Install and Configuration Guide

Active Content Manager (ACM) Version 11.1

Last revised December 6, 2011
Contents

Introduction 6
   Overview .................................................................................................................. 6
   Technical Support .................................................................................................. 6
   Deployment Planning ............................................................................................ 7

Hardware Requirements 8

Software Requirements 9
   Active Content Manager Software ..................................................................... 9
   Server .................................................................................................................... 9
   Admin and Visitor Browser ................................................................................... 9

Server Diagrams 10
   Server Diagram of a Single Site setup ................................................................. 10

Installation Checklist 11

IIS and ASP.NET 4.0 Install 12
   Installing IIS on Windows Server 2003 (IIS 6.0) ......................................................... 12
   Installing IIS on Windows Server 2008/2008 R2 (IIS 7/7.5) ....................................... 12
   Installing ASP.NET 4.0 .......................................................................................... 12

DNS Configuration 13
   Overview ............................................................................................................... 13
   FQDN (Fully Qualified Domain Name) .................................................................... 13
   Server Host Name .................................................................................................. 13

Application Files Install 14
   Installing the ACM Application Files ................................................................... 14
   Create the ACM Directory ..................................................................................... 14
   Copying the ACM application files ....................................................................... 14
   Renaming the default.aspx files ............................................................................ 14
   License Files Installation ....................................................................................... 14

Database Setup: SQL Server 16
   Overview ............................................................................................................... 16
   SQL Server Database Setup ................................................................................... 16
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Database Setup</td>
<td>17</td>
</tr>
<tr>
<td><strong>Database Connection String</strong></td>
<td>18</td>
</tr>
<tr>
<td>Default</td>
<td>18</td>
</tr>
<tr>
<td>SQL Server</td>
<td>18</td>
</tr>
<tr>
<td>Oracle</td>
<td>19</td>
</tr>
<tr>
<td>Save Database Connection Information to the Registry</td>
<td>21</td>
</tr>
<tr>
<td><strong>Web.config Configuration</strong></td>
<td>24</td>
</tr>
<tr>
<td><strong>Configure Directory Security</strong></td>
<td>27</td>
</tr>
<tr>
<td>Overview</td>
<td>27</td>
</tr>
<tr>
<td>Configuring permissions for Windows Server 2003</td>
<td>27</td>
</tr>
<tr>
<td>Configuring permissions for Windows Server 2008</td>
<td>28</td>
</tr>
<tr>
<td><strong>Configuring IIS</strong></td>
<td>29</td>
</tr>
<tr>
<td>IIS 6.0 (Windows Server 2003)</td>
<td>29</td>
</tr>
<tr>
<td>IIS 7.5 (Windows Server 2008 R2)</td>
<td>30</td>
</tr>
<tr>
<td><strong>ACM Testing and Configuration</strong></td>
<td>32</td>
</tr>
<tr>
<td>Overview</td>
<td>32</td>
</tr>
<tr>
<td>Default Administrator Password</td>
<td>32</td>
</tr>
<tr>
<td>System-wide Administrator Setup</td>
<td>32</td>
</tr>
<tr>
<td>Site Administrator Setup</td>
<td>33</td>
</tr>
<tr>
<td>Support Contact Information</td>
<td>33</td>
</tr>
<tr>
<td>Register Page Types and HTML Editors</td>
<td>33</td>
</tr>
<tr>
<td>FQDN Setup</td>
<td>34</td>
</tr>
<tr>
<td><strong>Health Monitor Install</strong></td>
<td>35</td>
</tr>
<tr>
<td>Installation and Configuration</td>
<td>35</td>
</tr>
<tr>
<td>The Health Monitor package</td>
<td>35</td>
</tr>
<tr>
<td>Installation</td>
<td>35</td>
</tr>
<tr>
<td>Enable Health Monitor Auto Start</td>
<td>36</td>
</tr>
<tr>
<td>Configuration</td>
<td>36</td>
</tr>
<tr>
<td><strong>Appendix A: IIS Bindings</strong></td>
<td>37</td>
</tr>
<tr>
<td>Configuring IIS Bindings</td>
<td>37</td>
</tr>
<tr>
<td><strong>Appendix B: Redirects</strong></td>
<td>39</td>
</tr>
<tr>
<td>Overview</td>
<td>39</td>
</tr>
<tr>
<td>Authority Redirects</td>
<td>39</td>
</tr>
<tr>
<td>301 Redirects</td>
<td>39</td>
</tr>
<tr>
<td>FQDN Mapping</td>
<td>40</td>
</tr>
<tr>
<td><strong>Appendix C: Multiple Sites on a Single Install</strong></td>
<td>41</td>
</tr>
<tr>
<td>Overview</td>
<td>41</td>
</tr>
<tr>
<td>IIS Configuration</td>
<td>41</td>
</tr>
<tr>
<td>Appendix</td>
<td>Title</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>D</td>
<td>Video Service</td>
</tr>
<tr>
<td>E</td>
<td>Search Page</td>
</tr>
<tr>
<td>F</td>
<td>Static HTML Export</td>
</tr>
<tr>
<td>G</td>
<td>Shared Folders</td>
</tr>
<tr>
<td>H</td>
<td>Multi-Server Setup</td>
</tr>
<tr>
<td>I</td>
<td>Log File Locations</td>
</tr>
<tr>
<td>J</td>
<td>Backup Procedures</td>
</tr>
</tbody>
</table>
Database Backup......................................................................................................................... 66
Shared Folders Backup............................................................................................................... 66
ACM Application Files.............................................................................................................. 67
Introduction

Overview

This guide provides detailed instructions for installing the Active Content Manager on a server to host one or more sites.

Note The audience for this guide is IT staff and/or system administrators who will be installing, configuring and maintaining ACM. This guide assumes that you are skilled at configuring Microsoft Servers (Windows, IIS, SQL Server, etc.), and have a thorough understanding of DNS and TCP/IP.

It is recommended that you read through this document completely before installing the Active Content Manager.

Installing and Configuring ACM involves the following high-level steps:

- Conduct deployment planning
- Review Hardware and Software Requirements
- Deploy the ACM Application Files
- Configure Microsoft SQL Server or Oracle DBMS
- Configure IIS
- Configure Directory Security for ASP.NET
- Configure ACM through web.config
- Configure your DNS
- Test Correct Operations
- Configure the Indexing Service
- Install and Configure Health Monitor

Once ACM is operating correctly, remember to plan:

- Backup and Restore Procedures

Technical Support

Technical support is available through the online support center at:

http://customerportal.activenetwork.com

In order to use this site you must have a valid user name and password.

Support Telephone: 604.431.4636
Toll free Support: 1.800.663.4991
Deployment Planning

The Active Content Manager is a flexible enterprise software system that can service the needs of small/simple installations and very complex and highly scalable installations:

- In a small deployment, ACM and all supporting software will be installed on a single computer; this would be appropriate for small or departmental websites. This deployment scenario offers little in the way of scalability, redundancy or survivability\(^1\).

- In a large deployment, ACM can be installed a web-farm scenario with multiple application servers connected to a SQL Server Cluster. This would be appropriate to support large site, many small sites, and/or high-traffic websites. This deployment scenario offers very high scalability, redundancy and survivability.

It is important that you understand your requirements and plan the appropriate deployment environment for your needs. Some items to consider:

- How many websites will you be hosting?
- How much traffic will the websites get?
- Are you deploying internet, intranet or extranet sites? How many of each?
- How many authenticated viewers will you have?
- How many content contributors will you have?

It is beyond the scope of this Guide to provide help with Deployment Planning. For detailed analysis of deployment options, please contact your Active Account Executive who will arrange an analyst to work with your organization.

\(^1\) Survivability is the ability of the system to survive in the face of catastrophic (and therefore infrequent) failure. For example, can the system continue to service requests in the event of a disk-array failing, a computer ceasing to function, or in the event of a power outage?
Hardware Requirements

The Active Content Manager can be installed in a variety of configurations depending upon load and scalability needs. In the simplest configuration, the application and all supporting software is installed on a single computer. In more demanding environments, the database can be moved to a separate server (and optionally in a cluster) and multiple application servers can be used.

We recommend working with your Active Content Manager Consultant to determine the hardware requirements for your organization. However, the ACM Hardware and Software Requirements document provides server specifications that will be sufficient for most ACM installations. High traffic sites may wish to consider multiple servers in a web farm.
Software Requirements

Active Content Manager Software

Before proceeding with installation, make sure you have received the following files:

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM_X_X_X_X.zip</td>
<td>Standard ACM release build. Contact the ACM Upgrades team for information on the password to extract the file.</td>
</tr>
<tr>
<td>Licenses.zip</td>
<td>Standard ACM page type licenses</td>
</tr>
</tbody>
</table>

Server

Please refer to the ACM *Hardware and Software Requirements* document for ACM specific installation requirements. Read the documentation accompanying each prerequisite software product for additional requirements. Before installing any prerequisite software, it is highly recommended that you read Microsoft documentation about how to ensure the security of your platform:

Admin and Visitor Browser

Please refer to the ACM *Hardware and Software Requirements* document.

2 [http://www.microsoft.com/security/]
Server Diagrams

Server Diagram of a Single Site setup

This is a diagram of a simple single web server setup for an externally accessible site. Each customer’s environment may be quite different, but this is the core part of the ACM architecture.

ACM Basic Site Configuration Diagram

External DNS
Hosts your externally accessible DNS zone

SMTP Server
Relays emails from ACM

ACM Web Server
ACM Application files reside here. The live site is served here

Database Server
Houses the ACM Database

Internet

ACM Control Panel

Domain Name Registrar

User's Computer

Firewall for DMZ

User

Firewall for Internal Network

All ports are assuming the use of default ports for that application.
Installation Checklist

This checklist can be used as a guide for someone who is familiar with the installation process to follow. It is recommended to follow the full instructions to ensure nothing is missed during an installation. Any small item missed can result in the site not coming up.

1. Install IIS and ASP.NET
2. Configure DNS for the site
3. Extract ACM application files
4. Copy Install files into the CMSroot
5. Obtain license files and apply to CMSroot
6. Set up Database
7. Configure Database Connection in ACM
8. Configure web.config file
9. Apply directory permissions
10. Configure the site in IIS
11. Test and configure ACM
12. Install and configure Health Monitor service
13. Perform necessary Appendices
IIS and ASP.NET 4.0 Install

Installing IIS on Windows Server 2003 (IIS 6.0)

These instructions should be followed if your server is running Windows Server 2003, and IIS is not already installed. Microsoft has a number of resources for installing IIS that can be found at:


Installing IIS on Windows Server 2008/2008 R2 (IIS 7/7.5)

Follow these instructions to install IIS, if your server is running Windows Server 2008 or 2008 R2, and IIS is not already installed. Microsoft has a number of resources for installing IIS that can be found at:

http://learn.iis.net/page.aspx/26/installing-and-configuring-iis-7/

Installing ASP.NET 4.0

ACM uses ASP.NET Framework version 4.0. You must download and install .NET 4.0 on the server running as the ACM Application server:

DNS Configuration

Overview

The URL to access ACM will be the same as the one used to browse the site as a non-user, unless the site is using the Static Export functionality. It is important to choose the method which will be used to browse ACM.

FQDN (Fully Qualified Domain Name)

Selecting a fully qualified domain name is recommended. This will require you to register a DNS name for this site, or configure your existing FQDN to point to the server hosting the ACM site once the site is finished implementing. If only used internally, the DNS zone may be configured on the internal network only. Consult your DNS administrator for more information on configuring this.

Server Host Name

You can access the server using host name (the name of the computer). Usually the DNS settings within more networks allow computers to recognize other computer on the same network by using the host name. e.g. http://myServer/.

This setting requires minimal configuration and may be a good interim solution until a FQDN is created or until the site is fully implemented and ready to go live.
Application Files Install

Installing the ACM Application Files

Installing the application files consists of creating a directory for the root of the site and the ACM application files in place. There are no changes to the registry required.

It is recommended that you close all other programs before you begin the ACM installation process.

Create the ACM Directory

Create a directory that will be used to install the ACM application files. For example, C:\ACM\Site. For the purposes of this document, we’ll refer to the ACM Directory as CMSroot

- You can use any local drive for the ACM application files directory.
- The ACM does not rely on the name used for the application files. However, this path will be used when configuring IIS.

The recommended structure of the ACM directory is:

C:\ACM\Backup – contains backups of the site before an upgrade
C:\ACM\Build Files – contains downloaded application files
C:\ACM\Site – contains the application files (the root of the ACM install)

Copying the ACM application files

Unzip ACM_X_X_X_X.zip and copy all of the files and folders within the \Install files\ folder into the CMSroot folder.

Renaming the default.aspx files

After copying the ACM files and folders into CMSroot, rename 2 files:

1. Rename the root default.aspx file:
   a. Rename CMSroot\ironpointdefault.aspx to default.aspx if you would like to control the default.aspx file from the server manually.
   b. Rename CMSroot\ACMdefault.aspx to default.aspx if you would like ACM to control the default.aspx file instead.

2. Rename CMSroot\Admin\ironpointdefault.aspx to default.aspx. This allows /admin to be the default redirect to the login page.

License Files Installation
You will receive a separate .zip file of standard ACM licenses (e.g. Licenses.zip). If unsure, contact your Account Manager or the ACM Support Team to inquire about obtaining the license files.

1. Unzip the license file (The extracted files should contain a number of .lic files)
2. Copy all files (.lic format) into the CMSroot\bin folder of your ACM.
Database Setup: SQL Server

Overview

Configuring databases is beyond the scope of this guide. Consult Microsoft or Oracle respectively for more information on these processes.

It is also a good idea to set up a maintenance schedule to regularly back up, re-index and run other diagnostics on the databases. Consult your database administrator for more information on that.

SQL Server Database Setup

ACM requires two database logins: mcw and CM. mcw is the user which ACM uses to pull and manipulate data in the database. The CM user is the owner of all the objects in the database. The login names should not change, however the passwords can be updated.

Note SQL Server MUST allow Mixed Mode Authentication (SQL Server and Windows Authentication mode).

Note The instructions on how to run queries are beyond the scope of this document. Please refer to Microsoft documentation for more details instructions here

1. Open CMSroot\DatabaseScripts\IronPoint.Install.sql in a text editor
2. Find and Replace IronpointCM with the desired database name
3. Replace C:\Program Files\Microsoft SQL Server\MSSQL\Data\ with the desired physical location of the .mdf and .ldf files on the database server
4. Locate this line and replace iggy with the desired password for the mcw database login:
   
   exec sp_addlogin N'mcw', 'iggy', @logindb, @loginlang

   Note SQL Server 2005 and higher by default, requires strict password complexity which should be considered when creating this password
5. Locate this line and replace the second CM with the desired password for the CM database login:
   
   exec sp_addlogin N'CM', 'CM', @logindb, @loginlang

   Note SQL Server 2005 and higher by default, requires strict password complexity which should be considered when creating this password
6. Open SQL Server Management Studio as an System Administrator
7. Run the modified query from IronPoint.Install.sql above
8. Once the query has run successfully the ACM database has been created.
Oracle Database Setup

Note  These instructions have been written with the expectation that a qualified Oracle DBA will be executing these steps. Details on exact steps are beyond the scope of this document. Consult Oracle resources for more information on specific steps if necessary.

1. Create a new Oracle Database or identify an existing database into which the ACM schema can be imported.

2. Run these scripts in Oracle:
   - `CMSroot\DatabaseScripts\Oracle.Install\create_tablespaces.sql`
   - `CMSroot\DatabaseScripts\Oracle.Install\create_users.sql`

3. Import the `CMSroot\DatabaseScripts\Oracle.Install\IronPointCM_7.500.017_Oracle.dmp` file using the following command in a DOS command prompt.

   ```
   imp <DBAUser>/<DBApassword>@<SID> buffer=32000
   file='C:\<path to .dmp file>'
   grants=y indexes=y
   rows=y log=OracleImport.log fromuser=CM touser=CM
   commit=y constraints=y compile=y
   ```

   Replace `<DBAUser>`, `<DBApassword>`, and `<SID>` with the appropriate values for your database. Replace `<path to .dmp file>` with the directory the dump file is saved.


   Be sure to run these scripts in the order they are listed.

As of ACM 11.0, new Oracle Data Access Components must be installed on the server. To download the Data Access Components visit:


Choose either the 32-bit or 64-bit versions corresponding to your server.
Database Connection String

Default

By default, Active Content Manager is configured to connect to a SQL Server database running on the default instance of SQL Server on the same computer as the application. If your SQL Server is on a different computer, if you are using a named instance of SQL Server or if you are using an Oracle Database, then you must follow the appropriate steps below to modify the data source identifier used by the ACM application to connect to the database.

SQL Server

Follow these instructions if ACM is connecting to a SQL Server database.

To connect ACM to a SQL Server:

1. Open CMSroot\bin\IronPoint.DataAccess.dll.config in a text editor
2. In the section of the config file named dataSources, locate the dataSource element with the name attribute “SQL”
3. The connectionString attribute configures how ACM connects to SQL Server. Modify the values of the parameters in the connection string to configure which database ACM looks at. There are four settings you can adjust in the connectionString:
   a. Data Source: This is the host name or IP address of your SQL Server instance. Port number is also specified here using a comma to denote the port (e.g. 10.1.216.225,2433 for port 2433). If the SQL instance is a named instance, the name is denoted by a backslash (e.g. 10.1.216.225\SQLEXPRESS for a named instance called SQLEXPRESS).
   b. Initial Catalog: This is the database name within the specified SQL Server instance.
   c. User ID: This is the user that ACM will use to connect to SQL Server.
   d. Password: This is the password of the User ID above.

Note: You can also configure your database connection through a separate application. This application encrypts the IronPoint.DataAccess.dll.config file and writes the database connection information to the registry. You can then manage this information from within ACM. See the Save Database Connection Information to the Registry section for details.
Follow these instructions if ACM is connecting to an Oracle database.

**To connect to an Oracle Database or to configure advanced settings:**

1. Open `CMSroot\bin\IronPoint.DataAccess.dll.config` in a text editor.

2. Comment out the `<dataProvider>` tag with
   `connectionType="System.Data.OracleClient.OracleConnection"`

   e.g.
   ```
   -->
   ```

3. Uncomment the `<dataProvider>` tag with
   `connectionType="DataAccess.Client.OracleConnection"

   e.g.
   ```
   <dataProvider name="Oracle"
   connectionType="Oracle.DataAccess.Client.OracleConnection, Oracle.DataAccess, Version=9.2.0.401, Culture=neutral, PublicKeyToken=89b483f429c47342"
   commandType="Oracle.DataAccess.Client.OracleCommand, Oracle.DataAccess, Version=9.2.0.401, Culture=neutral, PublicKeyToken=89b483f429c47342"
   ```
4. Ensure that the version number value in each version parameter above matches the Oracle Client dll version installed on your ACM server. In the above example, the Oracle Client version that should be installed on that server is 9.2.0.401.

5. Locate the dataSources tag with name="SQLClient" and ensure the SQL data source is commented out, or is not present.

e.g.
<!-- <dataSource name="SQL" default="true" provider="SqlClient"

connectionString="Data Source=Pollock;Initial Catalog=IronPointCM71;User ID=mcw;Password=iggy"

dataOperationsDir=""

dataOperationsFileMask="SqlClient.CM.Commands *.config"
/> -->

6. Locate the dataSource tag with the name="Oracle" and uncomment this section.

e.g.
<dataSource name="Oracle"

provider="Oracle"

connectionString="Data Source=IPDEV;User ID=system;password=system"

dataOperationsDir=""
databaseOperationsFileMask="Oracle.CM.Collections*.config"
 />

7. In the **connectionString** attribute you can configure how ACM connects to Oracle. There are three settings you can adjust in the connectionString:

   a. **Data Source**: This is the address name connected to the desired database SID, found in the tnsnames.ora file on the ACM web server.
   
   b. **User ID**: This is the user that ACM will use to connect to Oracle.
   
   c. **Password**: This is the password used to connect to Oracle.

8. Add `default="true"` after `dataSource` name="Oracle"

   e.g. `<dataSource name="Oracle" default="true"`

   **Note** You now have the ability to configure your database connection through a separate application. This application encrypts the `IronPoint.DataAccess.dll.config` file and writes the database connection information to the registry. You can then manage this information from within ACM. See the **Save Database Connection Information to the Registry** section for details.

---

**Save Database Connection Information to the Registry**

This is an optional process. You can use the ACM Configuration tool to input the database connection information instead of using the `IronPoint.DataAccess.dll.config`. This method also allows you to store the connection information in the registry rather than leaving it in the config file.

1. Open **CMS\root\bin\DataAccessSetupApp.exe** file to launch the ACM Configuration Tool.

   **Note** For Windows 2008, you must open the DataAccessSetupApp.exe with the **Run as Administrator** option.
2. Enter a name value for this ACM installation.

3. Click the **Browse** button to browse to and select the root directory of your ACM installation.

4. Select the **Registry (Secure)** option to write the connection information to the registry, or **IronPoint.DataAccess.dll.config** to write to the config file.

**Simple Mode**

5. Select **SQL Server** or **Oracle** depending on the database platform which ACM database resides on.

6. Fill in the other fields
   a. **Server**: Host name or IP address of the database server (SQL Server only)
   b. **Database Name**: Name of the database (SQL Server), or database SID (Oracle)
   c. **Username**: The user that will connect to the database
   d. **Password**: Password of the user that will connect to the database

7. Click **Save** to write the changes to either the registry or config file.

**Advanced Mode**

5. In the **Provider** field, type “SqlClient” for SQL or “Oracle” for Oracle.
6. In the Connection String field use the Connection string found in CMSroot\bin\IronPoint.DataAccess.dll.config.
   e.g. Data Source=Pollock;Initial Catalog=IronPointCM71;User ID=mcw;Password=iggy

7. In the Data Ops File Mask field:
   a. Type “SqlClient.CM.Commands*.config” if you are using a SQL database.
   b. Type ”Oracle.CM.Commands*.config” if you are using an Oracle database.

8. If there are any parameter name prefixes associated with the SQL files, type the prefix in the Param Name Prefix field, otherwise you can leave it blank.

9. Click Save to write the changes to either the registry or config file.
Web.config Configuration

Some application specific settings can be configured through the CMSroot\web.config file. The web.config variables can be edited through a text editor. Additionally, a limited set of variables in the web.config file can be edited through ACM: System > Click Configuration Files > web.config tab.

Most settings can be left with the default setting. Most installs need only configure the SMTP server, but here is a list of the ACM application specific settings that can be configured for further tweaking and configuration.

<table>
<thead>
<tr>
<th>KEY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhysicalPathToSharedFolder</td>
<td>The physical path to the shared folder. This is the folder that contains all data that is not contained in the database. For example: C:\ACM\Sites</td>
</tr>
<tr>
<td>VirtualPathToSharedFolder</td>
<td>The virtual path to the shared folder. For example: CMSroot\Sites</td>
</tr>
<tr>
<td>PhysicalPathToPrivateSharedFolder</td>
<td>The physical path to the private shared folder. This is the folder that contains all site resources that must be secured. If ACM is configured to secure all access to digital assets, this folder must be located in a non-http accessible location. For example: C:\Inetpub\cmsPrivate.</td>
</tr>
<tr>
<td>CustomErrors</td>
<td>Determines if the ACM should show detailed error messages to users. Default value: RemoteOnly</td>
</tr>
<tr>
<td>Compilation</td>
<td>Determines if the application is set to ASP.NET “debug” mode. Default value: false:</td>
</tr>
<tr>
<td>Trace</td>
<td>Determines if the application should use ASP.NET tracing.</td>
</tr>
<tr>
<td>SessionState</td>
<td>Determines configuration settings for session management. Can be in-process for single application servers, or out-of-process for web farms.</td>
</tr>
<tr>
<td>Hitpruntime</td>
<td>Set max request length and request timeout.</td>
</tr>
<tr>
<td>AsyncKeepAliveEnabled</td>
<td>False</td>
</tr>
<tr>
<td>AsyncJobServerEnabled</td>
<td>True</td>
</tr>
<tr>
<td>AsyncJobInterval</td>
<td>1</td>
</tr>
<tr>
<td>AsyncPollingInterval</td>
<td>1</td>
</tr>
<tr>
<td>AsyncJobRestartInterval</td>
<td>60</td>
</tr>
<tr>
<td>AsyncJobRemovalInterval</td>
<td>1440</td>
</tr>
<tr>
<td>SMTP_ServerHost</td>
<td>The SMTP server host to use for sending email from the system. For example: smtp.fusemail.com. Default value: none.</td>
</tr>
<tr>
<td>SMTP_ServerPort</td>
<td>The SMTP server port to use for sending email. Default value: 2500</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SMTP_UserName</td>
<td>The SMTP user name to use to authenticate against the SMTP server. Default value: none.</td>
</tr>
<tr>
<td>SMTP_Password</td>
<td>The SMTP password to use to authenticate against the SMTP server. Default value: none.</td>
</tr>
<tr>
<td>SMTP_SAS</td>
<td></td>
</tr>
<tr>
<td>SMTP_SSLProtocol</td>
<td></td>
</tr>
<tr>
<td>DoDatabaseValidation</td>
<td>Determines if the application should perform a database validation check at application start. Default value: False</td>
</tr>
<tr>
<td>DoAssetAuthorizationCheck</td>
<td>Determines if the application should perform Digital Asset authorization checks. This setting is only required if digital assets access must be controlled. In a public Internet deployment, this value should be False. Default value: True</td>
</tr>
<tr>
<td>UseRadEditor</td>
<td>Determines if the application with use the Telerik r.a.d. Editor for WYSYWIG content. If False, a normal text editor is used. Default value: True</td>
</tr>
<tr>
<td>RequestHistory</td>
<td>Sets the number of requests to record in logging. Default value: 5</td>
</tr>
<tr>
<td>EnableCaching</td>
<td>Determines if the application should enable caching. Default value: True</td>
</tr>
<tr>
<td>EnableMultiServerCache</td>
<td>Determines if the application instance will support a multi-server cache configuration. This setting is only required if multiple application servers are used. Default value: False</td>
</tr>
<tr>
<td>ShowQuickEditIcon</td>
<td>Determines if the application will show the QuickEdit icon when editing content. Default value: True</td>
</tr>
<tr>
<td>UseWindowsEventLog</td>
<td>Provides for the option to record ACM system events in the Windows Event Log. This can make supporting multiple instances of the ACM application on a single server more convenient. Default value: False</td>
</tr>
<tr>
<td>SessionTimeoutAnonymous</td>
<td>Provides the option to set the anonymous session timeout value in minutes. Default value: 60</td>
</tr>
<tr>
<td>SessionTimeoutAuthenticated</td>
<td>Provides the option to set the authenticated session timeout value in minutes. Default value: 60</td>
</tr>
<tr>
<td>SessionTimeoutAnonymousKeepAliveInterval</td>
<td>Provides the option to send an Ajax call to keep the anonymous session alive. If this value is less than the SessionTimeoutAnonymous value, the session will be preserved until the user closes their browser or browses off the site. Default value: 30</td>
</tr>
<tr>
<td>SessionTimeoutAuthenticatedKeepAliveInterval</td>
<td>Provides the option to send an Ajax call to keep the authenticated session alive. If this value is less than the SessionTimeoutAuthenticated value, the session will be preserved until the user closes their browser or browses off the site. Default value: 30</td>
</tr>
</tbody>
</table>

**Note** You can encrypt the information within the web.config file as it contains password information for your SMTP server. To do so, log into ACM > System > System Information > expand the WEB.CONFIG SETTINGS section > click
Encrypt or Decrypt to perform those operations on the web.config file.
Configure Directory Security

Overview

The ACM application, via the ASP.NET worker process, needs file permissions to create and change files in the ACM application files.

The following files and folders need require the ASP.NET worker process to be able to modify them:

- CMSroot\CM\WebUI
- CMSroot\Sites\n- CMSroot\System\n- CMSroot\Web.config (only if you want to allow modification of these settings through the application via Admin Center > Configuration Files > Web.config tab)

The ASP.NET worker process runs as different users depending on the version of Windows, so please note the differences below.

**Note** It is also possible to configure a new Windows account and instruct ASP.Net to use this account. This is called impersonation and is required for the multi-server setup of the ACM.

Configuring permissions for Windows Server 2003

In Windows 2003, by default, the ASP.NET worker process runs under the local Windows account called NETWORK SERVICE. If the application is running as another user, that user must be substituted for NETWORK SERVICE in the instructions below.

To adjust the permissions of a file or folder:

1. Right-click the file or folder > Click **Properties**
2. Click on **Security** tab
3. Click on **Add** (if NETWORK SERVICE is not present)
4. Make sure the location is set to the local server. Do not select domain name
5. Type **NETWORK SERVICE**
6. Click the **Check Name** button
7. Click on **OK**
8. Enable the **Modify** checkbox for NETWORK SERVICE
9. Click on **OK**
10. Repeat these steps for all files and folders listed above
Configuring permissions for Windows Server 2008

In Windows 2008, by default, the ASP.NET worker process runs the ApplicationPoolIdentity user (this user is created when the Application Pool is created). The ASP.NET worker process can also run as the NETWORK SERVICE user as in Windows 2003. We will assume the ApplicationPoolIdentity user is used as that is more option according to Microsoft.

To adjust the permissions of a file or folder:

1. Right-click the file or folder > Click Properties
2. Click on Security tab
3. Click Edit
4. Click on Add (if ApplicationPoolIdentity is not present)
5. Make sure the location is set to the local server. Do not select domain name
6. Type IIS APPPOOL\NAME (replace NAME with the name of the Application Pool created for this site in IIS)
7. Click on Check Name button
8. Click on OK
9. Enable the Modify checkbox for the ApplicationPoolIdentity user
10. Click on OK
11. Repeat these steps for all files and folders listed above
Configuring IIS

IIS 6.0 (Windows Server 2003)

For a basic installation of ACM, IIS requires very little setup. Most default configuration can be used.

1. Open IIS Manager
2. Create a new Application Pool
   
   Note: Each IIS site should have its own application pool
3. Right-click on the Application Pool > Click Properties
4. Disable Recycle worker processes
5. Enable Recycle worker processes at the following time, set this to off peak hours (e.g. 2:00am)
6. Select the Performance tab
7. Disable Shutdown worker processes after being idle for
8. Click Ok
9. Create a new site in IIS. Assuming this is the only site in IIS on this server, then use the following settings. For IIS instances with multiple sites or more advanced configuration here, refer to the Appendix for IIS Bindings.
   a. Description: Enter a name for your site that will appear in IIS
   b. IP address: All Unassigned
   c. Port: 80
   d. Host header: blank
   e. Path: Select the CMSroot folder
   f. Web Site Access Permissions: Enable Read and Run scripts
10. Right-click on the site in IIS > Click Properties
11. Click Advanced > add any additional bindings necessary
12. Select the Home Directory tab
   a. Select the Application Pool created in step 2 in the Application Pool dropdown menu.
13. Select the Documents tab
   a. Ensure Default.aspx is in the default content list
14. Select the ASP.NET tab
   a. ASP.NET version: select 4.0
15. Ensure the bindings are correct (that this site is set to listen on the right IP address, TCP Port and Host Header values). If this is the only site on this server, by default, it will listen for any IP/Port/Host request.

If using Friendly URLs will be used for this site
16. Right-click on the site in IIS > Click **Properties**

17. Select the **Home Directory** tab

18. Click **Configuration**
   a. Click **Insert…**
   b. Set **Executable** to
      
      \%SYSTEMROOT\%Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
   
   **Note** Use the 64-bit framework version if this is a 64-bit operating system
   c. Uncheck **Verify that file exists**
   d. Click **OK**
   e. Ensure there are no handler mappings for *.htm and *.html

---

**IIS 7.5 (Windows Server 2008 R2)**

It is recommended to run ACM in 64-bit mode to take advantage of the improved memory addressing capabilities. For these instructions we will assume this application will be configured in 64-bit mode, however, 32-bit mode will work as well with different configuration.

**Note** Specific instructions have not been included for IIS 7.0 as very few sites are running IIS 7.0 (was only available in the original Windows Server 2008 ‘R1’ version)

1. Open IIS Manager

2. Right-click in the IIS instance > select **Add Web Site.** Assuming this is the only site in IIS on this server, then use the following settings. For IIS instances with multiple sites or more advanced configuration here, refer to the Appendix for IIS Bindings.
   - **Site Name:** Enter a name for your site that will appear in IIS
   - **Physical path:** click on … and select the CMSroot folder
   - **Type:** http
   - **IP address:** All Unassigned
   - **Port:** 80
   - **Host name:** blank

3. Click on **Application Pools**

4. Right-click on the Application Pool with the name entered into **Site Name** above > Click **Properties**
   - **.NET Framework Version:** Set to v4.0
   - **Enable 32-Bit Applications:** Set to **False**
   - **Managed Pipeline Mode:** Set to **Classic**
   - **Load User Profile:** Set to **True**
   - **Idle Time-out:** Set to a high number (e.g. 600)
   - **Click Ok**

5. Right-click on the Application Pool with the name entered into **Site Name** above > Click **Recycling**
   a. Uncheck **Regular time intervals**
   b. Enable **Specific time(s)**
   c. Enter an off peak time (e.g. 2:00 AM)
d. Click Next
e. Click Finish

**If using Friendly URLs will be used for this site**

6. Open **Handler Mappings**
7. Click **Add Script Map**
   - **Request path:** *
   - **Executable:**
     - `%SYSTEMROOT%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll`
   - **Name:** ACM Wildcard Friendly URL
8. Click **Yes** to allow this ISAPI extension
9. Ensure there are no handler mappings for *.htm and *.html
ACM Testing and Configuration

Overview

At this point, you are ready to test the site. There can be multiple ways to access the site and they all depend on how the IIS bindings and DNS are set up.

If an FQDN is set up via DNS, then browse the FQDN to access the site (e.g. http://www.mySite.com).

If the site is currently using the server host name, then browse the name of the host name of the server (e.g. http://myServer/) to access the site.

Note The first time a site starts up, it may take a few minutes as ACM loads all pages and digital asset into memory during startup to improve performance.

After starting the site, select the Login page and ensure you can log in.

Default Administrator Password

The Default Administrator username and password are:

Username: activecm
Password: good

Note It is important to change the default administrator password after you login to the system for the first time.

System-wide Administrator Setup

The System-wide Administrator is notified of system-wide issues through email, and is the From address in some emails sent to users from the system. To set an administrator:

1. Log into ACM
2. System > Click Global System Variables
3. Select the System Variables tab
4. Fill in the System-wide administration email address and System-wide administration email name fields
5. Click Save
Site Administrator Setup

The Site Administrator is notified of issues with the site and is the From address in some emails sent regarding a specific site (e.g. Approved for Publication emails).

To set an administrator:

1. Log into ACM
2. System > Click Sites
3. Select the site (most likely Your Site #1 if this is a new install)
4. Active: enabled
5. **Site Name**: the name of the Site as shown in ACM
6. **Default Email**: email address of Site Administrator
7. **Email Display Name**: display name when emails are sent from the Site Administrator
8. **Dynamic External FQDN**: The FQDN or hostname of the site (including http://). Leave blank if no current FQDN or host name is configured
9. **Enable Friendly URLS**: Enable if the friendly URL settings were enabled during the IIS setup and you wish to use friendly URLs instead of /pageXXX.aspx URLs

Support Contact Information

You can configure what support contact information users will see if they click on the Help > About ACM menu in the Admin Toolbar.

To configure the contact information:

1. Log into ACM
2. System > Click Global System Variables
3. Select the Support tab
4. Configure the information here
5. Click Save

*Note* The support contact information can be set at a site by site basis through the Sites Manager.

Register Page Types and HTML Editors

Registering page types will add all the page types which you have licenses for into the database and make them available for you to use. Registering HTML Editors will do the same for different HTML Editors in the system.

1. Log into ACM
2. System > Click Page Types
3. Click Register Page Types
4. Ensure the expected pages are registered, not all pages will be registered if you do not have the licenses for those pages
5. System > Click System Information
6. Expand HTML EDITORS
7. Click Register HTML Editors
8. Ensure the r.a.d., TinyMCE and RadAjax editors are registered successfully

FQDN Setup

ACM uses the FQDN when it needs to build a fully-qualified domain name. This field is typically not used in most operations, but in some that require the domain name of the correct site, it may not build the correct link without configuring this option.

1. System > Click Sites
2. Select the site
3. Fill in the FQDN in the External FQDN field (e.g. http://www.domain.com)
4. If the server cannot browse the internet or resolve the URL in the External FQDN field, fill in a URL that the server can resolve in the Internal FQDN field as the server will use this to build links for operations such as the static or search export (e.g. http://servername/)
5. If the site is using Friendly URLs, enable the FQDN checkbox. Make sure the Handler Mappings in the Configuring IIS section is enabled before doing this.
6. Click Save
Health Monitor Install

Installation and Configuration

The Health Monitor is used to ensure that the system is alive in memory. ASP.NET applications by default will shut down after being idle for a certain amount of time. If it’s shut off, then any scheduled tasks may not run as it requires the system to be running to poll what needs to be done at a specific time, and any users who do browse the site will have to wait for pre-caching of pages and digital assets upon the first startup of the site, which can take a while. The HealthMonitor is implemented as a system service to prevent the site from being taken offline and keep all the cache in place.

The Health Monitor package

The Health Monitor is located in the Health Monitor folder of the extracted zip file containing the ACM application files. You will receive a separate.zip file that will contain all files necessary for the Health Monitor installation.

Installation

1. Create folder to hold the Health Monitor (e.g. C:\ACM\Health Monitor).

   **Note** Do not place this within the CMSroot folder as it will need to be uninstalled before an upgrade

   **Note** This folder cannot be moved without reinstalling Health Monitor.

2. Copy the contents of the Health Monitor folder into C:\ACM\Health Monitor.

3. Open the HealthMonitor.config file in a text editor
   a. Change LogSuccess to False
   b. Fill in the SiteDownEmail details if you would like the Health Monitor service to send an email if it detects the ACM site is down.
   c. Change the MonitorURL to the URL of the site /keepalive.aspx (e.g. http://www.activenetwork.com/keepalive.aspx). This URL must be browseable on the ACM Server itself.
   d. Add additional instances if the Health Monitor needs to monitor multiple sites by adding additional <IronpointInstance> tags

4. Install the service using .NET InstallUtil.exe which is located in the following directory
   a. Open Command Prompt (with the Run as Administrator option if in Windows 2008 Server)
   b. Type in
      %SYSTEMROOT%\Microsoft.NET\Framework\v4.0.30319\installutil.exe /i "C:\ACM\Health Monitor\IronPoint.CM.HealthMonitorService.exe"
Enable Health Monitor Auto Start

1. Open Windows Services (Start > Run > type services.msc)
2. Right-click on IronPoint Health Monitor service > Click Properties
3. Select Automatic for Startup type
4. Click Start
5. Click OK

Configuration

If the HealthMonitor.Config is edited after installation, you must restart the IronPoint Health Monitor service to push the changes through. The service does not need to be reinstalled.

Uninstalling Health Monitor

If you need to uninstall the Health Monitor, you must utilize the –u flag on the installutil.exe:

1. Open Command Prompt (with the Run as Administrator option if in Windows 2008 Server)
2. Type in (if previous Health Monitor was from before 11.0)
   %SYSTEMROOT%\Microsoft.NET\Framework\v2.0.50727\installutil.exe /u "C:\ACM\Health Monitor\IronPoint.CM.HealthMonitorService.exe"
3. Type in (if previous Health Monitor was after 11.0)
   %SYSTEMROOT%\Microsoft.NET\Framework\v4.0.30319\installutil.exe /u "C:\ACM\Health Monitor\IronPoint.CM.HealthMonitorService.exe"
Appendix A: IIS Bindings

Configuring IIS Bindings

IIS can host multiple sites at a time. The way that IIS distinguishes requests for different sites is through the IIS Bindings. You can bind a specific combination of IP addresses, Port Numbers, and Host headers for each site so that a request to that combination is picked up by the right site.

The bindings are requested during the creation of a site in IIS, but are also configurable from the site properties after the site is created.

If this ACM site is the only site on this server, you can keep the default bindings:

- **IP address**: All Unassigned (a request for any IP address)
- **Port**: 80
- **Host name**: blank (a request for any host name or URL)

If there are multiple sites, the bindings must be unique across different sites in the same instance of IIS. If you have another site that listens for the exact same IP, Port, and Host, then IIS will stop one of the sites.
Common use cases for host headers are if there are 2 IIS sites (e.g. www.activenetwork.com and www.activegovernment.com), both listening on the same IP address and port 80. And the server only has a single IP address. In this scenario, you can distinguish the 2 using Host. To set this up use these bindings when setting up the IIS site:

www.activenetwork.com site:
- IP address: All Unassigned
- Port: 80
- Host name: www.activegovernment.com

www.activegovernment.com site:
- IP address: All Unassigned
- Port: 80
- Host name: www.activegovernment.com

It would be a good idea to set each site to add additional bindings for the non-www version of the domain name as well because you can create redirects in ACM to redirect requests to the non-www version of the URL to the www version using Authority Redirects. There is more information on this, in the Redirects Appendix.

www.activenetwork.com site:
- IP address: All Unassigned
- Port: 80
- Host name: activegovernment.com

www.activegovernment.com site:
- IP address: All Unassigned
- Port: 80
- Host name: activegovernment.com

For more information about bindings, this is a link to a Microsoft Blog: http://blogs.technet.com/b/chrad/archive/2010/01/24/understanding-iis-bindings-websites-virtual-directories-and-lastly-application-pools.aspx, there are also many resources with Microsoft that explain how bindings work if you require more detailed information.
Appendix B: Redirects

Overview

ACM allows you to create Authority Redirects, 301 Redirects and FQDN Mappings. These settings can be configured in the Ironpoint.config tab located in the Configuration Files section of the Admin Center.

These settings are all redirects that can be used to improve SEO (Search Engine Optimization), prevent 404 errors when moving domains, and provide an easy interface to create different types of redirects within the application.

These 3 types of redirects take priority in the order mentioned (and shown in the configuration screen).

Authority Redirects

Multiple authority redirects can be configured and each one takes an ‘authorityIn’ and a ‘targetAuthority’.

Upon receiving a request, ACM will check the authority of the request URL to see if a redirect has been configured. If a match is found, it will rebuild the URL changing the requested domain with the domain in Target Authority.

Using the example below, a request to http://domain.com/parks/animals.htm would be 301 redirected to http://www.domain.com/parks/animals.htm.

The most common use of Authority Redirects is to redirect requests to the non-www version of a URL to the www version.

301 Redirects

Multiple 301 redirects can be configured, each taking a ‘targetURL’ and defining multiple semicolon delimited URLs that will redirect to the target.

Upon receiving a request, ACM will see if the requested URL matches any of the ‘Redirect301’ path list URLs and performs a redirect to the target URL.

Using the example below, if a request is made to http://www.domain.com/home.htm or http://www.domain.com/site3.aspx the request will be redirected to http://www.domain.com/.
2 common uses of this redirect are:

1. Redirect all the different ways of reaching the home page to a single way (as above).

   **Note** You must set up an FQDN Mapping redirect in order for the above scenario to work as the default.aspx will redirect a request to www.domain.com to www.domain.com/site3.aspx

2. Shorten URLs by redirecting a simple, easier to type and remember URL to a longer one (e.g. www.domain.com/parks redirecting to www.domain.com/areas/green/parks.htm).

---

**FQDN Mapping**

Multiple FQDN mappings can be configured, each requiring an ‘FQDN’ and a target page. This will allow a user to click or type in the ‘FQDN’ and see that remain in the address bar when the actual page is loaded.

Upon receiving a request that contains only the authority, ACM will check if the request URL matches with one of the configured FQDN settings in the list of mappings. If one is found, ACM will rewrite the path server side to the specified target page, but keep the same requested URL in the browser.

Using the example below, requesting http://www.domain.com will load the Home page while remaining http://www.domain.com on the address bar.

---

A common use for this feature is in conjunction with the 301 redirects. Setting up the 301 redirects to redirect requests to www.domain.com/page4.aspx, www.domain.com/site3.aspx, www.domain.com/home.htm, and www.domain.com/default.aspx to www.domain.com, which is then caught by the FQDN Mapping and produces the home page. The net effect is, any way you access the home page will count as a hit towards www.domain.com.
Appendix C: Multiple Sites on a Single Install

Overview

ACM allows you to create multiple sites within a single install of ACM. If you wish to use different URLs or Domains to access the individual Sites created in ACM, there are 2 ways to accomplish.

1. Set up FQDN Mappings for each domain to perform the redirect depending on the requested domain.
2. Use the default.aspx file to redirect to various sites depending on the requested domain.

IIS Configuration

Ensure that the IIS instance that ACM runs on is configured to listen for each domain for each site in this ACM install by configuring the IIS bindings. See the IIS Bindings Appendix for more information.

Note You can also configure an IIS site to listen for all domains by leaving the Host Header field blank. This allows you to add new sites without needing to update the IIS Configuration to add the new domain to the bindings list.

FQDN Mapping Method

This is the preferred way to separate sites since it works in conjunction with setting up SEO-friendly URLs mentioned in the Redirects Appendix.

1. Log into ACM
2. System > Click Configuration Files
3. Select the Ironpoint.config tab
4. Click Add in the FQDN MAPPINGS section
5. Type in the domain name of the page in the FQDN column (e.g. http://www.WebSiteOne.com)
6. Click <<Select Page>> in the TARGET PAGE column and select the home page of the site this domain name should link to. Use the Site dropdown menu to select a different site if necessary
7. Repeat step 4 to 6 for each site using a different domain name
8. **OPTIONAL:** Follow the **Redirects** Appendix to complete all the redirects to minimize the number of different URLs somebody could browse the home page of your site (which increases search rankings on Google).

---

**Default.aspx Method**

As noted in the beginning of this section, the CMS\Default.aspx can be configured to redirect a request to the desired site based on the requested domain.

The default.aspx can be controlled via the ACM Configuration Files interface, or modified directly from the server using a text editor. By default, the CMS\Default.aspx will redirect requests to Site ID 3 using this syntax:

```csharp
<% Response.Redirect("~/site3.aspx") %>
```

Here is an example of syntax to redirect www.WebSiteOne.com to Site ID 3, and www.WebSiteTwo.com to Site ID 4. And return the default error 404 page it the domain does not match either of these.

```csharp
<% dim strURL as string = UCase(Request-url.tostring)

If InStr(strURL, UCase("www.WebSiteOne.com")) > 0 then
    Response.Redirect("~/site3.aspx")
ElseIf InStr(strURL, UCase("www.WebSiteTwo.com")) > 0 then
    Response.Redirect("~/site4.aspx")
Else
    Response.Redirect("~/System/Error404.htm")
End If
%>
```

There are many way to achieve this using VB.NET code, the above is simply one example.

The Default.aspx can also be managed directly from the Admin Center of ACM as well. In order to configure this:

1. Log into ACM
2. System > Click Configuration Files
3. Select the Default.aspx tab
4. Configure this page to add/edit/remove redirects for the default.aspx
The example below will have the same result as editing the default.aspx file directly.

Additionally, if you know what page you would like the **www.WebSiteOne.com** to load, you can exclude the custom response code and simply select the page in the redirect page column.
Appendix D: Video Service

Overview

The Media Center page type utilizes a video service that needs to be installed external to ACM. The Media Center page type uses the video service to encode video that is uploaded through the Digital Asset Manager as a FlashVideo file type, or through the Media Center page into an .flv format.

The service uses ffmpeg to encode the videos. For more information on ffmpeg, please refer to http://ffmpeg.org. The service is responsible for video file conversions, thumbnail generation, and parameters update (duration, size, etc.).

The version of the Video Service must match or be higher than the version of ACM.

Install the ACM Video Service

The Video Service can be installed on a server different than the ACM Server. This would only be necessary if you expect a lot of videos to be encoded constantly and would like to separate the CPU usage from the service from the website itself.

1. Install .NET 4.0 on the server that will run the video service. This can be obtained from http://www.microsoft.com/download/en/details.aspx?id=17851
2. Create a folder for the service to reside in (e.g. C:\ACM\VideoService)
3. Copy the following files from the CMSroot\bin folder to the C:\ACM\VideoService folder
   a. ffmpeg.exe
   b. VideoProcessor.Config
   c. VideoProcessorService.exe
   d. VideoProcessorService.XmlSerializers.dll
4. Open C:\ACM\VideoService\VideoProcessor.Config in a text editor
   a. Update the ffmpeg path to the video service path
      <FFmpegPath>C:\ACM\VideoService\ffmpeg.exe</FFmpegPath>
   b. Update the ACM Instance URL and path to Sites folder
      <ACMInstance>
         <SitesFolderPath>C:\ACM\Sites</SitesFolderPath>
         <QScale>9"</QScale>
      </ACMInstance>
5. To configure more sites, add additional ACMInstance tags like so:
   <ACMInstance>
      <SitesFolderPath>C:\ACM\Sites</SitesFolderPath>
      <QScale>9"</QScale>
   </ACMInstance>
<ACMInstance>
  <SitesFolderPath>C:\ACM\Sites2</SitesFolderPath>
  <QScale>9</QScale>
</ACMInstance>

6. Adjust the quality of the video conversion using the QScale number. The lower the number, the better the quality.

   **Note** Higher quality videos will mean larger digital asset sizes generated from the video conversion process.

7. Save the config file

8. Test the Digital Asset Service, browse http://www.domain.com/CM/WebServices/DigitalAssetService.asmx. The URL should display various functions that are allowed in this web service.

9. Register the ACM Video Service in Windows
   a. On the Video Service server
   b. Open the Command Prompt
   c. Run the following command
      
      %SYSTEMROOT%\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /i "C:\ACM\VideoService\VideoProcessorService.exe"
      
   d. Verify the installation completed successfully

10. Start > Click Run > Type in services.msc

11. Right-click on **Active CM Video Processor Service** > Click Properties
    a. Click **Start**
    b. Ensure Startup type is set to **Automatic**

12. Log into ACM

13. System > Click **System Events**

14. Ensure that the **Application** log has a message indicating **The video processor service has been started.**

15. Test the service by uploading videos to a Media Center page to ensure they convert properly.

   **Note** Any additional changes made to the VideoService.config file requires a restart of the Active CM Video Processor Service
Appendix E: Search Page

Overview

The following steps are necessary to configure ACM and server to support the Search page type. If you plan to not use the ACM Search page, this does not need to be set up.

How the Search Page works

The ACM Search page uses Windows Search 4.0 to index the site and perform the search operations. ACM needs to be configured to generate static versions of each page which Windows Search indexes.

When someone submits a search term, the ACM Search page then uses this index created from Windows Search to find the pages containing those words.

Install Windows Search 4.0

Windows Search 4.0 needs to be installed on the server in order for the ACM Search page to be able to use it.

Note  The Windows Search service can’t be installed if the Indexing Service (Microsoft’s previous search service used by ACM 10.3 and lower versions) is on the same computer.

Windows Server 2003

Download Windows Search 4.0 from Microsoft and install it on the ACM Server: http://support.microsoft.com/kb/940157

Windows Server 2008

1. Log into the ACM Server
2. Open Server Manager
3. Click Roles in the left menu
4. Click Add Roles in the right pane
5. Click Server Roles in the left menu
6. Enable the File Services checkbox
7. Click Next twice
8. Enable the Windows Search Service checkbox > Next
9. Enable the checkbox for the volume containing ACM to index > Click Next
10. Click Install

---

**Configure Windows Search 4.0**

Windows Search needs to be configured after install to work with ACM. In previous version

1. Start > Control Panel
2. Search for and select **Indexing Options** (you may need to set **View by:** to **Small icons** to see this option)
3. Click **Modify**
4. Disable the checkboxes on all folders from search except the `CMSroot\Sites` folder
5. Click **OK**

The Windows Search Service will start indexing and automatically continue to index.

---

**Installing Adobe’s iFilter**

In order to index contents of pdf files (be able search for words inside of pdf files through the ACM search page), you must install the Adobe iFilter on the ACM Server. The Adobe iFilter is bundled with the Adobe Acrobat Reader software.

To install the latest version of Adobe Acrobat Reader:


---

**Static Export of SearchSite files**

In order to create the SearchSite files, ACM must be configured to statically export the search files on each site that will be included in the search. This process must be scheduled in order to keep the SearchSite files and contents up to date.

1. Login to ACM
2. **System** > Click **Sites**
3. Click on the Site Name of the site you wish to enable search functionality on
4. Enter the FQDN (Fully Qualified Domain Name) that will resolve to this site in the **External FQDN** field (e.g. http://www.domain.com).

**Note** The FQDN must be browseable from the ACM Server itself. If the server is not connected to a DNS server or cannot resolve the External
FQDN, enter the IP address or an FQDN that the server can browse to, to pull up this site in the **Internal FQDN** field. (e.g. http://127.0.0.1)

5. Click **Save**

6. Perform a Static SearchSite Export
   a. **System** > Click **Export**
   b. Select the site this page is on in the **Sites** dropdown menu
   c. Ensure that the whole site is selected in **Page(s) to Export**
   d. Enable the **File Deletion** checkbox
   e. Ensure it says **SearchSite will be created** below the **Export Now** button. If it is not, the site will need to be configured to generate SearchSite files.
   f. Click **Export Now**

7. Check for errors during the export
   a. **System** > Click **System Events**
   b. Select **Export** in the **Available Logs** dropdown menu
   c. Ensure there are no errors from the export process

   **Note** Some page types will cause an error message here when exported because they do not support static search exports such as the Category and GoogleMiniSearch page types.

8. Schedule the Export to run automatically on a regular interval
   a. Select all pages in the site within the **Page(s) to Export** field
   b. Enable the days the export should occur in the **Export on Schedule** field
   c. Set the time the export should occur

   **Note** It is recommended to select a time outside of normal hours as a static export can use up CPU power on the server.

   d. Enable the **File Deletion** checkbox
   e. Click **Save**

---

**Configure the ACM Search Page**

To use the Windows Search Service, the ACM Search page must be configured to use this service

1. Log into ACM
2. Create a new Search Page
3. In the **Search Provider** field, ensure that Windows Search is selected

   **Note** The Indexing Service option is for the previous search index service that Microsoft used and has is deprecated. It is recommended to use the Windows Search server for better results because Microsoft supports it. To install the Indexing Service, refer to previous ACM Installation Guides.

4. Type **SystemIndex** in the **Catalog Name** field
5. Configure any other options that are desired
6. Publish the page
Removing Specific Pages from the Search

Pages can be configured to be removed from the search. To do this:

1. Log into ACM
2. **System** > Click **Site Design Manager**
3. Navigate to the page that needs to be removed from search > Click **Edit**
4. Uncheck **Include in Search**

This will cause this page to not be exported during a Static Search Site Export. You must either perform an export after this, with the File Deletion option enabled.

An export will initiate a static export

1. **System** > Click **Export**
2. Select the site this page is on in the **Sites** dropdown menu
3. Ensure that the whole site is selected in **Page(s) to Export**
4. Enable the **File Deletion** checkbox
5. Ensure it says **SearchSite will be created** below the **Export Now** button. If it is not, the site will need to be configured to generate SearchSite files.
6. Click **Export Now**
7. The pages removed from search will be deleted from the SearchSite folder, and then Windows Search will remove them from the index.
Appendix F: Static HTML Export

Overview

These instructions are only for customers who plan on hosting their live website using statically generated HTML pages from ACM rather than the dynamic ACM pages.

ACM can be configured to export static HTML versions of each page in the system, and then FTP this to a remote web server hosting the website. This allows ACM to be hosted on a different server than the live site which is hosting the static copy of the site.

This setup is not recommended; please see the Advantages and Disadvantages of Static Sites section for more information.

All ports are assuming the use of default ports for that application.
Definitions used in this section:

Static: the website that runs the public facing content. This is a static site that receives its contents from a static HTML export from ACM. This server does not have ACM installed.

Dynamic: the website that runs ACM. Content Providers will edit content using this website, and this performs the export of static HTML files.

Advantages and Disadvantages of Static Sites

There are some advantages and disadvantages of a static/dynamic setup as opposed to a traditional dynamic only ACM site.

Advantages of a Static/Dynamic site setup

- Ability to host the server which content providers edit content on, within a different server than the server the live site resides in.
- Ability to create new pages and entire sections of a site and view the results without publishing live.

Disadvantages of a Static/Dynamic site setup

- There are more systems and dependencies on scheduled processes, which leads to more points of failure and more maintenance involved.
- Some page types are not supported in a dynamic environment, and some require a hybrid mode in order to be supported, which is equivalent to browsing the dynamic server.
- The dynamic server needs to be externally accessible for hybrid pages to work. Some pages need to be in hybrid mode to keep the dynamic functionality available (e.g. Survey, Calendar, and Login page types).
- Pages are not published instantly. It requires content be pushed through a scheduled export process (typically once a day), or using Emergency Publish which only System Administrator users have access to.
- Exported links are different than what’s shown in the dynamic site, which can cause confusion from the content provider end.
- Personalization (the ability to restrict pages from being viewed by users who aren’t in a certain group(s)) does not work in a static/dynamic environment.
- The File Deletion checkbox (which is needed to remove pages from the static side when they are archived/inactivated/deleted in ACM) will also delete any other non ACM created file in the HTMLSites folder preventing you from storing any non-ACM files there.

Configure the Site to Export and FTP Static HTML Pages

1. Log into ACM
2. System > Click Sites
3. Select the site to be exported
4. Configure **STATIC PROPERTIES** settings:
   a. **Generate HTML Files**: This needs to be enabled in order for the Export process to statically export HTML files
   b. **FQDN**: This is the fully qualified domain name used to build a full URL for relative links. If the dynamic site has a link like “/page123.aspx”, then the export process will render the link as FQDN/page123.aspx (e.g. http://www.staticdomain.com/page123.aspx)
   c. **Virtual Directory (Alias)**: If the site will be exported into a virtual directory of the static server, type in the directory path here.
   d. **FTP URL**: This is the URL of the FTP server that the exported files will be transferred to. If this is blank, the FTP process is disabled.
   e. **FTP Protocol/Connection Mode/UserName/Password**: These options depend on the settings of your FTP server. Contact your FTP administrator for more information.
   f. **File Extension**: Files generated from the export will use this extension, typically set to .htm or .html

   **Note**: Friendly URLs will also use this extension to render their URLs

5. Configure **DYNAMIC PROPERTIES** settings:
   a. **External FQDN**: The export process will browse each page in the site to export. The way it does this is, it uses the FQDN/pageXXX.aspx?pagemode=HTML  The server will browse this link for each page. The dynamic server must be able to browse the FQDN.
   b. **Internal FQDN**: If this is specified, it will override the External FQDN in order to build the links for the server to browse each page during the export process

---

**Schedule the Export to Automatically Occur**

1. Log into ACM
2. **System** > Click Export
3. Select the site this page is on in the **Sites** dropdown menu
4. In the **SCHEDULED EXPORT** section, ensure that the whole site is selected in **Page(s) to Export**
5. Enable the **File Deletion** checkbox
6. Ensure it says **SearchSite will be created** below the **Export Now** button. If it is not, the site will need to be configured to generate SearchSite files.
7. Click **Save**
8. Test the export by performing an unscheduled export with the same options. Check the files and **System Events > Export Log** to ensure the export completed successfully.
Configuring Server Side Includes (Static Server Setup)

Server Side Includes must be enabled for the dynamic elements of a static site, such as the Section Menu, to work properly. Static sites utilize server side includes to pull dynamic content to their pages. To enable server side includes for a static website running on IIS, follow these steps:

**IIS 6.0 (Windows Server 2003)**

1. Log into the dynamic ACM Server
2. Open IIS Manager
3. Expand Web Sites
4. Right-click the ACM site > click Properties
5. Select the Home Directory tab
6. Click Configuration…
7. Check if .htm and .html are included in the Application extensions list. If they are, ensure that the below settings are correct for these extensions. If not, add them following the next steps.
8. Click Add… if the extension does not exist, and skip to step 9
9. Select the .htm extension > click Edit… if the extension already exists
10. Configure the application extension mapping as per the following figure.

```
Add/Edit Application Extension Mapping

Executable: C:\WINDOWS\system32\netsrv\ssinc.dll
Extension: .htm

Verbs
- All verbs
- Limit to: GET,POST

- Script engine
- Verify that file exists

OK Cancel Help

11. Click OK
12. Repeat step 5 to 9 for .html
13. Click OK

**IIS 7.5 (Windows Server 2008)**

1. Log into the dynamic ACM Server
2. Open IIS Manager
3. Expand the IIS instance (indicated by the server name)
4. Expand Sites
5. Select the dynamic ACM site
6. Open Handler Mappings
7. Check if `.htm` and `.html` are included in the Handler Mappings list. If they are, ensure that the below settings are correct for these extensions. If not, add them following the next steps.
8. Click Add Module Mapping…
9. Fill in the details as per this screenshot:

![Add Module Mapping](image)

10. Click OK
11. Repeat step 8 to 10 for *.html

---

**Configuring Server Side Includes (Dynamic Server Setup)**

**IIS 6.0 (Windows Server 2003)**

1. Log into the static website server
2. Open IIS Manager
3. Click Web Service Extensions in the left pane
4. Click Server Side Include
5. Click Allow

**IIS 7.5 (Windows Server 2008)**

1. Log into the static website server
2. Open Server Manager
3. Select Roles in the left menu
4. Navigate to the Web Server (IIS) section in the right pane
5. Click Add Role Services
6. Expand Application Development
7. Enable the Server Side Includes checkbox
8. Click Next and Finish
Appendix G: Shared Folders

Overview

In addition to storing data in a Database (SQL Server or Oracle), the ACM also stores data on an NTFS Volume we call Shared Folders. The Shared Folders contains all data that is not stored in the database such as digital assets and attachments uploaded from a Survey page type.

It is not necessary to configure the Shared Folders outside of what’s default, but this allows you some flexibility as to where these files are stored.

With no additional setup, all of the Shared Sites folder will automatically be stored in CMS\Sites. However, the Shared Folders can be configured to be stored in a remote location on the server or on an external File Server or NAS.

Note A central Shared Folders location is required for the ACM Multi-server setup.

Understanding Shared Folders

The contents of the Shared Folders include:

- One folder for each site, denoted by Site ID (e.g. CMS\Sites\3).
- The current template design package for each site (e.g. CMS\Sites\3\Templates).
- Archived template design packages for each site (e.g. CMS\Sites\3\archive)
- Digital Assets - that contains all documents, images, pdfs, etc. that are managed by the ACM (CMS\Sites\DigitalAssets).
- HTML files generated for Search functionality (e.g. CMS\Sites\3\SearchSite)
- HTML files generated for Static File Exports (e.g. CMS\Sites\3\HTMLSite)
- Attachments from various page types and other functionality in ACM (e.g. CMS\Sites\3\Attachments)

Note in some older versions of ACM, the attachments folder was stored directly in the Sites folder instead of underneath a specific Site ID folder.

Setting up Shared Folders in a Non-Default Location

These instructions will explain how to move the Shared Folders (/Sites) from being stored in the default CMS\Sites folder to a folder in a remote location, such as a File Server or a NAS.
Note The server that ACM resides on must be part of a domain if the Shared Folders are stored on a different server. This is because it requires domain user authentication between the ACM Server and the remote file server or NAS.

1. Create a file share on the desired location where the Shared Folders will be stored.

2. Create a domain user (that will be used as the impersonation user) whose password does not expire, and ensure this domain user has read/write access to the Shared Folders and read/write access to the file share for this Shared Folders.

3. Copy the contents of the current CMSroot\Sites folder into the SharedSites file share

4. Create a Virtual Directory (that will take place of the /Sites folder)

   **Windows Server 2003**
   
   a. Open IIS Manager
   
   b. Expand the IIS instance (indicated by the server name)
   
   c. Expand Web Sites
   
   d. Right-click on the ACM site > New > Click Virtual Directory
   
   e. Click Next
   
   f. Type SharedSites in the Alias field > Click Next
   
   g. Choose any folder in Path field (this will be changed later) > Click Next
   
   h. Click Next
   
   i. Click Finish
   
   j. Right-click SharedSites > click Properties
   
   k. Select a share located on another computer
   
   l. Type the UNC path to the share created in step 1 (e.g. \FileServer\ShareName) in the Network directory field
   
   m. Click Connect As…
   
   n. Uncheck Always use the authenticated user’s credentials when validating access to the network directory.
   
   o. Type in the User name and Password into these 2 fields. The User name field must contain the domain name (e.g. DOMAIN\jsmith)
   
   p. Click OK
   
   q. Click OK

   **Windows Server 2008**
   
   a. Open IIS Manager
   
   b. Expand the IIS instance (indicated by the server name)
   
   c. Expand Sites
   
   d. Right-click Add Virtual Directory
   
   e. Type SharedSites in the Alias folder
   
   f. Type the UNC path to the share created in step 1 (e.g. \FileServer\ShareName)
   
   g. Click OK

5. Update the web.config file

   a. Open CMSroot\web.config in a text editor

   b. Find the PhysicalPathToSharedFolder key and update the value to the file share that was created:
<add key="PhysicalPathToSharedFolder" value="\FileServer\ShareName" />

c. Find the VirtualPathToSharedFolder key and update the value to the virtual directory created in step 4.

<add key="VirtualPathToSharedFolder" value="/SharedSites" />

d. Add the following line on the line right after <system.web>

<identity impersonate="true"
    userName="DOMAIN\UserName" password="Password" />

6. Add the user Add the impersonation user to the IIS worker process group.

**Windows Server 2003**

In Windows 2003, the IIS worker process group is IIS_WPG. Add the impersonation user to this group. For more information on this group, refer to http://technet.microsoft.com/en-us/library/cc739233%28WS.10%29.aspx.

**Windows Server 2008**

In Windows 2008, the IIS worker process group is IIS_IUSRS. Add the impersonation user to this group. For more information on this group, refer to http://learn.iis.net/page.aspx/140/understanding-built-in-user-and-group-accounts-in-iis-7/.

7. Set the permissions on the ACM files for the impersonation user

8. Right-click on the Shared Folders > click Properties

9. Select the Security tab

10. Ensure that the impersonation user has Modify permissions on this folder

11. Click OK

12. Repeat this process for the following folders on the ACM Server
    - CMSroot\CM\WebUI
    - CMSroot\System
    - CMSroot\web.config (only if you want the web.config file to be configurable through ACM)

---

**Securing Digital Assets from Direct Physical Access**

By storing the physical digital asset files in CMSroot\Sites\DigitalAssets, this makes it vulnerable to viewers browsing directly to the files. ACM renames the physical files to a long string of characters making it very difficult to guess, but in order to fully prevent users from browsing directly to these files:

**Windows Server 2003**

1. Open IIS Manager
2. Expand the IIS instance (indicated by the server name)
3. Expand Sites
4. Expand the ACM Site
5. Expand Sites folder (or Virtual Directory containing the Shared Folder)
6. Right-click DigitalAssets > Click Properties
**Windows Server 2008**

1. Open IIS Manager
2. Expand the IIS instance (indicated by the server name)
3. Expand **Sites**
4. Expand the ACM Site
5. Expand **Sites** folder (or Virtual Directory containing the Shared Folder)
6. Click the **DigitalAssets** folder
7. Open **Authentication**
8. Click **Anonymous Authentication** > click **Disable** on the right pane

Since ACM will access the digital assets directly rather than the client browser accessing the physical digital asset file when requested, this will not affect ACM from retrieving the digital asset, but still block external browsers from viewing the file.
Appendix H: Multi-Server Setup

Overview

This section discusses how to set up multiple ACM Servers, connected to the same database can be configured to work in a load balanced environment. For most uses of ASP.NET, a single server can handle all requests in a timely manner. However, in order to handle high volumes of traffic or meet redundancy requirements, you may need to set up multiple ACM Servers to handle the processing and traffic.

The instructions below assume ACM is already set up in a single server environment.

The Concept of Multiple Servers in ACM

A multi-server setup with ACM consists of multiple Web servers with ACM installed, pointing at the same database and same shared /Sites folders. A file server should be provisioned to allow storage of the shared /Sites files and folders.

Additionally a load balancing mechanism is used to receive requests from users, and then distribute them among the different Web servers.

To handle caching across multiple servers, ACM uses the Cache Invalidation Service which allows servers to notify other servers; when data has changed on one server, it invalidates cache on other servers.

Something else to consider are how to manage sessions across multiple servers. With the default in process (InProc) setting, sessions are stored on the web server; if a load balancer pushes the connection to another server, the session information will not exist on the next server, and that session would be lost.

To handle this, there are a few ways to configure this:

1. Use the ASP.NET State Service. This is the optimal way to allow proper load balancing across servers because it does not rely on the load balancer to handle session affinity (same session always goes to the same web server). However this introduces a new single point of failure. But the State Service is generally regarded as a more reliable service than having a single web server as a point of failure.

2. Use SQL Server to set up a database to manage sessions. This requires additional setup on the SQL Server, and behaves much like the ASP.NET state service. This method won’t be covered in these instructions as it is recommended to use the ASP.NET state service due to its simplicity and ease to setup.

3. Allow the load balancer to handle sessions along with balancing the load. This is the simplest way to handle multiple sessions as it does not require any additional setup within ACM.
Appendix H: Multi-Server Setup

Install and Config Guide

Setting up State Server Service

If the Load Balancer is set to handle session affinity, this section can be ignored. Otherwise, follow these instructions if the ASP.NET state service is set up to manage sessions across multiple servers. Perform these operations on the server that will manage the sessions which has to be one that each web server can communicate with over.

1. Install .NET 4.0 on the ASP.NET State Service server.
2. Configure the state server to allow connections from remote machines by setting the following registry key to 1
   a. Start > Click Run
   b. Type in regedit > click OK
   c. Open
      HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_state\Parameters\AllowRemoteConnection
   d. Set Value = 1
3. Start the Service
Setting up the ACM Cache Invalidation Service

Follow these instructions on the server that will run the ACM Cache Invalidation Service (CIS). The cache invalidation service ensures that pages that have changed on one server, notifies the other servers to invalidate the cache for that page.

1. Install .NET 4.0 on the server that will run the CIS.
2. Copy all the contents of the CMSroot\bin folder into a folder on the CIS server. We will refer to this folder as the CISroot folder.

Note: The files used for the CIS must be the same ACM version as the application files on the ACM Servers.

3. Ensure license file (CacheInvalidationService.lic) is located in the CISroot folder. Contact the ACM Support Team if this license does not exist.
5. Ensure the Connection String is pointing to the correct ACM database.
6. Modify the default ports for CIS if desired
   a. Open CISroot\CacheInvalidationService.config in a text editor.
   b. Modify the <webServerPort> tag value to change which port each web server will listen on for the CIS traffic.
   c. Modify the <cisPort> tag value to change which port the CIS server will listen for the CIS traffic.
   d. Save and close CISroot\CacheInvalidationService.config.
7. Register the ACM Cache Invalidation Service
   a. Start > Run > type cmd
   b. Run the following command:
      ```
      %SYSTEMROOT%\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /i
      CISroot\CacheInvalidationService.exe
      ```
   c. Verify that the final lines written to the console by InstallUtil.exe are:
      ```
      The Commit phase completed successfully.
      The transacted install has completed.
      ```
8. Control Panel > Administrative Tools > Open Services
9. Right-click on ASP.NET State Service > click Start
10. Right-click on ASP.NET State Service > click Properties
11. Ensure Startup type is set to Automatic.
12. Log into ACM

13. **System** > Click **System Events**

14. Ensure a message is logged in the **Application** log indicating **The cache invalidation service has been started.**

**Note** The default ports which the CIS listens for traffic is port 9943, and each ACM Server listens on port 9942. These ports must be open between the CIS and ACM Servers in order for the CIS to function correctly. The ports used can be configured to use any port via the **CISroot\CacheInvalidationService.config** file.

If the CIS is not running, the ACM site will still continue to function, however changes to various pages may not show up on other server right away. This prevents the CIS from being a single point of failure, but it is imperative that the service is fixed and restarted in the event of an issue to prevent old data from being displayed on the ACM site.

---

**Creating Shared Sites folder**

In order to access the same Shared Folders between the different web servers, a central location must be created to store these files. It is recommended to set up a share on a file server to store these files.

Follow the instructions in the **Shared Folders** Appendix in the **Setting up Shared Folders** section (not to be confused with the **Setting up a Private/Public Shared Folders** section), to configure each server to point to a central folder which all ACM Servers can access.

If this central file share is not accessible, none of the templates and digital assets will be accessible on the site, which would likely leave the site displaying only text.

**Note** Ensure that the central file share is on a stable environment and is regularly backed up to ensure recoverability.

---

**ACM Server Configuration**

Follow these instructions on each ACM Server in the pool. These steps assume that the web server has been correctly configured for single-server ACM operation with the ACM files installed in **CMSroot**. Please note a number of these parameters are case sensitive.

1. Open **CMSroot\web.config** in a text editor

2. **OPTIONAL:** Immediately after the **<system.web>** element specify an encryption key to use for ViewState.

```xml
<machineKey validationKey="0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF" decryptionKey="FEDCBA9876543210FEDCBA9876543210FEDCBA9876543210"
  validation="SHA1"
  decryption="AES" />
```
The validationKey and decryptionKey should be set to 48 random hexadecimal characters, and each web server should have the same values. This enhances security by preventing rogue servers from joining the server pool.

3. If the ASP.NET State Service was chosen as the method to handle sessions, follow these instructions. Otherwise, ignore this step. Modify the sessionState settings:
   a. Open CMSroot\Web.config in a text editor
   b. Find the <sessionState> tag
   c. Set mode to “StateServer”
   d. Set stateConnectionString to “tcpip=IP:PORT” (e.g. “tcpip=127.0.0.1:42424”)

   Note IP is the host name or IP address of the server containing the state service and PORT is the port which the state service is listening on.

4. Find the EnableMultiServerCache key and set the value = True
   <add key="EnableMultiServerCache" value="True" />

5. Find the CacheInvalidationServiceAddress and change the value to the IP address of the CIS server.
   <add key="CacheInvalidationServiceAddress" value="192.168.0.48" />

6. Find the CacheInvalidationWebServerAddress and change the value to the IP address of the web server this web.config file is located on.
   Note This will be different on each web server in a cluster
   <add key="CacheInvalidationWebServerAddress" value="192.168.0.47" />

7. Add the following keys into the web.config right before the </appSettings> tag:
   <add key="MultiServerWebServerPort" value="9942"/>
   <add key="MultiServerCacheServicePort" value="9943"/>

   Note These keys only need to be added if non-standard ports are used to communicate with the CIS server. If not specified, ACM will use the default ports shown above.
Appendix I: Log File Locations

Overview

ACM sites will generate a number of log files. Here is a listing in order to help you troubleshoot issues, and know where to look when space usage is being consumed by log files.

IIS Logs

IIS, by default, logs information about every request to IIS. This logging can be configured to include or remove various pieces of information, and can be deleted safely without harming the site. To find the location of the log files:

**Windows Server 2003**
1. Open IIS Manager
2. Expand the instance (indicated by the server name)
3. Expand Web Sites
4. Right-click on the site > Click Properties
5. In the Enable Logging section of the Web Site tab, click Properties
6. The Log file directory field is the location of the IIS log files

**Windows Server 2008**
1. Open IIS Manager
2. Expand the instance (indicated by the server name)
3. Expand Web Sites
4. Click on the ACM site
5. Open Logging
6. The Directory field is the location of the IIS log files

Follow these instructions on each ACM Server in the pool. These steps assume that the web server has been correctly configured for single-server ACM operation with the ACM files installed in CMSroot.

These files can grow rapidly depending on the amount of traffic, so developing strategy to maintain these files is recommended (e.g. scheduling the files be moved to another server or compressed on a regular basis)
ACM System Event Logs

These logs are stored in the database and will log up to a certain limit defined in the ironpoint.config setting. They log important information regarding events that occur within ACM. To access them:

1. Log into ACM
2. System > Click System Events
3. Select the log type in the Available Logs dropdown menu
4. Click on the log entry to view the details

The logs are stored in the CM.LogMessages table in the database. If the site is having issues and ACM cannot be accessed, the database can be queried for information about each log entry.

Windows Event Logs

The Windows Event logs can store information about events that happen in .NET which can affect the site. Some errors will be logged in both ACM System Event Logs as well as the Windows Event Logs.


FileNotFoundException Logs

These logs are only created when Friendly URLs are created in ACM. Since ACM will handle all requests in IIS with Friendly URLs enabled, requests returning error 404 codes are not captured in the IIS logs anymore. In order to capture this information, these requests are logged in CMSroot\Sites\FileNotFoundException
Appendix J: Backup Procedures

Overview

ACM stores data in (up to) three locations: the database instance, the public shared folder, and the private shared folder (note that in most types of deployments, the public shared folder and the private shared folder will be the same location). To backup all data, each of these data repositories must be addressed.

Database Backup

Refer to your Database Administrator for best practices on backing up the database to minimize the amount of storage space needed, but maximize the ability to restore data.

Shared Folders Backup

The Shared folders should be backed up to a similar schedule as the database as the files should be about the same age, otherwise unexpected problems could occur, such as:

- Missing Template files that exist in the database, but do not physically exist in the Shared Folders causing any page to use it to not be browseable.
- Missing digital assets that exist in the database, but do not physically exist in the Shared Folders.

The default location of the Shared Folders is CMSroot\Sites. If the folder is in a non-standard location:

1. Open CMSroot\web.config in a text editor
2. Find the PhysicalPathToSharedFolder key and the value parameter is the location of these files.
3. This folder should be backed up according to the backup schedule

If Private Shared Folders are enabled:

1. Open CMSroot\web.config in a text editor
2. Find the PhysicalPathToSharedFolder key and the value parameter is the location of these files.
3. This folder should be backed up according to the backup schedule
ACM Application Files

The ACM application files (The content of CMSroot minus the Shared Folders), do not need to be regularly backed up. These files should not change often unless a configuration change is made directly on the files which we typically do not recommend.