Unified Communication Center Administrator’s Guide

Edition 1.0
April 2002
Part number 585-313-511

Avaya Inc.
211 Mount Airy Road
Basking Ridge, New Jersey 07920

www.avaya.com

Your comments are welcome. They can assist us in improving our documentation. Please address your comments to infodev@avaya.com.

Release 1.0
Edition 1
April 2002

Contents

UCC Initial Configuration

UCC User Administration

UCC Avaya Web Collaboration System Administration

UCC Avaya Web Messaging Administration & Maintenance

Unified Communication Center Administrator's Guide Overview

The Unified Communication Center (UCC) Administrator's Guide explains how to administer and maintain the Avaya Web Collaboration and Avaya Web Messaging components of UCC. This Administrator's Guide consists of the following:

- UCC System Requirements contains the hardware and software requirements for the base server and the software requirements for the end-user.
- UCC Wireless Feature contains a list of the supported wireless devices, their requirements, and the UCC features they support.
- UCC Licensing explains how to administer the license and includes instructions on how to upgrade your license, how to reset your password, how to restart the license server, and how to view license error logs.
- UCC Initial Configuration provides instructions on how to configure UCC immediately after installation and includes instructions on how to administer the dial plan, how to administer the Tserver device table, and how to enter the information about new users into the LDAP directory.
- UCC User Administration provides procedures for administering the Tserver device table, adding, editing, and deleting user profile information and changing users' passwords.

- UCC Avaya Web Collaboration explains how to administer Avaya Web Collaboration and contains the following topics:
  - What You Need to Know explains the components and architecture of Avaya Web Collaboration and describes some key features.
  - Administering the Dial Plan explains what the dial plan is, how it works, and how to administer it.
  - System Administration Concepts provides an overview of how the GUI is structured to help you navigate through it.
  - System Administration Tasks provides instructions for all the tasks involved in administering Avaya Web Collaboration.
- UCC Avaya Web Messaging explains how to administer Avaya Web Messaging and contains the following topics:
  - Avaya Web Messaging Administration and Maintenance explains how to change configuration, view the user list, and monitor statistics.
  - Maintenance Tools explains how to use the maintenance tools that are available from the desktop Start menu's Avaya Web Messaging tools directory.
  - Trace Manager explains how to use the Trace Manager utility as a diagnostic tool for troubleshooting.
  - User Issues is an overview of some of the Avaya Voice Player, fax viewer, and file association issues users might encounter.
- UCC Glossary provides a list of terms and their definitions that may be useful to you as you read this guide.
- UCC Legal Information provides legal information regarding the Avaya Unified Communication Center.

What You Need to Know

This System Administrator's Guide is designed for those who administer and maintain the Unified Communication Center base server. As system administrators and authorized service providers for Unified Communication Center, you must be familiar with Microsoft Windows™ 2000 terminology and procedures and have a basic understanding of Windows 2000, the Windows 2000 server, LDAP directory servers, and Microsoft Internet Information Server™ (IIS) operation. You must also be familiar with the operation of INTUITY AUDIX and Octel message servers.

UCC Administration Launch Page

To open the Administration Launch page go to:

Start Menu -> **Programs** -> **Avaya UCC Administration**

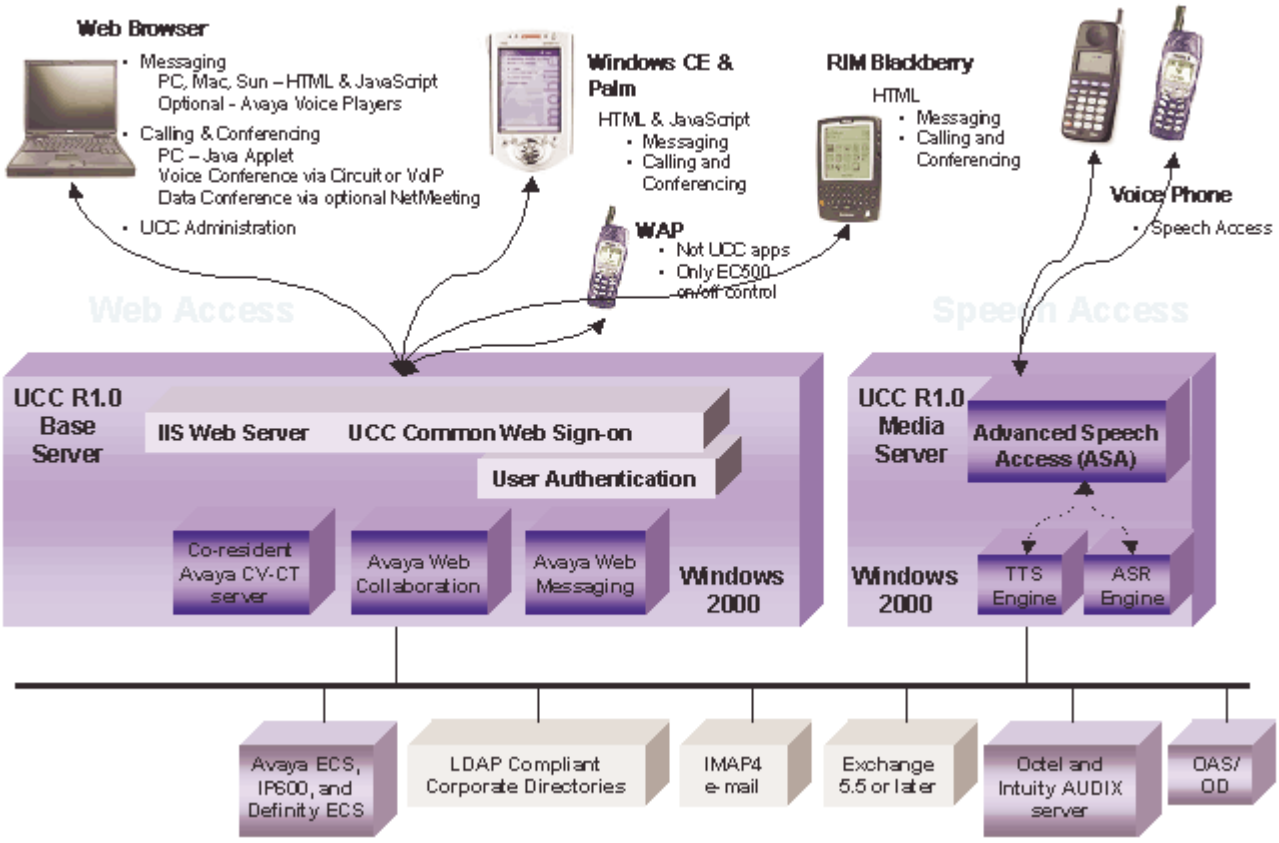
The following links are available from the launch page:

Link	Description
About UCC	Click this link to see the UCC release number, the Web Collaboration and Web Messaging version numbers, and the installed components.
Avaya License Manager	Click this link to use the Avaya License Manager. See UCC Licensing for more information.
Avaya Advanced Speech Access	Click this link to access the Avaya Advanced Speech Access Administration interface.
Avaya Web Collaboration	Click this link to access the Avaya Web Collaboration Administration interface. See UCC Avaya Web Collaboration for more information.

Link	Description
Avaya Web Messaging	Click this link to access the Avaya Web Messaging Administration interface. See UCC Avaya Web Messaging for more information.
UCC User	Click this link to access the UCC User Administration interface. See UCC User Administration for more information
Download J2RE (plugin)	Click this link to download the Java 2 Runtime Environment (J2RE) if is not installed on your computer. J2RE is necessary to enable the Java applet that is a part of the Administration Web pages.
Admin Guide	Click this link to open this admin guide.

UCC Architecture

The following illustrates the architecture of Avaya Unified Communication Center:



User Security

Security is provided for the user through a common login and password that controls access to Web Collaboration and Web Messaging components.

For Web Messaging, additional security is provided at the message server. For Octel message servers, security is also provided at the OctelAccess Server. All access to the LAN from the telephone system is restricted by the message server. Before logging on, the end user must enter a password recognized by the message server.

Administrator Security

To minimize the risk of unauthorized server use, the Web servers used for the Unified Communication Center are intended to be configured in accordance with the customer's security policies and installed within the customer's intranet firewall, which manages intranet access from the Internet.

For Avaya Web Collaboration, there are the three levels of administrative security, each protected by a login and password:

- **System Administration Graphical User Interface (GUI).** A login and password with administrative permissions are required to access the System Administration GUI . This login is initialized when you install. You can change this password through the iPlanet Directory Server or in the end user's Change Password dialog box.
- **IIS Web Server.** A login and password are required to access this server to perform functions such as changing the configuration (for example, where the applet is stored, which server preferences are in use, and whether or not the system has SSL security).
- **iPlanet Directory Server.** A Directory Manager login and password are required to access the Directory Server interface. This login is initialized when you install the Directory Server.

For Avaya Web Messaging, administrators and technical support must enter a password on the Web server to access Avaya Web Messaging administration and maintenance pages. The two default logon names are configured:

- **admin** for the system administrator
- **services** for technical support

The passwords should be changed after initial use.

Avaya Web Messaging supports Secure Socket Layer (SSL) technology for security.

PCAnywhere for Fault Resolution

Remote access to the Web server is required for fault resolution activities covered under warranty and post-warranty support plans. Remote Access must be configured in accordance with the customer's security policies. Symantec pcAnywhere, Version 10 or later must be installed on the server. A modem and dial access connection must also be installed on the server if required by your authorized service provider.

Statement of Responsibility

The statement of responsibility defines the extent of Avaya’s responsibilities for a product. The customer is responsible for initial problem source identification. In the event that the customer requires Avaya assistance to isolate the problem and the fault is found to be in components for which the customer is responsible, Avaya reserves the right to bill its time at the current rate. Generally, Avaya is responsible for all Avaya equipment and software warrantied by Avaya. The customer is responsible for administering the latest software updates and security patches for the Web server.

UCC System Requirements

UCC Base Server Hardware

The UCC base server meets the following PC hardware requirements:

- 1 GHz processor.
- 1 GB of RAM.
- 20 GB of available space (NTFS format) on the hard drive, regardless of which software components you plan to install. (Only 350 MB are required for the software alone, but 20 GB are required for correct operation of the software in the customer environment.)
- Modem access for remote support.
- CD-ROM drive.
- Network Interface Cards (NICs). Use of two NICs is strongly recommended, one for connecting to the corporate LAN and the other for connecting to the PBX (as a private connection).

The base server hardware must be installed on the network at the customer site in the same domain as the Microsoft Exchange Server.

UCC Base Server Software

The following software is required on the UCC base server:

- Microsoft Windows 2000 Server, including:
  - Windows 2000 Server Service Pack 2
  - Microsoft Internet Information Server 5.0
  - Microsoft Internet Explorer 5.5 with its Service Pack 2
- Symantec pcAnywhere version 10 or later for remote access and support
- Virus protection software with the latest updates (recommended)

User Requirements

The operating system for the user's computer can be one of the following:

- Microsoft Windows 98, ME, NT4, 2000

The browser for the user's computer can be one of the following:

- Microsoft Internet Explorer 5.0 SP1 and 5.5
- Netscape 4.5x or later except 6.0 (Netscape not supported by Advanced Speech Access)

The recommended screen resolution is 1024x768 pixels.

Note: Users with Windows 98 and Netscape 4.7.2 may experience a system crash if they select either of the check boxes on the Edit Web Collaboration Settings page. These check boxes are called Start with dashboard GUI? and Allow Interaction with other PC applications.

UCC Wireless Feature

Users can access the wireless versions of Avaya Web Messaging and Avaya Web Collaboration for their PDA devices from the same Avaya™ Unified Communication Center (UCC) URL. UCC detects which type of device is used and provides the appropriate version, whether they log in from the desktop or from a wireless PDA device.

Devices and Minimum Requirements

The following is a table that shows which wireless PDA devices are supported by UCC R1 and what the requirements are for each of those devices:

Table 1. Wireless PDA Devices and Requirements

Device	Minimum Requirements
Palm OS Devices: ■ Palm ■ Handspring ■ Sony	■ Palm OS Version 3.x ■ 8 MB of RAM minimum ■ Internet connection ■ Some devices have modems built in; others require an external modem. Browsers: 1. Palm.net web clipping 2. Go America 3. AvantGo
RIM Blackberry devices (857 and 957 models only) (These devices are the same but have different radio interfaces.)	■ Any RIM OS Version ■ Internet Connection Browsers: Go America
Windows CE devices (Pocket PC) ■ Compaq iPAQ ■ HP Jornada ■ Casio E-125 /EM-500	■ Windows CE, Version 3 + (Pocket PC) ■ 16 MB of RAM ■ Internet connection Browsers: ■ Pocket IE ■ Go America ■ AvantGo

Port Redirect Issues

If you are setting up a port-redirected server to be used with Palm devices that require web clipping browsers, check the Palm Web site (www.palm.com) for the port numbers to use. Use of the wrong port numbers will cause users to be denied access.

If you are setting up a port-redirected server for wireless devices, users may lose access to Avaya Web Messaging from their desktop. Use of the wireless device changes the URL setting for Avaya Web Messaging by appending the port number. To solve this problem, put the port redirect value under IIS so it will listen at the same port.

Avaya Web Messaging Features

Avaya Web Messaging wireless provides many of the features that are provided in Avaya Web Messaging desktop. Avaya Web Messaging users can access the wireless PDA version of the application either by entering the UCC URL in the URL field of the wireless device or, for certain models of Palm and RIM devices, by using a Web Clipping file. The user must download the Web Clipping file to use Web Clipping. For Web Collaboration and Web Messaging, directions for downloading these files are in the user Help.

Avaya Web Messaging wireless provides the following features:

- Common logon to the Messaging inbox that connects users from the UCC launch page and allows them to access the UCC user profile information.
- Inbox display of message headers suitable for the wireless PDA device screen.
- Playback of audio messages by telephone to the phone number/extension specified at log on. Includes Play, Stop, Rewind and Hang Up.
- Display of message text with page forward and backward (for INTUITY users).
- Display of messages to be printed at a fax machine (for messages that are not Audio Only—for INTUITY users).
- Moving and deleting messages (the specifics are dependent on which message server users have).
- Logging off of a current mailbox session.
- Changing audio playback number.
- Changing the voice mail server password. The application changes the password in the UCC common user profile after the password has been changed on the voice mail server.
- Changing the fax default print number (for INTUITY users).

- Calling the originator of a selected message (for all AUDIX users).
- Quick reply to sender only (not to outside callers). Can record a voice message as part of the reply. Can add a text message (for INTUITY users only). Can mark messages as Urgent or Private.
- Message sorting by media type, originator, time/date received, message status, subject, and in ascending or descending order.
- Finding messages (voice mail only).

Avaya Web Collaboration Features

The Avaya Web Collaboration Application—wireless provides many of the features that are provided in the desktop version, including placing calls, creating and joining conferences with multiple participants, using Bookmarks and Speed Dials, and managing your call routing.

Users can access the wireless PDA version of the application either by entering the UCC URL in the URL field of the wireless device, or for certain models of Palm and RIM devices, by using a Web Clipping file that places an Avaya Web Collaboration icon on the wireless PDA device.

Avaya Web Collaboration—wireless provides the following features:

- Making outgoing calls in several ways, from the Phone page, the Status page, the Bookmarks page, or the Speed Dials page
- Setting up conference calls with up to five parties, as well as adding and dropping parties as needed
- Accessing Avaya Web Messaging to manage your voice, e-mail, and fax messages by clicking the Inbox link on the Phone page
- Using Speed Dials for one-touch dialing for frequently called numbers (the Speed Dial numbers must be created in the desktop version of the application)

- Using Bookmarks to call groups of people you call on a regular basis (the bookmarks must be created in the desktop version of the application)
- Turning on or off call routing features, including Send All Calls, Call Forwarding, Auto Answer, the Avaya EC500 Extension to Cellular
- Searching for phone numbers in any of the directories administered on your system by last name, full name, or phone number

See the online Help systems within Avaya Web Collaboration—wireless and Avaya Web Messaging—wireless for further details about what you can do with these applications.

UCC Licensing

Access to the Avaya™ Unified Communication Center (UCC) applications is controlled by the UCC license file. The license file is needed to activate the UCC software solution and identifies the set of UCC applications that have been ordered.

As part of the installation process, the UCC license server is installed on the same server as the UCC base server. The license server obtains license data from the license file at startup.

Click the following links to learn about licensing:

Administering Licenses

1. To open the Administration Web pages go to:

   Start Menu -> **Programs** -> **Avaya UCC Administration**

   The Unified Communication Center Administration page is displayed.

2. Click the **Avaya™ License Manager** link.

   The Avaya™ License Manager main page (WebLM) is displayed, showing which applications are licensed. No licensed products are displayed here until you install the initial license file.

   The Host ID number is also displayed on this page. You will need to provide the Host ID number when requesting a license file.

3. Click the **License Administration** link to go to the Login page.

   On the Login page, the User name is displayed as admin. The first time you log on, the default password is displayed. (If you have already logged on for the first time, skip to step 7.)

4. Click **Continue**.

   The first time you log on, the page called Select a New Password is displayed.

5. Type your new password in the field called New password.

6. Type your new password again in the field called Re-type new password to confirm it.

7. Click **Continue**.

   The License Administration page is displayed.

Installing an Upgrade License File

When you are ready to upgrade so you can add users, you must contact your Avaya representative. A new license file is then sent to you. The new license file, the Unified Communication Controller file, is configured to include all the applications the customer has purchased. Follow the instructions that come with the license file that explain where to put the file. Perform the following steps to install an upgrade license file:

1. On the License Administration page under Install License File, click **Browse** to locate the Unified

Communication Controller file (or specify the file if you know the path).

2. Click **Install** to upload the file to the WebLM server, which installs the license file. Once the license file is installed, you can add users by clicking the Avaya UCC User link on the Unified Communication Center Administration page.

Restarting the License Manager

It might be necessary to restart the License Manager in cases in which there are problems with the servers. Restarting forces the license server to re-read the license file. To start the License Manager again, click **Restart** in the License Administration page. After you click Restart, a page is displayed to indicate that the restart was successful.

Changing the Administrator Password

You can change the administrator password at whatever intervals you want to maintain security. It is recommended to change the password at least every 6 months. Perform the following steps to change the administrator password:

1. Type your old password in the field called Old password.
2. Type your new password in the field called New password.
3. Type your new password again in the field called Re-type new password to confirm it.
4. Click **Change password**.

Viewing License Error Logs

Error handling is limited in UCC Release 1 to base Windows 2000 server exception handling. The licensing server will start or fail to start with no additional exception handling beyond standard OS support.

Troubleshooting

If you replace the primary NIC card for any reason (thereby changing the MAC address of the card), Avaya Unified Communication Center will stop working because the NIC card address is linked to the license file. In this case, the WebLM Administration page will display "no licenses installed," even though the old license file is still present in the licenses directory.

You will need a new license file for the new MAC address of the new primary NIC card. Contact your Avaya representative for this file. When you receive the new license file, install the file in the usual way. See the previous section, "Installing the Initial License File."

UCC Initial Configuration

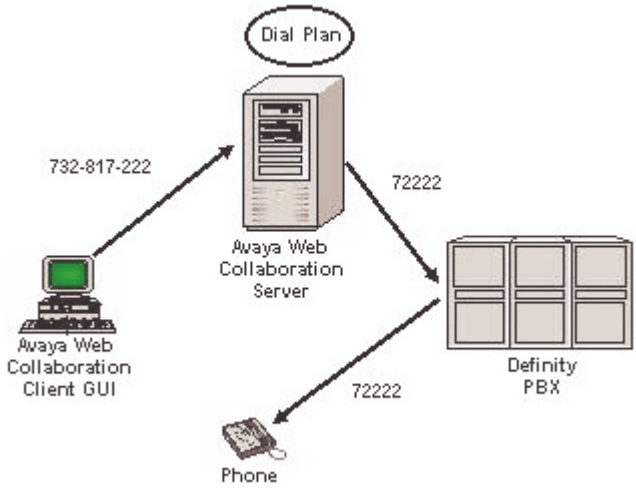
This section contains the main steps you will perform to configure the Unified Communication Center after it has been installed. The essential steps are creating a dial plan and adding users to the LDAP directory. Administering the Tserver table is optional. Additional configuration is required to configure Avaya Advanced Speech Access. This section contains the following topics:

Dial Plan Overview

The Avaya Web Collaboration application provides a dial plan so that audio calls can be made more efficiently. The dial plan translates phone numbers entered by the user (or phone numbers selected using Search) to the numbers that are sent to the Definity PBX when the call is made.

The following figure depicts the Avaya Web Collaboration application dial plan feature.

Figure 1. Dial Plan Diagram



For example, each user in a Definity PBX has a telephone number of the type 732-817-$$$$ and a corresponding extension number of the type 7$$$$. If a user makes a call to a number of the type 732-817-$$$$ using the Avaya Web Collaboration application client GUI, the Dial Plan receives the number and sends a number of the type 7$$$$ to the Definity PBX.

Dial Plan Description and Rules

The following table is a sample Avaya Web Collaboration dial plan for a US-based customer.The Full Number Mask column shows the types of number formats a user may input. The Dialable Number Mask column shows the number formats the Dial Plan sends to the Definity PBX.The Local to Switch column indicates whether the number is in the local switch. These are the three settings the system administrator specifies when setting up the dial plan. The following rules govern the dial plan:

- **$ Mask.** The "$" character is used by the Dial Plan as the "wild card" mask to represent numbers that will vary within a group. For example, 732-817-$$$$ represents all numbers from 732-817-0000 to 732-817-9999.
- **Use of Dashes.** In the "Full Number Mask" column, dashes must be used. In the "Dialable Number Mask" column, dashes must not be used. The format must match the format stored in the directory.If a number entered does not match those

shown in the Full Number Mask column, the original number is sent to the PBX. If the call cannot be made a message is displayed to the user.

- **Dial Plan Order.** The number matching is done in the order of the dial plan entries. For example, in the dial plan below, because the full number mask 732-817-$$$$ is above the full number mask 732-$$$-$$$$, the number 732-817-1234 is translated into 71234. If the order were reversed, the number 732-817-1234 would be translated into 98171234.
- **Multiple Definity PBXs**. If multiple Definity PBXs are controlled by an Avaya Web Collaboration server, each PBX has its own dial plan.

Table 2. Sample Dial Plan

Full Number Mask	Dialable Number Mask	Local to Switch	Description
732-817-$$$$	7$$$$	True	Internal Users
3$$$	3$$$	True	Remote (AWOH) Users
303-538-$$$$	8$$$$	False	Extensions on another PBX
9-$$$-$$$$	9$$$$$$$	False	Local call outside PBX
732-$$$-$$$$	9$$$$$$$	False	Local call outside PBX
9-1-$$$-$$$-$$$$	91$$$$$$$$$$	False	Long distance call
$$$-$$$-$$$$	91$$$$$$$$$$	False	Long distance call
$-$$$-$$$-$$$$	9011$$$$$$$$$$$	False	International call
$-$-$$$-$$$-$$$$	9011$$$$$$$$$$$$	False	International call

Create the Dial Plan

To create the Dial Plan:

1. On the Avaya Web Collaboration Administration page, click **Directory Admin**.
2. Select the **Switches** tab.
3. Double click on the switch or select it and click **Edit**.
4. Select "G3V8 or newer" from the Switch Release drop-down menu.
5. Select the **Multiple Calls for Remote** checkbox.
6. Click **Administer Dial Plan ...**. The Dial Plan Information dialog box appears.

Input Field	Description	Action
Full Number Mask	The full number mask entries define the valid numbers that can be dialed. **Note:** The format must match the format of the number stored in the directory.	Type the full number mask.
Dialable Number Mask	The dialable number mask entries are the numbers that will be sent to the PBX. Do not use dashes.	Type the dialable number mask.
Is this mapping for an extension on this switch?	This should be checked for all numbers that are local to the switch (including AWOH numbers) and unchecked for all other numbers.	Select the checkbox if the number is local to the switch.

7. Click **Add** when the entry is complete. Add additional entries as necessary.
8. Use the Up and Down buttons as necessary to arrange the order of the entries.
9. Once all the appropriate entries have been made, click **OK**. This will return you to the Edit Switch Object dialog box.
10. Click **Apply**. The Changing Switch Object dialog box appears. Click **Yes**.
11. To make your changes take effect, turn the Avaya Web Collaboration server off, wait 30 seconds and then turn it back on. For instructions on how to turn the server on and off see Turn the Server On and Off.

Administering the Tserver Device Table

The Tserver Device Table is part of Avaya CentreVu Computer Telephony. This application sends messages from the PBX to the Avaya Web Collaboration server. If you use the Tserver Device Table, you must add a device for each phone of each user.

Note: Administering the Tserver Device Table is optional. The Device Table is only needed if the CentreVu Computer Telephony Security Database has been installed.

Add a Device

To add a device to the Tserver Device Table:

1. Access the Tserver Device table by going to:

   Start Menu -> **Programs** -> **TS WIN32 Client** -> **Telephony Services Admin**

2. Select the Tserver from the drop-down menu. Type your Login and Password and click **OK**. The Telephony Services Administrator 32-bit dialog box appears.
3. Click **Devices** on the left side of the dialog box. The right frame is populated.

4. Select **Add Device** from the Action drop-down menu or click the **Create Device** icon from along the top (Create Device is the single telephone icon).

5. Enter the device and its location using the tips in the table below.

Field	Action
Device ID:	Type the extension number.
Location:	Type the person's name or the location of the extension. A unique entry will help you identify the device later.
Device Type:	Select **PHONE**.
Tlink Group:	Select **Any Tlink**.

6. To enter more than one extension, click **Apply**. The fields will be cleared for the next entry.

7. When all extensions have been entered, click **OK**.

Note: To change the information about one of the devices in this table double-click on the entry on the Telephony Services Administrator 32-bit dialog box.

Refresh System After Adding or Changing User Information

When a device, station, AWOH extension, VOIP extension, or Xmobile extension is added to the Tserver Device Table or the Definity G3/IP600 (PBX), you must make your changes take effect by refreshing the system. To do this:

1. Open the Avaya Unified Communication Center Administration page.

2. Click **Avaya Web Collaboration**. The Avaya Web Collaboration Administration page opens.

3. Click **Server Options**.The Server Options page has two buttons: Clear Cache and Refresh Tserver.

4. Click **Clear Cache**. Wait thirty seconds.

5. Click **Refresh Tserver**.

Add a User Quickly With Default Settings

The Quick Add button saves time by making use of default settings. Once you have set the defaults, these fields are automatically populated when you use the Quick Add feature.

The first time you click Quick Add during a session the Quick Add Default Settings dialog box will appear. These settings are valid for the duration of the session.

To set permanent default settings, see Set Permanent Default Settings for the Quick Add Feature. The permanent default settings are overridden by default settings set using the Quick Add Default Setting dialog box.

If you have already set the default settings, skip ahead one section to Add a User Through Quick Add.

Specify Default Settings for User Information

1. On the Unified Communication Center page, click **UCC User**
2. Type your login and password and click **OK**.
3. Click **Quick Add**. The Quick Add Default Settings dialog box displays if you have not previously set the default settings.
4. If you have previously set the default settings and are editing them, click **Default Settings...** on the Quick Add dialog box.
5. Complete the input fields as follows:

Fields	Description and Action
Default Switch	Select the switch you want to appear by default when adding users.
Messaging URL	Type your URL for Web Messaging.
Language	Select the default language.

Fields	Description and Action
Voice Mail Server	Type the name of the Voice Mail Server (the server on which Avaya Web Messaging resides). For an Intuity, type the host name or IP address. For a Octel message server, type **<voicemail server name@OctelAccess server name>**.
Speech URL	Type the URL for the ASA for UCC User Preferences web site. Use the format: **<http://ASA server name/ASAOnline>** where ASA server name is the name of the server on which ASA resides.
Create Computer Name from User ID and the following Suffix:	Accept the default and verify the checkbox is selected.
Create Host Name from Computer Name and the following Suffix?	Accept the default and verify the checkbox is selected.
Create Email Address from User ID and the following Suffix?	Type the Suffix and verify the checkbox is selected. For example, @avaya.com. By default, when you enter a user using Quick Add, the Email Address field will be populated with their User ID and the suffix you specify.
Create Address Book Name from User ID and the following Suffix?	Accept the default and verify the checkbox is selected.
Create Worktop Name from User ID and the following Suffix?	Accept the default and verify the checkbox is selected.
Users	Select the appropriate organizational unit from the drop-down menu.

Fields	Description and Action
Telephones	Select the appropriate organizational unit from the drop-down menu.
Computers	Select the appropriate organizational unit from the drop-down menu.
Worktops	Select the appropriate organizational unit from the drop-down menu.
Address Books	Select the appropriate organizational unit from the drop-down menu.

Add a User Through Quick Add

Before you begin, consider the following three prerequisites:

- Administer the physical, AWOH, VOIP, and EC500 extensions on the switch. See the configuration notes.
- Administer the physical, AWOH, VoIP, and EC500 extensions on the Tserver Device Table if you use this optional feature. See the section Administering the Tserver Device Table.
- If you have not already, administer the Dial Plan. See the section Administering the Dial Plan.

1. On the Unified Communication Center page, click **UCC User**.
2. Type your login and password and click **OK**.
3. Click **Quick Add**.
4. Complete the input fields as follows:

Field	Description and Action
First Name	Type the user's first name. (required)
Last Name	Type the user's last name. (required)
User ID (Unique)	Type the user's User ID. The User ID must be unique. (required)
Password	Type the user's password. (required)
Telephone Number	Type the telephone number. Make sure the format matches that used in the directory. The required format is a 10 digit number using dashes. For example, 408-555-1212. (required)
AWOH Extension	Type the AWOH Extension.(This must be administered on the switch.)
First Xmobile Ext	Type the Xmobile Extension. The Xmobile Extension is the extension for a user's cellular phone. An extension must be administered for the user to have access to the EC500 Extension to Cellular feature. This extension must also be administered on the Tserver and switch.

Field	Description and Action
Second Xmobile Ext	Type the Xmobile Extension. The Xmobile Extension is the extension for a user's cellular phone. An extension must be administered for the user to have access to the EC500 Extension to Cellular feature. This extension must also be administered on the Tserver and switch.

Field	Description and Action
Remote VOIP Extension	A Remote VOIP Extension must be administered here and on the Tserver and switch for a user to have access to the VOIP feature. 1. Click the browse button (**...**). The Remote VOIP Extension Information dialog box appears. 2. Click **Find...** to search using LDAP attributes or complete the fields as follows: a. Select the switch on which the VOIP Extension has been administered. b. Type the Remote VOIP Extension. c. Type the VOIP Password. d. Type the GateKeeper IP Address. (This is the Security Code for the extension on the switch. It can be obtained from your switch administrator.) e. Select the organizational unit in which you store VOIP extensions. f. Click **Apply**.

Field	Description and Action
Switch	Accept the default. (required)
Email	Type the user's Email address.
Messaging URL	Accept the default.
Language	Accept the default.
Voice Mail Server	Accept the default.
Voice Mail Id	Type the ID the user uses for Avaya Web Messaging.
Voice Mail Password	Type the password the user uses for Avaya Web Messaging.
Speech URL	Accept the default.
Use Dynamic IP	Select the Use Dynamic IP checkbox. (required)

UCC User Administration

The Avaya Unified Communication Center (UCC) provides the ability to set up and edit a user profile for all the components of UCC in one place. The following section provides procedures for administering the Tserver device table, adding, editing, and deleting user profile information and changing users' passwords.

Choose from the following topics:

Note:
The UCC User Directory Administrator page utilizes an LDAP directory. It is not within the scope of this guide to describe an LDAP directory. General knowledge of an LDAP directory is assumed.

Administering the Tserver Device Table

The Tserver Device Table is part of CentreVu Computer Telephony 9.5. This application sends messages from the PBX to the Avaya Web Collaboration server. If you use the Tserver Device Table, you must add a device for each telephone of each user.

Note: Administering the Tserver Device Table is optional. The Device Table is only needed if the CentreVu Computer Telephony Security Database has been installed.

Add a Device

To add a device to the Tserver Device Table:

1. Access the Tserver Device table by going to:

   Start Menu -> **Programs** -> **TS WIN32 Client** -> **Telephony Services Admin**

2. Select the Tserver from the drop-down menu. Type your Login and Password and click **OK**.

3. The Telephony Services Administrator 32-bit dialog box appears.

4. Click **Devices** on the left side of the dialog box.

5. The right frame is populated.

6. Select **Add Device** from the Action drop-down menu or click the **Create Device** icon at the top of the screen (Create Device is the single telephone icon).

7. Type the information about the device by using the tips in the table that follows:

Field	Action
Device ID:	Type the extension number.
Location:	Type the person's name or the location of the extension. A unique entry will help you identify the device later.
Device Type:	Select **PHONE**.
Tlink Group:	Select **Any Tlink**.

- To enter more than one extension, click **Apply**. The fields will be cleared for the next entry. When all extensions have been typed in, click **OK**.

Note: To change the information about one of the devices in this table double-click in the entry in the Telephony Services Administrator 32-bit dialog box.

Refresh System After Adding or Changing User Information

When a device, station, AWOH extension, VOIP extension, or Xmobile extension is added to the Tserver Device Table or the Definity G3/IP600 (PBX), you must make your changes take effect by refreshing the system. To do this:

1. Open the **Avaya Unified Communication Center Administration** page.
2. Click **Avaya Web Collaboration**.
3. The Avaya Web Collaboration Administration page appears.
4. Click **Server Options**.The Server Options page has two buttons: Clear Cache and Refresh Tserver.
5. Click **Clear Cache**. Wait 30 seconds.
6. Click **Refresh Tserver**.

Administering User Information

The Avaya Unified Communication Center provides access to an LDAP directory through which you can administer user information for the Avaya Web Collaboration and Avaya Web Messaging applications.

Access User Information

To access user information:

1. On the Avaya Unified Communication Center Administration page, click **UCC User**.
2. Accept the default login (cn=Directory Manager), type your password, and click **OK**.
3. The Directory Administrator page appears.
4. Select the user's name.
5. The corresponding information appears in the fields on the right. The User Information fields list the following information:
   - First Name
   - Last Name
   - User ID
   - Telephone Number
   - AWOH Extension
   - Remote Number

- Remote VOIP Extension
- Email Address
- Worktop Name
- Computer Name
- Address Book

Directory Administrator Buttons

The following three buttons appear on every page in the Directory Administrator interface.

Refresh

The Refresh button reloads the current information.

Add Organizational Units

The Add Organizational Units button opens the Create Organization Unit dialog box that is used to set up the hierarchy for each component in the directory. If you have not set up an organizational unit for users, you can do so here.

To add an organizational unit:

1. Click **Add Organizational Units**.
2. Type the name (for example, **Users**) that you want to assign to the new organizational unit in the Organizational Unit Name text box.
3. Select the name of the root directory in which you want the new organizational unit to reside from the Organization Unit Of drop-down menu.
4. Click **Apply**.

Search for a User

To search for the information about a specific user:

1. On the Unified Communication Center page, click **UCC User**.
2. Type your login and password and click **OK**.
3. Click **Search**. The Search button is available from every tab on the Directory Administrator page.
4. In the Search dialog box, enter any information you have about the user and click **OK**. (Knowledge of an LDAP directory is assumed.)

Add a User Quickly with Default Settings

The Quick Add button saves time by making use of default settings. Once you have set the defaults, these fields are automatically populated when you use the Quick Add feature.

The first time you click Quick Add during a session the Quick Add Default Settings dialog box will appear. These settings are valid for the duration of the session.

To set permanent default settings, see Set Permanent Default Settings for the Quick Add Feature. The permanent default settings are overridden by default settings set using the Quick Add Default Setting dialog box.

If you have already set the default settings, skip ahead one section to Add a User Through Quick Add.

Specify Default Settings for User Information

1. On the Avaya Unified Communication Center page, click **UCC User**
2. Type your login and password and click **OK**.
3. Click **Quick Add**. The Quick Add Default Settings dialog box displays if you have not previously set the default settings.
4. If you have previously set the default settings and are editing them, click **Default Settings...** in the Quick Add dialog box.
5. Complete the fields as follows:

Fields	Description or Action
Default Switch	Select the switch you want to appear by default when you are adding users.
Messaging URL	Type your URL for Avaya Web Messaging.
Language	Select the language you want to be the default when entering user information.

Fields	Description or Action
Voice Mail Server	Type the name of the Voice Mail Server (the server on which Avaya Web Messaging resides). For Intuity, type the host name or IP address. For an Octel message server, type **<voicemail server name@OctelAccess server name>**.
Speech URL	Type the URL for the ASA for UCC User Preferences Web site.
Create Computer Name from User ID and the following Suffix:	Accept the default and verify that the check box is selected.
Create Host Name from Computer Name and the following Suffix?	Accept the default and verify the checkbox is selected.
Create Email Address from User ID and the following Suffix?	Type the Suffix and verify the checkbox is selected. For example, @avaya.com. By default, when you enter a user's information by using Quick Add, the Email Address field will be populated with that user's User ID and the suffix you specify.
Create Address Book Name from User ID and the following Suffix?	Accept the default and verify that the checkbox is selected.
Create Worktop Name from User ID and the following Suffix?	Accept the default and verify that the checkbox is selected.
Users	Select the appropriate organizational unit from the drop-down menu.
Telephones	Select the appropriate organizational unit from the drop-down menu.

Fields	Description or Action
Computers	Select the appropriate organizational unit from the drop-down menu.
Worktops	Select the appropriate organizational unit from the drop-down menu.
Address Books	Select the appropriate organizational unit from the drop-down menu.

Add a User Through Quick Add

Before you begin, consider the following three prerequisites:

- Physical and AWOH extensions on the switch must be administered. See the configuration notes.
- All extensions (including AWOH extensions) must be added to the Tserver Device Table if you use this optional feature. See the section Administering the Tserver Device Table.
- The Dial Plan must be administered. See the section Administering the Dial Plan.

To add a user by using Quick Add, do the following:

1. On the Avaya Unified Communication Center page, click **UCC User**.
2. Type your login and password and click **OK**.
3. Click **Quick Add**.
4. Complete the fields as follows:

Field	Description or Action
First Name	Type the user's first name (required).
Last Name	Type the user's last name (required).
User ID (Unique)	Type the user's User ID. The User ID must be unique (required).

Field	Description or Action
Password	Type a temporary password for the user (required).
Telephone Number	Type the telephone number. Make sure that the format matches the one used in the directory. The required format is a 10-digit number using dashes, for example, 408-555-1212 (required).
AWOH Extension	Type the AWOH Extension. (This extension must be administered on the switch.)
First Xmobile Ext	Type the First Xmobile Extension. The Xmobile Extension is the extension for a user's cellular phone. An extension must be administered for the user to have access to the EC500 Extension to Cellular feature. This extension must also be administered on the Tserver and switch.
Second Xmobile Ext	Type the Second Xmobile Extension. The Xmobile Extension is the extension for a user's cellular phone. An extension must be administered for the user to have access to the EC500 Extension to Cellular feature. This extension must also be administered on the Tserver and switch.

Field	Description or Action
Remote VOIP Extension	A Remote VOIP Extension must be administered here and on the Tserver and switch for a user to have access to the VOIP feature. 1. Click the browse button (**...**). The Remote VOIP Extension Information dialog box appears. 2. Click **Find...** to search using LDAP attributes or complete the fields as follows: a. Select the switch on which the VOIP Extension has been administered. b. Type the Remote VOIP Extension. c. Type the VOIP Password. d. Type the GateKeeper IP Address. (This is the Security Code for the extension on the switch. It can be obtained from your switch administrator.) e. Select the organizational unit in which you store VOIP extensions. f. Click **Apply**.

Field	Description or Action
Switch	Accept the default. (required)
Email	Type the user's Email address.
Messaging URL	Accept the default.
Language	Accept the default.
Voice Mail Server	Accept the default.
Voice Mail Id	Type the ID the user uses for Avaya Web Messaging.
Voice Mail Password	Type the password the user uses for Avaya Web Messaging.
Speech URL	Accept the default.
Use Dynamic IP	Select the **Use Dynamic IP** check box (required).

Add a User Without Default Settings

Before you begin, consider the following three prerequisites:

- Physical and AWOH (Administered WithOut Hardware) extensions on the switch must be administered. See the configuration notes.
- All extensions (including AWOH extensions) must be added to the Tserver Device Table if you use this optional feature. See the section Administering the Tserver Device Table.
- The Dial Plan must be administered. See the section Administering the Dial Plan.

To add a user without default settings:

1. On the Unified Communication Center page, click **UCC User**.
2. Type your login and password and click **OK**.
3. Click **Add** and complete the fields as follows:

Field	Description or Action
First Name	Type the user's first name (required).
Last Name	Type the user's last name (required).
User ID (Unique)	Type the user's User ID (required).
Password	Type a temporary password for the user (required).
Telephone Number	To enter the telephone number (required): 1. Click the browse button (**...**). 2. The Telephone Number Information dialog box appears. 3. Click **Find...** to search using LDAP attributes or complete the fields as follows: a. Select the switch on which the user's telephone number resides. b. Type the Telephone Number. c. Select the organizational unit. d. Click **Apply**.

Field	Description or Action
AWOH Extension	To enter the AWOH extension: 1. Click the browse button (**...**). 2. The AWOH Extension Information dialog box appears. 3. Click **Find...** to search using LDAP attributes or complete the fields as follows: a. Select the switch on which the user's AWOH Extension resides. b. Type the AWOH Extension. c. Select the organizational unit. d. Click **Apply**.

Field	Description or Action
First Xmobile Ext	The Xmobile Extension is the extension for a user's cellular phone. An extension must be administered here and on the Tserver and switch for the user to have access to the EC500 Extension to Cellular feature. To enter the Xmobile Extension: 1. Click the browse button (**...**). 2. The First Xmobile Extension Information dialog box appears. 3. Click **Find...** to search by using LDAP attributes or complete the fields as follows: a. Select the switch on which the user's First Xmobile Extension resides. b. Type the First Xmobile Extension. c. Select the organizational unit. d. Click **Apply**.

Field	Description or Action
Second Xmobile Ext	To enter the second Xmobile extension: 1. Click the browse button (**...**). 2. The Second Xmobile Extension Information dialog box appears. 3. Click **Find...** to search by using LDAP attributes or complete the fields as follows: a. Select the switch on which the user's Second Xmobile Extension resides. b. Type the Second Xmobile Extension. c. Select the organizational unit. d. Click **Apply**.
Remote Number	Leave the Remote Number input field blank. This field shows the last remote number that the user entered when logging in remotely.

Field	Description or Action
Remote VOIP Extension	To enter the remote VOIP extension: 1. Click the browse button (**...**). 2. The Remote VOIP Extension Information dialog box appears. 3. Click **Find...** to search by using LDAP attributes or complete the fields as follows: a. Select the switch on which the user's Remote VOIP Extension resides. b. Type the Remote VOIP Extension. c. Select the organizational unit. d. Click **Apply**.

Field	Description or Action
Address Book Name	To enter the address book name: 1. Click the browse button (**...**). 2. The Address Book Name Information dialog box appears. 3. Click **Find...** to search by using LDAP attributes or complete the fields as follows: a. Select the switch on which the user's Address Book resides. b. Type the Address Book Name. c. Select the organizational unit. d. Click **Apply**.

Field	Description or Action
Worktop Name	To enter the worktop name: 1. Click the browse button (**...**). 2. The Worktop Name Information dialog box appears. 3. Click **Find...** to search by using LDAP attributes or complete the fields as follows: a. Select the switch on which the user's Worktop resides. b. Type the Worktop Name. c. Select the organizational unit. d. Click **Apply**.
Email Address	Type the user's Email Address. This consists of the user's ID and a suffix. (for example, userID@avaya.com)
Messaging URL	Type the URL for Avaya Web Messaging. **Note:** If you do not complete this field, the user will not have access to Avaya Web Messaging.
Language	Select the appropriate language for the user.
Voice Mail Server	Type the name of the Mailbox Server on which Avaya Web Messaging resides.

Field	Description or Action
Voice Mail Id	Type the ID that the user uses to access Avaya Web Messaging.
Voice Mail Password	This is the password that the user will use to access voicemail through Avaya Web Messaging.
Speech URL	Type the URL for the ASA for UCC User Preferences web site. Use the format: **<http://ASA server name/ASAOnline>** where ASA server name is the name of the server on which ASA resides.
Organizational Unit	Accept the default.

Edit User Information

To edit user information:

1. On the Avaya Unified Communication Center page, click **UCC User**.
2. Type your login and password and click **OK**.
3. Click **Edit**.
4. The Edit dialog box appears.
5. Change the fields you need to change. For explanations of particular fields, see the Add a User Without Using Default Settings section.
6. Click **Apply**.

Note:
User passwords can be changed from the Edit User Information dialog box.

Reset Passwords

See the Edit User Information section above. User passwords can be changed from the Edit User Information dialog box.

Delete a User

To delete a user:

1. On the Avaya Unified Communication Center page, click **UCC User**.
2. Type your login and password and click **OK**.
3. Select the user you want to delete.
4. Click **Delete**.
5. A confirmation dialog box appears.
6. Click **OK**.
7. All profile information about the selected user is deleted from the directory.

UCC Avaya Web Collaboration System Administration

The Avaya Web Collaboration application is a conferencing and collaboration Internet application. It provides directory-based conferencing with DEFINITY quality circuit and IP voice communications.

Choose from the following topics:

- Monitor Data Conferences (future availability)
- Refresh System After Adding or Changing User Information on the Tserver
- View Avaya Web Collaboration Information
- Display Error or Maintenance Log
- View/Print System Administration Guide
- Manage User Information
- Switch (PBX) Information
- Tserver Information
- View the Avaya Web Collaboration Server Configuration Settings
- Avaya Web Collaboration Server Information
- Administer Error Log Settings
- Directory Tree Information
- Start and Stop the Tserver
- Access Windows 2000 Services Through the Control Panel
- System Maintenance

What You Need to Know

Components and Systems

Avaya Web Collaboration resides on an intranet or extranet and connects to a business telephone system, such as DEFINITY® ECS, through a LAN interface card. Avaya Web Collaboration utilizes a Definity (switch) that supports the Avaya CentreVu Computer Telephony that bridges the switch to the server.

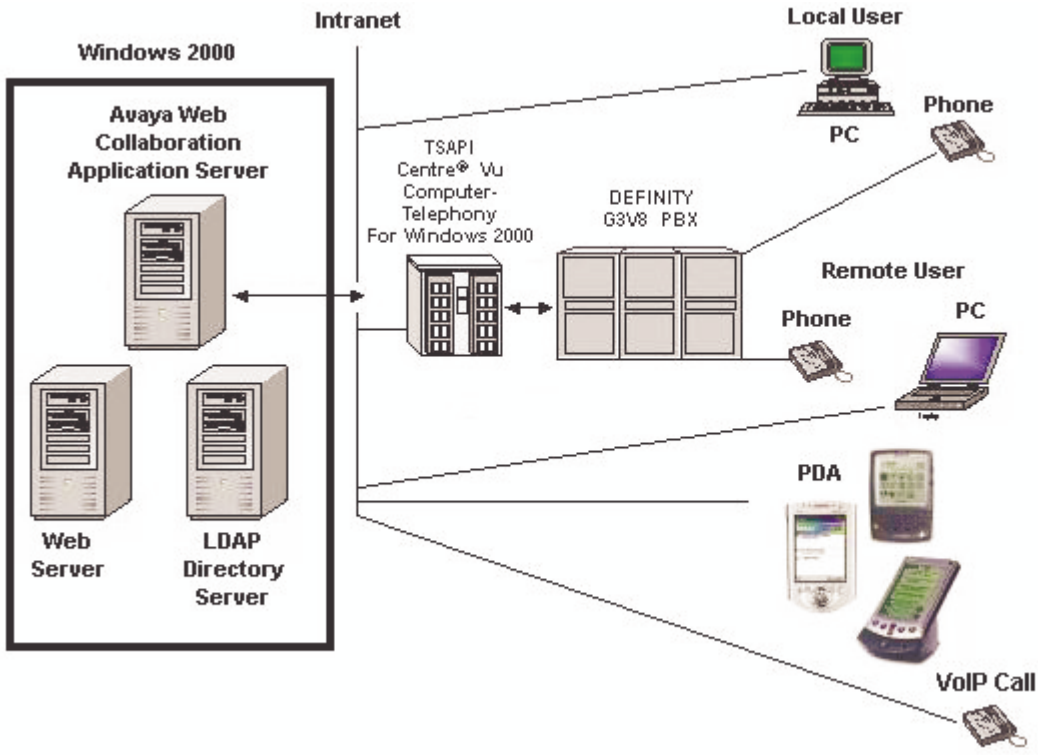
Users require:

- An extension connected to a Definity PBX
- A computer with a Java-enabled Internet browser

No Avaya-provided software is installed directly on the client computer. For circuit-switched voice carried over the standard voice network, no computer sound system (soundboard, microphone, speakers, and software) is required.

The following diagram (Figure 2) shows a typical configuration with both local and remote users connected to Avaya Web Collaboration.

Figure 2. Avaya Web Collaboration Configuration



Note: What is commonly referred to as the Avaya Web Collaboration server is actually a set of interrelated server applications, each of which runs as a Windows 2000 service. The main server applications are the Avaya Web Collaboration server application, the Web server application, and the LDAP directory server application. The latter is used as the data store for the application server's data, such as user IDs and passwords.

LDAP Directory

The Directory Administrator page utilizes an LDAP directory. It is *not* within the scope of this guide to describe how an LDAP directory works. General knowledge of an LDAP directory is assumed.

EC500 Extension to Cellular

Avaya Web Collaboration provides the ability to turn your EC500 Extension to Cellular feature on and off. The EC500 Extension to Cellular feature is not included with Avaya Web Collaboration and must be purchased separately. The EC500 Extension to Cellular feature allows a cellular phone to be treated as a local extension to the DEFINITY switch. The cellular phone can use the same features and capabilities for incoming calls as the office phone. Whenever the office phone rings, the administered cellular phone also rings. Calls made to the cellular phone that are routed through DEFINITY are answered by the corporate

voice mail. If the user's administered phone has call waiting, up to two calls can be received.

Note: An extension (known as an Xmobile extension) must be administered on the Tserver and the switch for the user to have access to this feature.

Voice Over IP (VOIP)

The Avaya Unified Communication Center provides the ability for the remote user to place and receive H.323 audio calls or what is commonly referred to as "voice over IP". With this feature, only one line is needed, since the audio call is now placed and received on the same line that is being used to access the corporate data network for the application client-server interface. These users must be administered with a voice over IP extension, also known as a "media extension." A corresponding encrypted Security Code or password is administered. The user must download the required audio codec as well as support files for voice over IP; this is a one-time download of a self-extracting executable file.

Note: An extension (known as a VoIP extension) must be administered on the Tserver and the switch for the user to have access to this function.

Wireless Feature

Wireless versions of the Avaya Web Collaboration and Avaya Web Messaging GUIs can be accessed through many wireless devices. See UCC Wireless Featurefor more details.

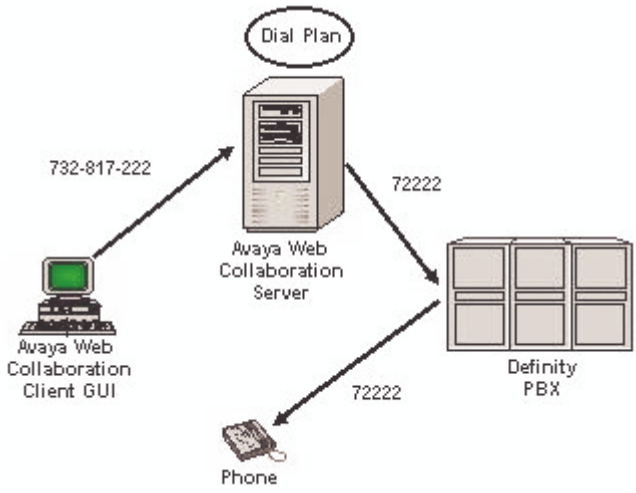
Administering the Dial Plan for Avaya Web Collaboration

Dial Plan Overview

Avaya Web Collaboration provides a dial plan so that audio calls can be made more efficiently. The dial plan translates phone numbers entered by the user or phone numbers selected through Search to the numbers that are sent to the Definity PBX when the call is made.

The following figure (Figure 3) depicts the Avaya Web Collaboration dial plan feature.

Figure 3. Dial Plan Diagram



For example, each user in a Definity PBX has a telephone number of the type 732-817-$$$$ and a corresponding extension number of the type 7$$$$. If a user makes a call to a number of the type 732-817-$$$$ through the Avaya Web Collaboration client GUI, the Dial Plan receives

the number and sends a number of the type 7$$$$ to the Definity PBX.

Dial Plan Description and Rules

The following table (Table 3.) is a sample Avaya Web Collaboration dial plan for a US-based customer. The Full Number Mask column shows the types of number formats a user may input. The Dialable Number Mask column shows the number formats the Dial Plan sends to the Definity PBX. The Local to Switch column indicates whether the number is in the local switch. These are the three settings the system administrator specifies when setting up the dial plan. The following rules govern the dial plan:

- **$ Mask.** The "$" character is used by the Dial Plan as the "wild card" mask to represent numbers that will vary within a group. For example, 732-817-$$$$ represents all numbers from 732-817-0000 to 732-817-9999.
- **Use of Dashes.** In the "Full Number Mask" column, dashes must be used. In the "Dialable Number Mask" column, dashes must not be used. The format must match the format stored in the directory. If a number entered does not match the numbers shown in the Full Number Mask column, the original number is sent to the PBX. If the call cannot be made, a message is displayed to the user.
- **Dial Plan Order.** The matching of the numbers is done in the order of the dial plan entries. For example, in the dial plan below, because the full number mask 732-817-$$$$ is above the full number mask 732-$$$-$$$$, the number 732-817-1234 is translated into 71234. If the order were reversed, the number 732-817-1234 would be translated into 98171234.
- **Multiple Definity PBXs.** If multiple Definity PBXs are controlled by an Avaya Web Collaboration server, each PBX has its own dial plan.

Table 3. Sample Dial Plan

Full Number Mask	Dialable Number Mask	Local to Switch	Description
732-817-$$$$	7$$$$	True	Internal Users

3$$$	3$$$	True	Remote (AWOH) Users
303-538-$$$$	8$$$$	False	Extensions on another PBX
9-$$$-$$$$	9$$$$$$$	False	Local call outside PBX
732-$$$-$$$$	9$$$$$$$	False	Local call outside PBX
9-1-$$$-$$$-$$$$	91$$$$$$$$$$	False	Long distance call
$$$-$$$-$$$$	91$$$$$$$$$$	False	Long distance call
$-$$$-$$$-$$$$	9011$$$$$$$$$$$	False	International call
$-$-$$$-$$$-$$$$	9011$$$$$$$$$$$$	False	International call

Create the Dial Plan

To create the Dial Plan:

1. On the Avaya Web Collaboration Administration page, click **Directory Admin**.
2. Select the **Switches** tab.
3. Double-click the switch or select it and click **Edit**.
4. Select **G3V8 or newer** from the Switch Release drop-down menu.
5. Select the **Multiple Calls for Remote** check box.
6. Click **Administer Dial Plan …** .
7. The Dial Plan Information dialog box appears. Data contained in this dialog box is shown in Table 2.

Input Field	Description	Action
Full Number Mask	The full number mask entries define the valid numbers that can be dialed. **Note:** The format must match the format of the number stored in the directory.	Type the full number mask.
Dialable Number Mask	The dialable number mask entries are the numbers that will be sent to the PBX. Do not use dashes.	Type the dialable number mask.
Is this mapping for an extension on this switch?	This check box should be selected for all numbers that are local to the switch (including AWOH numbers) and cleared for all other numbers.	Select the check box if the number is local to the switch.

8. Click **Add** when the entry is complete. Add additional entries as necessary.
9. Use the **Up** and **Down** buttons as necessary to arrange the order of the entries.
10. Once all the appropriate entries have been made, click **OK**. This action will return you to the Edit Switch Object dialog box.
11. Click **Apply**.
12. The Changing Switch Object dialog box appears.
13. Click **Yes**.
14. To make your changes take effect, turn the Avaya Web Collaboration server off, wait 30 seconds, and

then turn the server back on. For instructions on how to turn the server on and off, see Turn the Server On and Off.

Avaya Web Collaboration System Administration Concepts

The System Administration Graphical User Interface (GUI) provides access to various Web pages and dialog boxes that are used to operate, administer, and maintain Avaya Web Collaboration. The GUI consists of the following two main pages with various secondary pages: an Avaya Web Collaboration Administration page and a Directory Administrator page that is accessible from the Directory Admin button on the Avaya Web Collaboration Administration page.

Avaya Web Collaboration Administration Page

The Administration page (Figure 4) provides access to all administrative information and functions. When one of the buttons on the left side of the page is clicked, the corresponding information appears on the right side (except the Directory Admin button, which opens the Directory Administrator page). The buttons include:

- Directory Admin — provides access to the Directory Administrator pages to manage user information
- Server On/Off — provides the ability to send broadcasts to users and turn the server on and off
- System Usage — provides information about the number of users

- Data Conferences — provides information about the number of conferences and conferees (future availability)
- Server Options — provides the ability to refresh the directory and Tserver device list
- About AWC — provides information about the Avaya Web Collaboration release number, license limit, and so on
- Display Log — displays the error or maintenance log depending on which is selected from the pull-down menu above the Display Log button
- Admin Guide — provides access the UCC System Administrator's Guide

Figure 4. Avaya Web Collaboration Administration Page

Directory Administrator Page

The Directory Admin button on the Avaya Web Collaboration Administration page opens a new window that provides access to the configuration data and user

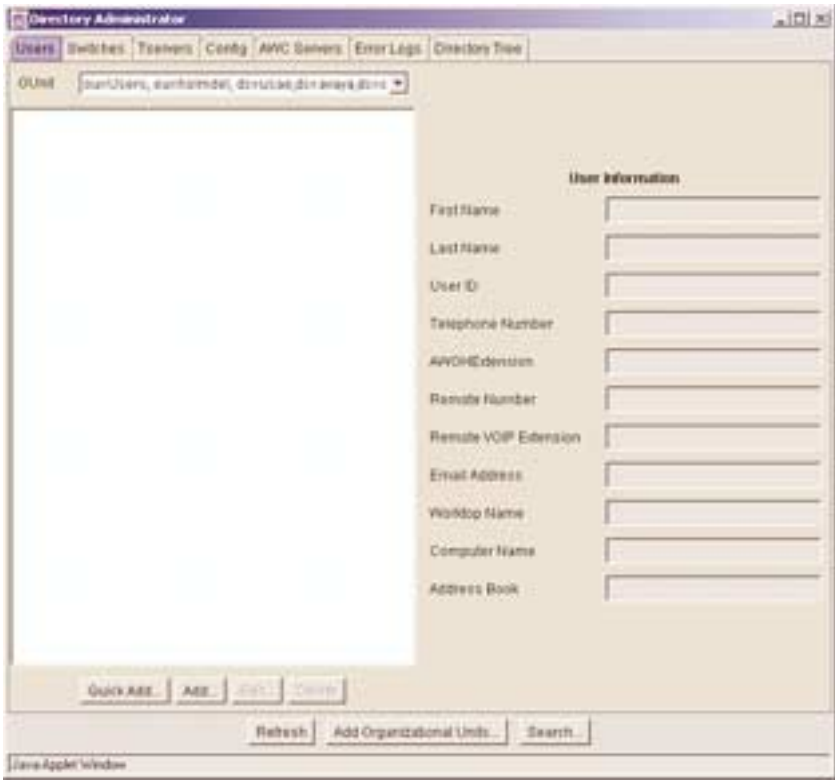
profile information stored in the Directory Server. A login and password are required to open this page. The Directory Admin button opens a Java applet; therefore, it could take some time initially to download and start.

Note:
A page entitled Directory Administration is opened with the Administrator Login. This page can be minimized or closed.

The Directory Administrator GUI (Figure 5) consists of the following eight tabs:

- Users — provides access to the LDAP directory for administering users for Avaya Web Collaboration and Avaya Web Messaging. When the Directory Administrator page is displayed, the Users tab is the default selection.
- Switches — provides the ability to view, add, edit, or delete switch information.
- Tservers — provides the ability to view, add, edit, or delete switch information.
- Config — provides the ability to view the Avaya Web Collaboration Server configuration information.
- AWC Servers — provides the ability to view, add, edit, or delete Avaya Web Collaboration server information.
- Error Logs — provides the ability to set preferences for what is written to the logs and the size of the logs.
- Directory Tree — provides the ability to view, add, edit, or delete directory tree information.

Figure 5. Directory Administrator Page



Directory Administrator Buttons

The Refresh, Add Organizational Units..., and Search... buttons appear on the bottom of every tab of the Directory Administrator page. See Figure 5.

Refresh

The Refresh button reloads the current information.

Add Organizational Units

The Add Organizational Units button opens the Create Organization Unit dialog box that is used to set up the hierarchy for each component in the directory. If you have not set up an organizational unit for Users, you can do this here.

To add an organizational unit:

1. Click **Add Organizational Units**.
2. Type the name (for example, Users) that you want to assign to the new organizational unit in the **Organizational Unit Name** field.

3. Select the name of the root directory in which you want the new organizational unit to reside from the **Organization Unit Of** drop-down menu.

4. Click **Apply**.

Search for a User

To search for the information about a specific user:

1. On the Avaya Unified Communication Center page, click **UCC User**.

2. Type your login and password and click **OK**.

3. Click **Search...** . The Search button is available from every tab on the Directory Administrator page.

4. In the Search dialog box, enter any information you have about the user and click **OK**. (Knowledge of an LDAP directory is assumed.)

Avaya Web Collaboration System Administration Tasks

Turn the Server On and Off

To access the Server On and Server Off buttons:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. The Server On/Off page appears by default.
4. If it is not displayed, click **Server On/Off**.

The Server On and Server Off buttons start and stop the following Windows 2000 services: the Avaya Web Collaboration server and the Avaya Web Collaboration Services Monitor.

If a user is in a conference and the server is turned off, existing audio calls will remain connected. However, an error box will appear that states that communication with the server has been lost. Data calls will be dropped, and users will no longer be able to log on until the server is turned back on.

When you click either of these buttons, messages are displayed to describe the status of the request. For example, if you click Server On, the following message is displayed:

Server Request On: Sent

One of these two messages then appears in the same area to indicate whether or not the request to turn on the server succeeded:

- Server Request: Success
- Server Request: Failed

If a Server Request: Failed message is received, another request under the Server Request: Failed text appears to provide a reason for failure. For example, if the server is currently on and the administrator presses the Server On button, the result would be the following sequence of messages:

Server Request On: Sent

Server Request: Failed

An instance of the server is already running

Send a Broadcast to Users

To send a broadcast to users:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. The Server On/Off page is displayed by default. If it is not displayed, click **Server On/Off**.

The Send Broadcast button provides the ability to send broadcast messages to users. A default message appears in the text area. You can edit this message by clicking within the text area. When you click the Send Broadcast button is clicked, the message appears as a dialog box to all logged-in users.

Verify that Email Capability is Functioning

The Send Test Email button provides the ability to send an email notice to the administrator to verify that the Send Broadcast capability is functioning.

Note: Prior to using this feature, you must specify the email server and email handle and restart the system. To do this, select the **AWC Servers** tab on the Directory Administrator page.

Monitor Current Users

To monitor current users:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **System Usage**.

The System Usage page displays the following information:

- **Current Total.** Displays how many users are currently logged in.
- **Current Remote.** Displays how many remote users are currently logged in.
- **Peak.** Displays the largest number of users logged in at one time since the last time the server was restarted.
- **Limit.** Displays the total number of users that the system allows. This number is determined by the system license your company purchased.
- **Update button.** Reloads the current values.
- **User Tasks.** The User Tasks button opens the List of Logged in Users dialog box. This dialog box provides the following information about each user currently logged in:
  - Name
  - User Id
  - Number
  - IP Address
  - Remote
  - Date/Time
  - On an Audio call
  - On a Data call

Monitor Data Conferences

To monitor data conferences:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **Data Conferences**.

The Data Conferences button displays the following information about T.120 data conferences and conferees.

- **Current Number of Conferences.** Displays the number of currently active data conferences.
- **Peak Number of Conferences.** Displays the highest number of data conferences since the server was last restarted or reset.
- **Running Total Number of Conferences.** Displays the total number of data conferences since the server was last restarted or reset.
- **Current Number of Conferees.** Displays the number of currently active conferees.
- **Peak Number of Conferees.** Displays the highest number of conferees since the server was last restarted or reset.
- **Running Total Number of Conferees.** Displays the total number of conferees since the server was last restarted or reset.

Refresh System After Adding or Changing User Information on the Tserver

To refresh the system after adding or changing user information on the Tserver:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **Server Options**.

The Server Options page is accessible from the Avaya Web Collaboration Administration page and has two buttons — Clear Cache and Refresh Tserver.

Clear Cache. Clears the directory Cache. This button needs to be clicked every time a new user is administered on the Tserver.

Refresh Tserver. Refreshes the Tserver device list when a device is added to the Tserver database while the Avaya Web Collaboration server is running.

View Avaya Web Collaboration Information

To view information about Avaya Web Collaboration:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **About AWC...**.

The About AWC button displays the following information:

- Avaya Web Collaboration software release number
- Serial number
- Concurrent login limit
- Data license limit
- Remote user limit
- JTAPI version
- Copyright information

Display Error or Maintenance Log

To display the Error or Maintenance Log:

1. Open the **Avaya Web Collaboration Administration** page.
2. Select either **Error** or **Maintenance** from the System Logs drop-down menu.
3. Click **Display Log**. In a new browser window.

4. The Error Log or Maintenance Log is displayed.

Manage User Information

Viewing, adding, editing, and deleting user information is all done from the Users tab on the Directory Administrator page. For further information about managing user information, see User Administration for the Unified Communication Center.

View/Print System Administration Guide

The Admin Guide button on the Avaya Web Collaboration Administration page opens this guide in a new browser window.

Switch (PBX) Information

The Switches tab on the Directory Administrator page provides access to the switch (PBX) information in the directory and the dial plan information.

Access Switch Information

To access switch information:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **Directory Admin**.
4. Type your login and password and click **OK**.
5. The Directory Administrator page appears.
6. Select the **Switches** tab.
7. If the switch you are looking for is not displayed, select the Organizational Unit that contains the switch you are looking for from the Ounit drop-down menu.
8. Select the switch.
9. The corresponding information will appear in the fields on the right.

Add a Switch (PBX)

To add a switch:

1. On the Switches tab on the Directory Administrator page, click **Add**.
2. In the Add Switch Object dialog box complete the input fields as follows:

Field	Description and Action
Switch Name	Type the name of the switch you are adding.
Domain Type	Verify Voice is selected on the Domain Type drop-down menu.
Transport Type	Verify Switched is selected on the Transport Type drop-down menu.
Switch Release	Verify G3V8 or Newer is selected on the Switch Release drop-down menu.
Organizational Unit	Accept the default or select the appropriate organizational unit.
Multiple Calls for Remote	Select the **Multiple Calls for Remote Use** checkbox if you will be administering a dial plan for this switch.
Drop AWOH on Internal Calls	Verify that Drop AWOH on Internal Calls is **not** selected.

Field	Description and Action
Sequential Calling Timeout	Type the number of minutes you want sequential calling to be left running. The recommended setting is 2 (minutes).
Administer Dial Plan...	If you want to add number formats to the dial plan, click **Administer Dial Plan...**. See the Administering the Dial Plan for Avaya Web Collaboration section for more information.

Edit Switch (PBX) Information

To edit the information for a switch:

1. On the Switches tab on the Directory Administrator page, click **Edit** or double-click the switch you want to edit.
2. In the Edit Switch Object dialog box edit the desired information. For more information about the input fields, see the Add a Switch section.

   Caution: You need to be careful in editing the name or Organizational Unit of a switch. These can be referenced by other objects (such as phone objects) in the directory.

Delete a Switch (PBX)

To delete a switch:

1. On the Switches tab on the Directory Administrator page, select the switch you want to delete.
2. Click **Delete**.
3. A confirmation dialog box appears.
4. Click **OK**.
5. All profile information about the selected switch is deleted from the directory.

Tserver Information

The Tservers tab on the Directory Administrator page provides access to the Tserver information in the directory.

Selecting an entry in the left frame displays information for that Tserver on the right. Double-clicking on the entry allows the Directory Manager to edit it.

Add a Tserver

To add a Tserver:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **Directory Admin**.
4. Type your login and password and click **OK**.
5. Select the **Tservers** tab.
6. Click **Add**.
7. In the Add Tserver Object dialog box, complete the following fields and then click **Apply**:

Field	Description and Action
Tserver Name	Type the name of the Tserver.
Owner	Type the name of the owner.
Description	Type a description of the Tserver that will help you identify it.
Telephony Server Login	Enter the user ID that you will use to access the telephony server. It is recommended that you use the same User ID throughout the UCC administration applications.
Telephony Server Password	Enter the password that you will use to access the telephony server. It is recommended that you use the same password throughout the UCC administration applications.

Field	Description and Action
Computer	To enter the computer: 1. Click the browse button (**...**). 2. The Computer Information dialog box appears. 3. Click **Find...** to search by using LDAP attributes or complete the fields as follows: a. In the Computer Information dialog box, type the Computer Name. b. Type the IP Address. c. Do not select the Dynamic IP Address check box. The IP Address cannot be dynamic. d. Type the Host Name. e. The organizational unit must be correct by default. If it is not, select the correct organizational unit. f. Click **Apply**.
Telephony Server Port Number	Type the port number of the telephony server.

Field	Description and Action
Services	To add a service: 1. Click the left-pointing arrows (<<). The Add Telephony Server Service dialog box appears. 2. Skip to the **Vendor Name** field. The first Service Name text field becomes populated as you enter information in the following fields. 3. Type the vendor name. 4. Type the service name. This is the switch name designated in CVCT. 5. Verify that the service type is CSTA. 6. Type the computer name (where the Tserver resides). 7. Select the switch from the Switch drop-down menu in order to show where it resides in the LDAP directory. 8. Select the appropriate organizational unit if it is not already selected. 9. Click **Apply**.

Field	Description and Action
Drivers	This field lists the switches that are associated with the Tserver. To add a Tserver: ▪ Click the left-pointing arrows (<<). To delete a Tserver: ▪ Click the right-pointing arrows (>>).
Organizational Unit	If it is not already selected, select the appropriate organizational unit.

Edit Tserver Information

To edit the information for a Tserver:

1. On the Tservers tab on the Directory Administrator page, click **Edit** or double-click the Tserver you want to edit.
2. In the Edit Telephony Server Object dialog box edit the desired information. For more information about the input fields, see the Add a Tserver section.

Delete a Tserver

To delete a Tserver:

1. On the Tservers tab on the Directory Administrator page, select the Tserver you want to delete.
2. Click **Delete**.
3. A confirmation dialog box appears.
4. Click **OK**.
5. All profile information about the selected Tserver is deleted from the directory.

View Avaya Web Collaboration Server Configuration Settings

To view the Avaya Web Collaboration server configuration settings:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **Directory Admin**.
4. Type your login and password and click **OK**.
5. Select the **Configuration** tab.

The Configuration Tab on the Directory Administrator page lists the following settings:

- LDAP Provider URL
- Search Base
- Default Login DN
- Avaya Web Collaboration Server

Note: The configuration settings are found in the propfile.txt configuration file located on the server. The file must be edited locally to change the settings.

Web Collaboration Server Information

Set Permanent Defaults for the Quick Add Feature

The following ten fields are available after clicking Add or Edit. These fields set the permanent default settings used when adding users with the Quick Add feature. To make changes to these fields take effect, you must close the session and start a new session. See Add a User Quickly with Default Settings for more information.

- Email Suffix
- Host Name Suffix
- Address Book Suffix
- Worktop Suffix
- Computer Name Suffix
- Voice Mail Server

- Default Messaging URL
- Default Speech URL
- Default Language
- Default Switch

Access Web Collaboration Server Information

To access the Web Collaboration Server information:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **Directory Admin**.
4. Type your login and password and click **OK**.
5. Select the **WC Servers** tab.
6. Select the **Web Collaboration Server** on the left. The information about it appears on the right.

Add a Web Collaboration Server

To add a Web Collaboration Server:

1. From the Web Collaboration Server tab, click **Add**.
2. The Add Web Collaboration Servers Object dialog box appears.
3. Complete the following input fields:

Input Fields	Description and Action
WC Server Name	Type the name of the WC Server.
Owner	Type the name of the owner.
Description	Type a description of the server that will help you identify it.

Input Fields	Description and Action
Computer	To enter the computer: 1. Click the browse button (**...**). The Computer Information dialog box appears. 2. On the Computer Information dialog box, type the computer name. 3. Type the IP address. 4. Verify the Dynamic IP Address checkbox is not selected. 5. Type the host name. 6. The Organizational Unit should be correct by default. If it is not, select the correct Organizational Unit. 7. Click **Apply**.
Email Suffix	Type the suffix that you want to be the default when adding users (for example, @avaya.com).
HostName Suffix	Type the suffix for the host name that you want to be the default when adding users (also known as the domain name).
Address Book Suffix	Type the address book suffix that you want to be the default when adding users (for example, _ AddressBook).
Worktop Suffix	Type the worktop suffix that you want to be the default when adding users (for example, _Worktop).

Input Fields	Description and Action
Computer Name Suffix	Type the computer name suffix that you want to be the default when adding users (for example, _ Computer).
Voice Mail Server	Type the name of the Voice Mail Server (the server on which Avaya Web Messaging resides). For Intuity, type the host name or IP address. For an Octel message server, type **<voicemail server name@OctelAccess server name>**.
Default Messaging URL	Type your URL for Web Messaging.
Default Speech URL	Type the URL for the ASA for UCC User Preferences Web site.
Default Language	Type the language that you want to be the default when adding users.
Default Switch	Type the switch that you want to be the default when adding users.
TLINKs	To add a TLINK: 1. Click the left-pointing arrows (<<). 2. The Choose Telephony Server Service (TLINK) dialog box appears. 3. If the TLINK you want is not displayed, choose the organizational unit in which it resides. 4. Select the TLINK you want. 5. Click **OK**.

Input Fields	Description and Action
Presence Status?	If you want users to be able to detect whether other users are logged in and available, select the **Presence Status?** check box.
Call Screening?	If you want users to be able to screen calls by listening as callers leave voice messages, select the **Call Screening?** check box.
Notifications - Email Server	Type the name of the EMail Server if it has not been automatically populated. You must complete this step to enable the Send Test EMail function available on the Server On/Off page.
Notifications - Email Handle	Type the name of the EMail Handle of the administrator if it has not been automatically populated. You must complete this step to enable the Send Test EMail function available on the Server On/Off page.
Personal Entry Limit	The recommended setting for the Personal Entry Limit is 50.
Personal Folder Limit	The recommended setting for the Personal Folder Limit is 50.
Organizational Unit	The organizational unit should be correct by default. If it is not, select the correct Organizational Unit.

Input Fields	Description and Action
LDAP Settings...	To change LDAP Count Limit or Time Limit settings or to add or delete LDAP Servers: 1. Click **LDAP Settings...**. 2. The LDAP Settings dialog box appears. 3. Type the appropriate Count Limit. 4. Type the appropriate Time Limit. 5. To add an LDAP server click **Add>>**. 6. When the Add additional LDAP Servers dialog box appears, complete the fields by using the tips in the dialog box for assistance. 7. To delete an LDAP server, select it and click **Delete**<<. 8. Click **OK**.
Default Organizational Units...	Click this button to set the Default Organizational Unit for users, worktops, computers, telephones, address books, telephony servers, Avaya Web Collaboration servers, and switches. See Set Default Organizational Units.

Edit Web Collaboration Server Information

To edit the information for a Web Collaboration Server:

1. On the WC Servers tab on the Directory Administrator page, click **Edit**. The Edit Web Collaboration Server dialog box appears.
2. In the Edit Web Collaboration Server Object dialog box, edit the desired information. For more information about the fields, see the Add a Web Collaboration Server section.

Delete an Avaya Web Collaboration Server

To delete a Web Collaboration Server:

1. On the WC Server tab on the Directory Administrator page, select the Web Collaboration Server you want to delete.
2. Click **Delete**.
3. A confirmation dialog box appears.
4. Click **OK**.
5. All profile information about the selected Web Collaboration Server is deleted from the directory.

Set Default Organizational Units

Setting the default organizational units will save you time. The Organizational Units drop-down menu will be automatically populated with the correct Organizational Units, whenever you are in the System Administration GUI. The Default Organizational Units dialog box provides the ability to set the Default Organizational Unit for:

- Users
- Worktops
- Computers
- Telephones
- Address Books
- Telephony Servers
- Avaya Web Collaboration Servers
- Switches

To set default organizational units:

1. On the WC Servers tab on the Directory Administrator page, click **Add**.
2. The Web Collaboration Server Information dialog box appears.
3. Click **Default Organizational Units...**.
4. Select the appropriate Organizational Unit from each drop-down menu on the Default Organizational Units dialog box.
5. Click **Apply**.

Administer Error Log Settings

The Error Logs tab provides the ability to control the settings for the error log that is available from the Display Log button on the Avaya Web Collaboration Administration page.

To administer the Error Log Settings:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **Directory Admin.**
4. Type your login and password and click **OK**.
5. Select the Error Logs tab.
6. Select the appropriate Avaya Web Collaboration Server from the Avaya Web Collaboration Server drop-down menu.
7. Select the Error Log levels you want listed in the error log from the list of check boxes entitled Error Log Settings.
8. Click **Apply**.

Directory Tree Information

The Directory Tree tab lists the entire directory structure. All objects and attributes in the directory server are shown. Knowledge of an LDAP directory is assumed.

> Caution: Care must be taken in manually editing any entries within this tab.

Access Directory Tree

To access the Directory Tree:

1. On the Unified Communication Center page, click **Avaya Web Collaboration**.
2. Type your login and password and click **OK**.
3. Click **Directory Admin**.
4. Type your login and password and click **OK**.
5. Select the Directory Tree tab.

Add a New Directory Entry

To add a new directory entry:

1. From the Directory Tree tab on the Directory Administrator page, click **Add...** (below the Directory Tree window).
2. In the Add Directory Entry dialog box, type the leading DN attribute and value and any other attributes and values.
3. Click **Apply**.

Delete a Directory Entry

To delete a directory entry:

1. On the Directory Tree tab on the Directory Administrator page, select the directory entry you want to delete.
2. Click **Delete**.
3. All information in that directory entry is deleted.

Add a New Directory Entry Attribute

To add a new directory entry attribute:

1. On the Directory Tree tab on the Directory Administrator page, select the directory entry to which you want to add the attribute and value.
2. Click **Add** (below the Entry Attributes window).
3. In the Add Attribute-Value dialog box, type the Attribute Name and Value.
4. Click **OK**.
5. Click **Apply**.

Delete a Directory Entry Attribute

To delete a directory entry attribute:

1. On the Directory Tree tab on the Directory Administrator page, select the directory entry from which you want to delete the attribute.
2. Click **Delete** (below the Entry Attributes window).
3. Click **Apply**.

Start and Stop the Tserver

To access the TSAPI Telephony Services Controller dialog box, use the following path:

Start Menu > **Programs** > **TSAPI Telephony Services** > **TSAPI Telephony Services Controller**

The TSAPI Telephony Services Controller dialog box appears. When the Tserver is running, the state will indicate RUNNING.

To stop the Tserver:

1. Click **Stop**.
2. Wait until you get confirmation that the server is stopped.

To restart the Tserver:

1. Click **Start**.
2. Wait until you get confirmation that the server restarted.

Change the Machine-name Alias After Installation

If the machine-name alias changes after installation the following two things must be done:

- Change the references to the alias name
- Create a new Palm Query Application (PQA) file

Change the References to the Alias Name

To change the references to the alias name:

1. Open the file C:\Avaya\UCC\Tomcat\webapps\UCC\WEB-INF\configs.xml using Notepad or Wordpad.
2. Replace the six occurrences of the old machine-name alias with the new machine-name alias. They occur in the following places:
   - <AWCServerSettings>

     <ServerName>**old_machine-name_alias**.com<AWCServerSettings>
   - <AuthServlet>

     <URL>http://**old_machine-name_alias**.com/UCC/servlet/AuthServlet</URL>

- <UserSettingsServlet>

  <URL>http://**old_machine-name_alias**.com/UCC/servlet/UserSettingsServlet</URL>

- <ProcessLoginServlet>

  <URL>http://**old_machine-name_alias**.com/UCC/servlet/ProcessLogin</URL>

- <SpeechAccess>

  <ErrorPage>http://**old_machine-name_alias**.com/UCC/errSpeechAccess.jsp</ErrorPage>

- <ClientApplet>

  <JarURL>http://**old_machine-name_alias**.com/UCC/client.jar</JarURL>

3. Save and close the file.
4. Go to **Start Menu > Settings > Control Panel > Administrative Tools > Services**.

   Warning: All users will be logged off when Tomcat is restarted. Verify that no users are logged on before restarting.

5. Select **Tomcat**.
6. From the Action menu, click **Restart**.

Create a New PQA

To create a new Palm Query Application (PQA) file:

1. From a command prompt on the server machine, type **C:** and click Enter.
2. cd to \Avaya\UCC\tomcat\webapps\UCC\PQA .
3. Type **BuildPQA <protocol><full machine name>** and click Enter. For example,

   BuildPQA http://www.avaya.com

   The protocol can be either http or https. If you need to access a different port, add the port number to the end of the machine name. For example,

   https://www.avaya.com:8080

4. A new PQA file is generated.

Access Windows 2000 Services Through the Control Panel

The Services Control Panel provides the ability to monitor Windows 2000 services, turn Windows 2000 services on, and turn Windows 2000 services off. These services include the AWC Services Monitor, AWC, the AWC Log Messages, the iPlanet Administration Server 5.1, the iPlanet Directory Server 5, Tomcat, and the World Wide Web Publishing Server.

Use the following path to access the Services Control Panel:

Start Menu > **Administrative Tools** > **Server Management > Services**

System Maintenance

The following backups are expected to occur:

- Backup of the Windows 2000 server on a regular basis
- Backup of the Directory Server on a regular basis (or at any time changes are made)

Note: The Avaya Web Collaboration Services Monitor might restart the Avaya Web Collaboration server application when it detects an alarm condition. When the system has restarted, an entry can be found in the maintenance log.

UCC Avaya Web Messaging Administration & Maintenance

The Web pages for Avaya Web Messaging Administration & Maintenance are installed when the Avaya Web Messaging application is installed.

Use these Web pages to configure, update, monitor, and troubleshoot Avaya Web Messaging.

Access the Administration & Maintenance pages from the Web server used for Avaya Web Messaging or from another computer that has access to the Web server administration logon page for Avaya Web Messaging. In the Browser Location box, type

<Web server URL>/<virtual directory name for Avaya Web Messaging application>/admin.

From the Administration & Maintenance pages, you can perform these tasks:

- Configure, modify, and delete message servers for Avaya Web Messaging.
- Enable or disable IMAP4 access by configuring the LDAP directory for IMAP4 access.
- Schedule the Names Directory download for each message server and force immediate download of the Names Directory.
- Review the list of Avaya Web Messaging users.
- Restrict users from logging on to Avaya Web Messaging.

- Enable users to use the Avaya Voice Player to hear their messages by using their computers rather than their phones.
- Enable the use of certain wireless devices, such as personal digital assistants, (PDAs) for accessing messages.
- Bypass the Logon page.
- Review performance and usage statistics.
- Use the maintenance tools to verify that the Avaya Web Messaging server is correctly connected.
- Reset the Web server used for Avaya Web Messaging.
- Back up and restore critical Avaya Web Messaging data.
- For INTUITY servers, reserve seats for specific mailbox numbers.

Logging On

To access the Avaya Web Messaging Administration & Maintenance pages, you must enter the logon ID and password.

Two logon names are configured for Avaya Web Messaging.

- **admin** is the administrator's logon name.
- **services** is the technical support logon name.

From the Maintenance and Administration Log On page, the default password for admin is admin1. See Change Password or Logon ID from the Change Password page.

All administrative activity is recorded to the Administrator's History log. Separate logon tracks the changes made by the administrator or technical support.

Note: If you log on but are not actively using the Administration & Maintenance pages, you are automatically logged off if the server timeout expires. The default is 20 minutes of inactivity. This amount of time can be changed on

the Options page. When you try to access the page, you are automatically returned to the Logon page.

To log on to the Administration & Maintenance site, follow these steps:

1. From the browser, enter the Avaya Web Messaging administration URL, type

   <Web server URL> / <virtual directory name for Avaya Web Messaging> / admin.

   The Avaya Web Messaging admin logon page is displayed.

2. Enter the Logon name, either **admin** or **services**

3. Enter the password.

   The default password for the Admin logon is **admin1**, and the default password for Services is **Services1**.

4. Click **Login.** The Administration & Maintenance page is displayed.

Figure 6. Avaya Web Messaging Administration & Maintenance Page

Administration & Maintenance Web Page

The three categories on the Avaya Web Messaging Web server Administration & Maintenance page provide links to administrator features, application tools, and system usage data.

- Administration. Use the subcategories shown to make changes to message server settings as well as Avaya Web Messaging Web server settings and passwords. One subcategory allows you to view a history of server administration.
- Maintenance. Use the Maintenance subpages to perform tests to diagnose and troubleshoot logon activities, software functions, and performance.
- System Usage. Use the System Usage subpages to collect and display data on averages and hourly logon activities, types of files being transmitted, and message functions implemented by users.

Note: When you view the Administration & Maintenance subpages, failures and errors are displayed in red, and important information is displayed in blue.

Administration

The administration section for Avaya Web Messaging includes the following pages:

- **Message Servers**. Lists the INTUITY AUDIX message servers and the OctelAccess Servers that are accessible from Avaya Web Messaging. From this page, you add message servers and configure their Names Directory download schedule. You can add, modify, and delete message servers.
- **User List**. Lists all users who have successfully logged on to Avaya Web Messaging and the number of INTUITY AUDIX seats being used and remaining. From this page, you can restrict users from logging on to the INTUITY AUDIX message server.
- **Options and Settings**. Allows you to set the URL option, change the corporate logo that is displayed on the Avaya Web Messaging user logon page, set the Avaya Web Messaging session time out, enable

the use of the Avaya Voice Player to hear messages through the computer, and enable the use of wireless devices for access.

- **Administration History**. Displays the history of server administration, including the logon type and changes made to the configuration.
- **Change Login ID or Password**. Allows you to change the password for the Administration & Maintenance logon.
- **Schedule Maintenance**. Allows you to schedule maintenance activities according to your needs. The default settings assume that you want to run various tests and monitor Avaya Web Messaging.

Message Servers

Use the Message Servers page to configure the message servers for Avaya Web Messaging. The Message Servers page lists all Message servers that you have configured. See Figure 7.

The Message Server page shows the following:

- **Server name.** This is either the INTUITY AUDIX message server name or the OctelAccess server name. The server names shown here are seen by users when they are selecting their message server. You can also enter an IP address.
- **Type**. INTUITY is the Intuity Audix message server, 200/300 is an Octel 200/300 message server, and 250/350 is an Octel 250/350 message server
- **Names Directory Retrieval**
  - The Retrieved column shows the date and time of the Names Directory downloaded. Failed is displayed if the download was unsuccessful. In Progress is displayed if retrieval is in progress.
  - The Scheduled column shows scheduled retrieval time.
  - The Mailbox column is for INTUITY AUDIX servers only to list the mailbox configured on the message server for the Names Directory retrieval.

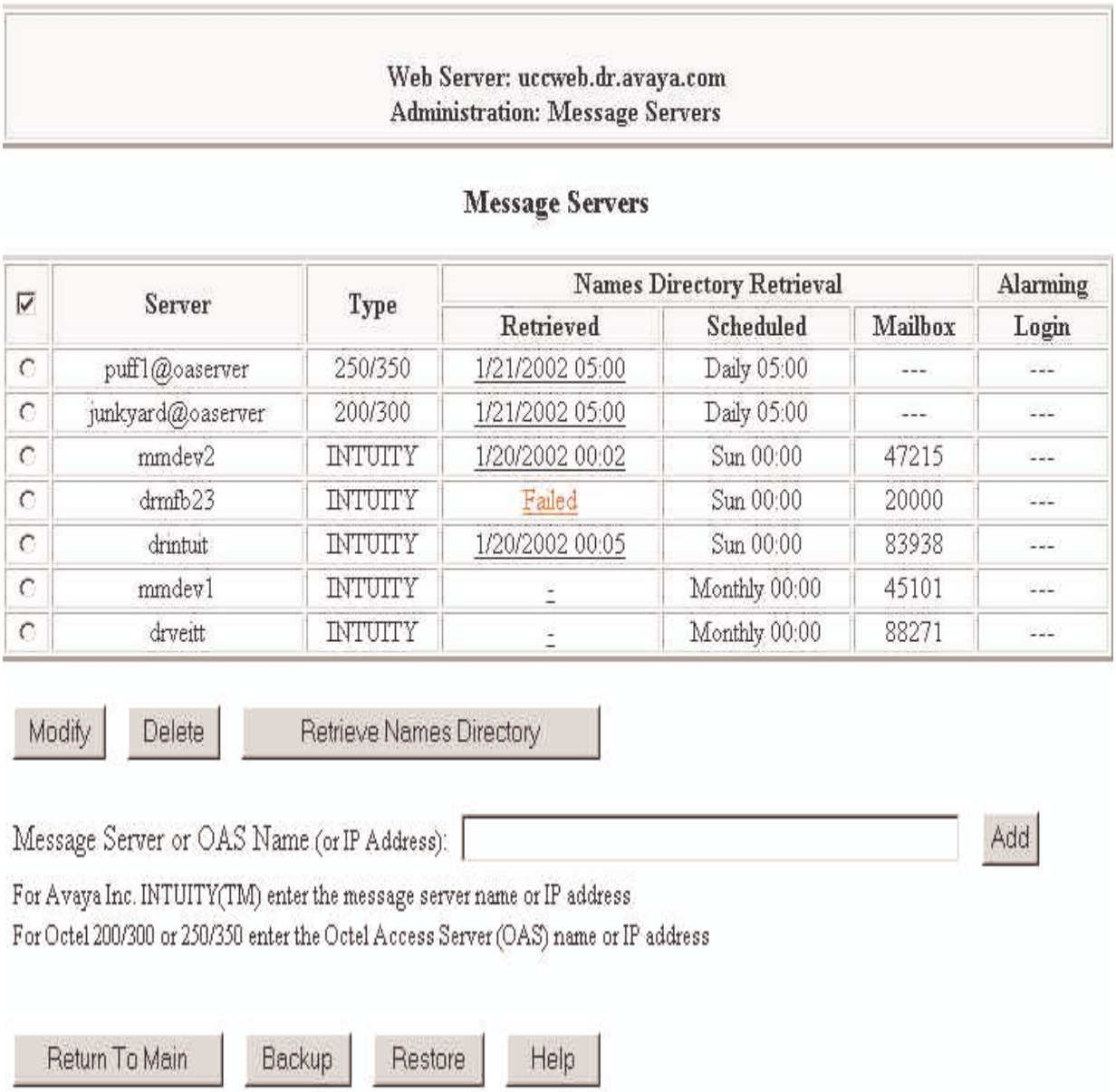
- For the INTUITY AUDIX, **Alarming**. If Trusted Server alarming has been configured, this column displays the login.

From the Message Servers page, you can do the following:

- Add, modify, and delete the message servers available to your Avaya Web Messaging users. When you add or modify a message server, you must define a Names Directory Retrieval schedule. For the INTUITY AUDIX message server, you can provide alarming information (optional).
- Download a message server's Names Directory for immediate use and configure the Names Directory download schedule.
- Back up and restore message server information.

The message server names displayed in the server table are the only message servers accessible to end users when they log on to Avaya Web Messaging. An example of the Message Server page is shown in Figure 7.

Figure 7. Message Server Page



Configuring Message Servers

Add Message Servers

1. On the Message Server page, in the Message Server or OAS Name box, enter the following information:
   - For INTUITY AUDIX message servers, the message server name or IP address
   - For Octel message servers, the OctelAccess name or IP address

2. Click **Add**.

   A test is run to verify LAN connectivity on the server. If the server address is correct, a new page appears that displays the server name.

3. Restart the Tomcat service.

Additional Instructions for Octel Message Servers

1. Select the frequency for Names Directory retrieval. If you specify weekly, enter the day of the week. If you specify monthly, the retrieval takes place the first day of the month.

2. Enter the retrieval time for the Names Directory download.

   Note: When you download the Names Directory downloaded from the OctelAccess Server, for the most current Names Directory you should configure the Avaya Web Messaging schedule to be later than the Names download schedule configured for the OctelAccess Server.

3. Click **Submit.** The Message Server page reappears with the message server you added.

For INTUITY AUDIX Message Servers

The INTUITY AUDIX message server communicates with the Avaya Web Messaging Web server.

For the INTUITY AUDIX message server, the mailbox used to retrieve the Names Directory and the Names Directory schedule must be configured.

Important: The mailbox used to retrieve the Names Directory must be password protected.

Note: As an optional feature, the trusted server alarming can be configured.

To configure the INTUITY AUDIX mailbox:

1. Enter the INTUITY AUDIX mailbox number that is used to retrieve the Names Directory.

2. Enter the password for this mailbox.

Note: If the mailbox password is changed, the password must also be changed in the Avaya Web Messaging configuration for that message server.

3. Select how often you want to have the Names Directory retrieved.

   If you specify weekly, enter the day of the week. If you specify monthly, the retrieval is the first day of the month.

4. Enter the retrieval time for the Names Directory download.

5. The Windows 2000 Web server on which Avaya Web Messaging resides must be administered on the INTUITY AUDIX as a trusted server so that when a problem appears on the Avaya Web Messaging Web server, Avaya Web Messaging sets off an alarm on the INTUITY AUDIX message server.

   Allowing Avaya Web Messaging to set off an alarm speeds up recognition of problems with Avaya Web Messaging. Alarms set off by a trusted server are always minor alarms on the INTUITY AUDIX message server.

   To administer a Trusted Server, the IP address of the Web server is required as well as a Trusted Server name and password.

   For Trusted Server alarming notification, enter the following:

   - Trusted Server logon
   - Trusted Server password
   - IMAPI password (only if administered on the INTUITY AUDIX message server)

   Note: Only one INTUITY AUDIX message server in an Avaya Web Messaging configuration must be configured for alarming so that an alarm call is sent only to one message server.

6. Click **Submit.** The Message Server page is displayed, with the new entry listed.

   When you click **Submit**, Avaya Web Messaging verifies that this is a valid trusted server login. It will try to log in as a trusted server on the INTUITY

AUDIX. If the information is not valid, this page does not close.

To Modify Information

1. On the Message Server page, check the server to be modified and click **Modify**.
2. Change the Names Directory Retrieval schedule or the Alarming information. Follow the steps outlined in Add Message Servers.
3. Restart the Tomcat service.

Delete Message Servers

A message server can be deleted from the Message Server list. When you delete a message server, it is no longer available from Avaya Web Messaging. Before you delete a message server, it is recommended that you notify the end users.

To delete a message server:

1. On the Message Server page, select the server to delete.
2. Click **Delete**. The message server is deleted.
3. Restart the Tomcat service.

Restart the Tomcat Service After Adding or Modifying Message Server Information

Whenever you administer the Message servers, restart the Tomcat service to make your changes take effect. To restart the Tomcat service:

1. Go to **Start Menu > Settings > Control Panel > Administrative Tools > Services**.

   Warning: All users will be logged off when Tomcat is restarted. Verify that no users are logged on before restarting.

2. Select **Tomcat**.
3. From the Action menu, click **Restart**.

Manual Retrieval of Names Directory

You can initiate the retrieval of a message server's Names Directory at any time. After you have finished adding the message servers, you need to initiate an immediate Names Directory download so that Avaya Web Messaging

end users can use the addressing feature when they first log on. If there are major changes to the Names Directory before the next scheduled download, you may want to initiate the retrieval so that the newest changes are available.

From the Message Server page, check the box for the message server and click **Retrieve Names Directory**. The Names Directory download begins immediately. The message "In Progress [X]%" is displayed in the Retrieved column. The percent displayed shows the retrieval status of the Names Download.

Once the message "In Progress [x]%" is displayed, this message does not change until you refresh the screen. To update the In Progress information or to see if the Names Directory download is complete, use the browser **Refresh** or **Reload** button to refresh the screen. When the Names download is complete, the Retrieved column displays the time of the download.

If the download was not successful, the message "Failed" is displayed in the Retrieved column. To see the explanation of the download failure, move the mouse over the word "Failed." A ToolTip appears with an explanation. You can also check the Administration History log for the failure reason.

Depending on the size of the Names Directory, the Names Directory download could take a few minutes more.

Backup and Restore

You can back up the message server configuration and restore it from the Message Server page.

Backup

1. Click **Backup**.

   You are queried as to whether you wish to perform the backup since doing so will remove the information from your previous backup.

2. Click **OK** to confirm that you want to back up the message server list.

Restore

Click **Restore**. You are queried as to whether you want to perform the restore since doing so will overwrite your current settings.

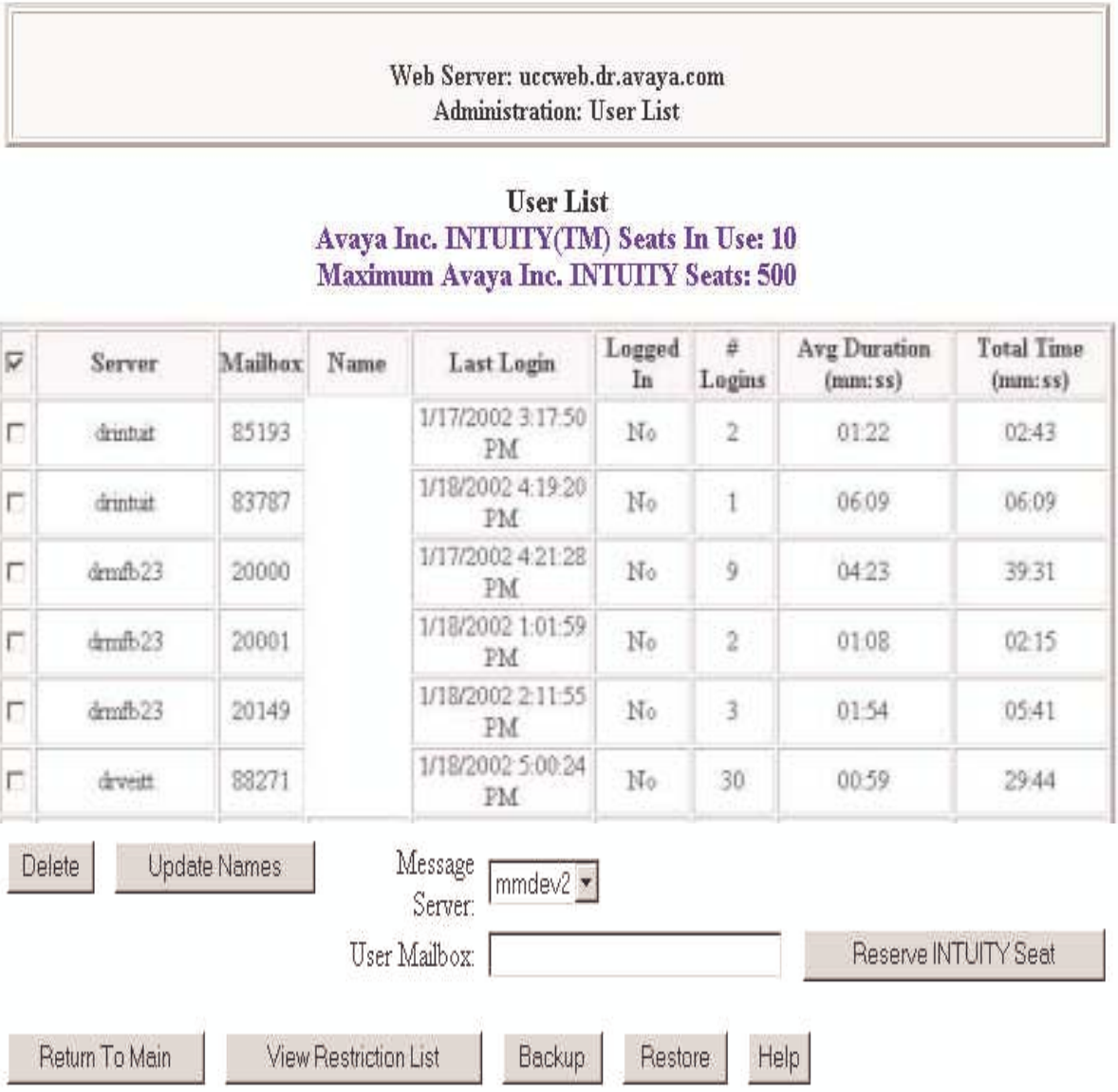
Important: If you do not have a backup and you click **Restore**, the message server information is lost.

User List

The User List page, shown in Figure 8, is used for the following:

- To display all end-user mailboxes that can use or have used Avaya Web Messaging. The entries are sorted first by message server and then in the order of the oldest logon to the newest. The information is added to the User List the first time an end user logs on to Avaya Web Messaging.
- To delete mailboxes.
- To update the Names column.
- To view the Restriction List.
- For the INTUITY AUDIX message server, to view the number of seats in use and the maximum number of seats available.

Figure 8. User List Page



For INTUITY AUDIX message servers, the User List page shows the number of seats in use and the maximum number of INTUITY AUDIX seats available. Seats can be reserved for INTUITY AUDIX users. This information is displayed only when Avaya Web Messaging is configured with an INTUITY AUDIX message server.

Note: For Octel message servers, the number of licensed seats used and available is determined by Capacity on Demand (COD). You can view the number of licenses used and available for each message server.

To access the User List page, do one of the following:

- From the Octel 200/300 message servers, use the List Feature command (@L F).

  The number of mailboxes and licenses purchased and used is shown.

- From the Octel 250/350 system managers terminal, go to menu 13.15.

  The number of licenses purchased is shown.

The User List page displays information about who has logged on to Avaya Web Messaging, including:

- **Server**. Name or IP address of the message server.
- **Mailbox**. User's mailbox number.
- **Name**. Name as it appears in the message server's Names Directory.
- **Last Login**. Day and time the end user last logged on to Avaya Web Messaging. For Reserved seats, this column displays "Reserved" in blue, until the users logs on for the first time.
- **Logged In**. The present logon status.
- **# Logins**. The number of times the end user logged on to Avaya Web Messaging. Octel message server users can have more than one logon simultaneously, whereas INTUITY AUDIX users cannot.
- **Avg Duration**. The average length of time in minutes and seconds that the end user logged on per session.
- **Total Time.** Average duration of users and the number of log ons.

Deleting Mailboxes

You can monitor Avaya Web Messaging usage and delete mailboxes. By reviewing the logon information you can determine if mailboxes are not being used and should be deleted.

Note: When a mailbox is removed from the list, for INTUITY AUDIX message servers, the number of seats available is increased.

To delete client mailboxes:

1. Click the checkbox in the first column for each mailbox number to be deleted.
2. Then click **Delete**. The mailboxes are removed from the list.

Update Names

Names are filled in on this page when users log on and the Names Directory has been downloaded. If there have been changes to the information, Update Names updates the information that is displayed in the User List from the latest Names Directory downloaded.

Reserving Mailboxes

For INTUITY AUDIX message servers, seats can be reserved for specific mailboxes. Each new mailbox user logon reserves one of the purchased seats. To control some or all of the seats, you can reserve mailbox numbers. Reserving a mailbox number automatically applies a licensed seat reservation for that mailbox. Thus an end user who may not log on to Avaya Web Messaging during the initial startup can be guaranteed a seat.

You can reserve as many seats as you have purchased for the INTUITY AUDIX message servers.

To reserve seats for INTUITY AUDIX mailboxes:

1. Scroll to the end of the User List Page.
2. Select the message server where the mailbox resides.
3. Enter the mailbox number in the User Mailbox field.
4. Click **Reserve Mailbox**. A seat is reserved for this mailbox logon to Avaya Web Messaging.
5. Repeat from step 2 to add additional mailboxes to be reserved.

Restricting User Access

You can restrict mailboxes from using Avaya Web Messaging. View Restriction List shows the restricted mailboxes.

To add mailboxes to the Restriction List:

1. Click **View Restriction List**.

   The page shows the restriction list by server name and mailbox number and name.

2. Select the message server to restrict mailboxes.

3. In the **User Mailbox** box, enter the mailbox number to be restricted.
4. Click **Add Restriction**.

   The Restrict Use Mailbox page is refreshed to show the restricted mailbox information.

To delete mailboxes from the Restricted User Mailbox list

1. Click the box next to the mailbox numbers to delete.
2. Click **Delete**.

   The mailboxes are removed from the list.

Bypass Log On Page

You can allow users to bypass the Avaya Web Messaging Log On page through a communication-enabled portal. The user's mailbox appears first instead of the Log On page, allowing the user to immediately access mail. Since the URL query string arguments need to be changed, contact Avaya Professional Services for more information. This feature is fee-based.

Backup and Restore User List and Restriction List

From the User List page, you can back up the User list and the Restriction list and restore them.

Back up

1. Click **Backup**.

   You are queried as to whether to perform the backup since doing so removes the information from your previous backup.
2. Click **OK** to confirm that you want to back up the User and Restriction list.

Restore

1. Click **Restore**.

   You are queried whether to perform the restore since this overwrites your current settings

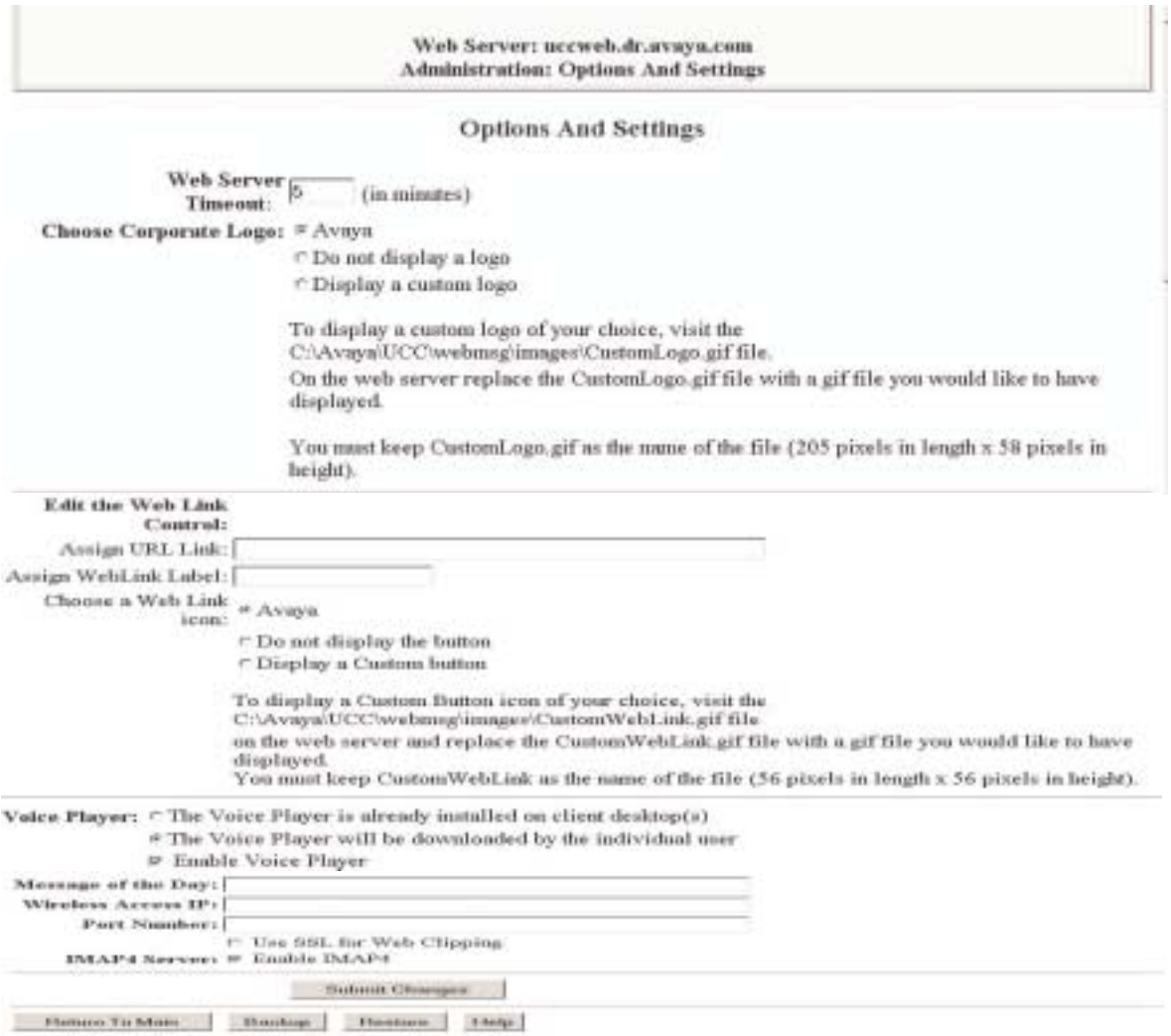
Important: If you do not have a backup and you click **Restore**, the user list and restriction list are emptied.

Options and Settings

The Options and Settings page, shown in Figure 9, is used to configure the following:

- Web Server timeout
- Web Link URL
- Message of the Day
- Access to Web Messaging through wireless Personal Digital Assistants (PDAs), such as Palm Pilots, Pocket PCs (for example, Compaq iPaq or HP Jornada), and Blackberrys
- Access to Avaya Voice Player.
- Corporate logo to be displayed

Figure 9. Options and Settings Page



Web Server Timeout

When Avaya Web Messaging users are not actively using Avaya Web Messaging, the Web server session is lost after the number of minutes configured here.

The INTUITY AUDIX message servers sets a time out that is separate from the Web Sever-configured time out. If the INTUITY AUDIX message server time out is shorter then the Web server timeout, inactive user pages are closed when message server configured time out is reached. Octel message servers do not have a time out feature, thus users are logged off Avaya Web Messaging when the page is inactive for the time configured here.

To establish a time limit for timeout, in the Web Server Timeout box, enter the number of minutes to wait before timing out. The default is 20 minutes.

Web Link URL

This feature is optional, and it can be used to provide end users a link to a customer's Web-based e-mail or to any important Web location that the customer designates.

To enable this feature, enter the URL in the Web Link URL location box. The icon to access this URL appears on the user's main Avaya Web Messaging page. When this icon is selected, the configured URL destination is launched.

Access for Wireless Devices

An IP address must be entered to enable users to use wireless devices (personal digital assistants, or PDAs) to access Avaya Web Messaging. This IP address is a proxy address so that if users access their messages from outside the Intranet, they will be directed automatically to the proxy server to maintain Intranet security.

Corporate Logo

The user's Avaya Web Messaging logon page can display either the Avaya logo or a customized logo.

To establish the logo you want to see displayed:

1. Check the correct Corporate Logo button to use, either the **Avaya** or **Custom**.
2. If you select **Avaya**, Click **Submit**. If you select **Custom**, go to step 3.
3. Go to the Avaya Web Messaging directory,

   <drive>:\<program directory>\webmsg\images.

   Replace the existing CustomLogo.gif file with a new CustomLogo.gif file that contains the graphics you

want displayed. For optimum presentation on the Web page, the new logo should be approximately the same size as the one being replaced.

Backup and Restore

From the Options and Setting page, you can back up the information you have configured and restore it.

To back up:

1. Click **Backup**.

   You are queried as to whether to perform the backup since doing so removes the information from your previous backup.

2. Click **OK**.

To restore:

1. Click **Restore**.

   You are queried as to whether to perform the restore since doing so overwrites your current settings

Important: If you do not have a backup and you click **Restore**, the information is restored to its default values.

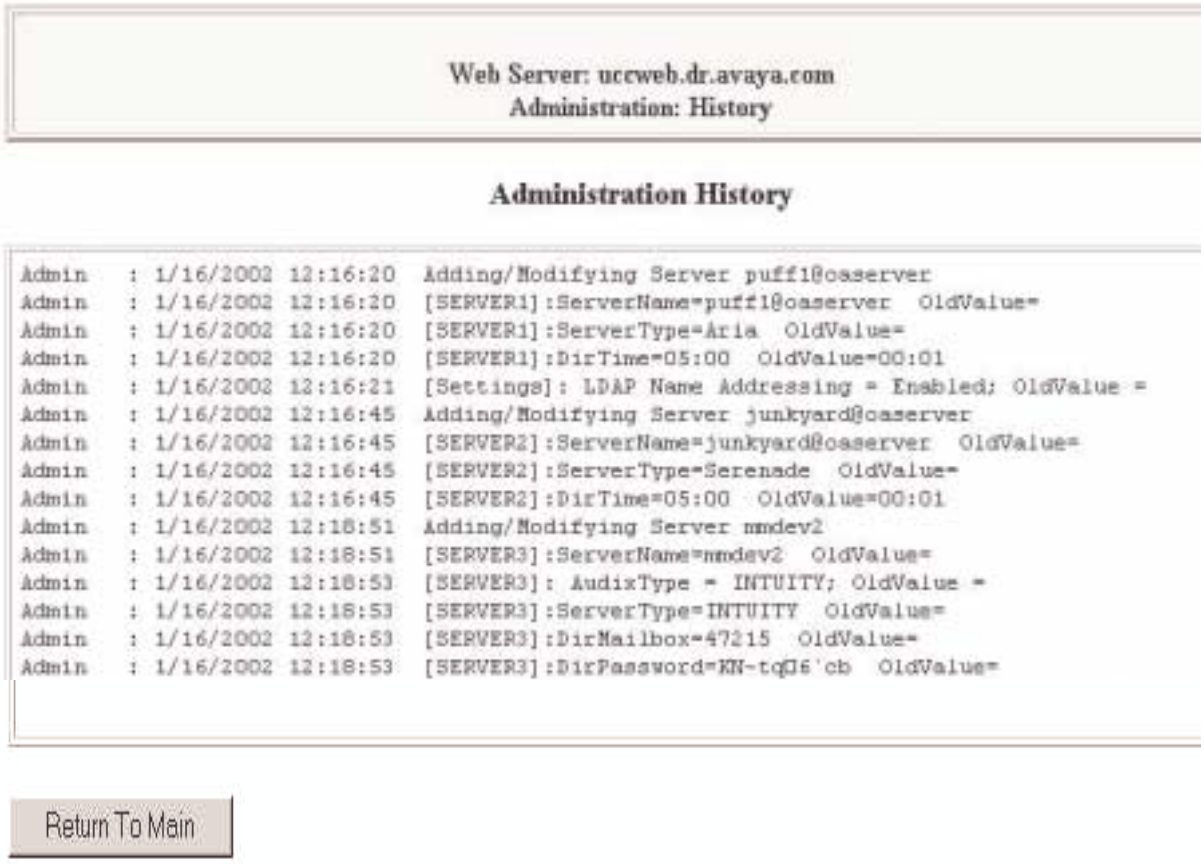
Administration History

The Administration History page, shown in Figure 10, records all logons, changes, and retrieval errors to the administration of Avaya Web Messaging, including configuration changes to the User List or Message Servers, failed logon attempts, and Names Directory retrieval errors. This Administration History page or log is primarily a service tool. The most recent information appears at the end of the log.

The History log shows the logon name, the date, the time and a description of the activity that took place.

Note: Two logon names can be shown in the Administration History log, **admin** and **services**. **Admin** denotes that the system administrator made the changes listed in the log. **Services** denotes that the changes were made by technical support.

Figure 10. Administration History Page



Change Password or Logon ID

The Avaya Web Messaging Administration & Maintenance page is password protected. The default password for admin logon is admin1. This password should be changed. You can also change your logon ID.

Only one Administrator password and one Services password are allowed. The maximum number of characters in the password is 10. There is no expiration date for the password.

Schedule Maintenance

You can schedule maintenance activities according to your needs. The default settings assume you want to run various tests and monitor Avaya Web Messaging. However, you can turn off the tests. The purpose of each of the tests is explained below.

CPU Availability	The CPU is constantly being monitored. You can set the number of times for the system to reboot.
IIS Test	If users are unable to access the Web pages for Avaya Web Messaging, you can schedule the Internet Information Server (IIS) test to detect problems.
Connectivity	Use the Connectivity test to verify that a connection exists between the Web server and the message servers. You can test the connectivity either for a specific message server or for all message servers. The Connectivity test is automatically run every 15 minutes. Errors are written to the Windows 2000 Event log. For some message servers, if errors and alarming are configured, an alarm is triggered on the message server
IVY	The Install Verify Test verifies and diagnoses Avaya Web Messaging installation problems. The Install Verification test can be run either from the Administration & Maintenance tools page or from the desktop. Both tests produce the same report. However, running the test from the Tools page gives you additional commands. You can save and print the report, change the filter for viewing data, and create different baselines for comparisons.
Periodic Windows 2000 Reboot	Microsoft recommends that you reboot the Windows 2000 server periodically to clear memory.

Maintenance

The maintenance links available for Avaya Web Messaging service are as follows:

- **Tools.** Four tools are available: connectivity test, ping test, trusted server alarming verification, and Avaya Web Messaging file version check. Information about each tool is explained in greater detail in the Tools section that follows.
- **Web Server Control**. End-user logon to Avaya Web Messaging can be blocked and unblocked. You can block logons for days, hours, and minutes. You can also reset the Web server from the Web Server Control page.
- **Services Log.** This link can be used to keep notes or to document information that you would like to

store. The information is stored in a text file that can be printed. The service log file name is wmService.log.

- **License File Information**. When INTUITY AUDIX message servers are configured, the number of licensed seats purchased for the INTUITY AUDIX is displayed.

Note: Some of the maintenance tools can be accessed from the Start>Programs> Avaya Web Messaging Tools as well as from the Administration Web pages.

Tools

The Maintenance Tools page is used to diagnose and troubleshoot Avaya Web Messaging problems. The four available tools are described in this section.

Connectivity Test

The Connectivity Test allows you to verify that there is a connection between the Web server and the message servers. You can either test the connectivity for a specific message server or to all message servers that are configured.

Note: The Connectivity Test is not intended to be used to locate intermittent network errors. If repeatedly executing this test produces different results, intermittent network problems could be the cause.

The Connectivity Test automatically verifies the following:

- Name and IP address of the Web server on which Avaya Web Messaging resides, as well as the connection to each of the message servers. For the Octel message servers, it also checks the connection to the OctelAccess Server.
- Configuration of the Web server for network access.
- IIS is running on the Web server.

The Connectivity test can be run either from the Administration & Maintenance pages or from the desktop. See the Maintenance section for information about available desktop tools.

To run the Connectivity test:

- From the Connectivity Test page, select a specific message server or All Servers from the list and click

Run Test. The details about the test are displayed in a box on this page.

Ping Test

The ping test is used to test connections from the Web server to the client's computer.

To run the ping test:

- From the Ping Test page, enter the IP address or computer name in the box and click **Run Test**.

  The test results are displayed in a box on the Ping Test page.

INTUITY Trusted Server Alarming

As an option, you can configure an alarming notification from Avaya Web Messaging to an INTUITY AUDIX server. You can configure the Web server used for Avaya Web Messaging as a Trusted Server.The INTUITY Trusted Server alarm tool can test that the Trusted Server is correctly configured for alarming notification.

Note: Trusted Server alarming is only used for Avaya Web Messaging with INTUITY AUDIX message servers. If no servers appear on the server list page, no INTUITY AUDIX servers are configured for alarming.

To test the trusted server:

1. From the **Message Server** box, select the INTUITY AUDIX message server to be tested.
2. Click **Trigger Alarm**. An alarm is sent to the message server.
3. Verify that an alarm was raised on the message server you selected.
4. Click **Clear Alarm** to clear the alarm from the INTUITY AUDIX message server.

Verify Installation

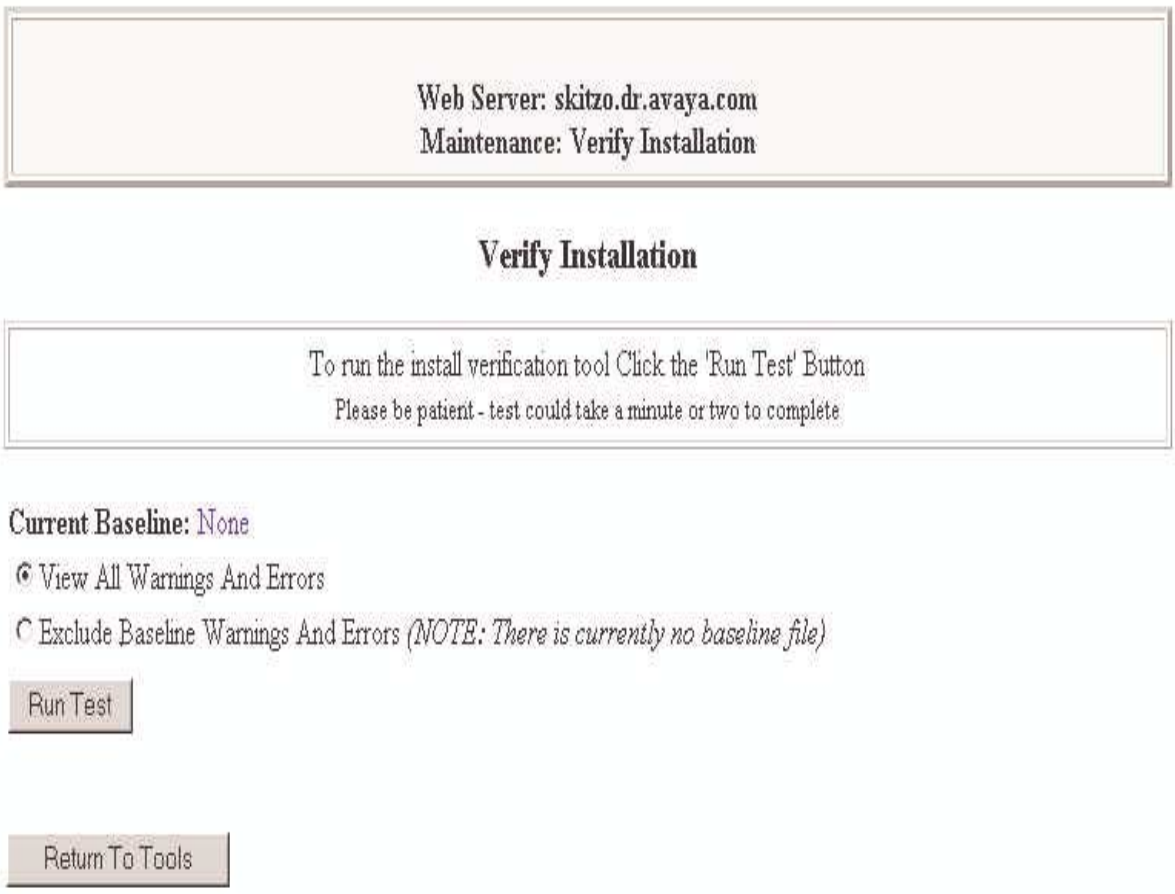
This test verifies that the correct files are installed on the Web server. The Verify Installation tool automatically compares the installed file list database against the current file list and flags differences such as size, date and version. Files that are missing or out of date can be identified.

The first time you verify the installation, you can establish a baseline. The baseline records the current warnings and errors. When you run the test after the baseline has been established, you can select not to show the errors and warnings recorded in the baseline. In this case, only the

new warnings and errors since the baseline was generated are displayed.

The report shows warnings in yellow and errors in red. In the example shown in Figure 11, a warning is displayed about the size of the file. In the size column, the number at the top, 22288, is the size expected, and the number at the bottom, 6144, is the actual size of the file.

Figure 11. Verify Installation Page



Web Server Control

The Web Server Control page, shown in Figure 12, is used to manage a graceful shutdown of Avaya Web Messaging when you perform an upgrade of the software or maintenance of the Web server and to reset Avaya Web Messaging.

From this page you can:

- Block new logons for a specific duration of time, days, hours, or minutes. When you block logons, users cannot logon to Avaya Web Messaging, but users who are currently logged on can still access their messages. Because this is a browser-based application, you cannot notify users through the web before you block logons or reset the Web server.
- Reset Avaya Web Messaging. All clients' sessions are immediately stopped, and the Internet Information Server (IIS) is stopped and immediately restarted. Because IIS is restarted, you are logged out of the Administration & Maintenance pages.

Figure 12. Web Server Control Page

To block new logons and reset the Web server

1. Enter the days, hours, or minutes during which you want to stop users from logging on to Avaya Web Messaging.
2. Click **Block Logins**.

   No new logons are allowed.
3. To reset the Web server, click **Reset Web Server**.

   An Information notice appears, verifying that you want to reset the Web server.
4. Click **OK**.

   The Web server is taken out of service. The Web server restarts automatically.

   Note: All users who are logged on are automatically logged off Avaya Web Messaging. Because you cannot notify all users automatically, you might want to schedule resetting the Web server when user logon is low. Check the User List to determine how many users are logged on to Avaya Web Messaging.
5. If the configured logon block time has not expired, after the Web server has restarted, log again on to the Maintenance and Administrator pages and go to the Web Server Control page.
6. Click **Clear Blocking** to allow users to log on to Avaya Web Messaging.

Service Log

The Service Log page is available for the administrator and technical support to enter information about service, maintenance or general operational notes. This information is displayed in the wmservices.log file with data and time and cannot be deleted from the Web page.

System Usage

The System Usage pages show performance statistics over periods of specific time. By using the information that is

available from these pages, you can determine logon patterns and usage.

Three types of system statistics are available:

- **Login Statistics**. Displays the number of user logons over a 24-hour period.
- **Data Transfer Statistics**. Displays statistics about what type of message components (voice, fax, text, or attachments) are sent while logged on to Avaya Web Messaging.
- **Message Event Statistics**. Displays statistics about how users use Avaya Web Messaging to send and receive messages.

Each of the pages allows you to change your viewing parameters. The common parameters that can be configured on each system usage page are as follows:

- View the data in a graph or in a table
- Select from which time frame the statistics should be shown

Each page also can be modified to select specific statistical information types. After you have selected how the statistical information should be viewed, click **Display Data** to display the information.

Login Statistics

The Login Statistics page, shown in Figure 13, displays the number of users that logged on at each hour of the day. This information shows usage trends. When you open this page, the graph that is displayed is for the current day and time. You can view logon statistics for the last 30 days.

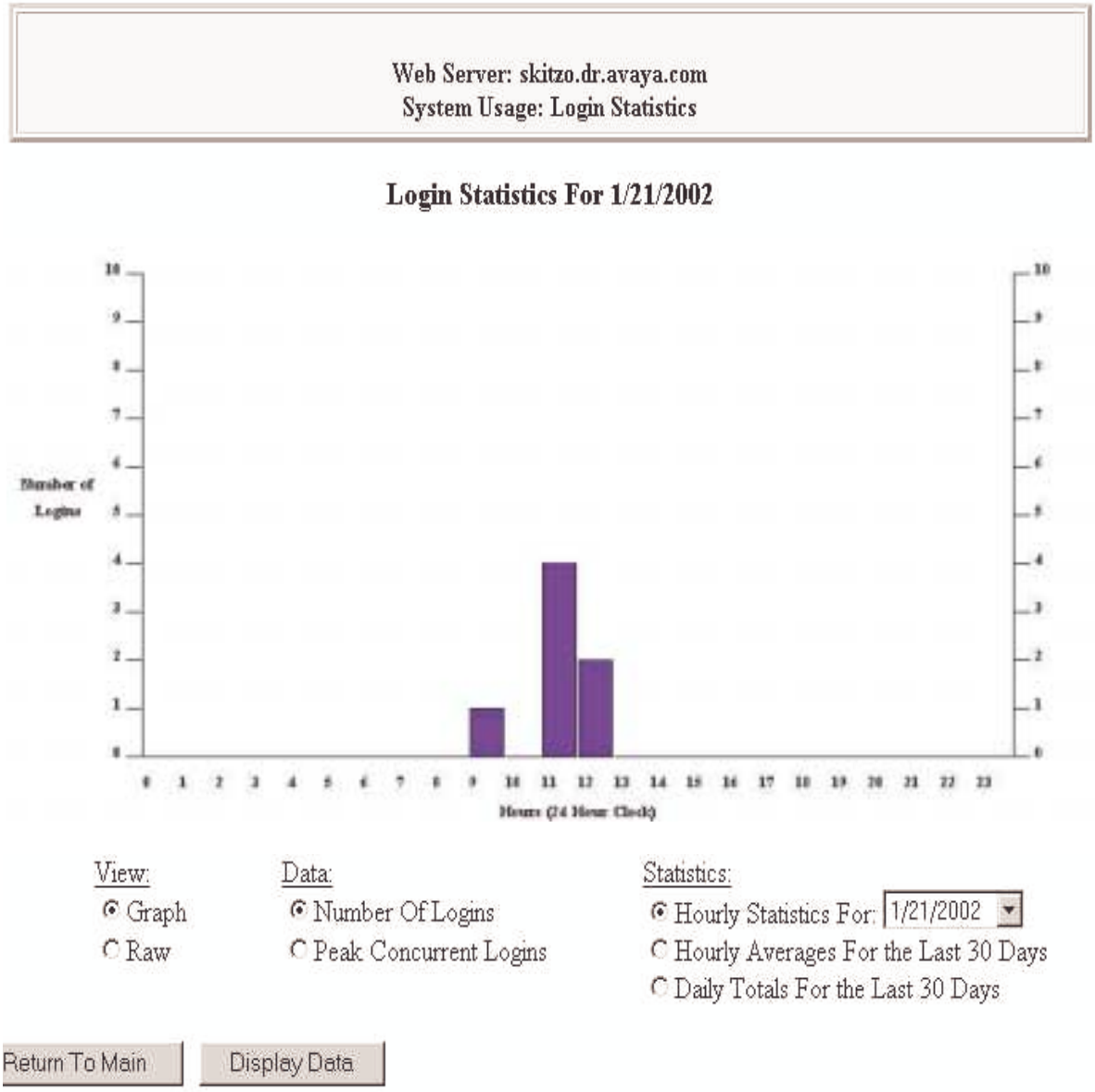
The statistics can show either the number of logons or the number of people logged on simultaneously (peak concurrent logons). The information can be displayed as

- Hourly logons for a specific day within the last 30
- Hourly averages for the last 30 days
- Daily totals for the last 30 days.

You can choose to view the information as raw data. The statistics are displayed in a table format. The figure that

follows is the default page that shows the number of users logged on for the current day.

Figure 13. Login Statistics Page



Data Transfer Statistics

The Data Transfer Statistics page, shown in Figure 14, displays statistics about how Avaya Web Messaging is used to send and receive messages. When you open this page, the graph that is displayed shows the number of voice messages that have been downloaded for the current day. You can view data transfer statistics for the last 30 days.

The data can be configured to show statistics about the following:

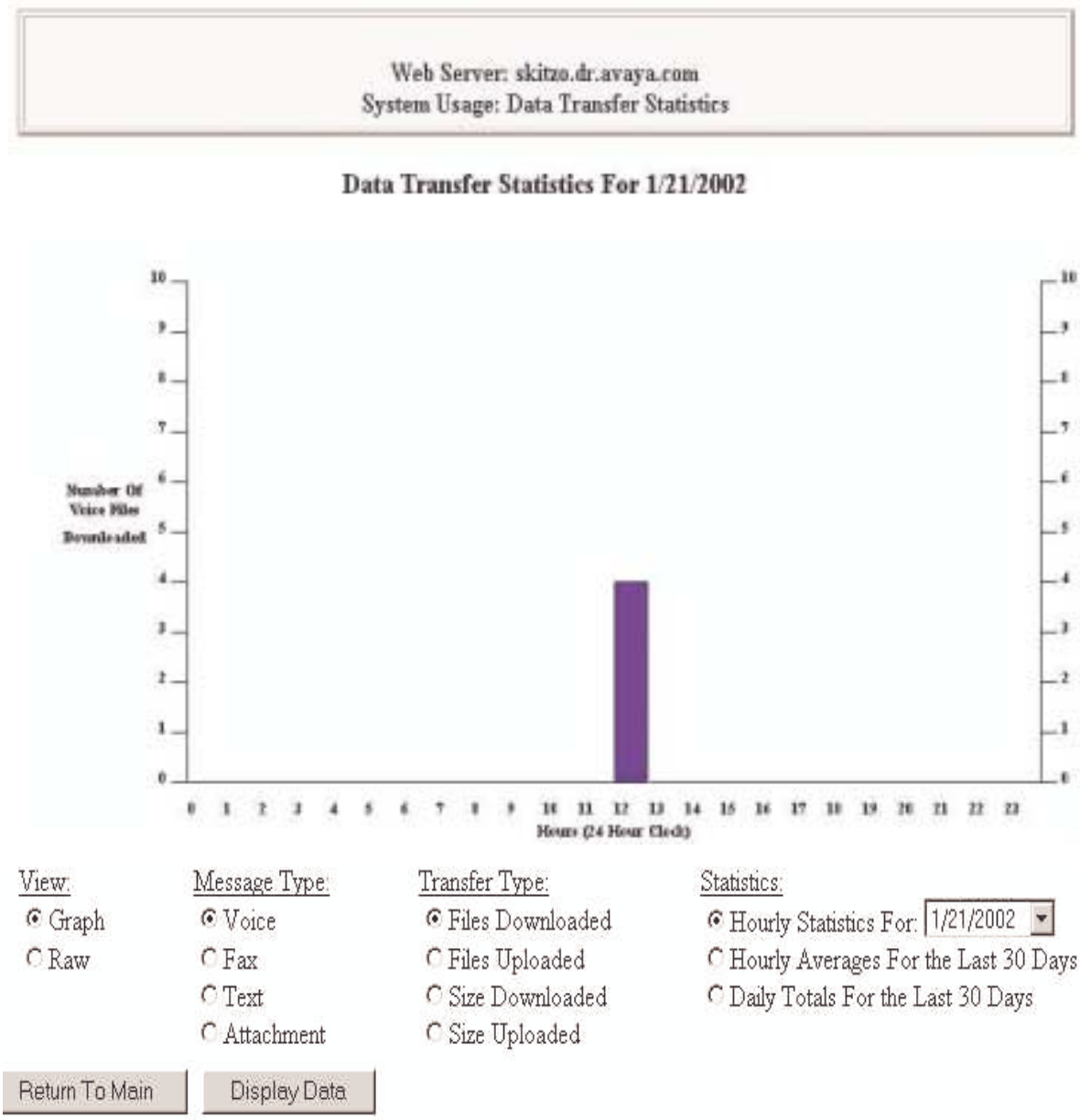
- **Message type**. Statistics for voice, fax, text messages, or message attachments can be displayed. Text messages and message attachments are available for INTUTIY AUDIX message servers.
- **Transfer Type**. For each message type statistics can be displayed about the number of files download or uploaded, or the size of the data uploaded or downloaded.

For each message type and transfer type selected, the following information can be displayed:

- Hourly statistics for a specific day within the last 30 days
- Hourly averages for the last 30 days
- Daily totals for the last 30 days.

You can choose to view the information as raw data. The statistics are displayed in a table format.

Figure 14. Data Transfer Statistics Page



Message Event Statistics

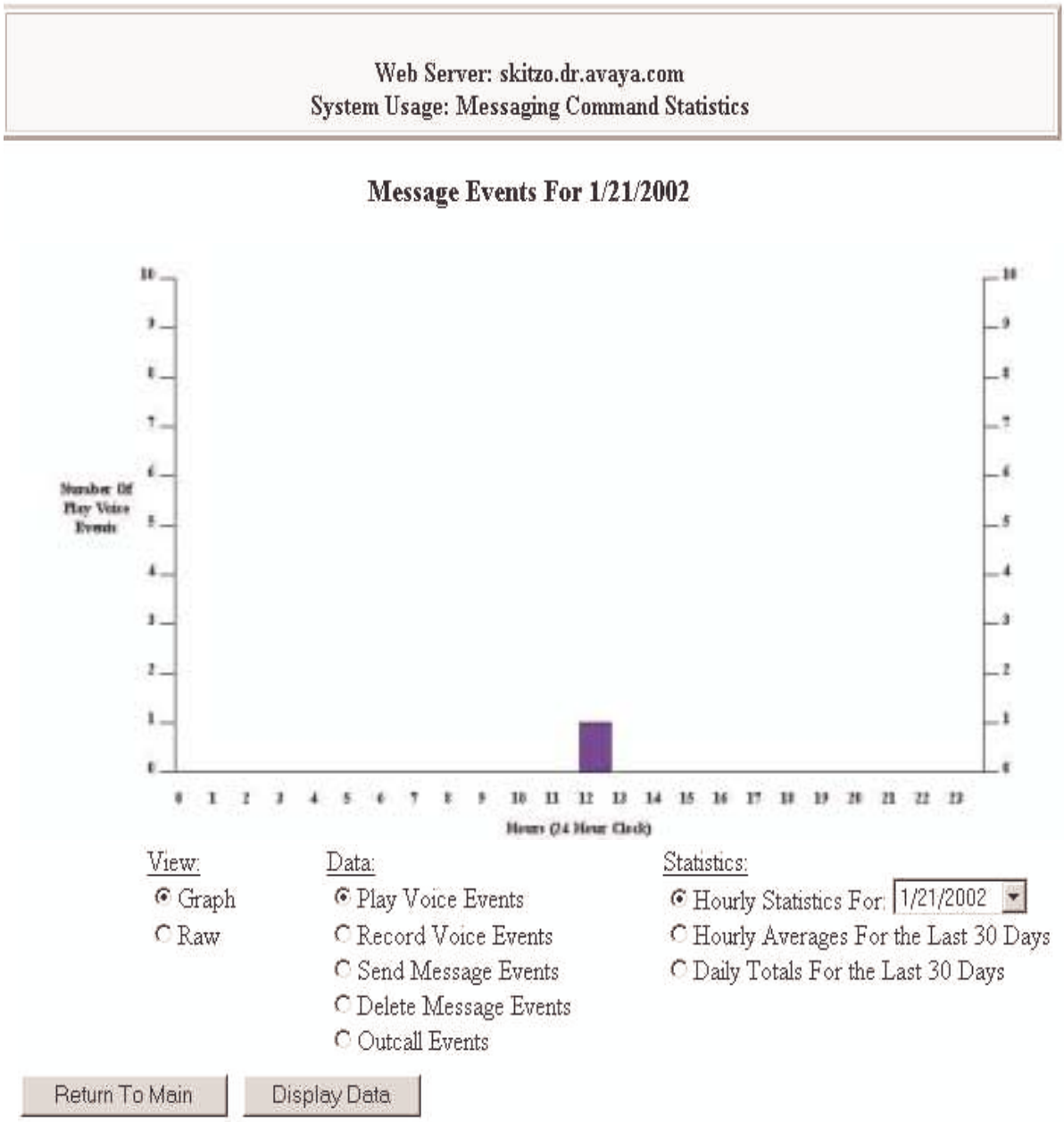
The Message Events page, shown in Figure 15, displays statistics about how Avaya Web Messaging users use the messaging features, play, record, send, and delete, from Avaya Web Messaging. When you open this page, the graph that is displayed is for the number of voice message played for the current day and time. You can view statistics for the last 30 days.

Data for the following events can be displayed:

- Messages played
- Messages recorded
- Messages sent
- Messages deleted
- Outcalls placed for the telephone

You can choose to view the information as raw data. The statistics are displayed in a table format.

Figure 15. Message Event Statistics Page



UCC Avaya Web Messaging Maintenance Tools

In addition to the maintenance tools available from the Administration & Maintenance pages, other maintenance tools are available on a Windows 2000 platform from:

Start > Programs > Avaya Web Messaging Tools

The tools can be used to:

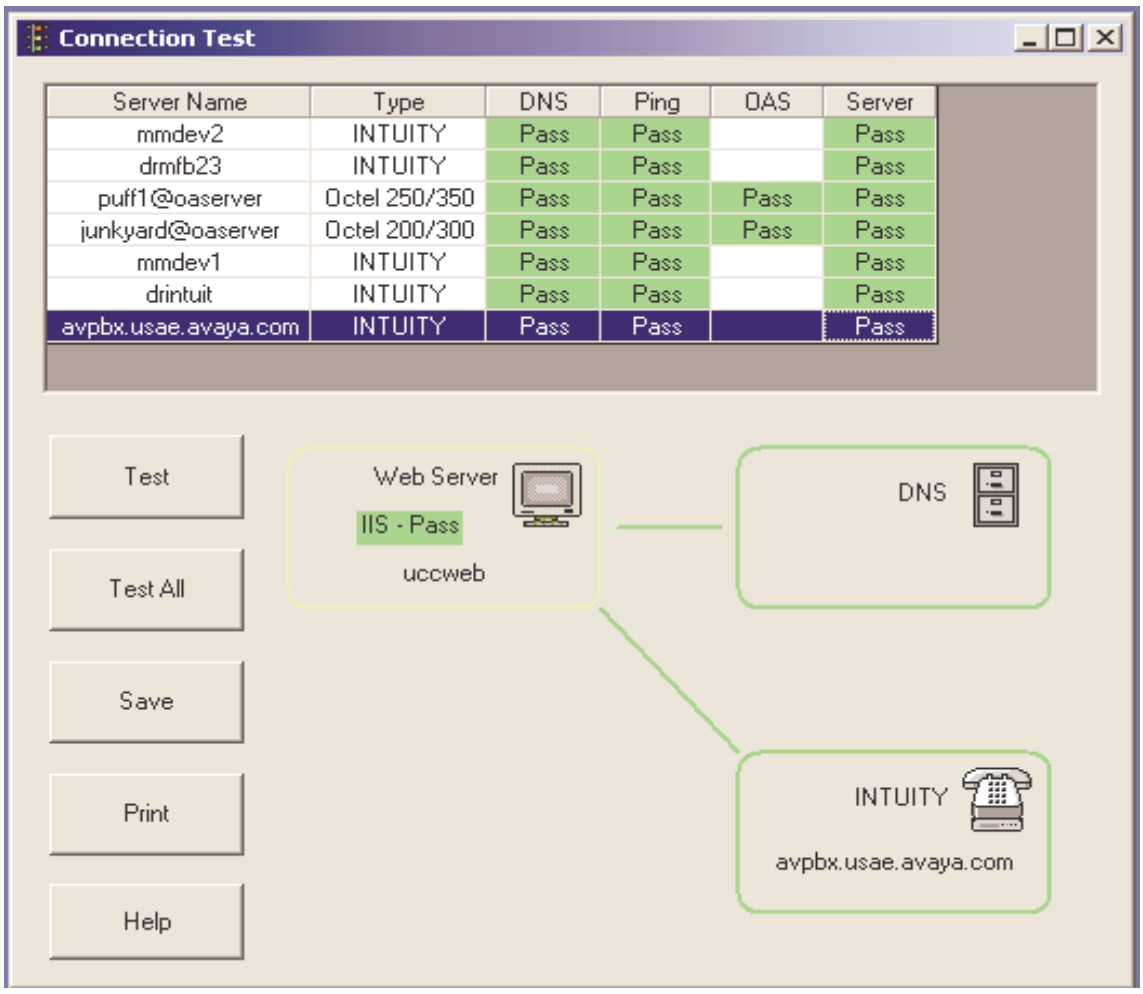
- Run the Connectivity Test.
- Run the Install Verify Test (IVY.)
- Reset the Web server.
- Start and stop the Web server.
- Run the Trace Viewer.

Connectivity Test

The Connectivity test can be run either from the Administration and Maintenance Pages or from the desktop. When you run the Connectivity test from the desktop, you view the connection test. See Figure 16.

Use the Connectivity test to verify that there is a connection between the Web server and the message servers. You can test the connectivity either for a specific message server or for all message servers. The Connectivity test is automatically run every 15 minutes. Errors are written to the Windows 2000 Event log. For INTUITY AUDIX message servers, if there are errors and alarming is configured, an alarm is triggered on the message server.

Figure 16. Connectivity Test Window



To run the Connectivity test from the desktop:

1. Use this path:

   Start>Programs>Avaya Web Messaging Tools.

2. Select **Connectivity Test**.

   The Connection Test dialog box appears with a list of all the message servers.

3. Do one of the following:

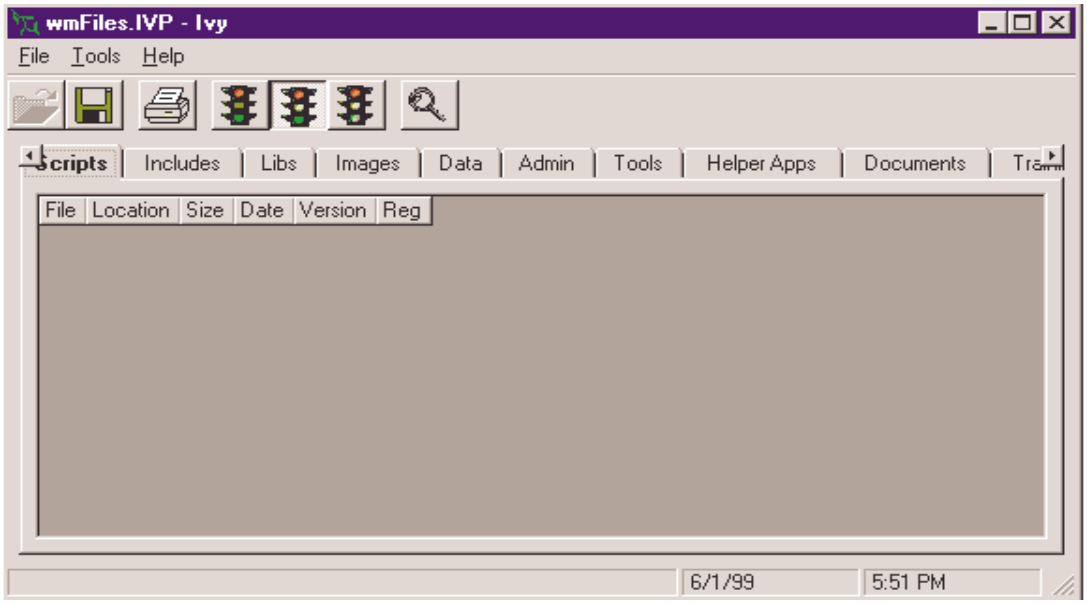
   - To test only one server, select the server name from the table that is displayed and click **Test**.
   - To test all the message servers configured for Avaya Web Messaging, click **Test All**.

The connectivity diagram appears. The test is automatically executed and displays the name and IP address of the Avaya Web Messaging server, as well as the name and IP address of the message server. The test verifies that the Web server is configured for network access and that IIS is running.

Install Verify Test

The Install Verify Test (IVY) is used to verify and diagnose Avaya Web Messaging installation problems. The Install Verification page from the Administration and Maintenance pages shows the same IVY report as that run from this tool. Using the IVY window (see Figure 17) from Avaya Web Messaging Tools gives you additional commands. You can save and print the report, change the filter for viewing data, and create different baselines for comparisons.

Figure 17. Install Verify Test Window



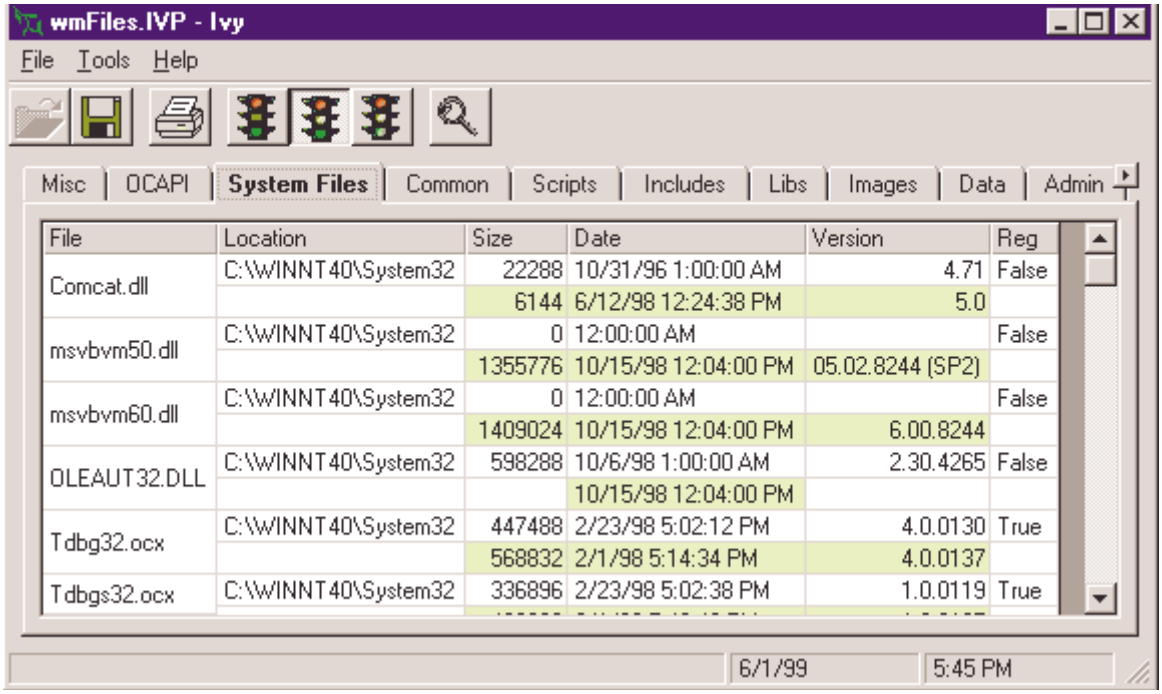
When you open IVY, it starts automatically, and the Install Verify Window appears. Each Avaya Web Messaging file is checked against the database. The status bar displays each file name as it is being checked. When the check is complete, the window displays a row of tabs. If the tab selected does not show any errors or warnings, the fields are empty, as in Figure 17.

The default is to create a report that shows only the errors and warnings. You can change the information you want to see by changing the stoplights on the toolbar. Red shows

only errors, yellow is the default that shows both errors and warning, and green shows all files.

IVY is used with various applications. Thus, the actual number of tabs and the names of the categories change depending on the application being tested. The categories have been created so that similar files could be grouped together. If a tab that shows errors or warnings is selected, the information is displayed. See Figure 18 for an example of such displayed information.

Figure 18. Installation Verification Test Results



Each file is checked for file name, location, size, date and version, and Registry entry. Errors appear against a red background, and warnings against a yellow background. The information contained in the IVY database is displayed on the first line for each file, and the information found on the Web server is displayed on the second line. Only information that is different between these two databases is displayed. A blank column on the second line indicates that the information matches.

You can create a baseline of the IVY report either from the Tools menu or from the magnifying glass icon on the tool bar. A baseline file contains information about the IVY database and system differences at the time the baseline was created.

When you review a report, you might notice some differences that do not represent an error or warning. For example, a newer version of a system file present on the server is usually not replaced with an older file, but the difference is displayed in the IVY report. When you set the baseline, you can exclude the differences from future IVY reports.

The baseline file is not used automatically when IVY creates a report. To view the differences from the IVY report and the baseline, click **Compare to Baseline** from the Tools menu. A new report is displayed that shows only the errors and warnings that are not in the Baseline file.

Note: Errors are logged to the Windows 2000 event log. For INTUITY AUDIX message servers, errors also trigger INTUITY alarming. When you create a baseline, any errors that exist at the time the baseline is created are not viewed as new errors. Thus, they are not logged to the Windows 2000 event log and they do not trigger an INTUITY alarm.

You can save and print the IVY reports. The file is a plain ASCII file that can be sent by e-mail. These reports are useful when relaying problems to your technical support center.

Reset Server

You can reset the Web server from either the Administration & Maintenance Pages, or from the desktop. Reset Server stops and automatically restarts the Web server. When the Web server is reset, all user logons are lost.

Starting and Stopping the Web Server

From the desktop, you can stop and start the Web server. A screen displays the process.

You can block user logons from the Administration and Maintenance pages before you stop the Web server. See Restricting User Access in UCC Avaya Web Messaging Administration & Maintenance

Trace Viewer

Trace Viewer opens the Trace Manager Utility that is used as a diagnostic tool for troubleshooting. Trace Manager is used with various Octel applications. Each application can be configured individually with its own trace levels and categories. See Table 4. for a list of the trace categories available for Avaya Web Messaging.

Table 4. Avaya Web Messaging Trace Categories

Category / Abbreviation	Event Description
Comp int	Internal to component. For Octel message servers, this is the.dll file that "talks" to the OctelAccess Server. For INTUITY AUDIX message servers, this is the.dll file that "talks" to the Audix.
APIwrapper	Engineering-level tracing for the API wrapper common to OCAPI and IMAPI.
OCAPI int	Sending of packets between the Avaya Web Messaging Web server and the OctelAccess server.
IMAPI Int	Sending of packets between the Avaya Web Messaging Web server and the IMAPI client.
Debug 1	Engineering-level traces that are useful when you are debugging Avaya Web Messaging.
Debug 2	Engineering-level traces useful when you are debugging Avaya Web Messaging.

Refer to Trace Manager for more information.

Trace Manager

Use the Trace Manager diagnostic utility to collect, filter, and view trace activities, and to export trace files to create custom reports. This utility is used with various Avaya applications. Any application can be configured individually with its own trace levels and categories. Trace Manager is installed automatically when you install your application.

Use Trace Manager to perform the following tasks:

- Set default trace levels for different applications.
- Change existing trace levels for data collection.
- Configure the file for collecting trace events.
- View both *active trace* (real-time) events and *off-line* (historical) events.
- Export off-line trace events to a text file.
- Back up existing trace files.

Starting Trace Manager

Trace Manager is started from the server. Separate trace-event databases are maintained for each environment. The traces you collect and view depend upon the environment from which Trace Manager is launched.

Before starting Trace Manager, make sure you know the name of the computer for which you want to view traces.

1. To start Avaya Web Messaging application traces, click the **Start** button on the desktop taskbar. Then click **Avaya Web Messaging—>Trace Viewer**.

2. When you start Trace Manager from the OctelAccess server you see the Select Computer dialog box.

3. The computer you are using (local computer) is highlighted. Click **OK** or **Cancel** to manage traces on the local computer. Or, if you want Trace Manager to access trace logs on a remote machine, select from the list a network computer to which you have access; then click **OK**.

   The Open New Trace Window appears.

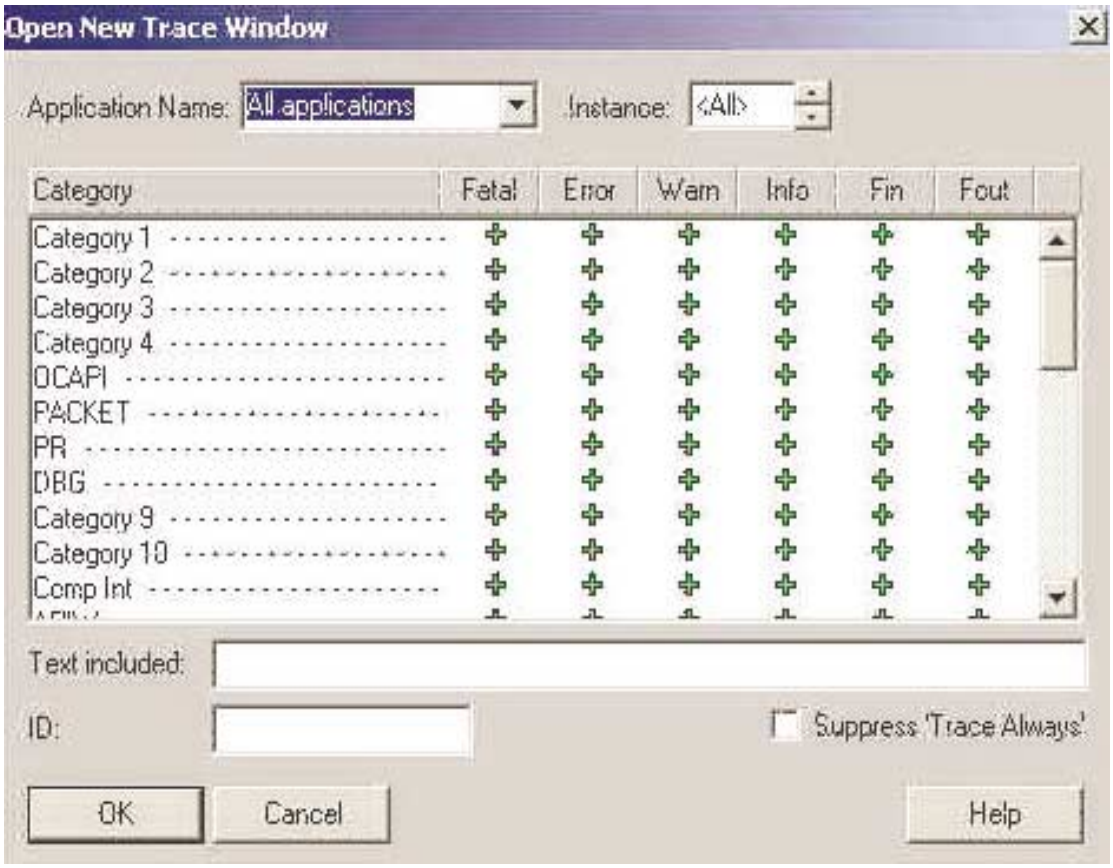
The following Setting Up a New Trace section describes using the Open New Trace Window to define the view for a new trace.

Setting Up a New Trace

Use the Open New Trace Window dialog box (see Figure 19) to define which of the collected traces to display in a new *active view* window. An active view displays trace events *as they occur* in the selected application (in real time). The Open New Trace Window appears whenever you activate Trace Manager (see Starting Trace Manager). It also appears when you select **New Window** from the Trace menu.

Note: Trace Manager also provides an *off-line* view that displays the historical trace events saved to the trace files. See Viewing a Trace for more information.

Figure 19. Open New Trace Window



The Open New Trace Window dialog box displays all of the trace categories available for the current Trace Manager environment. See Trace Categories for a description of the Avaya Web Messaging categories for which Trace Manager collects data.

From the Open New Trace Window dialog box, you can limit the information you see in an active view to a specific combination of applications, instances, and severity levels. You can further limit the view by matching specific text, or a specific session ID. By default, all severity levels are displayed for all categories in all applications.

Important: Traces selected in the Open New Trace Window affect only what you see in the view window. Your selections have no affect on what is collected into "raw" trace files. To change the types of traces being collected for a running application, use the Change Current option from the Trace menu. To change the types of default traces collected for an entire database, use the Set Default option from the Trace menu. See Modifying the Trace Log for more information.

Select Application

Use the Application Name field in the Open New Trace Window dialog box to select the running application for which you want to view traces. Click the down arrow, then select the application from the drop-down list. If the application for which you want to view traces is not on the list, verity that the application has been launched.

Select Instance

Use the Instance field in the Open New Trace Window dialog box to select the instance of the running application for which you want to view traces. Click the down arrow, then select the instance number from the drop-down list.

Match Specific Text

Use the Text included field in the Open New Trace Window to limit the view for the events displayed in an active window. Only trace events that contain the specified text string will be shown in the view. Multiple words are permitted, and matching is not case sensitive.

Match ID

The IDs are relevant only to your support representative, and refer to processes for applications currently running more than one instance. Specify an ID for categories other than App-Level traces only if told to do so by your support representative.

Suppress Trace Always

Normally Trace Always entries are always displayed in the Trace Log. As a debugging tool, the Suppress Trace Always function hides Trace Always entries in the Trace Log. This makes it easier to find a particular occurrence of a different type of log entry. The Trace Always entries are identified by a red pushpin at the left of the entry row.

Select Severity Levels

In the Open New Trace Window dialog box you can set or clear, by category, the severity levels to view in an active trace window. Fatal severity levels are the exception; they cannot be disabled. See Trace Categories for a description of the event activity reported by each category. See Table 6. for a description of the data logged for each severity level.

Viewing a Trace

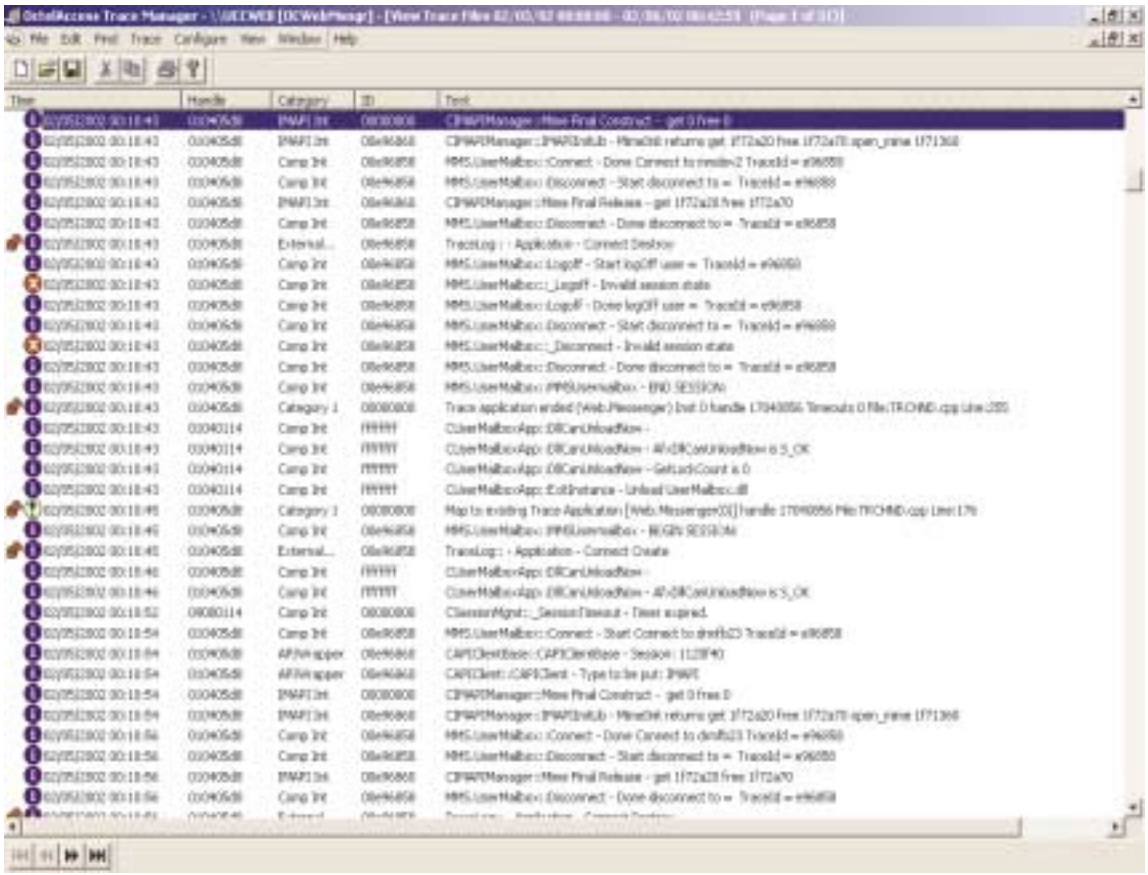
With Trace Manager, you view data in one of two ways

- **Active view**, which displays trace events as they occur in real time, *or*
- **Off-line view**, which displays the historical trace events saved to the trace files.

In both cases, the events you see depend upon how Trace Manager was set to collect traces at the time trace services were launched (see Change Trace File Criteria). However, you can use the **Change Current** option from the Trace menu to change the data being collected for *running* applications.

Use the Open New Trace Window to define the active view for a new trace (see Setting Up a New Trace). Several active trace windows can be open at one time — for different applications or for different views of the same application. Severity levels can be set individually for each active view. The Active window, shown here in Figure 20, shows an active view that traces all applications.

Figure 20. Active Window



The trace events and icons shown in an Active window (also in an off-line View Trace Files window) depend upon how severity levels are set for the trace categories (see Trace Severity Levels). The following information is provided for each trace event:

- Time — Date and time of the trace event
- Handle — The Windows 2000 handle ID assigned to the application instance being traced.
- Category — Type of activity being reported
- ID — Session identifier. The IDs are relevant only to your support representative, and refer to processes for applications currently running more than one instance.
- Text: — Description of the reported event.

Note: For the OCAPI category, see the Trace Manager Help, "Error Messages," for more information about the event.

To arrange active trace windows, click **Cascade** on the Window menu to *stack* the windows, or click **Tile** to view the windows concurrently.

Off-Line View

To view historical (off-line) traces, you can do one of the following:

- View the trace in the current Trace Manager session, *or*
- Export the trace to a specified file for later viewing.

Use the **Trace Manager File** menu for both options.

Off-line views provide the same information as active views. However, only the off-line views selected from within Trace Manager display severity-level icons and column headings. Exported off-line views take on the characteristics of the file type you define for the view.

To view off-line traces within Trace Manager

1. From the File menu, click **View Trace Files**.
2. From the View Trace File Options dialog box, select the time range (**General** tab), severity levels (**Levels** tab), and location (**From** tab) for the trace you want to view.
3. Click **OK** to load the View Trace Files window for the specified trace.

The View Trace Files window provides the same information as the Active window, but for a historical trace.

Note: See the Trace Manager online Help for detailed information about using the View Trace Files option.

To view an off-line trace outside of Trace Manager

1. From the File menu, click **Export Trace Files** to display the Export Trace Files dialog box.
2. At the **Export To** tab, enter a name for the file to which you want to export trace events. The Export feature creates ASCII text files (for viewing with Notepad, for example); so you'll need to use a

compatible file extension (such as**.txt**) when you specify a file name.

3. Click  to select the location to which you want to export the trace.
4. Select the time range (General tab), severity levels (Levels tab), and location (From tab) of the trace you want to view.
5. Click **OK** to export the selected trace to the specified location.
6. Use Explorer (or the appropriate application) to open and view the collected off-line trace.

Trace Categories

Categories are specific types of activities within an Octel server application that correspond to the various application modules within those environments. The applications, categories, and severity levels for which traces are collected are determined by the default trace settings that are in place when trace services are launched (see Change Default Settings). However, the Change Current option on the Trace menu allows you to change the categories and Trace Severity Levels (see Trace Severity Levels) for applications that are currently running. Whenever you launch Trace Manager or open a new trace window, you can select the severity levels to view for the trace categories being collected (see Setting Up a New Trace).

The Avaya Web Messaging trace categories that are displayed are shown in Table 5..

Table 5. Avaya Web Messaging Trace Categories

Category (Abbreviation)	Event Description
Comp int	Internal to component. For Octel message servers this is the.dll that talks to the OctelAccess Server. For INTUITY AUDIX message servers this is the.dll that talks to the Audix.
APIwrapper	Engineering-level tracing for the API wrapper common to OCAPI and IMAPI.
OCAPI int	Sending of packets between the Avaya Web Messaging Web server and the OctelAccess server.
IMAPI Int	Sending of packets between the Avaya Web Messaging Web server and the IMAPI client.
Debug 1	Engineering-level traces useful when debugging Avaya Web Messaging application.
Debug 2	Engineering-level traces useful when debugging Avaya Web Messaging application.

Trace Severity Levels

Trace Categories (see Trace Categories) are logged according to defined levels of severity. When Trace Manager is initially installed, all Fatal, Error, and Warning severity levels are turned *on* for all categories, and trace events for these levels are collected into the trace files. The Set Default option on the Trace menu allows you to specify the severity levels to collect whenever trace services are launched (only Fatal severity levels cannot be turned off). The Change Current option on the Trace menu allows you to change the trace events being collected for applications that are currently running (does not affect the default settings).

Whenever you launch Trace Manager or open a new trace window, you can select the severity levels to view for all categories for which traces are collected. The Trace Severity Levels table (see Table 6.) shows the severity-level icons used in an Active or View Trace Files window, and describes the type of information logged for each level.

We recommend using only Fatal, Warning and Error severity levels for "normal" (non-debug) application tracing. Turn on the Information severity level for debug-level traces. Do not use the Fin and Fout severity levels unless told to do so by your support representative. Fin/Fout are used only for troubleshooting purposes, and can adversely affect system performance.

Caution: Debug levels create a large amount of trace collection. The debug trace process can affect system performance, and can also cause the active viewer to omit blocks of trace information. Use the Export Trace Files or View Trace Files options on the File menu to view offline debug-level traces.

Caution: Setting the Fout level for some categories can cause an accumulation of large amounts of data, since the full binary image of all file transfers are traced. System performance is severely affected when Fout is set for these categories. ***Do not set*** Fout levels for these categories unless you are told to do so by your support representative.

Table 6. Trace Severity Levels

Icon	Level	Description
	Fatal	Shows that the server or the application is no longer running correctly. For each category, the Fatal level is set *on* by default, and cannot be turned *off*.
	Error	Indicates a significant problem that could lead to a fatal event. For example, bad commands and parameters are logged to Error events. If this level is set, all errors are logged for events that occur in the selected category when the application is running.
	Warning	Displays activity that could present a problem to the server or to an application. Often, user-input errors (such as an incorrect password) result in Warnings. If this level is set, warnings are traced for events that occur in the selected category when the application is running.

Table 6. Trace Severity Levels

Icon	Level	Description
	Information	Provides general details about the operation of the server or application. If this level is set, all information messages that occur in the selected category are traced. If Information levels are logged, the trace files can become large very quickly.
	Fin	Provides debug-level information for engineering use only. This level should always be *off*.
	Fout	Provides deep debug-level information for engineering use only. This level should always be *off*.
	(Applies to all levels)	Indicates a trace event that is always logged, regardless of how the severity levels are set.

In addition to the severity levels described, special information-level events are always logged. These events typically provide information about the status at the initial start up.

Modifying the Trace Log

You can modify the traces to be collected several ways:

- *Change the trace file criteria* for the number, size, and path of the files used to store information.
- *Change the category names* to names more meaningful to your applications.
- *Change the default settings* for traces that are collected the next time trace services are launched.
- *Change the current settings for* traces being collected for currently-running applications.

To change trace file criteria for category names, use the Options menu. To change collection criteria, use the Trace menu.

Change Trace File Criteria

Default trace file settings are based upon the expected usage for a particular database environment. Change these defaults only if you require more file space for trace management functions, or if you want to save trace files to a location other than the **c:\temp** directory. Use this rule when configuring trace files:

Number of Files X **File Size** = **Size of Database**

Trace events are collected continuously. If you create a large number of files or make the file size large, you can compromise the disk space available for other activities. The default is 10 trace files at 10000 MB each.

To change default trace files settings,

1. From the Options menu, click **Files**. The Configuration dialog box appears.
2. If you want to change the default path where trace files are stored, enter a new path name in the Trace Files Path field. The default is **c:/temp**
3. In the Number of files field, enter the maximum number of trace files to create for the database.
4. In the File Size field, enter the maximum file size (in megabytes) for each trace file.
5. Click **OK** to save the settings.

Change Category Names

To more easily identify particular trace events, you may want to change the default names given to specific trace categories. To change the category names,

1. From the Options menu, click **Categories**. The Set Categories Names dialog box appears.
2. Click once to select the category name you want to change; then click again and type the new name.

3. Repeat step 2 for each category you want to rename. Click **OK** to save the changes.

Change Default Settings

Changes you make to the default trace settings do not go into effect immediately. Rather, these setting are initialized for trace collection the next time an application using trace services is launched.

1. From the Trace menu, click **Set Default**.
2. From the Set Default Levels dialog box, use the drop-down text boxes to select the applications for which you want to change trace data collection, or select All applications.
3. Define the new severity levels you want to collect. See Select Severity Levels for instructions on selecting severity levels.

Note: Clicking **Delete** while a particular application is selected causes the default severity settings for the selected application to be changed to the default settings defined for All applications.

Change Current Settings

Changes you make to the current trace settings affect only the traces being collected for currently-running applications.

1. From the Trace menu, click **Change Current**.
2. From the Change Current Levels dialog box, use the drop-down text boxes to select the running application and application instance (if applicable) for which you want to change trace data collection.

   Note: Select an instance to trace only if you want to reduce the amount of trace activity to view.

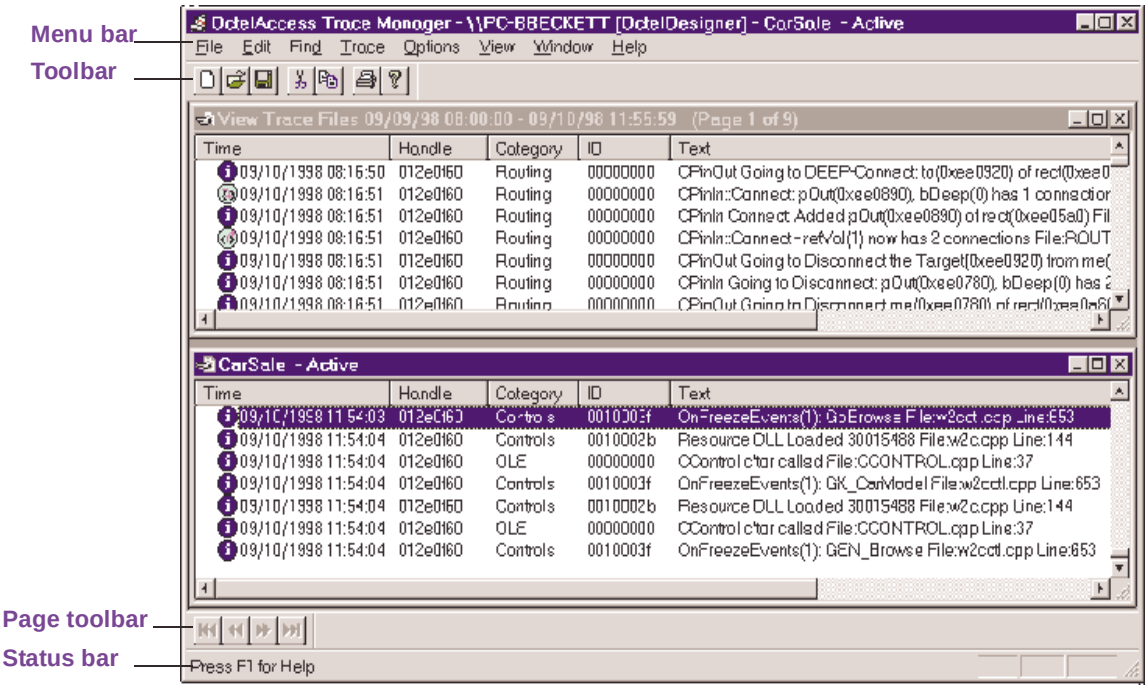
3. Define the new severity levels you want to collect. See Select Severity Levels for instructions on selecting severity levels.

Trace Manager Main Window

The Trace Manager main window appears when you start Trace Manager and select the computer for which you want to collect trace events.You can open Trace Manager main window, with two view windows open — one Active window and one View Trace Files (off-line) window. From the main window, you access the Trace Manager task menus that enable you to filter, view, save, print, back up, and export Trace Manager files.

You perform most trace management functions from the menu bar at the top of the window. Many functions are also available from the toolbar (click an icon to display its function). The Page toolbar enables you to move backward or forward in the selected view window (middle arrows), or to the beginning or ending page (left- and right-most arrows). Trace status is displayed in the status bar.

Figure 21. Trace Manager Main Menu



Trace Manager Menus

This table lists brief descriptions of the options available on each Trace Manager menu. Some of the options are described elsewhere in this section. See the Trace Manager online Help for detailed information about using all of the options.

Menu Name	Menu Selections	Function
File	Open	Open a saved (**.trc**) trace file.
	Close	Close the current window
	Save	Save the contents of the current window, and create a**.trc** file.
	Save As	Save the current window to another file name, and create a**.trc** file.
	View Trace Files	View specific off-line trace events (see Off-Line View)
	Export Trace Files	Export specific off-line events to a text file (see Off-Line View)
	Backup Trace Files	Back up trace files to a specific directory.
	Print	Print the contents of the current window.
	Print Preview	Preview how the file will print.
	Print Setup	Configure the printer.
Edit	Cut	Remove the selected lines from the view window, and copy them to the clipboard.
	Copy	Copy the selected lines from the view window to the clipboard.
	Clear	Clears all trace events from the current window.
Find	By Text	Find in the current view the next occurrence of the text entered
	By Level	Find in the current view the next occurrence of the selected severity level
	By ID	Find in the current vie the next occurrence of the selected event ID

Menu Name	Menu Selections	Function
	Find Next	Repeat the last search.
Trace	New Window	Open a new active trace window (see Setting Up a New Trace).
	Change Current	Change the traces that are collected the next time trace services are launched (see Change Current Settings).
	Set Default	Change the traces being collected for currently-running applications (see Change Default Settings).
	Stop	Stop trace events from displaying in the active trace window.
Options	Database Setup	Configure the location in which trace files are stored, and the number and size of the stored files (see Change Trace File Criteria.
	Category Names	Modify default category names (see Change Category Names).
View	Toolbar	Toggle toolbar view off and on.
	Status Bar	Toggle status bar view off and on
	Page Tool Bar	Toggle forward/back page arrows off and on.
Window	Cascade	Select a *stacked* window view.
	Tile	Select a concurrent window view.
	Arrange Icons	Arrange all minimized trace windows.
Help	Contents	Load Trace Manager online Help.
	About OctelAccess Trace Manager	View Trace Manager information.

UCC Avaya Web Messaging User Issues

This section is an overview of some of the issues users might encounter. See the Avaya Web Messaging Help for detailed How To... instructions and more information. An Avaya Web Messaging Quick Reference Guide is also available to give users an overview of Avaya Web Messaging features.

Avaya Voice Player, Avaya Voice Player Frequently Asked Questions, Fax Viewers, and File Associations issues are addressed in the following sections.

Avaya Voice Player

The Avaya Voice Player distributed by Avaya Inc. extends the Avaya Web Messaging capabilities by adding a voice component to messages. Users can play and record audio files through a computer sound card. See the Voice Player Help file for detailed information about how to use the player.

Users can log on to Avaya Web Messaging and download the voice player from these locations:

- **Main Page / Options / Audio Preferences**
- **Help / Download Avaya Voice Player**

Computer users must install the voice player from the computer desktop, and the computer must be equipped with a sound card and microphone so that the player can be used.

When users click **Download Avaya Voice Player**, instructions are displayed for doing the following:

- Downloading the voice player installation files
- Installing the voice player on the computer
- Checking the file association setup
- Completing the file association setup

You can print the voice player installation instructions from the Avaya Web Messaging User Help file.

The voice player works with your Netscape Navigator or Internet Explorer browser. When a browser encounters a sound file (with the.lvp extension), it hands off the data to the Avaya Voice Player (commonly called a "helper application") to play or display the file.

Separate voice players are available to run on Windows, Sun, and Apple Macintosh computers. When you troubleshoot the voice player, consider the different browser functions and computer function lists. Go to the page from the Avaya Web Messaging **Finding Solutions** Client Help page to see commonly asked questions about installing the voice player.

Avaya Voice Player Frequently Asked Questions

Here are frequently asked questions about using the voice player.

- Which servers can be connected to the voice player?

  INTUITY AUDIX, Octel 200, 250, 300, and 350 message servers.

- Can I attached a voice player file to an e-mail message and send the file to recipients who do not have the voice player?

  No. You can hear an .avp file only on the player. You can send a voice player file to recipients.

- Can the voice player be played on other platforms?

  Yes. Three different Avaya Voice Players are available to run: on Macintosh, Sun, and Windows computers.

- Do I have to operate the Avaya Voice Player on a browser?

  No. The voice player is also a stand-alone product. Record and play messages apart from other products.

- Can I convert .avp files to .wav files?

  Yes. The File menu contains a conversion option.

- Is the Avaya Voice Player a 32-bit system?

  The Windows Avaya Voice Player is a 32-bit system.

- Can I play my Avaya Voice Player through my telephone interface?

  No. You must play the Avaya Voice Player through your computer sound card. Select that option.

- How do I record messages from my computer with the Avaya Voice Player?

  You need to have a microphone connected to your computer to record messages.

- Is there a limit on the length of messages I can record?

  The message length is not determined by the Avaya Voice Player; instead, it depends on the amount of your computer's memory.

Note: If you want to download more copies of the voice player, it is available from this Web site:

//www.avaya.com/solutions/messaging/avp

Fax Viewers

The user needs a fax viewer to read faxes. You must install a compatible viewer, such as Image Viewer.

Note: You cannot create faxes in Avaya Web Messaging; you can only view and forward them.

Avaya Web Messaging does not provide or support any fax viewers. The following viewers have been tested with Avaya Web Messaging, and the results have been successful.

- Imaging for Windows is a component of the Microsoft Windows Operating System. Therefore, the fax viewer is free and included with the Windows 2000 and Windows 98 packages. Retrieve the fax viewer by following this path:

  Start / Programs / Accessories / Imaging

  If you cannot find the Viewer, it is possible that is has been installed on the operating system.

  Older versions of Windows 95 offer the fax viewer; however, you must contact Microsoft customer support.

- Key Viewer is another fax viewer that operates well with Avaya Web Messaging. To obtain a copy, go to www.keyview.com.

See the following topics in the Avaya Web Messaging Help for fax viewer procedures:

- **If you have fax problems**
- **If you don't have a fax viewer**

File Associations

Extension-type associations identify a file name extension as "belonging" to a certain application so that when you open any file with that extension, the application starts automatically. If the Avaya Voice Player does not launch, you might need to create a New File Type Association. See the following topics in the Avaya Web Messaging Help file for How to... procedures:

- **File Type Association with Netscape**
- **Create a New File Association for the voice player**

- **Create a New File Type Association**
- **Modify Default Action for File Type**

UCC Glossary

A

adjunct
A computer that communicates with DEFINITY ECS through an ASAI interface.

Adjunct-Switch Application Interface (ASAI)
A protocol supported by DEFINITY Enterprise Communication Server (ECS) that extends telephony features to adjuncts.

Administration Without Hardware (AWOH)
In Avaya Web Collaboration, extensions that must be administered in the Telephony and in the switch (PBX) Services database to allow remote access. Also referred to as softphone extensions or exports.

Advanced Speech Access
A Unified Communication Center application that allows people to use their voices to interact with and access their messages, tasks, and appointments. Advanced Speech Access also permits users to manage their phone calls and conferences.

Avaya Web Collaboration
A Unified Communication Center application that provides remote access to the voice and data capabilities of your DEFINITY Enterprise Communication Server (ECS).

Avaya Web Messaging
A Unified Communication Center application that provides a graphical user interface that allows users to view, manage, and manipulate the contents of their voicemail, e-mail, and fax messages, by using a browser.

AWOH
See *Administration Without Hardware*.

C

CentreVu® Computer Telephony (CV-CT)
Avaya's open, standards-based, API-neutral CTI server software. CentreVu Computer Telephony is the underlying CTI server software that integrates voice and data between customers' communications systems and their business application environment.

Internet Information Server (IIS)
Microsoft Web server software that enables access to UCC functionality through intranet web navigation.

D

DEFINITY Anywhere
The predecessor to Avaya Web Collaboration.

E

EC-500 Extension to Cellular
An Avaya Web Collaboration feature, formerly known as DEFINITY Global Cellular Solution. When this feature is administered for users, it allows a cellular phone to be treated as a local extension to the DEFINITY PBX. The cellular phone can use the same features and capabilities for incoming calls as the office phone. When the office phone rings, the administered cellular phone also rings.

L

License File
A file that enables client usage of UCC for a specified number of users.

P

Personal Digital Assistant (PDA)
A small consumer electronics device that performs specific tasks and, in some instances, connects to the Internet or is combined with a cell phone.

S

Services Monitor
An Avaya Web Collaboration feature that includes an error counter and detects when the Avaya Web Collaboration service is interrupted. If service is interrupted, the Services Monitor will initiate a server restart in 20 seconds.

U

Unified Communication Center (UCC)
A suite of Avaya applications that can include any or all of these applications: Advanced Speech Access, Avaya Web Collaboration, and Avaya Web Messaging.

V

Voice Player
Plug-in software that enables messages to be played and recorded through a computer equipped with a sound card and microphone. The voice player is distributed by Avaya Inc.

W

www.messenger
The predecessor to Avaya Web Messaging.