Administering Avaya Web Conferencing

Release 5.2 Service Pack 2
October 31, 2012
04-603434
Issue 1

© 2012 Avaya Inc. All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website:
http://www.avaya.com/support

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/LicenseInfo/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those product that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at:
http://support.avaya.com/ThirdPartyLicense/

You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider. The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose. In Meeting Exchange Release 5.2 the Client Registration Server, OCS Integration Server, Conference Viewer, Web Portel and Web Conferencing servers use the Windows Server Embedded 2003, and the Client Registration Server uses Microsoft SQL 2005 Embedded. While Microsoft informs us that most Service Providers already have SPLAs in place, Avaya recommends that you contact your Microsoft dealer to assure the proper licensing of these elements.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://www.avaya.com/support. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support website:

http://www.avaya.com/support

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introducing Avaya Web Conferencing 9

Chapter 2: Creating the databases 11

Creating the first database 11

Creating the first login. 12

Creating the second database 12

Creating the second login. 13

Chapter 3: Running scripts 15

Chapter 4: Installing Java on the AWC server 17

Chapter 5: Installing AWC on the AWC server. 19

Installing AWC using the installation wizard. 19

Applying the Avaya branding 21

Replacing the jar files 21

Restarting the server 22

Configuring the default website 22

Changing the DefaultAppPool identity 22

Changing directory security on the rp folder on the IIS default Web site 23

Adding Avaya to the IIS_WPG group 23

Configuring TEM files 24

Configuring spauthurl1.tem. 24

Configuring integratedstate.tem 25

Configuring the authenticator.properties file on the Web Portal server 25

Chapter 6: Configuring billing on the AWC server 27

Loading the CRSBilling.reg file 27

Restarting AWC server 28

Logging into AWC to verify billing 28

Setting the timezone on AWC. 29

Chapter 7: Integrating audio 31

Adding Meeting Exchange to the AWC Administration screens 31

Creating a sign-in on the Meeting Exchange application server 32

Verifying audio integration 32

Chapter 8: Licensing AWC 33

Chapter 9: Configuring the recording server 35

Configuring the playback server 35

Adding a publishing point. 35

Updating the Windows media services settings. 36

Updating general settings 37

Updating authorization settings 37

Updating logging settings. 37

Updating event notification settings 37

Updating authentication settings 37

Updating control protocol settings 38

Updating limits settings 38

Updating the publishing point settings 38

Updating the source settings 39

Updating the advertising settings 39

Updating the announce settings 39

Updating the properties settings 39

Updating the Windows Media Services login 41

Configuring the AWC server for recording. 41

Installing the recording patch. 41

Modifying the registry file 42

Configuring the recording server. 43

Installing the recording patch. 43

Adding the recording server to AWC. 44

Configuring the authenticator.properties file on the Web Portal server 44

Enabling audio recording 45

Chapter 10: Upgrading from AWC 5.2 47

Upgrading to the new version of AWC 47

Notifying the users of the upgrade 48

Enabling recording 49

Changing the DefaultAppPool identity 49

Changing directory security on the rp folder on the IIS default Web site 49

Adding Avaya to the IIS_WPG group 50

Restarting AWC services 50

Configuring the recording server. 51

Index 53

Chapter 1: Introducing Avaya Web Conferencing

Avaya Web Conferencing (AWC) is an application that enables audio conference participants to share data and video during their conferences. It is a component of the Meeting Exchange suite of conferencing products. In older releases of Meeting Exchange, AWC was sometimes called Data Xchange.

This guide describes how to install and configure AWC within your deployment of Meeting Exchange 5.2. This guide is aimed at Avaya business partners, Avaya support representatives, and system administrators at customer sites.

Note:

Unfortunately, this document does not contain the passwords that are necessary for the installation and configuration of AWC. In this document, the passwords have been replaced by ********. To obtain the passwords, you must contact your Avaya support representative.

For AWC users, the *Avaya Web Conferencing Quick Reference* is available from support.avaya.com. The Avaya Web Conferencing Quick Reference is a two page document that describes the main user features.

If your deployment includes the conference recording option, you must configure three different servers: The AWC server, the playback server, and the recording server. At the start of each series of steps, this document identifies the server on which you need to perform the steps.

Note:

In a multi-cabinet environment, AWC can only support a maximum of two Meeting Exchange application servers. For more information, see the *Meeting Exchange Release Notes* which are available on support.avaya.com.

The installation and configuration of AWC consists of the following tasks:

- Creating the databases
- Running scripts
- Installing Java on the AWC server
- Installing AWC on the AWC server
- Configuring billing on the AWC server
- Integrating audio
- Licensing AWC
- Configuring the recording server

Chapter 2: Creating the databases

AWC requires Microsoft SQL Server 2005 Service Pack 2. In Microsoft SQL Server Management Studio, you must create two new databases for AWC. Once you create the new databases for AWC, you must create two logins with administrative access. You create these databases on the Meeting Exchange Client Registration Server (CRS).

- Creating the first database
- Creating the first login
- Creating the second database
- Creating the second login

Creating the first database

To create a new database:

1. Navigate to **Start** > **Programs** > **Microsoft SQL Server 2005** > **Server Management Studio**.

   Server Management Studio opens.

2. In Server Management Studio, expand **Microsoft SQL Servers** > **SQL Server Group** > **(local)**.

   Under **(local)**, there is a folder called **Databases**.

3. Right-click on **Databases** and select **New Database...**

   Server Management Studio displays the **New Database** dialog.

4. Select the **General** tab.
5. In the **Database Name** field, enter **DCMS**.
6. Set the **Collation** to **<server default>**.
7. Select the **Options** tab.
8. Set the **Recovery model** to **Simple**.
9. Set the **Compatibility level** to **SQL Server 2000 (80)**.
10. In the **Initial size (MB)** field, enter **100**.
11. In the **File properties** area, select the **Automatically grow file** checkbox.
12. Select the **By percent** button and enter a value of **10**.

13. Select the **Unrestricted file growth** button.
14. Click **OK**.

    Server Management Studio creates the new DCMS database.

Creating the first login

You must create a new login for the DCMS database with administrative access so that you can write to the fields within the database tables. To create a new login:

1. In Server Management Studio, expand **Microsoft SQL Servers** > **SQL Server Group** > **(local)** > **Security**.
2. Right-click on **Logins** and select **New Login...**

   Server Management Studio displays the **SQL Server Login Properties** window.
3. Select the **General** tab.
4. In the **Login name** field, enter **avaya**.
5. Select **SQL Server Authentication**.
6. Uncheck **Enforce password policy**.
7. In the **Password** field, enter ************ and enter it again in the **Confirm password** field.
8. Set **Default database** to **DCMS**.
9. Set **Default language** to **<default>**.
10. Select the **User Mapping** tab.
11. In the **Database role membership for DCMS** area, select **db_owner** and **public**.
12. Click **OK**.
13. Confirm the password that you created for the **avaya** user.

    Server Management Studio creates the login.

Creating the second database

Now, you must create a billing database, called data_event. To create the second new database:

1. As before, navigate to **Start** > **Programs** > **Microsoft SQL Server 2005** > **Server Management Studio**.

   Server Management Studio opens.

2. In Server Management Studio, expand **Microsoft SQL Servers** > **SQL Server Group** > **(local)**.

   Under **(local)**, there is a folder called **Databases**.

3. Right-click on **Databases** and select **New Database...**

   Server Management Studio displays the **New Database** dialog.

4. Select the **General** tab.
5. In the **Database Name** field, enter **data_event**.
6. Set the **Collation** to **<server default>**.
7. Select the **Data Files** tab.
8. In the **Initial size (MB)** field, enter **200**.
9. In the **File properties** area, select the **Automatically grow file** checkbox.
10. Select the **By percent** button and enter a value of **100**.
11. Select the **Unrestricted file growth** button.
12. Click **OK**.

    Server Management Studio creates the new data_event database.

Creating the second login

Along with the second database, you must create a new login with administrative access so that you can write to the fields within the database tables. To create a new login:

1. In Server Management Studio, expand **Microsoft SQL Servers** > **SQL Server Group** > **(local)** > **Security**.
2. Right-click on **Logins** and select **New Login...**

   Server Management Studio displays the **SQL Server Login Properties** window.

3. Select the **General** tab.
4. In the **Login name** field, enter **spectel**.
5. Select **SQL Server Authentication**.
6. Uncheck **Enforce password policy**.
7. In the **Password** field, enter ******** and enter it again in the **Confirm password** field.

8. Set **Default database** to **data_event**.
9. Set **Default language** to **<default>**.
10. Select the **Options** tab.
11. Set the **Recovery model** to **Simple**.
12. Set the **Compatibility level** to **SQL Server 2000 (80)**.
13. In the **Initial size (MB)** field, enter **100**.
14. In the **File properties** area, select the **Automatically grow file** checkbox.
15. Select the **By percent** button and enter a value of **10**.
16. Select the **Unrestricted file growth** button.
17. Select the **User Mapping** tab.
18. In the **Database role membership for data_event** area, select **db_owner** and **public**.
19. Click **OK**.
20. Confirm the password that you created for the **spectel** user.

    Server Management Studio creates the login.

Chapter 3: Running scripts

Before you proceed with the AWC installation, you must run several Meeting Exchange 5.2 scripts on the newly created databases. These scripts are in the Meeting Exchange 5.2 software package. The Meeting Exchange 5.2 installation wizard automatically runs these scripts. If you run the Meeting Exchange 5.2 installation wizard at this point, you do not need to manually run these scripts. If you do not run the Meeting Exchange 5.2 installation wizard, you must run these scripts:

- Run the data_event.sql script on the data_event table to support AWC 5.2.
- Run the Data Conferencing Billing script on the SBill database.
- Run the Reports scripts, the Web script, and Data Conference Reports script on the Reports database. The Reports database is a Meeting Exchange 5.2 database.

Note:
All of these scripts run on the CRS server.

Chapter 4: Installing Java on the AWC server

In order to successfully run AWC, you must install Java on the AWC server. The AWC software package contains the correct version of Java. By default, the Java file is located here:

```
D:\Avaya Support\Installs\Avaya Software\AWC_5.2.x.x\
MeetingServer_Install\java
```

To run the Java file, double-click the Java executable. For example:

```
jre-6u3-windows-i586-p-s.exe.
```

This filename is an example. Your version number may differ.

You can accept all the default options for the installation of Java.

Note:
Meeting Exchange supports Java, up to version 6.0.

Chapter 5: Installing AWC on the AWC server

The installation of AWC consists of a number of steps, as follows:

- Installing AWC using the installation wizard
- Applying the Avaya branding
- Replacing the jar files
- Restarting the server
- Configuring the default website
- Changing the DefaultAppPool identity
- Changing directory security on the rp folder on the IIS default Web site
- Adding Avaya to the IIS_WPG group
- Configuring TEM files
- Configuring the authenticator.properties file on the Web Portal server

Installing AWC using the installation wizard

To install AWC on the AWC server, you can use the AWC installation wizard. The installation wizard is simple to use and it guides you through the process. This section does not list all the steps in the installation wizard. It lists the most important steps and describes the information that you should enter in those significant dialogs.

To install AWC:

1. Browse to:

   ```
   D:\Avaya Support\Installs\Avaya Software\<AWC_5.2.x.x>\
   MeetingServer_Install
   ```

2. Double-click `setup.exe`.

   The installation wizard begins. The installation wizard may use the term, **MeetingServer** to refer to AWC. In addition, the release number may differ.

3. Navigate through the installation wizard in the usual way but ensure that you make the following choices:

- On the **Choose Destination Location** dialog, change the destination folder to **D:\Conferencing**.
- On the **Select Server Type** dialog, select the **Combined Master and Conference server** button.
- On the **Base Product Name** dialog, in the **Base** field, enter **Conferencing**.
- On the **Logon Account** dialog, leave the **Domain** field blank, but in the **Username** field, enter **avaya** and in the **Password** field, enter ********. If your deployment includes the conference recording option, it is very important that you configure the same username and password for the AWC server, the recording server, and the playback server.
- On the **Master Server Configuration** dialog, in the **Address** field, enter the IP address of the local machine or the fully-qualified domain name.
- On the **Access Point Configuration** dialog, in the **Access** field, enter the IP address of the local machine. If you are accessing the server externally, enter the domain name of the address that AWC users will access.
- On the **Administrator Configuration** dialog, in the **Password** field, enter ********. You will use this password to perform additional configuration tasks on the AWC screens, so make a note of this password.
- On the **MeetingServer Database Location Configuration** dialog, in the **Location** field, enter the IP address or the domain name of the machine on which you created the databases in Creating the first database on page 11. In the **Name** field, enter the database name which you used in Creating the first database on page 11. For example, **DCMS**.
- On the **MeetingServer Database Userid Configuration** dialog, in the **UserID** field, enter the login name that you used in Creating the first login on page 12. In the **Password** field, enter the password that you used in Creating the first login on page 12. For example, **avaya** and ********.

After you review the installation settings, the installation wizard begins the installation process. When the installation process is complete, the installation wizard displays an information dialog. The information dialog displays the path and filename of the installation files. For example, `D:\Conferencing\Configuration\DCMSCFG.REG`.

4. Make a note of the path and filename of the installation files. This information is useful for future upgrades.
5. On the **InstallShield Wizard Complete** dialog, select **No, I will restart my computer later**. You must apply the Avaya branding before you restart the server.
6. Click **Finish** to complete the installation.

Applying the Avaya branding

To apply the Avaya branding to your installation of AWC:

1. Backup any existing branding files that are located in:

   `D:\Conferencing\client`

   `D:\Conferencing\Jenga`

   `D:\Conferencing\server`

2. Browse to:

   ```
   D:\Avaya Support\Installs\Avaya Software\<AWC 5.2.x.x>\
   AvayaBranding for <AWC 5.2.x.x>
   ```

3. Right-click the `AvayaBranding for <AWC 5.2.x.x>.zip` file and select **Extract to here**.
4. Copy the contents of the `client`, `Jenga`, and `server` folders to:

   `D:\Conferencing\client`

   `D:\Conferencing\Jenga`

   `D:\Conferencing\server`

5. Overwrite the existing folders.

Replacing the jar files

To replace the jar files:

1. Backup and delete the following files from `D:\Conferencing\Jenga`:

   `bapi.jar`

   `bcapi-1.6.jar`

2. Browse to:

   `D:\Avaya Support\Installs\Avaya Software\<AWC 5.2.x.x>`

3. Right-click on BC-API update for AWC 5.2.x.x(ACPIv61).zip.
4. Copy the files that are in the Jenga folder and paste them into:

   `D:\Conferencing\Jenga`

Restarting the server

To restart the server:

1. Navigate to **Start** > **Shutdown** and from the **What do you want the computer to do?** drop-down menu, select **Restart**.
2. From the **Option** drop-down menu, select **Application: Installation (Planned)**.
3. In the **Comment** field, enter a line of detail.
4. Click **OK**.

Configuring the default website

To configure the default website:

1. Navigate to **Start** > **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Expand **<Computer Name>(local computer)** > **Web Sites**.
3. Right-click **Default Web Site** and select **Properties**.

   The Internet Information Services (IIS) Manager displays the **Default Web Site Properties** dialog.
4. On the **Home Directory** tab, select **A directory located on this computer** and click **Browse**.
5. Browse to `D:\Conferencing\client` and click **Apply**.
6. Click **OK**.

Changing the DefaultAppPool identity

To update the DefaultAppPool identity:

1. If IIS Manager is not open already, navigate **Start** > **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Expand **<Computer Name>(local computer)** > **Application Pools**.
3. Right-click **DefaultAppPool** and select **Properties**.

   IIS Manager displays the **DefaultAppPool Properties** dialog.

4. On the **Identity** tab, select **Configurable** and click **Browse**.
5. On the **Select User** dialog, enter **Avaya** in the **Enter the object name to select** field and click **Check Names**.

   IIS Manager should auto-complete the **Enter the object name to select** field.
6. On the **Select User** dialog, click **OK**, and then on the **Default AppPool Properties** dialog, click **Apply** then **OK**.

Changing directory security on the rp folder on the IIS default Web site

1. If IIS Manager is not open already, navigate **Start** > **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Expand **<Computer Name>(local computer)** > **Web Sites** > **Default Web Site**.
3. Right-click the **rp** folder and select **Properties**.

   IIS Manager displays the **Properties** dialog.
4. On the **Directory Security** tab, in the **Authentication and access control** panel, click **Edit...**

   IIS Manager displays the **Authentication Methods** dialog.
5. Click **Browse**.
6. On the **Select User** dialog, enter **Avaya** in the **Enter the object name to select** field and click **Check Names**.

   IIS Manager should auto-complete the **Enter the object name to select** field.
7. On the **Authentication Methods** dialog, in the **Password** field, enter ********.
8. Click **OK**.
9. On the **Confirm Password** dialog, re-enter the password and click **OK**.
10. On the **Properties** dialog, click **Apply** then **OK**.

Adding Avaya to the IIS_WPG group

To add Avaya to the IIS_WPG group:

1. Navigate to **Start** > **Programs** > **Administrative Tools** > **Computer Management**.

2. On the **Computer Management** screen, expand **System Tools** > **Local Users and Groups** > **Groups** > **IIS_WPG**.
3. Right-click **IIS_WPG** and select **Properties**.

   The Computer Management application displays the **IIS_WPG Properties** dialog.
4. Click **Add**.
5. On the **Select User** dialog, enter **Avaya** in the **Enter the object name to select** field and click **Check Names**.

   IIS Manager should auto-complete the **Enter the object name to select** field.

   The Computer Management application adds Avaya to the group.

Configuring TEM files

There are two TEM files: `spauthurl1.tem` and `integratedstate.tem`.

- Configuring spauthurl1.tem
- Configuring integratedstate.tem

Configuring spauthurl1.tem

To configure `spauthurl1.tem`:

1. Browse to `D:\Conferencing\Jenga\branding`.
2. Right-click `spauthurl1.tem` and select **Edit**.

   The tem file opens in Notepad.
3. Find the following lines:

   ```
   !! !SET SP_AUTH_URL http://localhost/servlet/
   DCL.MeetingServer.Admin.DCMSAdmin?
   ```

   ```
   ! SET SP_AUTH_URL http://<yourserver>/Authenticator/servlet/
   Authenticator
   ```
4. Update `<yourserver>` with the IP address of the Web Portal server.
5. Save and close `spauthurl1.tem`.

Configuring integratedstate.tem

To configure `integratedstate.tem`:

1. Browse to `D:\Conferencing\Jenga\branding`.
2. Right-click `integratedstate.tem` and select **Edit**.

   The tem file opens in Notepad.
3. Verify that the following line is in the file:

   ```
   !SET INTEGRATED_AUDIO EXTERNAL
   ```
4. Save and close `integratedstate.tem`.

Configuring the authenticator.properties file on the Web Portal server

To configure authenticator.properties:

1. On the Web Portal server, browse to:

   ```
   D:\Webportal\Tomcat\webapps\Authenticator\Authenticator.properties
   ```
2. In the `# DataXchange Authenticator Servlet Properties File` section, enter the IP address of the CRS server in the `CRSIPADDRESS` parameter.

   ```
   CRSIPADDRESS=xxx.xxx.xxx.xxx
   ```
3. Save an close authenticator.properties.

Chapter 6: Configuring billing on the AWC server

Configuring billing consists of the following tasks:

- Loading the CRSBilling.reg file
- Restarting AWC server
- Logging into AWC to verify billing
- Setting the timezone on AWC

Loading the CRSBilling.reg file

To load the `CRSBilling.reg` file:

1. On the AWC server, browse to `D:\Conferencing\server\`.
2. Edit the `CRSBilling.reg` file as follows:
    a. Enter the IP address of the CRS server.
    b. Change the HKEY LOCAL MACHINE PATH from:

    ```
    [HKEY_LOCAL_MACHINE\SOFTWARE\Avaya\DCMS\Admin]
    ```

    `To`

    ```
    [HKEY_LOCAL_MACHINE\SOFTWARE\Data Connection\DCMS\Admin]
    ```

    `The updated file should appear like this:`

    ```
    [HKEY_LOCAL_MACHINE\SOFTWARE\Data Connection\DCMS\Admin]
    "BillingMethod"="database"
    "BillingUsername"="spectel"
    "BillingPassword"="*******"
    "BillingDatabase"="jdbc:sqlserver://<CRS IP ADDRESS>;
    DatabaseName=data_event;SelectMethod=cursor"
    ```
3. Save and close `CRSBilling.reg`.
4. Double-click `CRSBilling.reg` to add the setting to the registry.

5. Navigate to **Start** > **Run** and enter **regedit**.

   The computer opens the registry.

Restarting AWC server

To restart the AWC server:

1. On the AWC server, navigate to **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Stop the services **Conferencing Gateway** and **IIS Admin Service**.

   The **World Wide Web Publishing** service should stop too.
3. Start the services **World Wide Web Publishing** and **Conferencing Gateway**.

Logging into AWC to verify billing

Avaya recommend verifying if billing is successfully operating.

To verify billing:

1. Create an on-demand reservation. You can use any of the booking applications, such as CRS Front End, Web Portal, Bridge Talk, or either of the Avaya Plug-ins for Microsoft Outlook or IBM Lotus Notes.
2. Enter the conference using this IP address:

   ```
   http://<IP address of AWC>/Conferencing
   ```
3. On the **Join Conference** screen, enter the username, phone number, conference reference, and security code. Within the Meeting Exchange environment, security code is often called passcode. A moderator passcode grants access to moderator-level features and a conferee passcode grants access to conferee-level features.
4. Once you are in the conference, remain there for a few minutes and then, close the conference.
5. On the CRS server, where you have installed SQL Server Management Studio, select the `data_event` database.
6. Open the conference table and return all rows.
7. Confirm that there is a record for the conference you just created and used.

Setting the timezone on AWC

To set the timezone on the AWC server:

1. On the AWC server, browse to `D:\Conferencing\server\`.
2. Double-click `gettz.bat`.

   The `gettz.bat` file executes and changes the local timezone.

Chapter 7: Integrating audio

For the AWC integrated roster function to operate successfully, you must add the Meeting Exchange application server, or *bridge*, to the AWC Administration screens. The integrated roster function ensures that telephone icons are displayed in the **Participants** panel during a conference.

For the AWC integrated roster function to operate successfully, you must also create an operator sign-in on the Meeting Exchange application server. The operator sign-in must have the same username and password that you configure for the Meeting Exchange application server when you add it to the AWC Administration screens.

- Adding Meeting Exchange to the AWC Administration screens
- Creating a sign-in on the Meeting Exchange application server
- Verifying audio integration

Adding Meeting Exchange to the AWC Administration screens

To add the Meeting Exchange application server:

1. Log in to the AWC administration screens by entering the following string in your browser:

   ```
   http://<server IP>/Conferencing/admin
   ```

2. Log in as an administrator, using the password ********.
3. From the menu on the right of the screen, click **Manage Audio Bridges** > **Add a new audio bridge**.
4. Select the type of bridge that you want to add. For this release, select **Avaya Meeting Exchange Audio Conference Bridges**.
5. On the **Avaya Meeting Exchange Audio Conference Bridges** screen, enter the following information:
   - The hostname of the audio conferencing bridge (Meeting Exchange application server).
   - The authentication group. Avaya recommends entering `1`.
   - The IP address
   - The login username and password. For example, enter **data** and **data** for both of these fields.

Creating a sign-in on the Meeting Exchange application server

A sign-in consists of a login name and a password created for a Bridge Talk user. The privilege level for a sign-in specifies which Bridge Talk resources that sign-in can use and what management interface menus the sign-in can access. You can create sign-ins by logging in to Meeting Exchange as `dcbadmin` or `dcbmaint` and navigating to `System Administration Main Menu` > `Sign-In Management`. The operator sign-in that you create must have the same username and password as you entered in Adding Meeting Exchange to the AWC Administration screens. In this example, the username is **data** and the password is **data**.

For more information on sign-ins, see *Administering Meeting Exchange Servers*, which is available on support.avaya.com.

Verifying audio integration

To verify that audio integration is operating successfully, you can use the on-demand conference that you created in Logging into AWC to verify billing on page 28:

1. Dial into the conference using a telephone and entering the moderator or conferee passcode.
2. Access the Web conference using this IP address:

   ```
   http://<IP address of AWC>/Conferencing
   ```
3. On the **Join Conference** screen, enter the username, phone number, conference reference, and in the **Security Code** field, enter the same moderator or conferee passcode.

   You can see the participants who have joined by telephone in the **Participants** window.

Chapter 8: Licensing AWC

To add licenses at the customer site, you must copy the `licence.reg` file and execute it. By default, AWC ships with five licenses. These five licenses are intended for testing purposes. The statework of work will specify the type of licenses and also the number of licenses. Avaya recommends confirming the number of required licenses before you begin to load them.

To load the licenses:

1. On the AWC server, double-click `license.reg` to add the setting to the registry.
2. Restart the server:
    a. On the AWC server, navigate to **Start** > **Control Panel** > **Administrative Tools** > **Services**.
    b. Stop the services **Conferencing Gateway** and **IIS Admin Service**.

        The **World Wide Web Publishing** service should stop too.
    c. Start the services **World Wide Web Publishing** and **Conferencing Gateway**.
3. Log in to the AWC administration screens by entering the following string in your browser:

    `http://<server IP>/Conferencing/admin`
4. Log in as an administrator, using the password ********.

    You should now be able to see the types of licenses and also the number of licenses that you have loaded. You can enter multiple types of licenses at the same time.

Chapter 9: Configuring the recording server

The recording feature is an optional extra. You can buy the AWC solution without the recording feature. The recording feature requires two servers: A playback server and a recording server. The playback server is often called a streaming server.

- Configuring the playback server
- Configuring the AWC server for recording
- Configuring the recording server

Configuring the playback server

The playback server must be a Windows 2003 server. There are a number of steps in the configuration of the playback server, as follows:

- Adding a publishing point
- Updating the Windows media services settings
- Updating the publishing point settings
- Updating the Windows Media Services login

Adding a publishing point

To configure the playback server:

1. Navigate to **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Disable the following services:
    - IIS
    - www
    - Apache
    - Tomcat Conference Viewer
3. Copy the `i386` folder from the Windows 2003 server CD to the local hard drive so that you have all the services available locally.

4. Navigate to **Start** > **Control Panel** > **Add/Remove Programs** > **Add/Remove Windows Components**.
5. On the **Windows Components Wizard**, select the checkbox beside **Windows Media Services** and follow the steps.
6. Open **Windows Media Services** and navigate to **Action** > **Add Publishing Point (Wizard)** to start the **Add Publishing Point Wizard**.

   The wizard is simple to use and it guides you through the process. This section does not list all the steps in the wizard. It lists the most important steps and describes the information that you should enter in those significant dialogs.

   - On the **Publishing Point Name** dialog, in the **Name** field, enter **Recordings**.
   - On the **Content Type** dialog, select **Files (digital media or playlists)**.
   - On the **Publishing Point Type** dialog, select **On-demand publishing point**.
   - On the **Directory Location** dialog, in the **Location of directory** field, enter the location of you central recording files. For example, `\\<ipaddress of recording server>\Recording`.
   - On the **Content Playback** dialog, ensure that the **Loop** checkbox and the **Shuffle** checkbox are not selected.

   Note:
   If you want to monitor clients, you can enable logging, though it is not mandatory.

7. After you review the publishing settings, on the **Completing the Add Publishing Point Wizard** dialog, de-select **After the Wizard finishes** and click **Finish**.

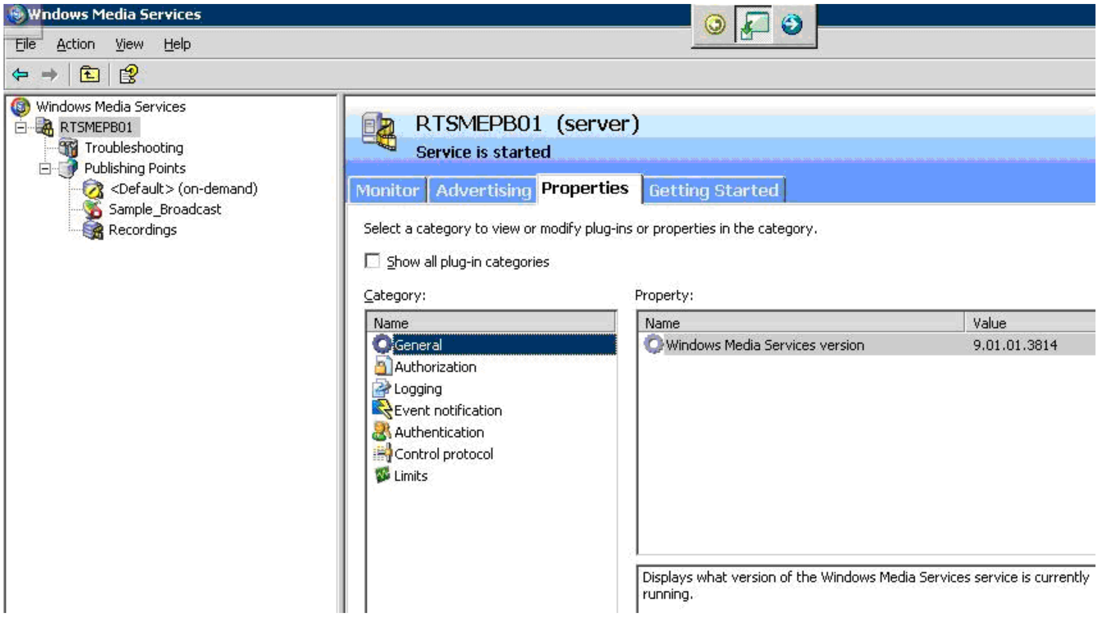
Updating the Windows media services settings

After you add the publishing point on the playback server, you must update the Windows Media Services settings. You must ensure that your configuration has the same settings as those listed here. There are a number of categories, as follows:

- Updating general settings
- Updating authorization settings
- Updating logging settings
- Updating event notification settings
- Updating authentication settings
- Updating control protocol settings
- Updating limits settings

Figure 1 shows the categories.

Figure 1: Windows Media Services Settings



RTSMEPB01 (server)

Service is started

Select a category to view or modify plug-ins or properties in the category.

☐ Show all plug-in categories

Category:

Name
General
Authorization
Logging
Event notification
Authentication
Control protocol
Limits

Property:

Name	Value
Windows Media Services version	9.01.01.3814

Displays what version of the Windows Media Services service is currently running.

Updating general settings

Ensure that Windows Media Services version is 9.01.01.3814.

Updating authorization settings

- Ensure that **WMS NTFS ACL Authorization** is disabled.
- Ensure that **WMS IP Address Authorization** is disabled.
- Ensure that **WMS Publishing Points ACL Authorization** is disabled.

Updating logging settings

Ensure that **WMS Client Logging** is enabled.

Updating event notification settings

Ensure that **WMS WMI Event Handler** is enabled.

Updating authentication settings

- Ensure that **WMS Anonymous User Authentication** is disabled.

- Ensure that **WMS Negotiate Authentication** is disabled.

Updating control protocol settings

- Ensure that **WMS HTTP Server Control Protocol** is enabled.
- Ensure that **WMS MMS Server Control Protocol** is enabled.
- Ensure that **WMS RTSP Server Control Protocol** is enabled.

Updating limits settings

Ensure that your configuration has the same settings as those listed in Table 1.

Table 1: Limits Settings

Limit	Value
Limit player connections	Unlimited
Limit outgoing distribution connections	Unlimited
Limit aggregate player bandwidth (Kbps)	Unlimited
Limit aggregate outgoing distribution bandwidth	Unlimited
Limit bandwidth per stream per player (Kbps)	Unlimited
Limit bandwidth per outgoing distribution stream	Unlimited
Limit connection rate (per second)	50
Limit player timeout activity (seconds)	3600
Limit connection acknowledgement (seconds)	60
Limit incoming bandwidth (Kbps)	Unlimited

Updating the publishing point settings

On the playback server, after you update the Windows Media Services settings, you must update the publishing point settings. You must ensure that your configuration has the same settings as those listed here. There are a number of categories:

- Updating the source settings
- Updating the advertising settings
- Updating the announce settings

- Updating the properties settings

To access the publishing point settings, right-click on the publishing point that you created in Adding a publishing point on page 35. In this example, the publishing point is called **Recordings**.

Updating the source settings

Ensure that the **Content Source** panel displays the directory that you entered on the **Directory Location** dialog in Adding a publishing point on page 35.

Updating the advertising settings

Ensure that, in the **Wrapper advertisements** panel, **Use a wrapper with this publishing point** is not selected.

Updating the announce settings

Ensure that, in the **Players can directly connect to your content** selection, the correct URL and prefix (`mms`) are displayed. This should display the URL of the playback server.

Updating the properties settings

Ensure that you enable settings, as listed in Table 2.

Table 2: Properties Settings

Category	Plug-in	Status
General		
	Enable Fast Cache	Enabled
	Enable caching by cache/proxy servers	Enabled
	Enable access to directory conent using wildcards	Disabled
Authorization		
	WMS NTFS ACL Authorization	Disabled
	WMS IP Address Authorization	Disabled
	WMS Publishing Points ACL Authorization	Disabled
Logging		
		1 of 2

Table 2: Properties Settings (continued)

Category	Plug-in	Status
	WMS Client Logging	Enabled
Event notification		
	WMS WMI Event Handler	Disabled
Authentication		
	WMS Anonymous User Authentication	Disabled
	WMS Negotiate Authentication	Disabled
Limits		
	Limit player connections	Unlimited
	Limit outgoing distribution connections	Unlimited
	Limit aggregate player bandwidth	Unlimited
	Limit aggregate outgoing distribution bandwidth	Unlimited
	Limit bandwidth per stream per player	Unlimited
	Limit bandwidth per outgoing distribution stream	Unlimited
	Limit Fast Start bandwidth per player	3500
	Limit Fast Cache content delivery rate	5
Playlist transform		
	WMS Playlist Transform	Enabled
Cache/Proxy		
	Cache expiration	Expire in 86400 seconds
Credentials		
	Specify distribution credentials	Not specified
		2 of 2

Updating the Windows Media Services login

To update the Windows Media Services login on the playback server:

1. Navigate to **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. In the list of services, right-click **Windows Media Services** and select **Properties**.
3. In the **Windows Media Services Properties** dialog, on the **Log On** tab, select **This account**.
4. In the **This account** field, enter `.\administrator`.
5. In the **Password** and **Confirm Password** fields, enter a new password.

   If your deployment includes the conference recording option, it is very important that you configure the same username and password for the AWC server, the recording server, and the playback server. The password should be ********.
6. Click **OK** to save the changes.

Configuring the AWC server for recording

You must configure the AWC server to enable recording. To configure the AWC server, there are a number of steps:

- Installing the recording patch
- Modifying the registry file

Installing the recording patch

To install the recording patch, you can use the installation wizard. This section does not list all the steps in the installation wizard. It lists the most important steps and describes the information that you should enter in those significant dialogs.

1. Run the recording patch by browsing to `D:\Avaya Support\Avaya Software\AWC\5.2\Meetingserver_x.x.x_RecordingOPInstall.zip` and extracting the files.
2. Click **setup.exe** to open the **Recording Option Pack Setup** installation wizard.
3. Navigate through the installation wizard in the usual way but ensure that you make the following choices:

- On the **Choose Destination Location** dialog, click **Browse** and enter the following path:

  `D:\Conferencing\Recording`
- On the **Setup Type** dialog, select **External Audio Bridge**.
- On the **Recordings Directory** dialog, enter the full IP and path of the recording folder on the recording server. You will create this folder in step 1 of Installing the recording patch on page 43.
- On the **Recording Server Access Point** dialog, in the **Name** field, enter the IP address of the recording server.
- On the **Streaming Server Publishing Point** dialog, in the **Name** field, enter the path of the recording folder that you created in Adding a publishing point on page 35.

4. When the installation wizard completes, make a note of the location where it has created the registry file.
5. Do no restart the server at this point.

Modifying the registry file

The installation wizard automatically creates a registry file. However, you must edit it. To modify the registry file:

1. On the AWC server, navigate to **Start** > **Run** and enter **regedit**.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE_Data_Connection\DCMS\Recorder`
3. In the Publishing Point data field, change the syntax from **mms** to **http**.
4. Browse to `D:\Conferencing\RecordingServer\Configuration\RecordingServer.reg.`
5. In the **RecordingServer.reg** file, change the syntax from **mms** to **http**.
6. Copy this file to a temporary folder on the recording server and make a note of the folder. For more information on this step, see 5 of Configuring the recording server on page 43.
7. Restart the AWC server.
8. Navigate to **Start** > **Add/Remove Programs** and verify that **Recording Options Pack** is listed in the Programs list.

Configuring the recording server

Next, you must configure the recording server. To configure the recording server, there are a number of steps:

- Installing the recording patch
- Adding the recording server to AWC
- Configuring the authenticator.properties file on the Web Portal server
- Enabling audio recording

Installing the recording patch

To record audio and video, the recording server requires a dialogic card.

To record video, but not audio, the recording server does not require a dialogic card.

To configure the recording server:

1. Create a folder on `D:\Recording`.
2. Change the permission on this folder to **Share to All**.
3. Ensure that the media server and the AWC server can access this folder without having to enter a username and a password. You should ensure that all the servers: The AWC server, the recording server, and the playback server have the same login ID and password.
4. Run the recording server patch by browsing to `D:\Avaya Support\Avaya Software\AWC\5.2\Meetingserver_x.x.x_RecordingOPInstall.zip` and extracting the files. Follow the same steps that you did in Installing the recording patch on page 41.
5. Edit the registry file that you copied to the recording server in step 6 of Modifying the registry file on page 42 to ensure that the username and password in the registry file is the same as the login ID and password of the recording server.
6. Restart the recording server.
7. Navigate to **Start** > **Add/Remove Programs** and verify that **Recording Server** is listed in the **Programs** list.
8. Navigate to **Start** > **Control Panel** > **Administrative Tools** > **Services** and verify that **Conferencing Gateway** is in the services list and that it has the status, **Started**.

   If Conferencing Gateway does not appear as a service, it may be that the username and password of the registry file is not the same as the login ID and password of the recording server.

Adding the recording server to AWC

To add the recording server to AWC:

1. Log in to the AWC administration screens by entering the following string in your browser:

   ```
   http://<server IP>/Conferencing/admin
   ```

2. Log in as an administrator, using the password ********.
3. From the menu on the right of the screen, click **Manage Recording Servers**.
4. Click **Add a new Recording Server**.
5. On the **Add new Recording Server** screen, enter the recording server details:
   - Recording Server name
   - IP Address
   - Recording Server DNS name
   - Number of telephone numbers (for example, 1)
6. In the **Recording Server name** field, ensure that you do not use spaces.
7. Click **Add**.
8. In the **Server Management** panel, in the **Telephone Number 1** field, enter a DDI for a SCAN type of conference. For more information on DDIs, SCAN conferences, and Meeting Exchange telephone number configuration, see *Administering Meeting Exchange Servers*, which is available on support.avaya.com.
9. Click **OK** and then log out of the AWC administration screens.

Configuring the authenticator.properties file on the Web Portal server

You must configure the authenticator.properties file on the Web Portal server to take account of AWC recording. The syntax of this code is very specific. You must ensure that you add the tilde (~) symbol and also the exact number of commas after the telephone number. The commas represent a timed pause during DTMF number collection.

To configure authenticator.properties:

1. On the Web Portal server, browse to:

   ```
   D:\Webportal\Tomcat\webapps\Authenticator\Authenticator.properties
   ```

2. If you would like to record audio and video:

   Towards the end of the file, enter the dial-in number to the Meeting Exchange application server, or bridge, in the DIALSTRING parameter, as follows:

   ```
   #The servlet will fill in the variables %REF, %P and %M to make up
   the SPJoining Details output parameter

   #DIALSTRING=<Telephone number of Meeting Exchange application
   server>~,,,,%P#

   DIALSTRING=<Telephone number of Meeting Exchange application
   server>~,,,,,,,,,,,%M#
   ```

   P is the conferee passcode and M is the moderator passcode.

3. If you would like to record video and not audio:

   Ensure that you comment out the following lines:

   ```
   #The servlet will fill in the variables %REF, %P and %M to make up
   the SPJoining Details output parameter

   #DIALSTRING=<Telephone number of Meeting Exchange application
   server>~,,,,%P#

   #DIALSTRING=<Telephone number of Meeting Exchange application
   server>~,,,,,,,,,,,%M#
   ```

4. Save an close authenticator.properties.

Enabling audio recording

Note:
You do not need to perform this step if you are only recording data. If you intend to record audio and data in your deployment, you must perform this step.

Run the entry for the dialogic board so that the registry contains the entry, **Digital Dialogic**.

Chapter 10: Upgrading from AWC 5.2

You can upgrade to Avaya Web Conferencing (AWC) 5.2 Service Pack 2 from AWC 5.2 or AWC 5.2 Service Pack 1. If you have an AWC recording server in your deployment, you must also enable the recording feature in the new version of AWC. If you do not have a recording server, you do not have to perform this task.

- Upgrading to the new version of AWC
- Notifying the users of the upgrade
- Enabling recording

Upgrading to the new version of AWC

The process of installing the 5.2 Service Pack 2 version of AWC involves running the installation wizard, applying a patch, applying a branding, and copying some Java files.

To install the new version of AWC:

1. Make a copy of the `Conferencing` directory and save it in a secure location.

   This is a back-up of the AWC 5.2 installation directory. You should save this folder in its current state before you attempt the upgrade.
2. Obtain the `MeetingServer_Install for AWC 5.2.2.0.3.zip` file and extract it to a temporary directory.
3. Run the `setup.exe` file as per a normal install.

   The upgrade wizard does not have many screens. Accept the defaults.
4. On the **InstallShield Wizard Complete** dialog, select **No, I will restart my computer later**.
5. Click **Finish** to complete the installation.
6. Obtain the `MeetingServer_Patch for AWC 5.2.2.0.3.zip` file and extract it to the directory in which you installed AWC.
7. Obtain the `AvayaBranding for AWC 5.2.2.0.3.zip` file and extract it to the directory in which you installed AWC.
8. Delete the following files from the directory in which you installed AWC:

   ```
   <location of AWC>/Jenga/bapi.jar
   ```

   ```
   <location of AWC>/Jenga/bcapi-1.6.jar
   ```

9. Obtain the `BC-API update for AWC 5.2.2.0.3.zip` file and extract it to a temporary directory.
10. Open the `BC-API update for AWC 5.2.2.0.3.zip` file and copy all the .jar files into the Jenga folder in the directory in which you installed AWC:

    ```
    <location of AWC>/Jenga
    ```
11. In the `Jenga` directory, open the `branding` folder
12. Right-click `spauthurl1.tem` and select **Edit**.

    The tem file opens in Notepad.
13. Find the following lines:

    ```
    !! !SET SP_AUTH_URL http://localhost/servlet/
    DCL.MeetingServer.Admin.DCMSAdmin?
    ```

    ```
    ! SET SP_AUTH_URL http://<yourserver>/Authenticator/servlet/
    Authenticator
    ```
14. Update `<yourserver>` with the IP address of the Web Portal server.
15. Save and close `spauthurl1.tem`.
16. Restart the server by navigating to **Start** > **Shutdown**> **Restart**.
17. From the **Option** drop-down menu, select **Application: Installation (Planned)**.
18. In the **Comment** field, enter a line of detail to describe the reason for the restart.
19. Click **OK**.

Notifying the users of the upgrade

It is important to notify the AWC users of any upgrade, for example, by sending them an e-mail. You must notify them because in order to access the new version of AWC, they must clear their browser cache. It is a good idea to provide the users with clear instructions on how to clear their browser cache. The instructions depend on the type of browser. For example:

To clear a browser cache:

1. On Microsoft Internet Explorer, navigate to **Tools**>**Internet Options**.
2. On the **General** tab, in the **Browsing history** panel, click **Settings**.
3. Click **View Files** and delete the contents of the folder.
4. Click **OK**.

Enabling recording

The process of enabling recording for the AWC upgrade involves the following tasks:

- Changing the DefaultAppPool identity
- Changing directory security on the rp folder on the IIS default Web site
- Adding Avaya to the IIS_WPG group
- Restarting AWC services
- Configuring the recording server

Changing the DefaultAppPool identity

To update the DefaultAppPool identity:

1. If IIS Manager is not open already, navigate **Start** > **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Expand **<Computer Name>(local computer)** > **Application Pools**.
3. Right-click **DefaultAppPool** and select **Properties**.

   IIS Manager displays the **DefaultAppPool Properties** dialog.
4. On the **Identity** tab, select **Configurable** and click **Browse**.
5. On the **Select User** dialog, enter **Avaya** in the **Enter the object name to select** field and click **Check Names**.

   IIS Manager should auto-complete the **Enter the object name to select** field.
6. On the **Select User** dialog, click **OK**, and then on the **Default AppPool Properties** dialog, click **Apply** then **OK**.

Changing directory security on the rp folder on the IIS default Web site

1. If IIS Manager is not open already, navigate to **Start** > **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Expand **<Computer Name>(local computer)** > **Web Sites** > **Default Web Site**.
3. Right-click the **rp** folder and select **Properties**.

   IIS Manager displays the **Properties** dialog.

4. On the **Directory Security** tab, in the **Authentication and access control** panel, click **Edit...**

   IIS Manager displays the **Authentication Methods** dialog.

5. Click **Browse**.
6. On the **Select User** dialog, enter **Avaya** in the **Enter the object name to select** field and click **Check Names**.

   IIS Manager should auto-complete the **Enter the object name to select** field.

7. On the **Authentication Methods** dialog, in the **Password** field, enter ********.
8. Click **OK**.
9. On the **Confirm Password** dialog, re-enter the password and click **OK**.
10. On the **Properties** dialog, click **Apply** then **OK**.

Adding Avaya to the IIS_WPG group

To add Avaya to the IIS_WPG group:

1. Navigate to **Start** > **Programs** > **Administrative Tools** > **Computer Management**.
2. On the **Computer Management** screen, expand **System Tools** > **Local Users and Groups** > **Groups** > **IIS_WPG**.
3. Right-click **IIS_WPG** and select **Properties**.

   The Computer Management application displays the **IIS_WPG Properties** dialog.

4. Click **Add**.
5. On the **Select User** dialog, enter **Avaya** in the **Enter the object name to select** field and click **Check Names**.

   IIS Manager should auto-complete the **Enter the object name to select** field.

   The Computer Management application adds Avaya to the group.

Restarting AWC services

To restart the AWC server:

1. On the AWC server, navigate to **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Stop the services **Conferencing Gateway** and **IIS Admin Service**.

   The **World Wide Web Publishing** service should stop too.

3. Start the services **World Wide Web Publishing** and **Conferencing Gateway**.

Configuring the recording server

Before you install the new file, you must uninstall the existing files.

1. Navigate to **Start** > **Run** and type `appwiz.cpl`.
2. Select **Recording Option Pack** from the list, click **Change/Remove** button and follow the prompts to remove the recording application from the system.
3. Obtain the `RecordingServer_Install for AWC 5.2.2.0.3.zip` file and extract it to a temporary directory.
4. Click `setup.exe` to open the **Recording Option Pack Setup** installation wizard.
5. Ensure all the installation details remain the same as during the previous installation.
6. Run the entry for the dialogic board so that the registry contains the entry, **Digital Dialogic**.
7. Restart the operating system on the recording server.

Index

A

advertising settings 39
announce settings 39
application server 32
audio integration 32
authentication settings 37
authenticator.properties 44
authorization settings 37
AWC
  administration screens 31, 44
  branding 21
  definition of 9
  further information 9
  installing 19
  introduction 9
  previous name 9
  server 41

B

billing 28
branding 21
  avaya 21

C

configuring
  authenticator.properties 25
  billing 27
  default website 22
  DefaultAppPool 22, 49
  playback 35
  publishing point 38
  recording 43
  TEM files 24
  windows media services 36
control protocol settings 38
CRS server 15
CRSBilling.reg 27

D

Data Xchange 9
data_event
  login 13
  passwords 13
database 11
  data_event 12
  DCMS 11
  passwords 12, 13
DCMS
  login 12
  passwords 12
default website 22
dialogic 45
directory security 23, 49

E

event notification settings 37

I

i386 folder 35
IIS_WPG 23
installation wizard 15, 19
integrated roster 31
integratedstate.tem 25

J

jar 21
Java 17
Jenga 21

L

licence.reg 33
licenses 33
limits settings 38
logging settings 37
logins 11

M

media services settings 36
MeetingServer 19

P

playback 35
properties settings 39
publishing point 36, 38

Q

quick reference 9

R

r folder 23, 49
recording 35
recording patch 41, 43
registry file .28, 42
restarting 22, 28, 50
roster 31

S

scripts. 15
  billing 15
  data conference reports 15
  data_event.sql 15
  reports 15
  web 15
source settings 39
spauthurl1.tem. 24
SQL. 11

T

timezone 29

V

verifying
  audio integration 32
  billing 28

W

Web Portal 44
Windows media 36
windows media services
  login 41