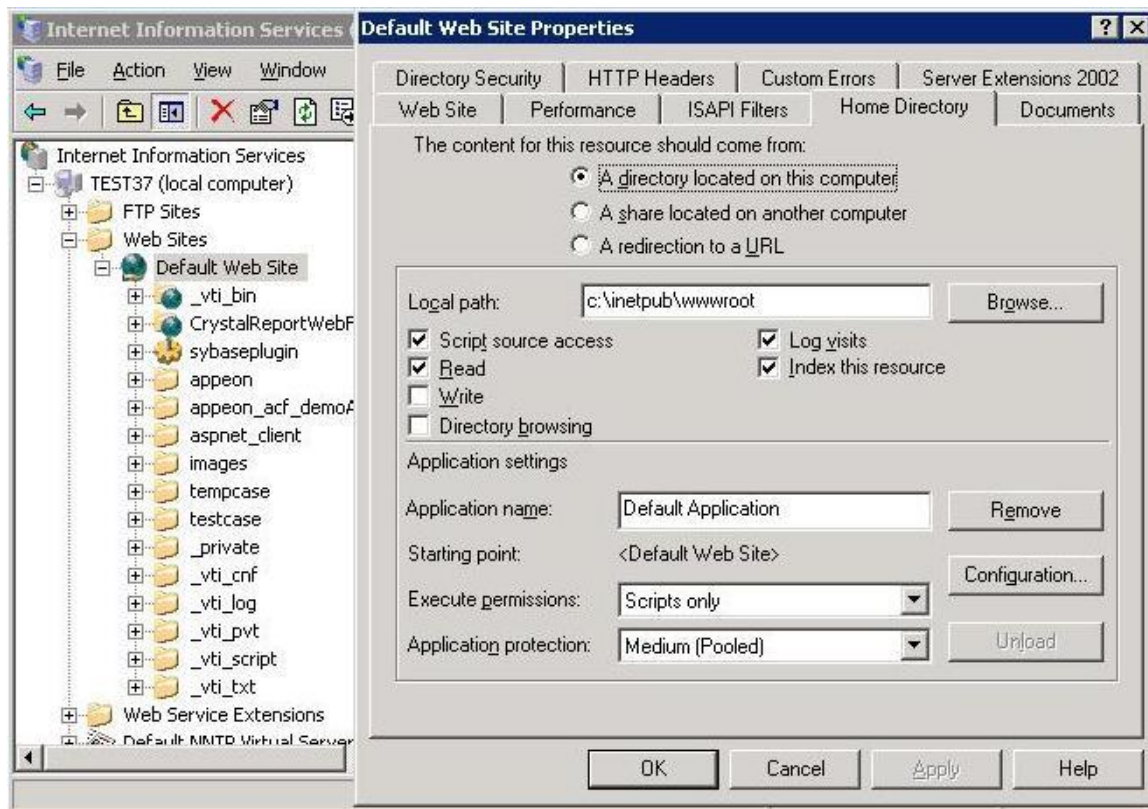
4.3.1.a Configuring IIS Web site

Step 1 – Select an existing IIS Web site or create a new Web site. The Default Web Site will be used as examples in the following steps.

Step 2 – Right click the Default Web Site and select Properties.

Step 3 – In the Default Web Site Properties window, select the Home Directory tab and set the Execute permissions to “Scripts only”.

Figure 4-1: Default Web Site Properties



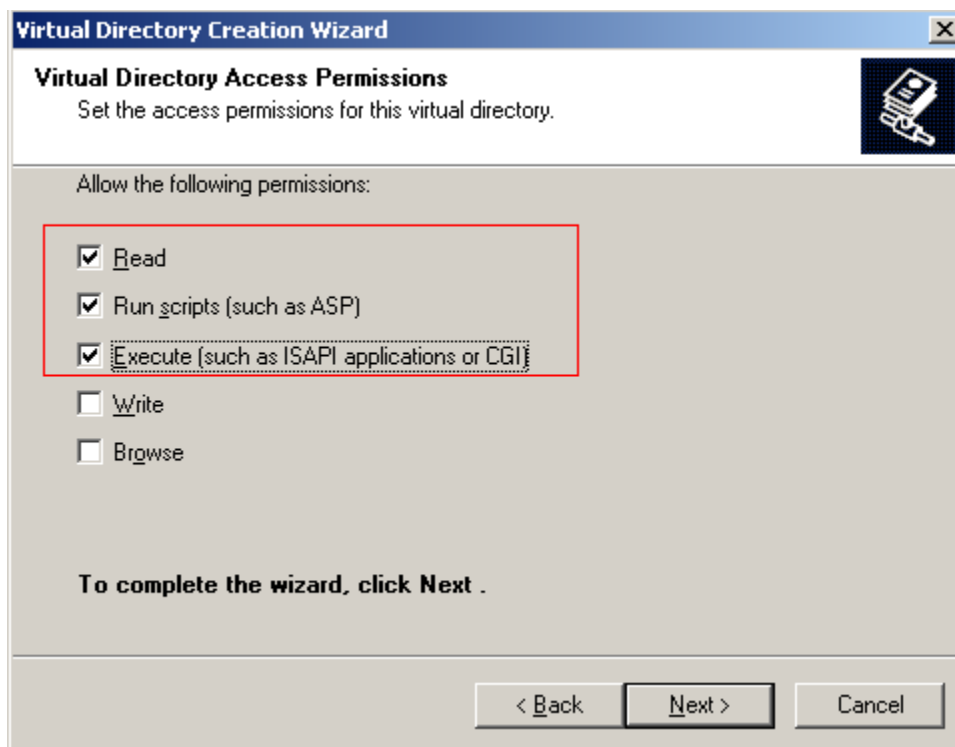
4.3.1.b Creating virtual directory

Step 1 – Right click the Default Web Site and select New | Virtual Directory.

Step 2 – Input the alias name (“ApbCluster” in this example), and select a mapping directory (“d:\iisplugin” in this example).

Step 3 – Allow the following permissions to the mapping directory: Read, Run scripts (such as ASP), and Execute (such as ISAPI application or CGI)

Figure 4-2: Create virtual directory



4.3.1.c Copying Appeon plug-in

Copy the plug-in “ApbCluster.dll” to the newly created virtual directory (“d:\iisplugin” in this example).

ApbCluster.dll resides in the %appeon%\plugin\IIS directory on the Appeon Server machine. You can get it from any machine with Appeon Server .NET installed.

4.3.1.d Editing configuration file

Step 1 – Copy the configuration file “cluster-config.xml” to the newly created virtual directory (“d:\iisplugin” in this example).

cluster-config.xml resides in the %appeon%\plugin\IIS directory on the Appeon Server machine. You can get it from any machine with Appeon Server .NET installed.

Step 2 – Modify the following information in the cluster-config.xml file: Appeon Server IP address, Appeon Server port number, and load balancing algorithm.

```
<?xml version="1.0" encoding="UTF-8"?>
<cluster-config arithmetic="1">
  <app-servers>
    <app-server host="IP_1" port="PORT_1"/>
    <app-server host="IP_2" port="PORT_2"/>
    <app-server host="IP_n" port="PORT_n"/>
  </app-servers>
</cluster-config>
```

Notes:

arithmetic="0" indicates that the random algorithm is used; *arithmetic="1"* indicates that the round-robin algorithm is used.

host indicates the IP address (recommended) or machine name of the Appeon Server.

port indicates the port number of the Appeon Server.

4.3.1.e Installing IIS filter

Step 1 – Right click the Default Web Site and select Properties.

Step 2 – In the Default Web Site Properties window, select the ISAPI Filters tab. Click Add and specify ApbCluster.dll as the ISAPI filter. Click OK.

4.3.1.f Creating redirector configuration file

Create the redirector configuration file (“ApbCluster.cfg” in this example) under the directory d:\iisplugin and copy the following commands to the file:

```
Extension_URI=/ApbCluster/ApbCluster.dll
MatchExpression=/AEM
MatchExpression=/servlet
Log=On
```

Notes:

The *Extension_URI* command points to the virtual directory where ApbCluster.dll resides (/ApbCluster/ApbCluster.dll in this example).

The *MatchExpression* command specifies the pages to be redirected.

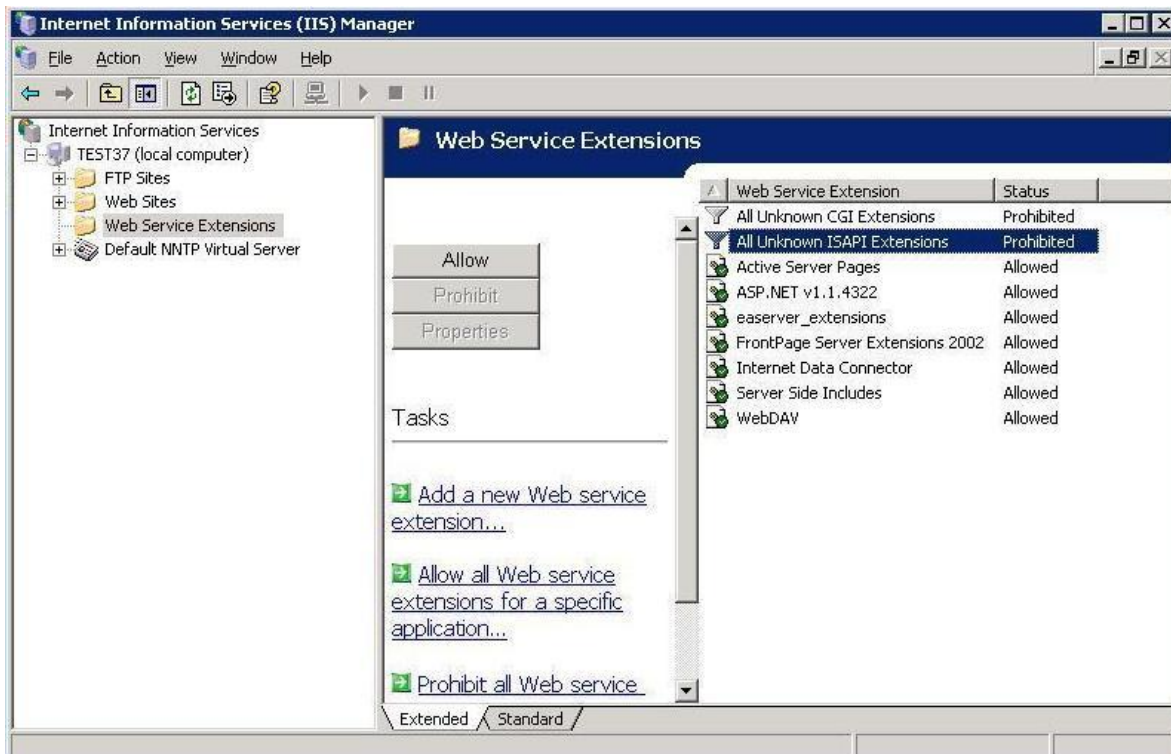
The *Log* command specifies whether logging is enabled. On indicates logging is enabled; Off indicates logging is disabled.

The commands and parameters are case insensitive.

4.3.1.g Activating ISAPI

Step 1 – Select the Web Services Extension. The ISAPI status will be displayed on the right.

Step 2 – Select “All Unknown ISAPI Extensions” and click the Allow button.

Figure 4-3: Web service extensions**4.3.1.h Adding new MIME type**

Step 1 – Right click the “local computer” and select Properties.

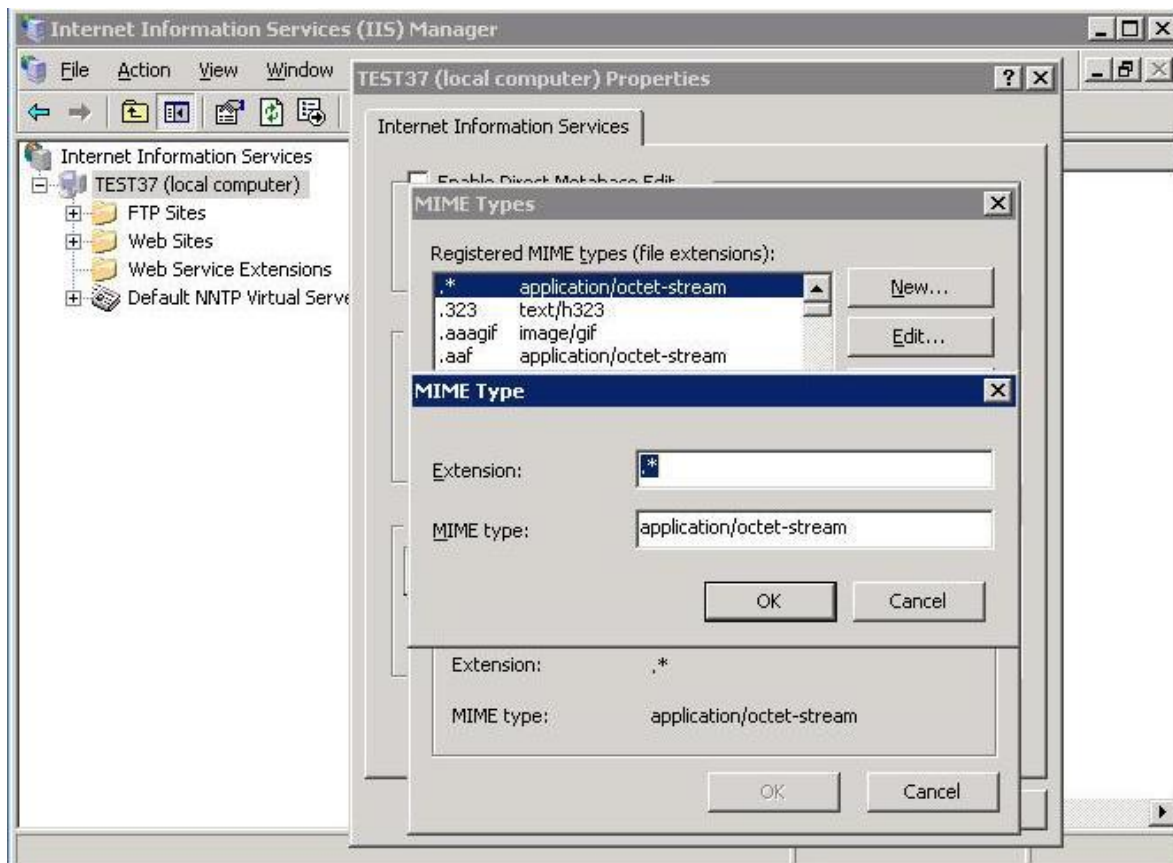
Step 2 – In the properties window, click the MIME Types button. In the MIME Types window, click New.

Input the following information:

Extension: *

MIME type: application/octet-stream

This is to ensure that pages without extension names or pages without MIME types defined can be accessed.

Figure 4-4: Add new MIME type

4.3.2 Installing Apeon Server Web Component

Step 1 – Create an “apeon” folder under the directory of the Web Site on the Web server (Default Web Site in this example).

Step 2 – Copy the entire “weblibrary_ax” folder from the Apeon Server installation directory on any Apeon Server machine to the “apeon” folder on the Web server.

4.3.3 Restarting IIS

Restart IIS Web server to make the changes take effect.

4.4 Deploying application

Deploy the application to the Web server and all Apeon Servers.

Notes:

- 1) When configuring the Apeon Server profile, be sure to create an Apeon Server profile for each Apeon Server implementing load balancing.
- 2) When configuring the deployment profile, be sure to select all Apeon Server profiles and the Web server profile.

For detailed instructions, refer to the *Apeon Developer User Guide*.

5 Configuring Windows 2003 Network Load Balancing

5.1 Overview

Besides using Apeon plug-in to implement load balancing with Apeon Server, you can also take advantage of the Windows 2003 Network Load Balancing feature to further improve the load balancing functionality of Apeon Server.

Be aware that the Windows 2003 Network Load Balancing feature is not automatically enabled. You can refer to the Windows 2003 help file for how to enable and configure this feature, or refer to the following sections which contain only the necessary configuration and the important information related with Apeon.

5.2 Introduction to Windows 2003 Network Load Balancing

Network Load Balancing provides high availability and scalability of servers using a cluster of two or more host computers working together.

5.2.1 How Network Load Balancing Works

Network Load Balancing delivers scaled performance by distributing the incoming network traffic among one or more virtual IP addresses (the cluster IP addresses) assigned to the Network Load Balancing cluster. The hosts in the cluster then concurrently respond to different client requests, even multiple requests from the same client. For example, a Web browser might obtain each of the multiple images in a single Web page from different hosts within a Network Load Balancing cluster. This speeds up processing and shortens the response time to clients. Network Load Balancing delivers high availability by redirecting incoming network traffic to working cluster hosts if a host fails or is offline.

5.2.2 Scalability

- Load balances requests for individual TCP/IP services across the cluster.
- Supports up to 32 computers in a single cluster.
- Load balances multiple server requests, from either the same client, or from several clients, across multiple hosts in the cluster.

5.2.3 Availability

- Automatically detects and recovers from a failed or offline computer.
- Automatically balances the network load when hosts are added or removed.

5.2.4 Manageability

- You can manage and configure multiple Network Load Balancing clusters and the cluster hosts from a single computer using Network Load Balancing Manager.
- You can specify the load balancing behavior for a single IP port or group of ports using port management rules.

5.3 Operating System

All operating systems as below support Network Load Balancing but it is highly recommended to keep the operating system consistent for all hosts in the same Network Load Balancing cluster.

- Microsoft® Windows Server™ 2003 Standard Edition
- Microsoft® Windows Server™ 2003 Enterprise Edition

5.4 Configuring Network Load Balancing

5.4.1 Creating a Network Load Balancing Cluster

- Open **Network Load Balancing Manager** (Windows Start → Control Panel → Management Tools).
- Right-click Network Load Balancing Clusters, and then click **New Cluster**.
- Enter the cluster's IP address and other cluster information and click **Next**. Please refer to the [Appendix](#) to learn which mode you should select for the cluster.
- If necessary, add appropriate port rules and then click **Next**.
- Type the name of a host that will be a member of your cluster and click **Connect**. After you click **Connect** the network adapters that are available on the host that you typed will be listed at the bottom of the dialog box. Click the network adapter that you want to use for Network Load Balancing and then click **Next**. The IP address configured on this network adapter will be the dedicated IP address for this host.
- Configure the remaining host parameters as appropriate, and then click **Finish**.

5.4.2 Adding a Host

- Open **Network Load Balancing Manager** and connect to the cluster.
- Right-click the cluster where you want to add the host and choose **Add Host To Cluster**.
- Enter the host's name and click **Connect**.
- After you click **Connect** the network adapters that are available on the host that you typed will be listed at the bottom of the dialog box. Click the network adapter that you want to use for Network Load Balancing and then click **Next**. The IP address configured on this network adapter will be the dedicated IP address for this host.
- Configure the remaining host parameters as appropriate, and then click **Finish**.
- Add additional hosts as needed.

5.4.3 Configuring Port Rules

- Open **Network Load Balancing Manager** and connect to the cluster.
- Right-click the cluster and then click **Cluster Properties**.
- Click the **Port Rules** tab.
- In the Defined port rules list, click a rule then click **Edit**.

- Select “Multiple Hosts” for the Filtering Mode, select “Single” for the Affinity, and then click OK.

Note: It is recommended to set the same password for Administrator of each node in the cluster for easy management.

5.5 Important Information

- If you are working from a computer that has a single network adapter that is bound to Network Load Balancing in unicast mode, you cannot use Network Load Balancing Manager on this computer to configure and manage other hosts because in unicast mode intrahost communication cannot take place. However, the computer will have no problem to communicate with any other hosts outside of the cluster.
- Ensure that all hosts in a cluster belong to the same subnet and that the cluster's clients are able to access this subnet.
- Network Load Balancing does not support a mixed unicast/multicast environment within a single cluster. Within each cluster, all network adapters in that cluster must be either multicast or unicast; otherwise, the cluster will not function properly.
- The Single option specifies that Network Load Balancing should direct multiple requests from the same client IP address to the same cluster host. This is the default setting for affinity and is also REQUIRED by Apeon Server.
- To properly balance the incoming traffic, Network Load Balancing requires that the network adapter supports the NDIS packet indications.

5.6 Appendix

Network Load Balancing can be configured using one of four different models as below.

NLB Model	Usage Scenario	Advantages	Disadvantages
Single Network Adapter in Unicast Mode (Unicast is set as default Filtering Mode)	This model is suitable for a cluster in which ordinary network communication among cluster hosts is not required and in which there is limited dedicated traffic from outside the cluster subnet to specific cluster hosts.	Only one network adapter is required. It is not necessary to install a second adapter. This model works with all routers.	Ordinary network communication among cluster hosts is not possible. Network Load Balancing itself does not affect network performance and a second network adapter is not a requirement. However, under certain conditions, a second adapter can improve overall network performance.
Multiple Network Adapters in Unicast Mode (Unicast is set as default Filtering Mode)	This model is suitable for a cluster in which ordinary network communication among cluster hosts is necessary or desirable. It is also appropriate when you want to separate the traffic used to manage the cluster from the traffic	Ordinary network communication among cluster hosts is permitted. This model works with all routers.	This model requires a second network adapter.

	occurring between the cluster and client computers.		
Single Network Adapter in Multicast Mode	This model is suitable for a cluster in which ordinary network communication among cluster hosts is necessary or desirable but in which there is limited dedicated traffic from outside the cluster subnet to specific cluster hosts.	Only one network adapter is required. This model permits ordinary network communication among cluster hosts.	Network Load Balancing itself does not affect network performance and a second network adapter is not a requirement. However, under certain conditions, a second adapter can improve overall network performance. Some routers might not support the use of a multicast media access control (MAC) address. This only affects the Network Load Balancing/MAC address (not all MAC addresses) and only when dynamic ARP replies are sent by the cluster to the router, not all MAC addresses.
Multiple Network Adapters in Multicast Mode	This model is suitable for a cluster in which ordinary network communication among cluster hosts is necessary and in which there is heavy dedicated traffic from outside the cluster subnet to specific cluster hosts.	Because there are at least two network adapters, overall network performance is typically enhanced. Ordinary network communication among cluster hosts is permitted.	Some routers might not support the use of a multicast media access control (MAC) address. This only affects the Network Load Balancing/MAC address (not all MAC addresses) and only when dynamic ARP replies are sent by the cluster to the router. not all MAC addresses.

6 AEM User Guide

6.1 Introduction

6.1.1 Overview

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

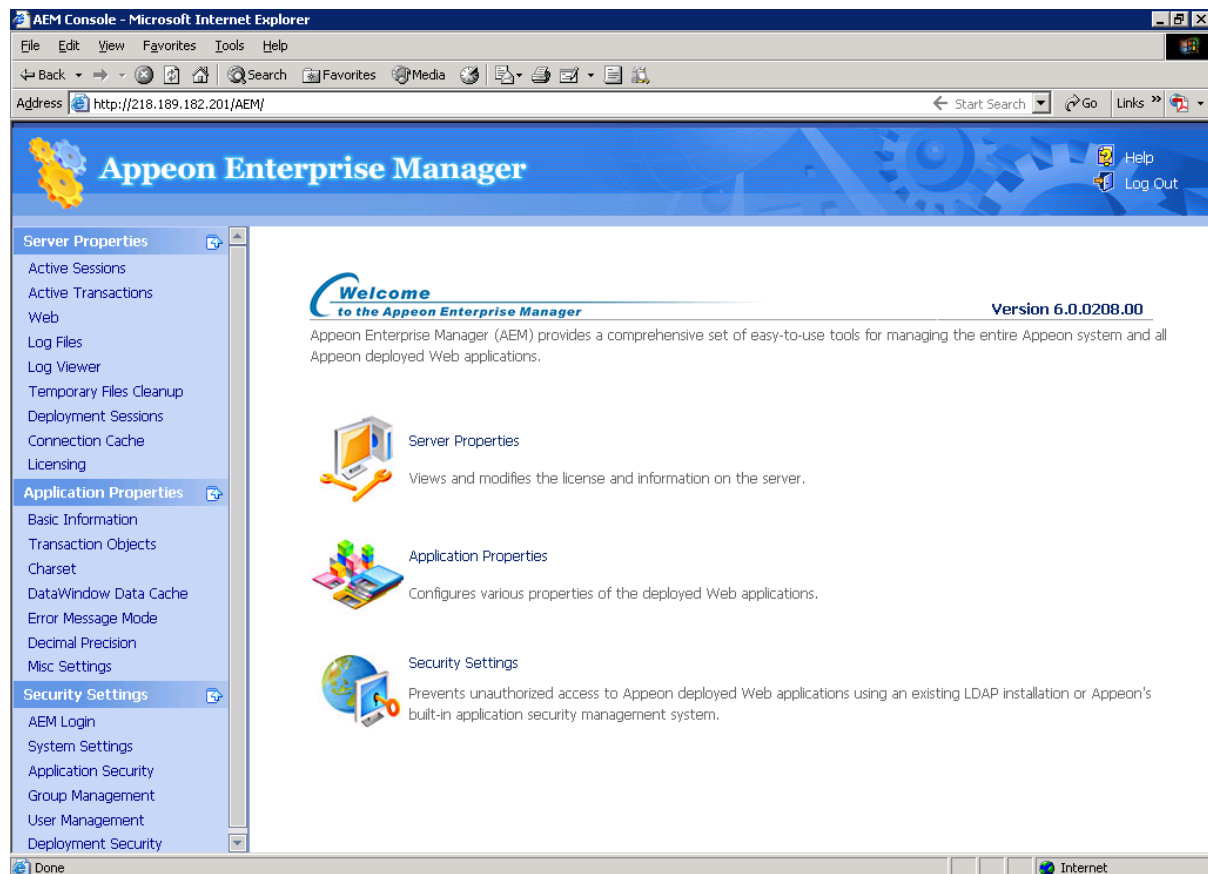
AEM provides an additional layer of security to the existing security already coded into your PowerBuilder application. It also allows the administrator to use the built-in Apeon security management system or LDAP security (recommended) to control the access rights at the application level.

All the settings configured in AEM are saved to several XML files in the %apeonserver%\AEM\Log folder, where %apeonserver% stands for the Apeon Server installation directory, for example, C:\Inetpub\wwwroot\apeon\AEM\Log.

6.1.2 AEM tools

AEM contains three sets of tools: Server Properties, Application Properties, and Security Settings. After login, you can access each tool either from the treeview window on the left or from the Welcome window on the right. Refer to Figure 6-1.

Figure 6-1: AEM Console

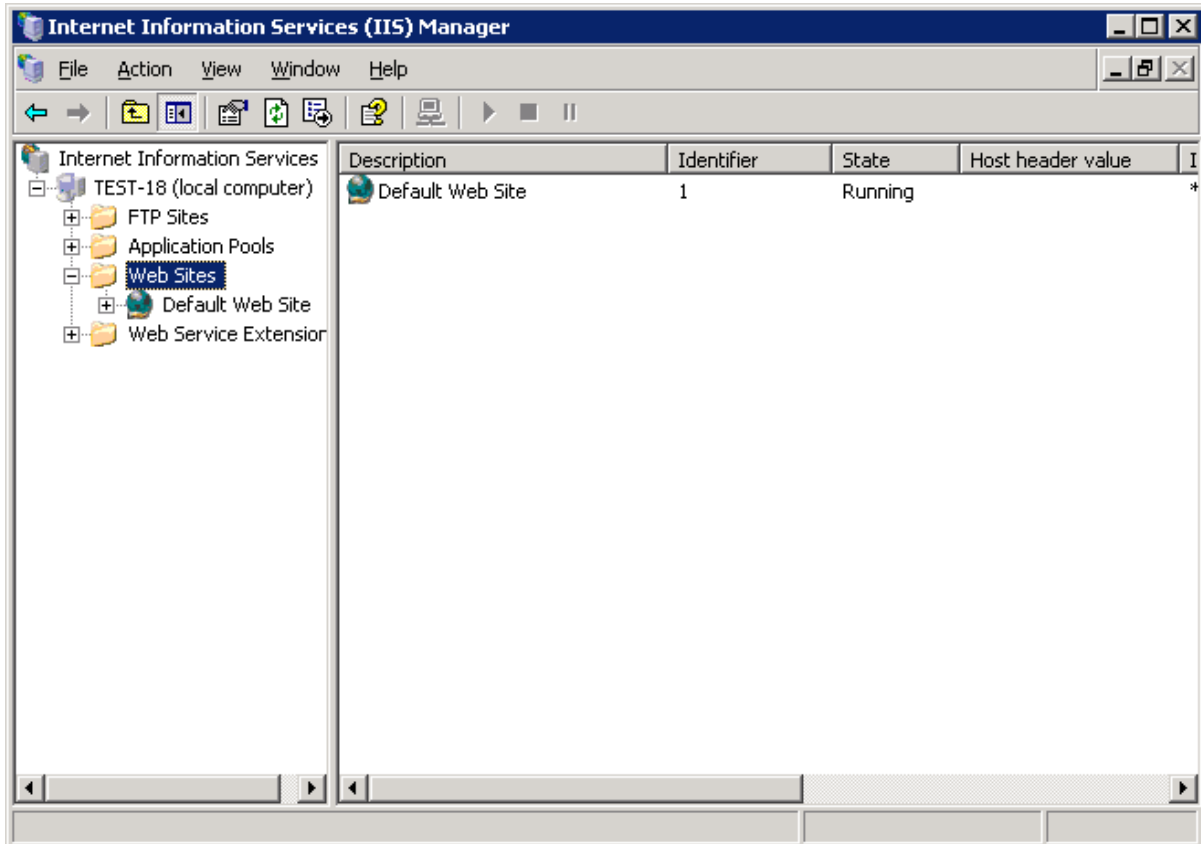


6.2 Getting started

6.2.1 Running Aepeon Server

Aepeon Server must be running before you start AEM.

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



6.2.2 Starting AEM

6.2.2.a AEM URL

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

During installation, you can specify the name and port for Aepeon Server. If you want to start AEM from the computer that hosts the Aepeon Server, 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.

6.2.2.b Three ways to launch AEM

There are three ways to launch AEM:

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

- On the computer where Appeon Server is installed, select *Programs / Appeon 6.0 for PowerBuilder / Appeon Server for .NET / Appeon Enterprise Manager* from the Windows Start menu.
- On the computer where Appeon Developer is installed, click the *AEM* button (🦋) in the Appeon Developer toolbar. Before doing this, ensure that the AEM URL has been configured correctly in Appeon Developer.

6.2.2.c AEM username and password

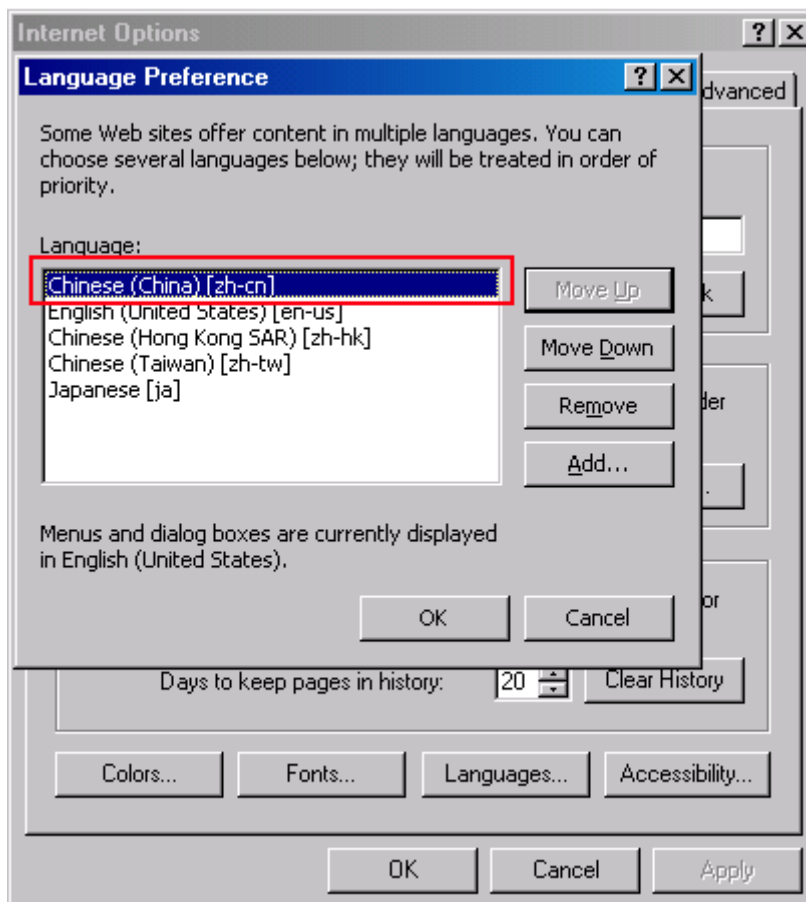
Enter a valid username and password for AEM. During the Appeon Server installation, you can specify the username and password. If you did not specify the username and password during the installation, you can use the default user name and password (both "admin") to log into AEM. For security purposes,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

6.2.2.d 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 Internet Explorer language settings. 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 content in simplified Chinese, select “Chinese (China) [zh-cn]” and move it to the top, as shown in Figure 6-2.

Figure 6-2: Language settings



6.2.3 AEM Help

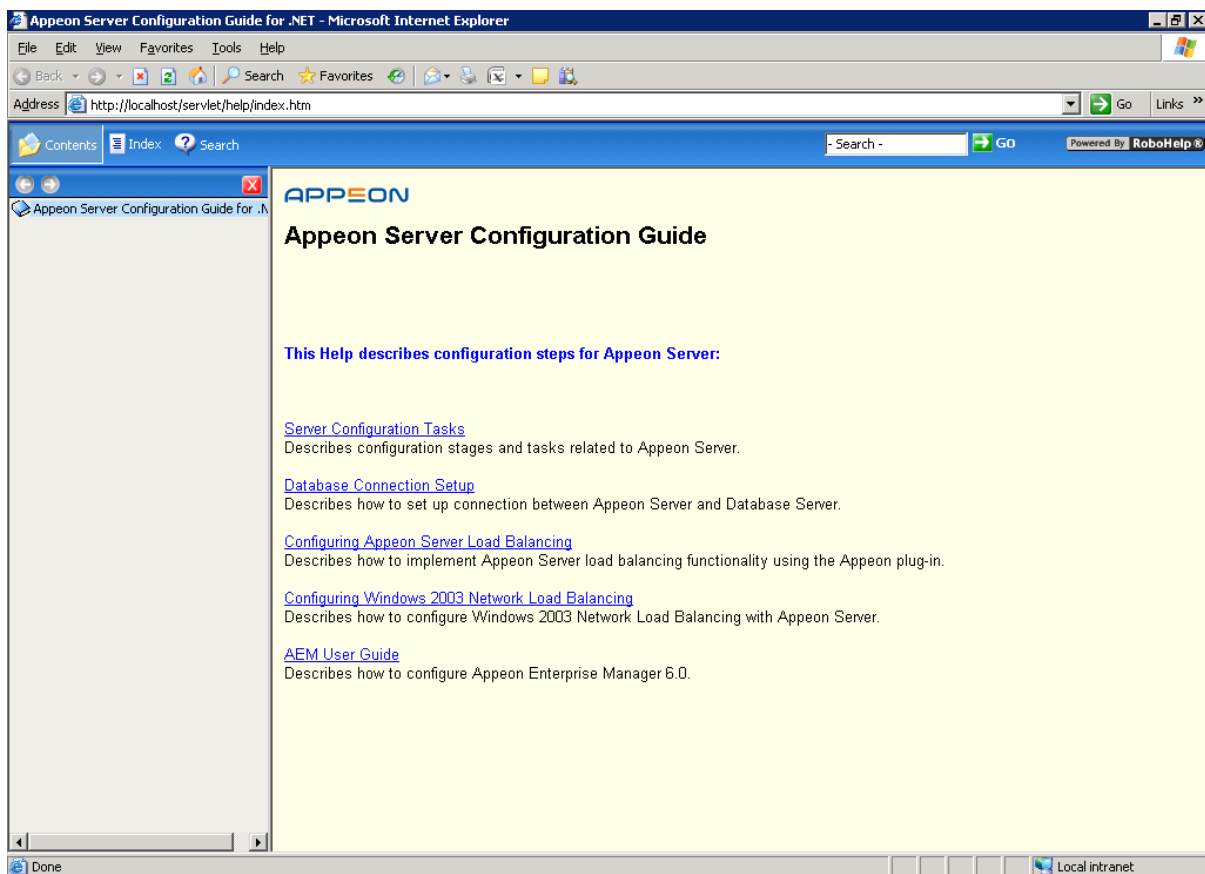
On the index of Apeon Enterprise Manager, the *Help* button provides easy access to AEM Help, as shown in Figure 6-3:

Figure 6-3: Help button



Click the Help button, find the topic on the left pane, and view the content on the right pane, as shown in Figure 6-4:

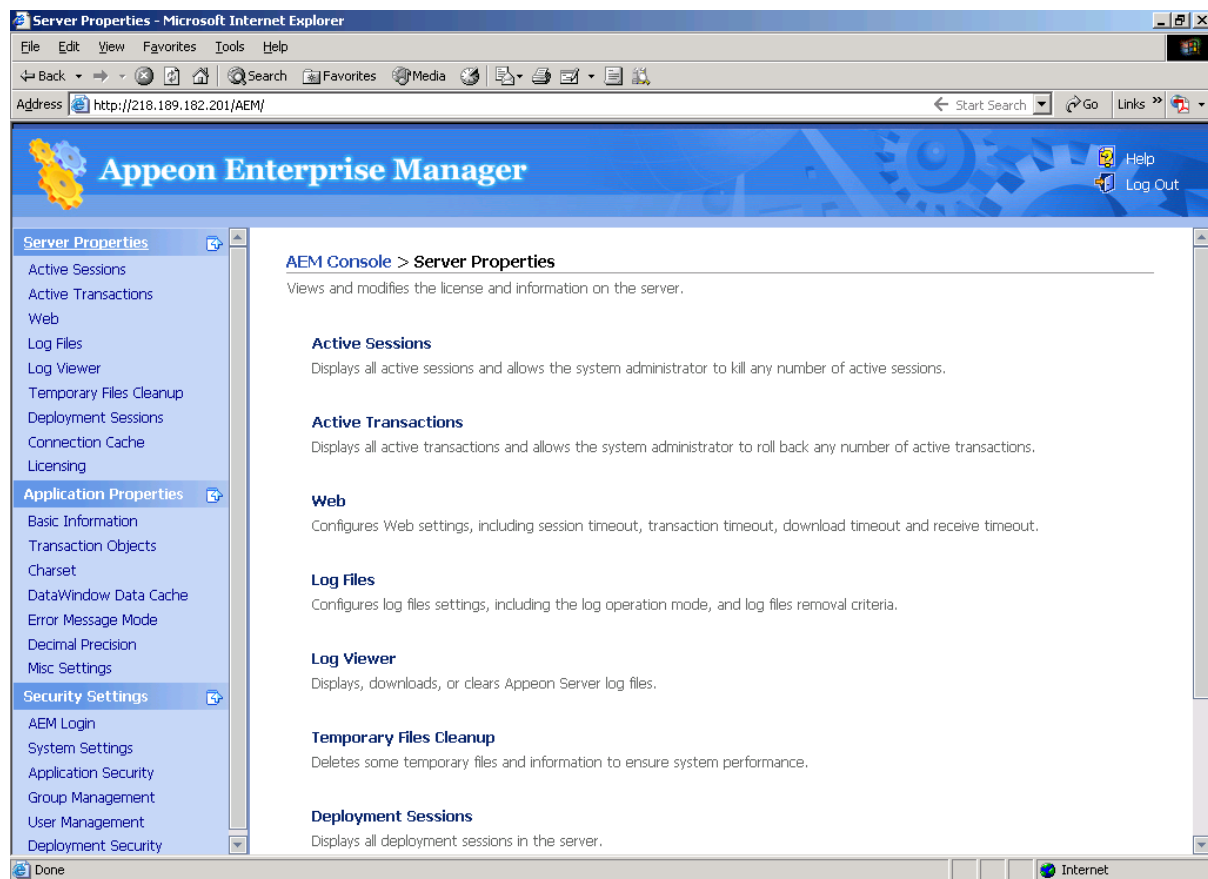
Figure 6-4: Apeon Help



6.3 Server Properties

6.3.1 Overview

Server Properties is a set of tools for viewing and modifying all configurable system settings. There are nine tools: Active Sessions, Active Transactions, Web, Log Files, Log Viewer, Temporary Files Cleanup, Deployment Sessions, Licensing and Connection Cache. Refer to Figure 6-5.

Figure 6-5: Server Properties

6.3.2 Active Sessions

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

Figure 6-6: Active Sessions

[AEM Console](#) > [Server Properties](#) > [Active Sessions](#)

Active Sessions				
Displays all active sessions and allows the system administrator to kill any number of active sessions.				
<input type="checkbox"/>	Session ID	User Name	IP Address	Application Name
<input type="checkbox"/>	1950125010		127.0.0.1	pet_world_ax
<input type="button" value="Kill"/>				

6.3.2.a Viewing active sessions

The Active Sessions table lists the current active sessions on the Apeon Server hosting AEM. You can sort the Active Sessions table by clicking any heading of the columns.

6.3.2.b Killing active session(s)

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

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

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

Step 2 – Click the *Kill* 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.

6.3.3 Active Transactions

The AEM Active Transactions tool helps you manage and monitor all active transactions on the system. Refer to Figure 6-7.

Figure 6-7: Active Transactions

[AEM Console](#) > [Server Properties](#) > [Active Transactions](#)

Active Transactions						
Displays all active transactions and allows the system administrator to roll back any number of active transactions.						
<input type="checkbox"/>	Transaction ID	Session ID	User Name	IP Address	Application Name	Process Time (s)
<input type="checkbox"/>	sqlca	1950125010		127.0.0.1	pet_world_ax	373
<input type="button" value="Rollback"/>						

6.3.3.a Viewing active transactions

The Active Transactions table lists the current active transactions on the Apeon Server hosting AEM. You can sort the Active Transactions table by clicking any heading of the columns.

6.3.3.b Rolling back active transaction(s)

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

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

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

Step 2 – Click the *Rollback* 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.

6.3.4 Web

The Web tool provides configuration for four important functions of Apeon Server for Web applications (refer to Figure 6-8):

- 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 receiving will timeout (Receive Timeout)

After making any changes to the configuration, remember to click the *Save* button.

Figure 6-8: Web tool in Server Properties

AEM Console > Server Properties > Web

Session Timeout	
Session timeout ends the user session and rolls back all database updates since the last commit for the user session. Setting the session timeout to "0" will disable the feature.	
Session Timeout:	<input type="text" value="3600"/> seconds
Transaction Timeout	
Transaction timeout rolls back all database updates since the last commit in the session. Setting the transaction timeout to "0" will disable the feature.	
Transaction Timeout:	<input type="text" value="0"/> seconds
Download Timeout	
Specifies a timeout value for file download. When the amount of time used for receiving data exceeds the specified value, an error message will pop up.	
Download Timeout :	<input type="text" value="3600"/> seconds
Receive Timeout	
Specifies a timeout value for receiving messages from the server after the client sends the request. When the amount of time used for receiving messages exceeds the specified value, an error message will pop up.	
Receive Timeout :	<input type="text" value="3600"/> seconds
<input type="button" value="Save"/>	

6.3.4.a Session timeout

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

- By default, the timeout period for a session is 3600 seconds.
- You can set a timeout interval that is shorter or longer than the default setting. The session timeout can be removed altogether by setting the timeout value to 0. This is not recommended because it will eventually exhaust system resources unless old sessions are manually cleared out using the Active Sessions functionality of AEM.

6.3.4.b Transaction timeout

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

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

- Database locking. When a Web application closes abnormally, the active transaction in it can neither commit nor roll back.
- Application locking. If an application is deadlocked, other applications cannot proceed.

6.3.4.c Download timeout

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

- By default, the timeout period for file download is 3600 seconds.
- You can set a timeout interval shorter or longer than the default setting. It is required to input a whole number within the range from 60 to 7200.

6.3.4.d Receive timeout

When Aepeon Server is running, the client will send protocols to the server. If the client sends a protocol but does not receive any protocol from the server during the timeout interval, a message will pop up asking if you want to keep on waiting.

- 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.

6.3.5 Log Files

Aepeon Server creates three different log files for record keeping and for future use in troubleshooting (Figure 6-9). You can view these log files using the Log Viewer tool or directly locate them in the %apeonserver%\AEM\Log folder.

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

- Log Mode
- Replace Log Files

Click the *Save* button to save changes.

Figure 6-9: Log Files

[AEM Console](#) > [Server Properties](#) > [Log Files](#)

Log Files Path
Aepeon Server log files are stored in the AEM\log directory of the Aepeon Server installation path.

Log Mode

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

Replace Log Files

- Never replace log files
- Replace log files.....
 - When size exceeds 2 MB
 - Every 1 days
 - Backup log files before replacing

Save

6.3.5.a Log mode

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

- Mode 1: Off

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

- Mode 2: Standard mode

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

- Mode 3: Developer mode

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

- Mode 4: Debug mode

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

6.3.5.b Replace log files

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

To configure log file settings:

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

- Option 1: Never replace log files

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

- Option 2: Replace log files ...

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

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

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

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

- Option 2: Replace log files every ___ days.

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 Aepeon Server to back up the log files before replacing them. If this option is checked, all log files are backed up before they are replaced so an archive of the log files is maintained. Maintaining this archive does not compromise

system performance, but there must be adequate hard disk space for the backup log files.

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

6.3.6 Log Viewer

The Log Viewer gives you direct access to the log files created by Aepeon Server.

Figure 6-10: Log Viewer

AEM Console > Server Properties > Log Viewer

Log Viewer			Log	Size (KB)
Actions				
View	Download	Clear	Server Log	0.00
View	Download	Clear	Error Log	0.00
View	Download	Clear	Deployment Log	0.00

Aepeon Server logs include:

- Server Log – Records messages logged from services and the core Aepeon Server runtime.
- Error Log – Records errors occurred on Aepeon Server.
- Deployment Log – Records interactions between Aepeon Server and Aepeon Developer during application deployments.

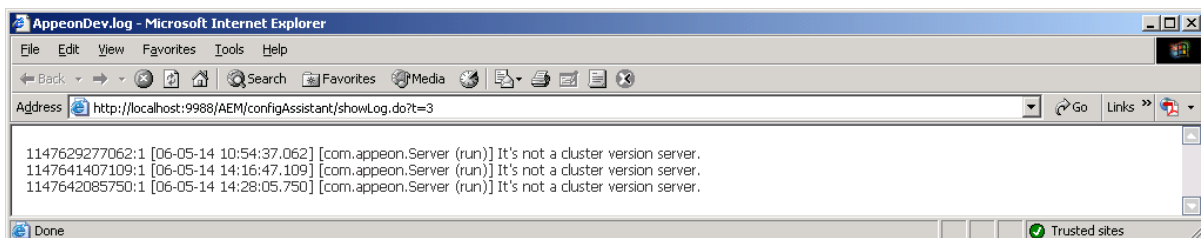
The Log Viewer tool provides the following manipulations:

- To view a log file

Click *View* to view the detailed information in the browser, as shown in Figure 6-10. The log file will be shown in a new window, as shown in Figure 6-11.

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 6-11: Deployment Log



- To download a log file

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

- To clear a log file

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

6.3.7 Temporary Files Cleanup

Temporary Files Cleanup helps you clean up the temporary registry and profile configuration files automatically or manually. Refer to Figure 6-12.

Figure 6-12: Temporary Files Cleanup

[AEM Console](#) > [Server Properties](#) > [Temporary Files Cleanup](#)

The screenshot displays two distinct sections for file cleanup. The first section, titled "Clean Up Periodically", features a text input field with the value "3" and a dropdown menu with the value "2", followed by the text "days" and "hours ago". Below this is a "Save" button. The second section, titled "Clean Up Now", contains a descriptive text "Clean up Aepeon mock registry and INI configuration files." and a "Clean Up Now!" button.

6.3.7.a Auto cleanup

To perform an auto-cleanup for temporary registry and profile configuration files in the “Cleanup Periodically” group box:

Step 1 – Specify cleanup time.

Specify a particular time based on which the temporary register and profile configuration files will be cleaned up. For example, "Clean up the temporary files created over 2 days 4 hours ago" denotes that all temporary register and profile configuration files that were created over 2 days and 4 hours ago will be cleaned up everyday.

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

6.3.7.b Manual cleanup

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

To perform a manual cleanup in the “Clean Up Now” group box:

Step 1 – Click the *Clean Up Now!* button to commit the cleanup.

The temporary registry and profile configuration files will be deleted immediately from the Aepeon Server hosting AEM.

6.3.8 Deployment Sessions

The Deployment Sessions tool can help you manage and monitor all the active deployment sessions on the system. Refer to Figure 6-13.

Figure 6-13: Deployment Sessions

[AEM Console](#) > [Server Properties](#) > [Deployment Sessions](#)

Deployment Sessions	
The currently active deployment sessions are listed. Each deployment session represents an Apeon Developer machine deploying an application to this Apeon Server. You may need to kill a deployment session if it terminates abnormally on the Apeon Developer machine.	
<input type="checkbox"/>	Deployment Session ID Application Name
Kill	

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

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

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

6.3.9 Connection Cache

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

Figure 6-14: Connection cache

[AEM Console](#) > [Server Properties](#) > [Connection Cache](#)

Connection Cache Settings		
Specifies the settings used to connect to the database at runtime.		
Actions	Connection Cache Name	Connection Type
edit delete Test Connection	appeonsample	ODBC Driver
edit delete Test Connection	appeonsample2	ODBC Driver
edit delete Test Connection	sppeonsample	ODBC Driver
Add Connection Cache		

6.3.9.a Adding a connection cache

Click *Add Connection Cache* below the connection cache list and specify the connection cache settings according to Table 6-1.

Figure 6-15: Add connection cache

[AEM Console](#) > [Server Properties](#) > [Connection Cache](#) > [Add Connection Cache](#)

 [Click to return to the previous page.](#)

Add Connection Cache

Connection Cache Name:	<input type="text"/>	
Connection Type:	<input type="text" value=""/>	
User Name:	<input type="text"/>	
Password:	<input type="password"/>	Hide Advanced Options
Maximum Connection Pool Size:	<input type="text" value="100"/>	
Minimum Connection Pool Size:	<input type="text" value="10"/>	
Connection Timeout(seconds):	<input type="text" value="120"/>	

Save and Add
Save
Test Connection

Table 6-1: Connection Cache Properties

Connection Cache Name	Type the name of the connection cache.
Connection Type	<p>Select the connection type.</p> <ul style="list-style-type: none"> Use “Oracle Native Driver” to connect with Oracle databases; Use “MS SQL Server Native Driver” to connect with Microsoft SQL Server databases; Use “ODBC Driver” to connect with Sybase ASA and Sybase ASE databases. Use “IBM Informix Native Driver” to connect with IBM Informix databases.
ODBC Data Source	(For “ODBC Driver” connection only) Select a system DSN. Apeon supports system DSN only, so only system DSN will be listed here.
NET Service Name	(For “Oracle Native Driver” connection only) Select a service name.
IBM Informix Server	(For "IBM Informix Native Driver" connection only) Specify the machine name or IP address of the Informix database server.
Database Host	(For “MS SQL Server Native Driver” connection only) Specify the machine name or IP address of the database server.
Database Port	(For “MS SQL Server Native Driver” connection only) Specify the port number of the database server.
Database Name	(For "MS SQL Server Native Driver" or "IBM Informix Native Driver" connection) 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.
Show/Hide Advanced Options	Select to show or hide advanced options, including minimum and maximum connection pool size.
Maximum Connection Pool Size	Specify the maximum number of connections Apeon Server opens and pools on startup.

Minimum Connection Pool Size	Specify the minimum number of connections Apeon Server opens and pools on startup.
Connection Timeout	Specify the timeout period for the connection.

Connection cache properties vary according to the different database types. For detailed description for each database type, refer to the Section 3.4: [Setting up Apeon Server connection caches](#).

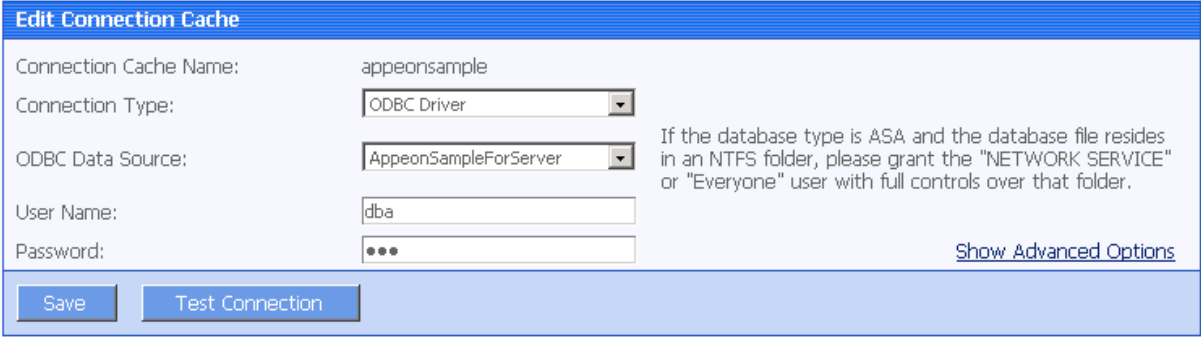
6.3.9.b Editing a connection cache

Click *Edit* and change the settings on the *Edit Connection Cache* page (Figure 6-16). The settings are specified the same way as on the *Add Connection Cache* page.

Figure 6-16: Edit connection cache

[AEM Console](#) > [Server Properties](#) > [Connection Cache](#) > [Edit Connection Cache](#) > [apeonsample]

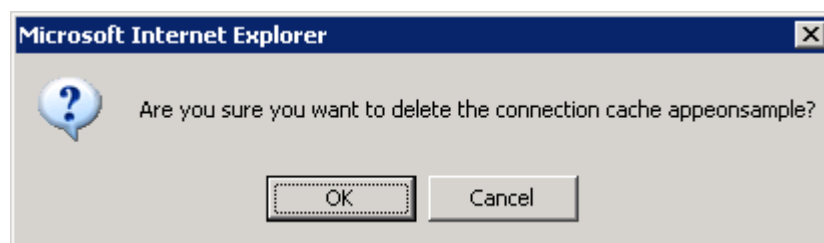
 [Click to return to the previous page.](#)



6.3.9.c Deleting a connection cache

Click *Delete* and you will be prompted whether to delete the specified connection cache. Click *OK* to proceed (Figure 6-17).

Figure 6-17: Delete connection cache



6.3.9.d Testing a connection cache

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

6.3.10 Licensing

Licensing enables you to view detailed information on your license, as shown in Figure 6-18.

Figure 6-18: Licensing

AEM Console > Server Properties > Licensing

Licensing	
Apeon Server must be activated within 30 days after installation. Each copy of Apeon Server is activated for a single network card.	
Edition:	ENTERPRISE
Days remaining:	42
Maximum Sessions:	*
Maximum Deployed Applications:	*
Number of CPUs licensed:	*
Network card physical address:	Not binding
Activation status:	Not activated
Product key:	SYBASE

Product Activation MAC Address

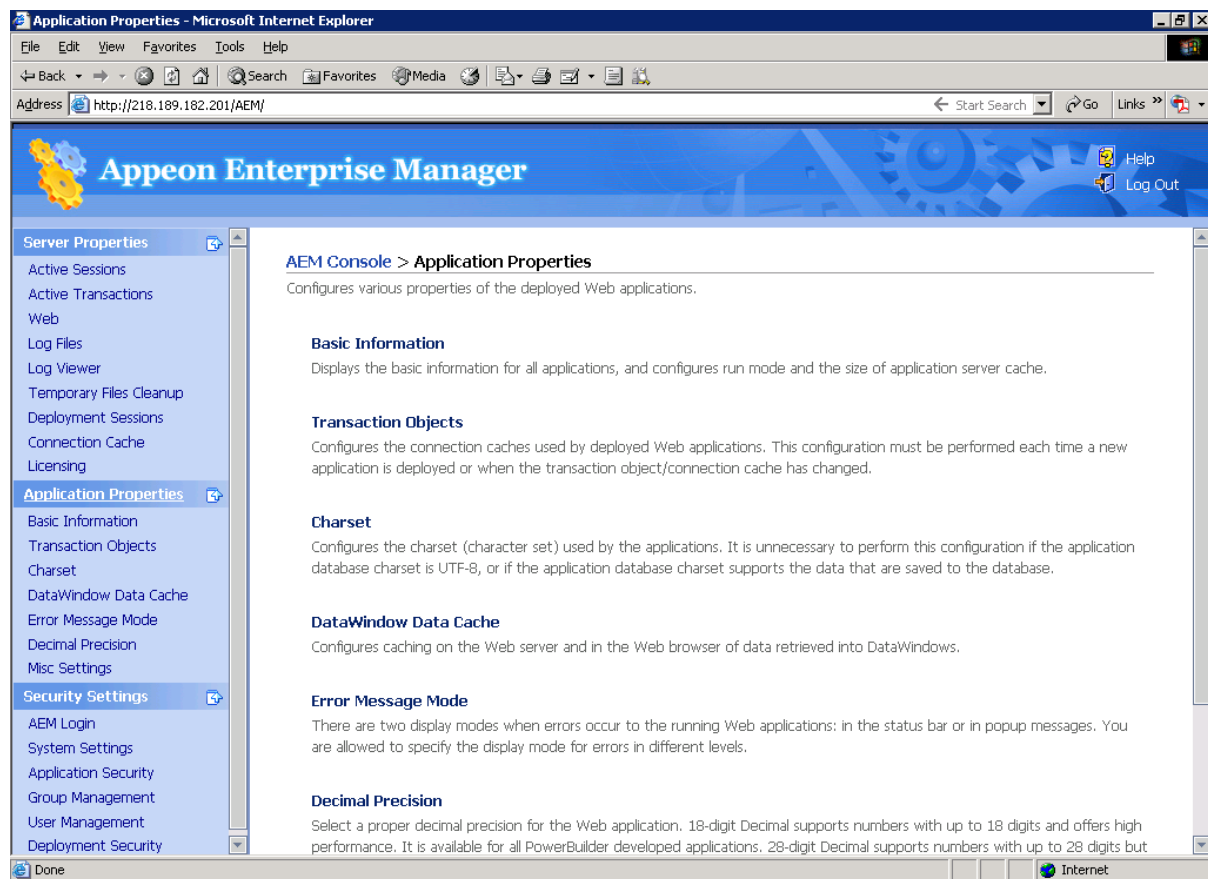
6.4 Application Properties

6.4.1 Overview

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

Application Properties are a set of tools for setting the server-related properties for Web applications. There are seven tools: Basic Information, Transaction Objects, Charset, DataWindow Data Cache, Error Message Mode, Decimal Precision, and Misc Setting, as shown in Figure 6-19. The settings for each application profile affect Web application(s) deployed from the application profile.

Figure 6-19: Application properties



6.4.2 Basic Information

The Basic Information tool displays the basic information of all deployed Web applications, including run mode, PowerBuilder version, application size, DLL/OCX file size, application server cache size, and cache usage. Among these items, you have the option to specify run mode and cache size (Figure 6-20).

Figure 6-20: Basic information

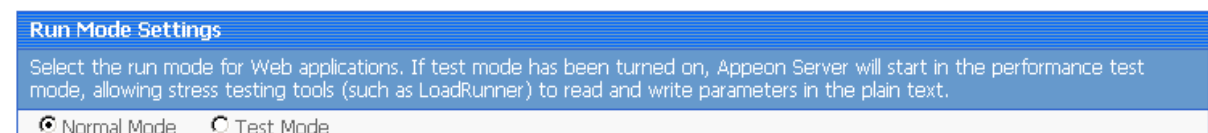
[AEM Console](#) > [Application Properties](#) > [Basic Information](#)

Basic Information						
Displays the basic information for all applications, and configures run mode and the size of application server cache.						
Application Name	Run Mode	PB Version	File Size (KB)	DLL Size (KB)	Cache (MB)	Cache Usage (KB)
appeon_acf_demo	Normal Mode	11.0	4531.38	0.00	3	0.000
appeon_code_examples	Normal Mode	11.0	5835.90	352.00	3	0.000
sales_application_demo	Normal Mode	11.0	1140.91	0.00	3	0.000

6.4.2.a Run Mode

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

Figure 6-21: Run mode



There are two Run Mode options:

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

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

6.4.2.b Application Server Cache

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

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

What is Application Server cache?

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

Depending on the cache size specified for an application, Appeon Server loads part or all of the application DataWindow syntax and embedded SQLs when the application starts. If Appeon Server only loads part of the DataWindow syntax and embedded SQLs of an application to the cache, the application runtime performance is affected because Appeon Server needs to read certain DataWindow syntax and embedded SQLs from the database instead of reading from the memory.

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

Modifying the Appeon Server cache setting for an application

In the Basic Information table (Figure 6-20), the Cache column shows the Appeon Server cache size allocated for the corresponding application, while the Cache Usage column shows how much cache the application currently occupies in the Appeon Server memory.

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

Step 1 – Click an application listed in the Basic Settings table. A new page opens and displays the current cache setting for the application, as shown in Figure 6-22.

Figure 6-22: Modify Cache Setting

Application Server Cache Settings

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

Cache size: MB

Save

Step 2 – Modify the cache size. You can:

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

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

- Set the size to “0”, which means that no cache is available for loading DataWindow syntax or Embedded SQLs. Appeon Server always reads the DataWindow syntax and embedded SQLs from the database.
- Set the size to less than “0” (-3, for example), which means that the cache has no limit. Appeon Server will load all the DataWindow syntax, DataWindow SQLs, and Embedded SQLs of the application into the cache.

Setting the size to “0” is not recommended because it will result in slow performance. If the server has enough memory and the number of the deployed applications is less than 10, it is recommended that you set the size for all applications to less than “0”. If the server does not have enough memory, but it contains many deployed applications, it is recommended that you set all important applications, as well as applications using many DataWindows and Embedded SQL, to less than “0” or much higher than 3M. Keep all other applications at the default setting.

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

6.4.3 Transaction Objects

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

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

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

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

The dynamic mapping in PowerScript has priority over the static mapping in AEM. This section introduces how to set up the static mapping in AEM. For information about the mapping in PowerScript, refer to Section 3.5.1: [Dynamic transaction object to connection cache mapping](#).

6.4.3.a Configuring transaction object mappings

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

Figure 6-23: Applications with transaction objects

[AEM Console](#) > [Application Properties](#) > [Transaction Objects](#)




Transaction Object Settings		
Specify the database for the transaction objects for each application.		
Application Name	Number	Transaction Object
apeon_acf_demo	1	[sqlca]
apeon_code_examples	3	[sqlca,its_sql,its_sqt]
sales_application_demo	1	[sqlca]

To view the static transaction object mappings for an application, click the application in the Transaction Objects tool. A new page opens and displays the current transaction mapping(s) for the application, as shown in Figure 6-24.

Figure 6-24: Configuring transaction object mappings for an application

[AEM Console](#) > [Application Properties](#) > [Transaction Objects](#) > [\[apeon_acf_demo\]](#)

 [Click to return to the previous page.](#)

Configure Transaction Object			
Actions	Transaction Object	Connection Cache	Database Type
  	sqlca	<input type="text" value="apeonsample"/>	<input type="text" value="Sybase ASA 7/8/9/10"/>
<input type="button" value="Add Transaction Object"/>			

Adding a transaction object mapping

Step 1 – Click the *Add Transaction Object* button in Figure 6-24. The Add Transaction Object page displays as shown in Figure 6-25.

Figure 6-25: Add transaction object

[AEM Console](#) > [Application Properties](#) > [Transaction Objects](#) > [Add Transaction Object](#) > [\[apeon_acf_demo\]](#)

 [Click to return to the previous page.](#)

Add Transaction Object	
Application Name:	apeon_acf_demo
Transaction Object:	<input type="text"/>
Connection Cache:	<input type="text"/>
Database Type:	<input type="text"/>
<input type="button" value="Save and Add"/> <input type="button" value="Save"/> <input type="button" value="Test Connection"/>	

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

Step 3 – Select the connection cache from the “Connection cache” dropdown list. The list displays the connection caches created in Apeon Server.

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

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

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

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

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

Step 7 – Click the *Save* button if testing connection cache succeeded.

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

Modifying an existing transaction object mapping

1) To change the connection cache

For each transaction object, there is a dropdown list in the “Connection Cache” column. The list box lists the connection caches created in Apeon Server.

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

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

2) To change the database type

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

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

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.

6.4.4 Charset

The character set conversion can be enabled at the connection cache level for each application if you specify the input Charset and database Charset for the cache in AEM. Refer to Figure 6-26.

You will find the Charset tool useful when:

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

Otherwise, it is unnecessary to use this tool.

Figure 6-26: Charset settings

[AEM Console](#) > [Application Properties](#) > [Charset](#)

Charset Settings		
Set the charset at the connection cache level. Aepeon Server will convert data from the input charset to the database charset. It is unnecessary to perform this configuration if the application database charset is UTF-8, or if the database charset supports the input charset.		
Application Name	Number	Connection Cache
apeeon_acf_demo	0	[]
apeeon_code_examples	0	[]
sales_application_demo	0	[]

6.4.4.a Configuring database Charset for a connection cache

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

Figure 6-27: Configure charset settings

[AEM Console](#) > [Application Properties](#) > [Charset](#) > [\[apeeon_acf_demo\]](#)

 [Click to return to the previous page.](#)

Configure Charset			
Actions	Connection Cache	Database Charset	Client-Side Charset
<input type="button" value="Add Charset"/>			

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

Figure 6-28: Add charset settings

[AEM Console](#) > [Application Properties](#) > [Charset](#) > [Add Charset](#) > [\[apeeon_acf_demo\]](#)

 [Click to return to the previous page.](#)

Add Charset	
Application Name:	apeeon_acf_demo
Connection Cache:	<input type="text" value=""/>
Database Charset:	<input type="text" value=""/>
Client-Side Charset:	<input type="text" value=""/>
<input type="button" value="Save and Add"/> <input type="button" value="Save"/>	

Step 3 – Select the connection cache from the “Connection cache” 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.

6.4.4.b Charset options given in the Charset fields

Table 6-2 lists all the Charset options provided in the “Database Charset” field and the “Client-side Charset” field, and provides a brief description of each Charset. If the actual database Charset or the input Charset is not provided as an option, you can use the following method to manually add the type as an option:

Step 1 – Open the file constant.config in the directory %appeonservice%\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 IIS 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 6-2: Charset and code pages

Page	Charset	Description	
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)	
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)	
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.)	
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)	*
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)	*

6.4.5 DataWindow Data Cache

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

- DataWindow Data Cache at the Apeon Server 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 Oracle 8i (though supported for Oracle 9i and 10g) databases.
- 2) Disable DataWindow Data Cache in AEM if the application is set to the Test Mode in the Run Mode 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 may be different from that in PowerBuilder.
- 4) DataWindows created dynamically cannot cache data on the server. Even though the Cache tool is enabled for such DataWindows, data will still be retrieved from the database.
- 5) DataWindow Data Cache at the Apeon Server or at the client will not be effective until you fulfill all the configuration requirements described in the following sections:
 - Configuration required for database servers
 - Configuration 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.

6.4.5.a Configuration required for database servers

Apeon 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.

Table 6-3 lists the SQL file that should be executed for the supported database server. %apeonserver% indicates the Apeon Server installation directory, for example, C:\inetpub\wwwroot\apeon.

Table 6-3: SQL files need be executed for each database server

Database Type	SQL File
Oracle	To enable the feature for Oracle, install %apeonserver%\sql\cache\install_apeon_cache_ORACLE.sql. To disable the feature for Oracle, uninstall %apeonserver%\sql\cache\uninstall_apeon_cache_ORACLE.sql.
Microsoft SQL Server	To enable the feature for Microsoft SQL Server, install %apeonserver%\sql\cache\install_apeon_cache_MSSQL.sql. To disable the feature for Microsoft SQL Server, uninstall %apeonserver%\sql\cache\uninstall_apeon_cache_MSSQL.sql.
ASE	To enable the feature for ASE, install %apeonserver%\sql\cache\install_apeon_cache_ASE.sql. To disable the feature for ASE, uninstall %apeonserver%\sql\cache\uninstall_apeon_cache_ASE.sql.
ASA	To enable the feature for ASA, install %apeonserver%\sql\cache\install_apeon_cache_ASA.sql. To disable the feature for ASA, uninstall %apeonserver%\sql\cache\uninstall_apeon_cache_ASA.sql.

Important notes

- 1) The SQL file for Oracle database does not work with 8i databases, though it works with 9i and 10g databases.
- 2) Executing the SQL files provided by Apeon is the same as executing any other SQL files, but you need to be aware of the following notes:
 - If a database server has multiple users, executing the SQL file under the login of one user will be effective for that user only. To make sure all users can use the DataWindow data-caching feature, you should use different logins to execute the SQL file.
 - When you execute the SQL for a database server, the current login user of the server must have the right to execute stored procedures and create functions.
 - There are two ways to execute SQLs in a database server - from the database server console or from the command line. Sometimes one way will fail while the other works. For example, executing the SQL for Microsoft SQL Server from the command line may result in “parameter -D” error, while executing the SQL from the server console is successful, if the server computer has both Microsoft SQL Server and Sybase ASE server installed.

6.4.5.b 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 Apeon Server and/or the client.

Step 1 – Select Application Properties | DataWindow Data Cache on the left pane of the AEM Console. The DataWindow Data Cache page displays on the right pane of the Console, as shown in Figure 6-29.

Figure 6-29: DataWindow Data Cache

[AEM Console](#) > [Application Properties](#) > [DataWindow Data Cache](#)

DataWindow Data Cache Settings		
Data retrieved into DataWindow objects can be cached at the Web server or the client to improve performance and scalability.		
Application Name	Server Cache	IE Cache
apeon_acf_demo	N	N
apeon_code_examples	N	N
sales_application_demo	N	N

Step 2 – Click “sales_application_demo” listed in the “Application Name” column of the table. The sales_application_demo page displays as shown in Figure 6-30.

Figure 6-30: DataWindow Data Cache for sale_application_demo

[AEM Console](#) > [Application Properties](#) > [DataWindow Data Cache](#) > [[sales_application_demo_ax](#)]

 [Click to return to the previous page.](#)

Application Cache Setting	
Data retrieved into DataWindow objects can be cached at the Web server or the client. Caching can significantly reduce server load and network traffic, boosting performance and scalability.	
Enable Cache: <input type="checkbox"/> Server Side <input type="checkbox"/> Client Side (IE)	

DataWindow Object Cache Setting	
<input checked="" type="checkbox"/> DataWindow Object Cache	DataWindow Object Cache
<input checked="" type="checkbox"/> d_cust_ar_tabular	<input checked="" type="checkbox"/> d_cust_filter
<input checked="" type="checkbox"/> d_cust_list_all	<input checked="" type="checkbox"/> d_cust_product_edit
<input checked="" type="checkbox"/> d_customer	<input checked="" type="checkbox"/> d_customer_info
<input checked="" type="checkbox"/> d_customer_maintenance	<input checked="" type="checkbox"/> d_customer_master
<input checked="" type="checkbox"/> d_customer_modify	<input checked="" type="checkbox"/> d_customer_new
<input checked="" type="checkbox"/> d_dddw_customers	<input checked="" type="checkbox"/> d_dddw_products
<input checked="" type="checkbox"/> d_dddw_sales_reps	<input checked="" type="checkbox"/> d_dddw_states
<input checked="" type="checkbox"/> d_order	<input checked="" type="checkbox"/> d_order_cust_list
<input checked="" type="checkbox"/> d_order_cust_modify	<input checked="" type="checkbox"/> d_order_cust_new
<input checked="" type="checkbox"/> d_order_detail	<input checked="" type="checkbox"/> d_order_detail_ar
<input checked="" type="checkbox"/> d_order_filter	<input checked="" type="checkbox"/> d_order_info

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

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

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

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

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

6.4.6 Error Message Mode

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

Figure 6-31: Error message mode

[AEM Console](#) > [Application Properties](#) > [Error Message Mode](#)

Error Message Mode Settings		
There are two display modes when errors occur to the running Web applications: in the status bar or in popup messages. You are allowed to specify the display mode for errors in different levels.		
Application Name	Display in the status bar	Display in a popup message
apeon_acf_demo	0	1,2,10
apeon_code_examples	0	1,2,10
sales_application_demo	0	1,2,10

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

Figure 6-32: Error model configuration

[AEM Console](#) > [Application Properties](#) > [Error Message Mode](#) > [[apeon_acf_demo](#)]

 [Click to return to the previous page.](#)

Error Message Mode Settings	
Error Level	Display Mode
0	<input checked="" type="radio"/> Display in the status bar <input type="radio"/> Display in a popup message
1	<input type="radio"/> Display in the status bar <input checked="" type="radio"/> Display in a popup message
2	<input type="radio"/> Display in the status bar <input checked="" type="radio"/> Display in a popup message
10	<input type="radio"/> Display in the status bar <input checked="" type="radio"/> Display in a popup message

Save

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

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

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

Table 6-4: Error message mode

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

6.4.7 Decimal Precision

Select a proper decimal precision for the Web application.

Figure 6-33: Decimal Precision configuration


[AEM Console](#) > [Application Properties](#) > [Decimal Precision](#)

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

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

Figure 6-34: Decimal Precision configuration

[AEM Console](#) > [Application Properties](#) > [Decimal Precision](#) > [[apeon_acf_demo](#)]

 [Click to return to the previous page.](#)

Decimal Precision Settings	
Decimal Precision:	<input checked="" type="radio"/> 15-digit Decimal <input type="radio"/> 28-digit Decimal
<input type="button" value="Save"/>	

6.4.8 Misc Settings

Misc settings include settings for multi-thread download, transfer encoding, registry mode, INI file mode, and DLL/OCX file download. Click the application name in the Misc Settings table to configure the settings.

Figure 6-35: Misc Settings

[AEM Console](#) > [Application Properties](#) > [Misc Settings](#)

Misc Settings				
Configures other settings for the application, including Multi-Thread Download, Transfer Encoding, Registry Mode, INI File Mode and DLL/OCX Download.				
Application Name	Max Download Threads	Transfer Encoding	INI File Mode	Registry Mode Settings
apeon_acf_demo	2	UTF-16LE	Server-side	Client machine Windows registry
apeon_code_examples	2	UTF-16LE	Server-side	Client machine Windows registry
sales_application_demo	2	UTF-16LE	Server-side	Client machine Windows registry

6.4.8.a Multi-Thread Download

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 file download process.

Figure 6-36: Maximum Threads

Maximum Threads Settings	
Download static resources using multi-threads to boost performance. The valid value should be within the range from 1 to 6; the default value is 2.	
Maximum Threads Settings :	<input type="text" value="2"/>

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

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

6.4.8.b Transfer Encoding

Transfer Encoding specifies the encoding format for data transferred between the clients and the server, as shown in Figure 6-37. The transfer speed varies when the encoding format changes.

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

Figure 6-37: Transfer encoding

Transfer Encoding Settings	
You are allowed to choose the encoding mode for transferring data in Apeon for PowerBuilder. The network traffic for the same data using different encoding modes varies. If the language of your project is English, it is strongly recommended that you choose the UTF-8 mode. If there are languages other than English in your project, choose the UTF-16LE mode.	
Transfer Encoding :	<input type="radio"/> UTF-8 <input checked="" type="radio"/> UTF-16LE

6.4.8.c Registry Mode

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

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

Figure 6-38: Registry Functions Execution Mode

Registry Mode Settings	
If the Web application uses PowerBuilder Registry function, you are allowed to specify the mode to execute the Registry function.	
Manipulation Mode:	<input checked="" type="radio"/> Client machine Windows registry <input type="radio"/> Apeon registry emulation

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

6.4.8.d INI File Mode

The INI File Mode tool determines whether Apeon Web applications would download XML files that emulate INI files to the clients for profile functions, or directly use the XML files stored in Apeon Server database.

Figure 6-39: Manipulation mode and download mode

INI File Mode Settings	
If the Web application uses PowerBuilder INI file manipulation function, you are allowed to specify the modes to execute and download the INI files.	
Manipulation Mode:	<input checked="" type="radio"/> Server-side <input type="radio"/> Client-side
Download Mode:	<input checked="" type="radio"/> Auto-download <input type="radio"/> Validation

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

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

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

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

(2) The “server-side” mode keeps the confidential profile information in Apeon Server database. It is securer than the “client-side” mode, which stores the profile information in the client computer.

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

- Auto-download – Default. The XML file is automatically downloaded to the client that executes the relevant profile information.
- Validation – The client Internet Explorer would prompt for the user’s validation before it downloads the XML file for executing relevant profile function.

Note: AEM does not allow the user to dynamically create an INI file on the local machine. Instead, AEM transfers the INI file from PowerBuilder into an XML file and allows the user to manipulate the XML file on the local machine. The INI file is transferred by Apeon Developer during the parsing process and deployed to Apeon Server. 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.

6.4.8.e DLL/OCX Files Download

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

- Configure the DLL or OCX files in the application profile, to deploy the files to Web server with the application. Refer to the *Additional Files* Section in the *Appeon Developer User Guide* on how to configure and deploy DLL or OCX files to Web server.
- Configure how the DLL or OCX files are downloaded to the Client using the AEM DLL/OCX Files Download tool.

Figure 6-40: Modify DLL/OCX Files Download install settings

DLL/OCX Files Download Settings	
To satisfy different needs, Appeon downloads and installs DLL/OCX files according to the settings specified by the user.	
Install Mode	Conflict Resolution Mode
<input checked="" type="radio"/> Install automatically without asking user <input type="radio"/> Confirm with user, then install automatically <input type="radio"/> Install manually (no automatic installation)	If a different file with the same name already exists, then: <input checked="" type="radio"/> Install anyway without asking user <input type="radio"/> Do not install; use existing file <input type="radio"/> Ask the user what to do

Save

“Install Mode” defines how the DLL or OCX files of the selected application should be installed to a client browser. Whichever install mode is selected, when a DLL or OCX file is downloaded to a client, the folder for keeping the DLL or OCX file at the client is %WINDOWS%\system32\AppeonPlugin\appname, where *appname* stands for the name of the Web application. You can select the install mode that is most suitable for the application according to the description in Table 6-5.

Table 6-5: Install mode options

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

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

Table 6-6: 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.

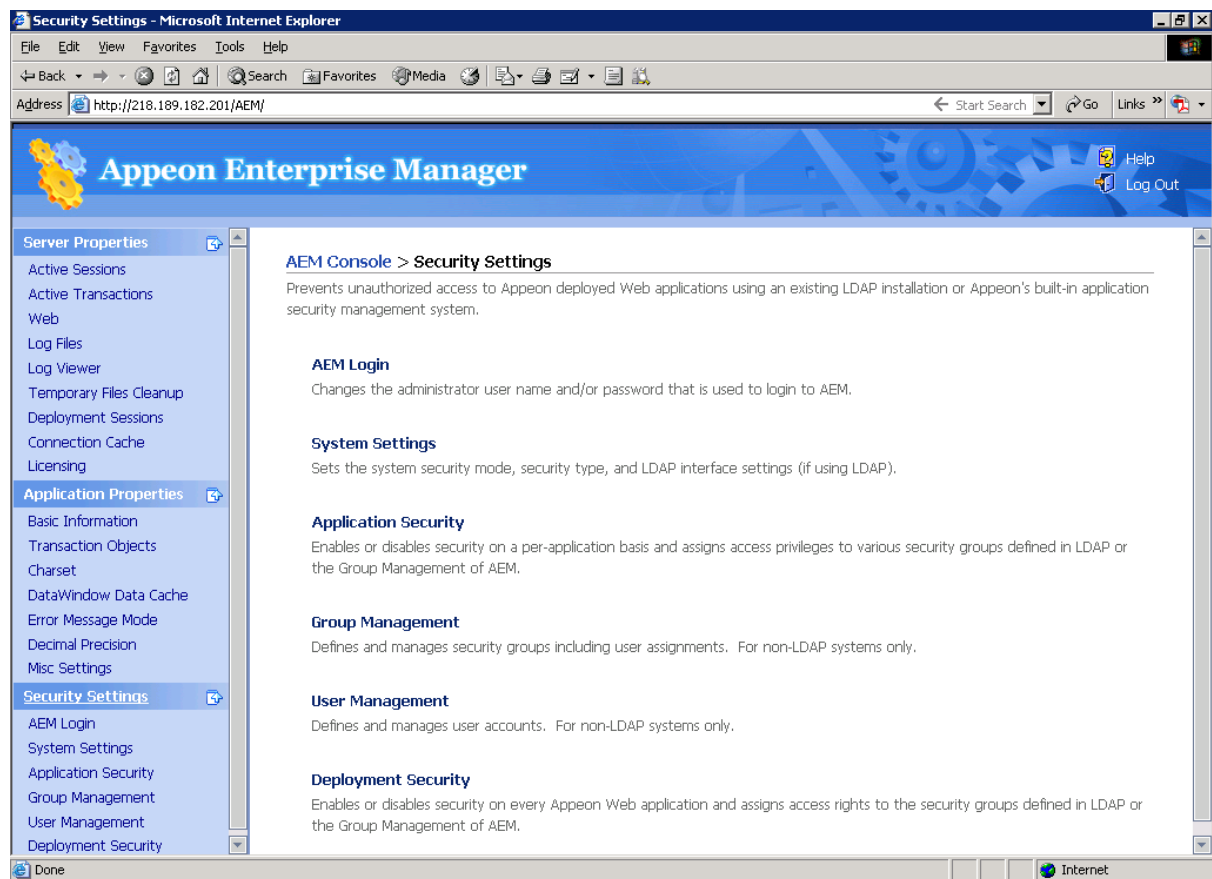
6.5 Security

6.5.1 Overview

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

- Security for accessing AEM. Configures the user name and password for AEM.
- Security for deploying applications to Apeon Servers. Configures the user group that has the right to deploy applications to Apeon Server. By default, all users have the right to deploy applications to Apeon Server.
- Security for accessing deployed applications. You can add an additional layer of security provided by AEM on top of any PowerBuilder security coded in the application. By default, all users have the right to access the Apeon Web applications.

Apeon provides the following six tools for AEM Security: AEM Login, System Settings, Application Security, Group Management, User Management, and Deployment Security. Refer to Figure 6-41.

Figure 6-41: Security

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

6.5.2 AEM login

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

Figure 6-42: AEM Login

AEM Console > Security Settings > AEM Login

Change AEM Password	Change AEM User Name
Once you have successfully changed your password, you will need to use your new password and the existing user name the next time you log in to AEM.	Once you have successfully changed your user name, you will need to use your new user name and the existing password the next time you log in to AEM.
Old password: <input type="text"/>	Old user name: <input type="text"/>
New password: <input type="text"/>	New user name: <input type="text"/>
Confirm Password: <input type="text"/>	Confirm user name: <input type="text"/>
<input type="button" value="Change"/>	<input type="button" value="Change"/>

1) Change AEM Password

The new password will overwrite the user's existing password, but the existing username will be used to login. In order to successfully change the password, the user must enter information in the following fields as shown in Figure 6-42:

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

- New password – Enter a new password to replace the old password (case sensitive).
- Confirm password – Retype the new password. The value entered in this field must match the ‘New password’ field (case sensitive).

2) Change AEM Username

The new username will overwrite the user’s existing username, but the existing password will be used to login. In order to successfully change the username, the user must enter information in the following fields as shown in Figure 6-42:

- 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 Aepeon Server. If you did not specify the username and password during the installation, the old user name and password are both “admin” by default. For security purposes, Aepeon recommends that you change the username and password after the initial login.

6.5.3 System Settings

Figure 6-43: System Settings

[AEM Console](#) > [Security Settings](#) > [System Settings](#)

Security Toggle

Off On

Security Type

Aepeon Security LDAP Security

LDAP Interface Settings

You must only provide LDAP settings if the Security Mode is set to LDAP Security (for MSLDAP only). Ignore this section if you plan to use Aepeon’s built-in application security management system.

LDAP Host:

LDAP Port:

LDAP OU:

Admin User Name:

Admin Password:

As Figure 6-43 illustrates, the System Settings covers three important issues:

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

- Security Type – Determines which system, Apeon 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 Apeon 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 Apeon Server. Apeon only supports Microsoft LDAP server, which requires Windows 2000 Active Directory.

6.5.3.a Security Toggle and Security Type

Table 6-7 shows how the Security Toggle and Security Type settings determine which security tools are applied and what security features are performed.

Table 6-7: Security toggle, Security type and Security Settings

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

- Apeon security and LDAP security provides the user with options of using Apeon Server or LDAP to assign groups to the application. The security groups will be read from either LDAP (if it is LDAP security) or Apeon Server (if it is Apeon security).
- When the user attempts to change the security type, a message box will prompt the user to confirm the change.

6.5.3.b LDAP Interface Settings

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

LDAP Interface Settings in AEM

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

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

- LDAP host – The IP address or domain name of the LDAP Server.
- LDAP port – Port of the LDAP Server.
- LDAP OU – The LDAP organization unit where the users and groups are created.

For Microsoft LDAP server, the LDAP OU should be “DC=AAA, DC=BBB, (DC=CCC)”, where AAA stands for the domain component (DC) that contains all the groups, and BBB stands for the domain component that contains the AAA component.

- 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.

After all the fields are filled, do the following:

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

User and group management at LDAP server side

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

1. Set up the LDAP server in the system
Refer to the documentation supplied by the LDAP server vendor for installation and setup instructions for your LDAP server.
2. Create an organization unit in the LDAP server.
Only a single organization unit can be used to host all the groups and users for the Apeon Web application.
3. Create/manage users and groups in the organization unit in accordance with the LDAP server documentation.

6.5.4 Application Security

Figure 6-44: Application Security

[AEM Console](#) > [Security Settings](#) > [Application Security](#)

Application Security Settings		
All deployed applications are listed below. The security settings for each application are configured individually. The application security settings are ignored and the user is not required to log in if the Security Mode in System Settings of AEM is set to Off.		
Application Name	Configured Groups	User Authentication
apeon_acf_demo	0	Security off
apeon_code_examples	0	Security off
sales_application_demo	0	Security off

6.5.4.a Viewing the current settings

1) View the current application security settings for all applications available in the Application Security page (as shown in Figure 6-44).

- **Application Name** – Lists the names of all the deployed applications. The names are automatically registered with AEM when an application is deployed by Aepeon Developer to the Aepeon Server.
- **Configured Groups** – The number of groups with access rights to the Web application. To view the names of the groups, click the link at the application name. To view details of the groups, go to the Group Management page.
- **User Authentication** – Shows the security mode for user authentication. “Security on” explicates that the user will be prompted to enter the username and password when accessing the selected application, while “Security off” requires no username and password for the application access. You can click the link of an application name listed in the Application Security Settings table and switch the security mode in the page that displays subsequently.

2) View the details of the current application security settings for a single application, by clicking an application. The detailed security settings for the selected application are displayed as shown in Figure 6-45.

Figure 6-45: Detailed security settings for an application

AEM Console > Security Settings > Application Security > [apeon_acf_demo_ax]

 [Click to return to the previous page.](#)

Application Security

User Authentication Security Off Security On

Security Permissions

If the Security Mode is set to LDAP Security, all user groups configured in LDAP are listed in the table below. If the Security Mode is set to Aepeon Security, all user groups configured in Group Management will be listed below.

Unassigned Groups

Assigned Groups

>>>

<<<

Save

As Table 6-8 shows, different application security settings determine different security behaviors in a Web application.

Table 6-8: Application security settings and security behaviors in a Web application

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

6.5.4.b Modifying the security settings of an application

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

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

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

In this page, you are able to:

1. Skip the login window when loading the application...

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

2. Display a login window before loading the application ...

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

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

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

4. Assign a group to the application...

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

By default, all the groups are listed in the Unassigned Groups list. The groups are read from the Apeon Server (if the security type is Apeon 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.

6.5.5 Group Management

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

Figure 6-46: Group Management

[AEM Console](#) > [Security Settings](#) > [Group Management](#)

6.5.5.a Viewing groups

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

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

2) Specify filter criteria to view groups:

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

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

Step 3 – Enable or disable the “Exact search”.

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

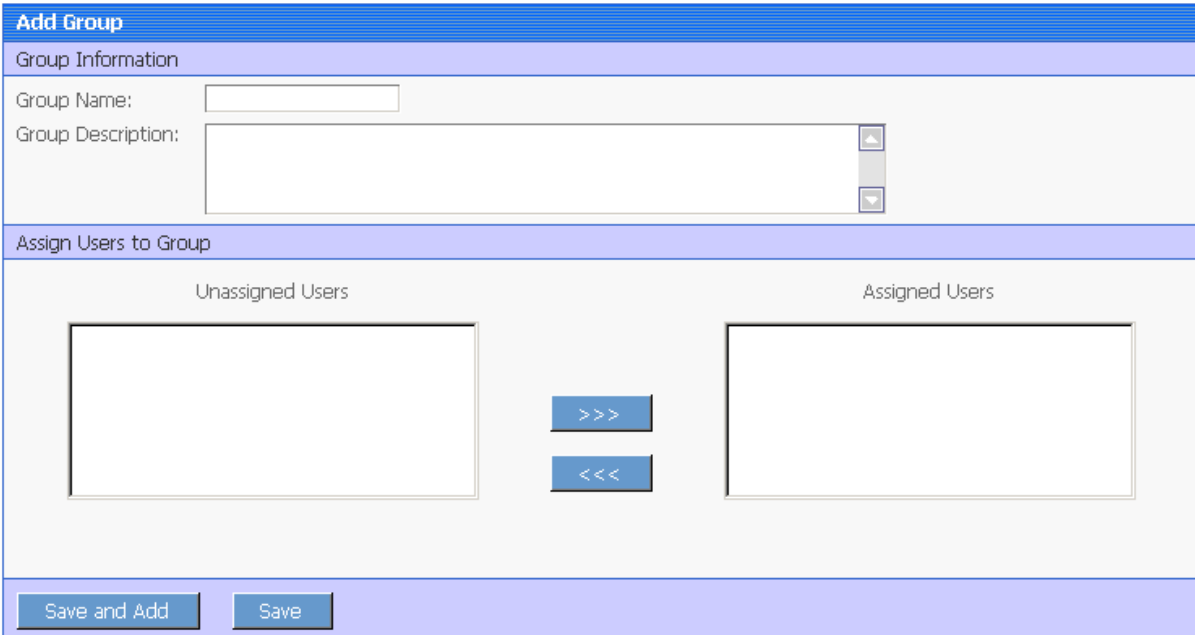
6.5.5.b Adding a new group

To add one or more groups, click the *Add Group* button in the Group Management page (as shown in Figure 6-46) and the Add Group page will be displayed as shown in Figure 6-47.

Figure 6-47: Add a group

[AEM Console](#) > [Security Settings](#) > [Group Management](#) > [Add Group](#)

 [Click to return to the previous page.](#)



- Group name – The group identifier. This field is required. Chinese characters are unsupported.
- Group description – Some explanation about the group. This field is optional.
- Assign or unassign users to the group.
 1. To assign a user to the group...

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

By default, all the users are listed in the Unassigned Users list. The users are configured in AEM User Management.
 2. To unassign a user from the application.

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

6.5.5.c Editing an existing group

To edit a specific group, click the *Edit* button in the Group Management page (as shown in Figure 6-46) and enter the Edit Group page.

The Edit Group page is similar to the Add Group page except that the group name is not editable. You can modify the group description, or assign (unassign) users to the group in the same way as instructed in Section 6.5.5.b: [Adding a new group](#).

6.5.5.d Deleting a group

Delete a group by clicking the *Delete* button in the Group Management page (as shown in Figure 6-46). 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.

6.5.6 User Management

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

Figure 6-48: User Management

AEM Console > Security Settings > User Management

User Management

The User Management functionality is a feature of Apeon's built-in application security system. It is intended for non-LDAP security configurations. If the Security Toggle is set to Off or if the Security Type is set to LDAP Security in the System Settings, these settings will not take effect.

Display users where the contains Exact search

Actions	User Name	Full Name	Account Status	Description
<input type="button" value="Add User"/>				

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

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

- 1) Click the *Show All* button to display all users.
- 2) Specify filter criteria to view users:

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

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

Step 3 – Enable or disable the “Exact search”.

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

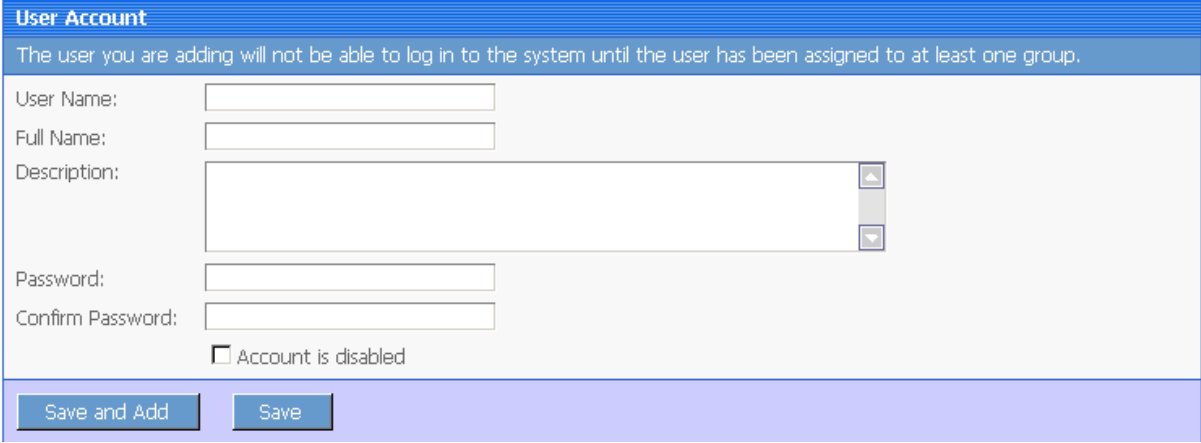
6.5.6.a Adding a new user

If you want to add one or more users, click the *Add User* button in the User Management page (refer to Figure 6-48) and the Add User page will be displayed as shown in Figure 6-49.

Figure 6-49: Add a user

[AEM Console](#) > [Security Settings](#) > [User Management](#) > [Add User](#)

 [Click to return to the previous page.](#)



- 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).

6.5.6.b Editing an existing user

By clicking the *Edit* button in the User Management page (refer to Figure 6-48), you can enter the Edit User page to edit an existing User.

The Edit User is similar to the Add User page except that the user name is not editable. You can modify the full name, the description, or change the password or account status in the same way as you were instructed in Section 6.5.6.a: [Adding a new user](#).

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

6.5.6.c Deleting a user

Delete a user by clicking the *Delete* button in the User Management page in Figure 6-48. 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.

6.5.7 Deployment Security

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

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

Figure 6-50: Deployment Security

[AEM Console](#) > [Security Settings](#) > [Deployment Security](#)

The Deployment Security tool enables you to do the following:

1) Disable deployment security for Aepeon Server

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

2) Enable deployment security for Aepeon Server

Step 1 – Select the “Security On” radio button.

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

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

type is LDAP security) in use. You can use back button (“<<<”) to shift the group to the Unassigned Groups list.

Index

A

- About This Book, 1
- Activating ISAPI, 24
- active sessions
 - killing, 35
 - viewing, 35
- active transactions
 - rolling back, 36
 - viewing, 36
- Add a Connection Cache, 42
- Adding a host, 28
- adding group, 71
- Adding new MIME type, 25
- adding transaction object mappings, 49
- adding user, 73
- advanced configurations, database connection
 - application security, 17
- AEM Help, 34
- AEM login
 - change AEM password, 65
 - change AEM username, 66
- AEM password, 33
- AEM URL, 32
- AEM user guide, 31
 - getting started, 32
- AEM username, 33
- AEM, accessing
 - AEM password, 33
 - AEM URL, 32
 - AEM username, 33
 - launching AEM, 32
- Appeon security, 19
- Appeon Server, running, 32
- application properties
 - DataWindow data cache, 56
 - Decimal Precision, 60
 - DLL/OCX Files Download, 63
 - Error Message Mode, 59
 - INI File Mode, 62
 - Multi-Thread Download, 61
 - Registry Mode, 61
 - Run Mode, 46
 - Transfer Encoding, 61
- application properties
 - application server cache, 47
 - application properties
 - transaction objects, 48
 - charset, 50
 - Application Properties
 - Basic Information, 46
 - Application Properties, 45
 - application security, 17
 - Application Security
 - application name, 69
 - configured groups, 69
 - modifying, 70
 - viewing, 69
 - application security workaround
 - incorporating Appeon security in PB code, 19
 - PB script coded security, 19
 - application security workarounds
 - connection security, 18
 - database security, 18
 - database security workarounds
 - predefined transaction objects, 18
 - application server cache, 47
 - application server cache, modifying, 47
 - audience, 1

C

- change AEM password, 65
- change AEM username, 66
- changing connection cache, 50
- changing database type, 50
- charset, 50
- charset configuration, 51
- charset options, 51
- Configuration during application deployment, 4
- Configuration during debugging, 5
- Configuration during performance management, 5
- Configuration during security management, 5
- Configuration during server information management, 6
- configuration required
 - for database servers, 57
- Configuring Appeon Server Load Balancing, 21

configuring charset, 51
 configuring for DataWindow Data Cache, 58
 Configuring IIS Web site, 21
 Configuring Network Load Balancing, 28
 Configuring port rules, 28
 Configuring Windows 2003 Network Load Balancing, 27
 connection cache mapping, setting up transaction object, 15
 Connection cache settings for Informix Native driver, 11
 Connection cache settings for ODBC driver, 8
 Connection cache settings for Oracle Native driver, 9
 Connection cache settings for SQL Server Native driver, 10
 Copying Apeon plug-in, 23
 Creating a Network Load Balancing Cluster, 28
 Creating redirector configuration file, 24
 Creating virtual directory, 22

D

database auditing workaround
 re-configuring database auditing, 20
 Database Connection Setup, 7
 Database Connection Types, 7
 DataWindow data cache, 56
 debug mode, log files operation mode, 39
 Delete a Connection Cache, 44
 deleting an existing transaction object mapping, 50
 deleting group, 72
 deleting user, 74
 Deploying application, 26
 Deployment Security, 74
 deployment sessions, 41
 developer mode, log files operation mode, 39
 Download timeout, 38

E

Edit a Connection Cache, 44
 Editing configuration file, 23
 editing group, 72
 editing user, 74

G

group management
 viewing, 71
 group management adding, 71
 group management editing, 72
 group management deleting, 72

H

How Network Load Balancing Works, 27
 how to use this book, 1

I

if you need help, 2
 Installing Apeon plug-in, 21
 Installing Apeon Server Web Component, 26
 Installing IIS filter, 24
 Introduction
 AEM tools, 31

K

killing active sessions, 35

L

launching AEM, 32
 LDAP interface settings, 67
 load balancing, 21
 log, 39
 log file
 log mode, 38
 replacing log files, 39
 log files operation mode
 debug mode, 39
 developer mode, 39
 off, 38
 standard mode, 39
 Log Viewer, 40

M

modifying Application Security, 70
 modifying application server cache, 47
 modifying transaction object mappings, 50

O

off, log files operation mode

P

password, 33

Preparing environment, 21

R

readers, 1

Receive timeout, 38

related documents, 1

replacing, 39

Restarting IIS, 26

rolling back active transactions, 36

running Appeon Server, 32

S

security

Application Security, 68

Deployment Security, 74

group management, 71

system settings, 66

user management, 73

security

AEM login, 65

Security, 64

security toggle, 67

security type, 67

Server Configuration Tasks

Scope of configurations, 3

Server Configuration Tasks, 3

server properties

active sessions, 35

server properties

active transactions, 36

server properties

Web, 36

server properties

log file, 38

server properties

temporary files cleanup, 41

server properties

deployment sessions, 41

server properties

Connection Cache, 42

server properties

Licensing, 44

Server Properties, 34

session timeout, 37

setting up Appeon Server connection
caches, 8

setting up database connection

advanced configurations, 17

Appeon security, 19

setting up Appeon Server connection
caches, 8

setting up transaction object, 15

setting up transaction object

mapping transaction object to

connection cache

dynamic, 16

static, 17, 49

setting up transaction object to connection
cache mapping, 15

standard mode, log files operation mode,
39

starting AEM, 32

system settings

LDAP interface settings, 67

security toggle, 67

security type, 67

T

temporary files cleanup

auto cleanup, 41

manual cleanup, 41

Test a Connection Cache, 44

transaction object mappings, adding, 49

transaction object mappings, modifying,
50

transaction timeout, 37

U

user and group management, LDAP server,
68

user management

adding, 73

deleting, 74

editing, 74

username, 33

V

viewing active sessions, 35

viewing active transactions, 36

viewing Application Security, 69

viewing group, 71

W

Web

session timeout, 37

transaction timeout, 37

What is Apeon Server connection cache,
7

working around database auditing, 20