



Administering Modular Messaging Web Client

November 2009

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site: <http://www.avaya.com/support>

Licenses

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE <http://www.avaya.com/support/LicenseInfo/> ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be,

without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Named User License (NU). Customer may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Product.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://www.avaya.com/support/ThirdPartyLicense/>

Preventing toll fraud

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

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: <http://www.avaya.com/support/>

Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, and Modular Messaging, are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

Contact Avaya Support

Avaya Inc. provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

Contents

Chapter 1: Introduction	7
Chapter 2: Administering message servers	9
Adding a message server to Web Client.....	9
Modifying a message server.....	10
Deleting a message server from Web Client.....	10
Downloading a server certificate for a message server.....	11
Message Servers page field descriptions.....	11
Chapter 3: Administering syslog servers	15
Adding a syslog server to Web Client.....	15
Deleting a syslog server from Web Client.....	15
Chapter 4: Administering passwords and IDs	17
Changing the administrator log-in ID.....	17
Changing the administrator password.....	17
Change Administration and Maintenance Password page field descriptions.....	18
Chapter 5: Administering user access	19
Viewing the list of users who have accessed Web Client.....	19
Deleting a user from the user list.....	19
Restricting user access to Web Client.....	20
Viewing the list of restricted users.....	20
Updating the names in the user list.....	20
Updating the names in the list of restricted users.....	21
Removing a user from the Restricted List.....	22
User List page field descriptions.....	22
Restricted User Mailboxes page field descriptions.....	23
Chapter 6: Administering Lightweight Directory Access Protocol	25
Adding an LDAP server.....	25
Modifying an LDAP server profile.....	25
Deleting an LDAP server profile.....	26
LDAP Administration page field descriptions.....	26
Chapter 7: Administering features and options	29
Setting a timeout for inactive users.....	29
Displaying a corporate logo in Web Client.....	29
Adding a Web link to the Web Client menu bar.....	30
Enabling notification of new messages.....	31
Enabling message subject line editing.....	31
Enabling executable scripts in text messages.....	31
Enabling users to send carbon copies of messages.....	32
Enabling users to send blind carbon copies of messages.....	32
Enabling message subject creation.....	33
Enabling users to create message text.....	33
Enabling users to add message attachments.....	34
Enabling users to send messages to email recipients.....	34
Enabling users to copy and paste within messages.....	35

- Setting message purge on user exit..... 35
- Enabling users to reply to all..... 36
- Enabling message search by attachment type..... 36
- Enabling voice player use..... 36
- Using alternate Web Client English..... 37
- Creating a message of the day..... 38
- Creating a callback number hint..... 38
- Options and Settings page field descriptions..... 39
- Chapter 8: Backing up and restoring settings.....43**
 - Backing up Web Client settings.....43
 - Restoring Web Client settings.....43
- Chapter 9: Viewing administration and maintenance history.....45**
 - Viewing the Administration History/Maintenance log.....45
 - Administration History/Maintenance log field descriptions.....45
- Chapter 10: Performing maintenance.....47**
 - Web Client maintenance tools and tests.....47
 - Scheduling maintenance activities.....49
 - Scheduling Web Client test execution.....49
 - Scheduling regular server reboots.....50
 - Changing the start time of a scheduled test.....50
 - Schedule Maintenance page field descriptions.....50
 - Using test tools.....52
 - Running a Connectivity test.....52
 - Running a Ping test.....52
 - Verifying installation results.....53
 - Verify Installation results page field descriptions.....53
 - Blocking Web Client user logins.....54
 - Resetting the Web Client server.....54
 - Unblocking Web Client user logins.....55
 - Web Server Control page field descriptions.....55
 - Using the Services Log page.....56
- Chapter 11: Viewing statistics.....57**
 - Web Client statistic types.....57
 - Viewing log-in statistics.....57
 - Viewing data transfer statistics.....58
 - Viewing message event statistics.....58
 - Login Statistics page field descriptions.....58
 - Data Transfer Statistics page field descriptions.....59
 - Message Event Statistics page field descriptions.....61
- Chapter 12: Send us your comments.....63**
- Index.....65**

Chapter 1: Introduction

You can use the AvayaModular Messaging Web Client Administration and Maintenance pages to:

- Administer message servers and user lists
- Administer options and settings
- Change log-in IDs and passwords
- Use maintenance tools and logs
- Monitor system usage

Chapter 2: Administering message servers

Adding a message server to Web Client

In order for users to check messages using Web Client, you must add the message servers on which Modular Messaging mailboxes reside.

1. Go to **Administration > Message Servers** .
2. On the Message Servers page, complete the **Message Server Name (or IP Address)** field, and click **Add**.
The system verifies that:
 - No server with the same fully qualified server name exists in the list of message servers.
 - The Web server and message server can connect.
3. If you want to add an alias for the message server, enter a value in the **Alias** field.
4. Enter the name or IP address of Voice Server (MAS) you want to use with Web Client. This field is mandatory, if you have set the LDAP port to “Authenticated Only” for the MSS in the MSS administration page.

 **Note:**

If LDAP port is set to “Authenticated Only” then system displays the message “This field is mandatory because LDAP port is set to “Authenticated Only” mode for this message server”.

5. If you want to add a Web Subscriber Options site to this message server, complete the following fields:
 - **Protocol**
 - **WSO URL**
 - **Port Number**
6. Click **Submit**.

Related topics:

[Modifying a message server](#) on page 10

[Message Servers page field descriptions](#) on page 11

Modifying a message server

1. Go to **Administration > Message Servers** .
2. On the Message Servers page, select the message server that you want to modify, and click **Modify**.
3. If you want to add an alias for the message server, enter a value in the **Alias** field.
4. Enter the name or IP address of Voice Server (MAS) you want to use with Web Client. This field is mandatory, if you have set the LDAP port to “Authenticated Only” for the MSS in the MSS administration page.



Note:

If LDAP port is set to “Authenticated Only” then system displays the message “This field is mandatory because LDAP port is set to "Authenticated Only" mode for this message server”.

5. If you want to add a Web Subscriber Options site to this message server, complete the following fields:
 - **Protocol**
 - **WSO URL**
 - **Port Number**
6. Click **Submit**.

Related topics:

[Adding a message server to Web Client](#) on page 9

[Message Servers page field descriptions](#) on page 11

Deleting a message server from Web Client

1. Go to **Administration > Message Servers** .
 2. On the Message Servers page, select the message server that you want to delete from the list of administered servers, and click **Delete**.
-

Related topics:

[Message Servers page field descriptions](#) on page 11

Downloading a server certificate for a message server

When you add or modify a message server, the system automatically attempts to download a server certificate. If a server certificate is present, that server can use secure Lightweight Directory Access Protocol (LDAP) for database searches. If the system cannot automatically download a server certificate, you can download a certificate manually.

1. Go to **Administration > Message Servers** .
2. On the Message Servers page, select the message server for which you want to download a server certificate, and click **Get Certificate**.
The system either updates the server list to indicate that a certificate has been downloaded for that server or displays a message indicating that a certificate cannot be downloaded.

Related topics:

[Database searches using LDAP](#)

[Message Servers page field descriptions](#) on page 11

Message Servers page field descriptions


The Message Servers page lists the Message Storage Servers (MSSs) currently administered for Web Client use and allows you to add, modify, and delete message servers.

The following table lists the fields that provide information about the message servers currently administered for Web Client.

Name	Description
Server	This read-only field indicates the name or IP address of the MSSs administered for use with Web Client.
Server Alias	This read-only field indicates the alias of each MSS administered for use with Web Client. If no alias is administered, the system uses the server name of the MSS. The server aliases are listed in the Server Name field on the Web Client user Logon page.
Connection Status	This read-only field indicates whether the Connectivity Test has been run successfully for each MSS in the server list. Failures are

Name	Description
	indicated by a red Failed link. Click the Failed link to go to the Connectivity Test.
Certificate	This read-only field indicates whether a server certificate has been downloaded for each MSS in the server list. If a server certificate is present, that server can use secure Lightweight Directory Access Protocol (LDAP). The system automatically attempts to download a server certificate each time you add or modify a message server. You can also download a certificate manually.
WSO URL	This read-only field lists the Web address of the Web Subscriber Options site associated with each MSS, if one is administered.
Voice Server	This read-only field indicates the name or IP address of the Voice Servers administered for use with Web Client.

Use the following fields to add or modify a message server for Web Client.

Name	Description
Message Server Name (or IP Address)	Enter the name or IP address of an MSS you want to use with Web Client. The server that you enter must be on the customer network and must be for Avaya Modular Messaging Release 2 or later.
Alias	Enter the alias that you want the system to use for this MSS. If you want the system to use the message server name as the alias, leave this field blank. The alias is the name the user sees when selecting the server on the Web Client user Logon page.
Voice Server Name (or IP Address)	<p>Enter the name or IP address of Voice Server (MAS) you want to use with Web Client. This field is mandatory, if you have set the LDAP port to "Authenticated Only" for the MSS in the MSS administration page.</p> <p> Caution: Verify that the name or IP address for Voice Server is valid and points to the corresponding message server.</p>
Protocol	If you are adding an associated Web Subscriber Options site to a message server, select the protocol, either HTTP or HTTPS , used by the Web Subscriber Options server.
WSO URL	If you want to add an associated Web Subscriber Options site to a message server, enter the URL of the Web Subscriber Options site. If you add a Web Subscriber Options site to a message server, users can access the Web Subscriber Options Quick Logon link if they are logged on to Web Client. Use the format <machine name>/<virtual directory>; for example, <code>http://machine.location.company.com/wso</code> .
Port Number	The port number used to access the specified Web Subscriber Options site. The default port number is 80.

Related topics:

[Adding a message server to Web Client](#) on page 9

[Modifying a message server](#) on page 10

Chapter 3: Administering syslog servers

Adding a syslog server to Web Client

The SysLog Servers page lists the SysLog Servers currently administered for Web Client use and allows you to add and delete syslog servers.

-
1. Go to **Administration > SysLog Servers** .
 2. On the SysLog Servers page, complete the **SysLog Server Name (or IP Address)** field, and click **Add**.
The system verifies that no server with the same fully qualified server name exists in the list of syslog servers.



Note:

After you add the new Syslog server, you must reset the web server for the changes to take effect.

Deleting a syslog server from Web Client

-
1. Go to **Administration > SysLog Servers** .
 2. On the SysLog Servers page, select the message server that you want to delete from the list of administered servers, and click **Delete**.
-

Chapter 4: Administering passwords and IDs

Changing the administrator log-in ID

-
1. Go to **Administration > Change Login ID or Password** .
 2. On the Change Administration and Maintenance Password page, enter a new log-in name in the **Login ID** field.
 3. Click **Submit**.
-

Related topics:

[Change Administration and Maintenance Password page field descriptions](#) on page 18

Changing the administrator password

-
1. Go to **Administration > Change Login ID or Password** .
 2. Complete the fields on the Change Administration and Maintenance Password page.
 3. Click **Submit**.
-

Related topics:

[Change Administration and Maintenance Password page field descriptions](#) on page 18

Change Administration and Maintenance Password page field descriptions

Name	Description
Login ID	The name that the administrator enters in the Log On field on the Administration and Maintenance Logon page. You can also change the default system administrator log-in ID to a different name. The default administrator ID is <code>admin</code> .
Old Password	The current administrator password. The default administrator password is <code>admin1</code> .
New Password	The new administrator password that you want to assign. The password has no expiration date and can be changed at any time. Your password must have at least one character and no more than 10 characters.
Verify New Password	The new administrator password that you specified in the New Password field.

Related topics:

[Changing the administrator log-in ID](#) on page 17

[Changing the administrator password](#) on page 17

Chapter 5: Administering user access

Viewing the list of users who have accessed Web Client

-
1. Go to **Administration > User List** .
 2. View the list that displays on the User List page.
-

Related topics:

[User List page field descriptions](#) on page 22

Deleting a user from the user list

Deleting a user from the user list does not restrict the user's access to Web Client. To prevent a user from logging in to Web Client, delete the user, and then add the user to the restricted list.

-
1. Go to **Administration > User List** .
 2. On the User List page, place a check in the first column of the user you want to delete, and click **Delete**.
-

Related topics:

[User List page field descriptions](#) on page 22

Restricting user access to Web Client

Avaya recommends that you restrict user access to Web Client if the Modular Messaging mailbox is being used improperly or you suspect a security issue.

Prerequisites

- Before you can restrict access for a user, you must delete that user from the user list.
- Because Web Client does not validate the mailboxes that you enter on this page, you must first verify the name or mailbox number of the user on the Modular Messaging system.

-
1. Go to **Administration > User List** .
 2. Click **View Restriction List**.
 3. On the Restricted User Mailboxes page, complete the fields to specify the user that you want to restrict.
 4. Click **Add Restriction**.

Related topics:

[Restricted User Mailboxes page field descriptions](#) on page 23

Viewing the list of restricted users

-
1. Go to **Administration > User List** , and click **View Restriction List**.
 2. View the list that displays on the Restricted User Mailboxes page.

Related topics:

[Restricted User Mailboxes page field descriptions](#) on page 23

Updating the names in the user list

Updating the names in the user list can be very slow, especially if the user list is long. You should only update the names in cases when it is necessary. For example, if a Modular Messaging administration change results in a change in the names associated with user

mailboxes, you might want to update the names in the user list. You can also update a name by deleting the name from the user list and then having the system automatically update the name when the user logs on to Web Client again.

 **Warning:**

If you delete a user from the list and have the system automatically update the name when the user logs on, you lose the log-in history for that user.

Go to **Administration > User List** , and click **Update Names**.

Related topics:

[User List page field descriptions](#) on page 22

Updating the names in the list of restricted users

Updating the names in the restricted user list can be very slow, especially if the list of restricted users is long. You should only update the names in cases when it is necessary. For example, if a Modular Messaging administration change results in a change in the names associated with user mailboxes, you might want to update the names in the restricted list. You can also update a name by deleting the name from the restricted user list and then re-adding the updated name, rather than having the system update all the names in the restricted user list.

If you are upgrading the Web Client software from the 3.0 release or earlier releases, you need to update names in order to populate the names column.

-
1. Go to **Administration > User List** .
 2. Click **View Restriction List**.
 3. Click **Update Names**.
-

Related topics:

[Restricted User Mailboxes page field descriptions](#) on page 23

Removing a user from the Restricted List

If you want a restricted user to be able to log in to Web Client again, remove that user from the restricted list.

-
1. Go to **Administration > User List**.
 2. Click **View Restriction List**.
 3. Place a check in the first column of the user that you want to remove from the restriction list, click **Delete**, and click **Return to User List**.
-

Related topics:

[Restricted User Mailboxes page field descriptions](#) on page 23

User List page field descriptions

The User List, which displays the Modular Messaging users who have logged in to Web Client, contains the following columns.

Name	Description
Server	Displays the name or IP address of the Modular Messaging server on which the user mailbox resides.
Mailbox	Displays the user mailbox number.
Name	Displays the name of the user as it appears in the Names Directory of the server.
Last Login	Displays the day and time that the user last logged in to the mailbox.
Logged In	Indicates whether the user is currently logged in to the mailbox.
# Logins	Displays the number of times that the user logged in to the mailbox.
Avg Duration (mm:ss)	Displays the average length of time that the user is logged in to the mailbox.
Total Time (mm:ss)	Displays the total time that the user has spent logged in to Web Client.

Related topics:

[Viewing the list of users who have accessed Web Client](#) on page 19

[Updating the names in the user list](#) on page 20

[Deleting a user from the user list](#) on page 19

Restricted User Mailboxes page field descriptions

The Restricted User Mailboxes page lists the users currently restricted from logging in to Web Client.

Name	Description
Server	Displays the message servers on which the restricted users reside.
Mailbox	Displays the mailbox numbers (with their associated server) that have been restricted access to Web Client.
Name	Displays the name of the user as it appears in the Names Directory of the server.

Related topics:

[Viewing the list of restricted users](#) on page 20

[Restricting user access to Web Client](#) on page 20

[Removing a user from the Restricted List](#) on page 22

[Updating the names in the list of restricted users](#) on page 21

Chapter 6: Administering Lightweight Directory Access Protocol

Adding an LDAP server

1. Go to **Administration > LDAP Administration** , and click **Add**.
 2. Complete the fields on the LDAP Administration page.
 3. Click **Submit** to save the LDAP server information.
-

Related topics:

[LDAP Administration page field descriptions](#) on page 26

Modifying an LDAP server profile

1. Go to **Administration > LDAP Administration** .
 2. On the LDAP Administration page, select the LDAP server that you want to modify, and then click **Modify**.
 3. Modify the fields that you want to change.
 4. Click **Submit** to save the updated LDAP server information.
-

Related topics:

[LDAP Administration page field descriptions](#) on page 26

Deleting an LDAP server profile

1. Go to **Administration > LDAP Administration** .
2. On the LDAP Administration page, select the LDAP server that you want to delete, and then click **Delete**.
3. When prompted to confirm that you want to delete the server, click **OK**.

Related topics:

[LDAP Administration page field descriptions](#) on page 26

LDAP Administration page field descriptions

Name	Description
LDAP Server	Type the fully qualified domain name of your LDAP server, such as <code>server.company.com</code> .
SSL Enabled	Specify whether Secure Sockets Layer (SSL) is used for LDAP searches. Using SSL provides additional security.
LDAP Port	Type the port used for LDAP searches. If you enable SSL, the system uses port 636 as the default LDAP port. If you disable SSL, the system uses port 389 as the LDAP port.
Base DN (distinguished name)	Type the LDAP query string used to connect to the LDAP server. Enter the string in the form <code>LDAP://donner/c=COUNTRY/o=ORG</code> , where <code>donner</code> is the server name. The country and org must match the values of the LDAP system.
User ID	If you want to restrict LDAP access to a single login, specify the user ID for that user login.
Password	If you want to restrict LDAP access to a single login, specify the password for that user login.
Display Name	Type the field name from the LDAP schema that will return the proper value on LDAP searches by name; for example, common name (cn), surname, displayname, or givenname.
Voice Mail Address	Type the field name from the LDAP schema that will return the proper value on LDAP searches by voice mail address; for example, voicemailaddress.

Name	Description
Alphanumeric Search Criteria/ Match Field	For alphanumeric database searches, enter the text you want to search on.
Alphanumeric Search Criteria/ Match Type	Select the criteria for the search: <ul style="list-style-type: none"> • Exact: Only exact matches of the search criteria are matches. • Left-Partial: Matches in which the left side of a string is missing are matches, for example *el. • Right-Partial: Matches in which the right side of a string is missing are matches, for example chap*. • Partial: Matches in which the right and left sides of a string are missing are matches, for example *hap*.
Numeric Search Criteria/Match Field	For numeric database searches, enter the text you want to search on.
Numeric Search Criteria/Match Type	Select the criteria for the search: <ul style="list-style-type: none"> • Exact: Only exact matches of the search criteria are matches. • Left-Partial: Matches in which the left side of a number is missing are matches, for example *0306. • Right-Partial: Matches in which the right side of a number is missing are matches, for example 538*. • Partial: Matches in which the right and left sides of a number are missing are matches, for example *8030*.

Related topics:

[Adding an LDAP server](#) on page 25

[Modifying an LDAP server profile](#) on page 25

Chapter 7: Administering features and options

Setting a timeout for inactive users

1. On the Options and Settings page, go to **Administration > Options and Settings**.
2. Complete the **Web Server Timeout** field.
3. Click **Submit Changes**.

 **Note:**

You can also change the server timeout from IIS. To change the server timeout from the IIS, go to **IIS Manager > WebClientAppPool > Shutdown worker processes after being idle for (time in minutes)**. The server timeout in the IIS is effective only after all users on the system are idle for the time defined in the IIS.

Related topics:

[Options and Settings page field descriptions](#) on page 39

Displaying a corporate logo in Web Client

Prerequisites

Make sure that you have a corporate logo in a .gif file. For best results, your logo file should be 158 pixels long by 54 pixels high (the same size as the default logo). If your logo is larger than the existing logo, the image might appear distorted.

1. On the Web Client server, navigate to the images directory and locate the **CustomLogo.gif** file; for example, `drive:\ProgramFiles\Avaya\webmsg\images`.
2. Rename the existing `CustomLogo.gif` file to save it.

3. Copy your corporate logo file to the images directory, and rename your logo file to `CustomLogo.gif`.
4. Go to **Administration > Options and Settings** .
5. On the Options and Settings page, select **Display a custom logo** in the **Choose Corporate Logo** field.
6. Click **Submit Changes**.

Related topics:

[Options and Settings page field descriptions](#) on page 39

Adding a Web link to the Web Client menu bar

Web Client provides a Web Link feature that allows you to add an intranet or Internet URL to the Web Client user interface for quick access. If you use this feature, a link to the site that you specify is added to the menu bar on each page of the Web Client user interface.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, complete the following fields:
 - **Assign URL Link**
 - **Assign Web Link Label**
 3. Click **Submit Changes**.

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling notification of new messages

Enable this feature to allow users to set message notification options in the Web Client user interface.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Enable new message notification** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling message subject line editing

If you enable this feature, users can edit the subject line of Modular Messaging messages they receive in their Web Client Inboxes.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Enable subject edit** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling executable scripts in text messages

By default, Web Client restricts the execution of scripts that are contained within received text messages. If you want to enable executable scripts on the client desktop, you can change this setting.



Warning:

Enabling executable scripts can threaten system security by opening the user computer to cross-site scripting attacks by hackers.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Enable Executable Scripting in Text Messages** check box.
 3. Click **Submit Changes**.

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling users to send carbon copies of messages

Enable this feature to allow users to send a carbon copy (Cc) of messages they create.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Allow Cc** check box.
 3. Click **Submit Changes**.

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling users to send blind carbon copies of messages

Enable this feature to allow users to send a blind carbon copy (Bcc) of messages they create.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Allow Bcc** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling message subject creation

If you enable this feature, users can create a subject for a message they are sending.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Allow Subject** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling users to create message text

Enable this feature to allow users to add text for a message they are creating.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Allow Message Text** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling users to add message attachments

Enable this feature to allow users to add attachments to a message.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Allow Attachments** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling users to send messages to email recipients

Enable this feature to allow users to send messages to external email addresses (addresses that are not for Modular Messaging mailboxes).

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Allow email addresses in To** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling users to copy and paste within messages

Enable this feature to allow users to copy message attachments or paste content from the clipboard to a message.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Allow message copy/paste** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Setting message purge on user exit

Select this option if you want the system to purge messages from the users' Deleted folder each time a user logs off or the user's Web Client session times out.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Purge Messages on exit** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling users to reply to all

Enable this feature if you want users to be able to reply to all when responding to a message.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Allow Reply All** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling message search by attachment type

Enable this feature if you want users to be able to search their messages for messages with a particular type of attachment.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Allow search by attachment type** check box.
 3. Click **Submit Changes**.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Enabling voice player use

This option allows users to record and play voice messages through the sound card on their computers rather than on their telephones. Users can use Avaya Voice Player or another local

player such as Windows Media Player. After you enable this option, you must specify which voice player features you want users to be able to access.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Enable Voice Player** check box.
 3. Select the voice player features you want users to be able to access.
 4. Specify how the voice player will be downloaded.
 5. Click **Submit Changes**.

Related topics:

[Options and Settings page field descriptions](#) on page 39

Using alternate Web Client English

You can specify to change the Web Client user interface so that it displays an alternate set of English strings. This alternate form of English is focused on voice mail. For example, if you enable this option, the users' primary mailbox folder is labeled Voicemail instead of Inbox.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, check the **Use Secure Web Client (English) string set** check box.
 3. Click **Submit Changes**.

Related topics:

[Options and Settings page field descriptions](#) on page 39

Creating a message of the day

Creating a message of the day is useful if you want to alert users to scheduled system maintenance or a change to system settings. The message you create displays at the top of the Web Client user Logon page.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, complete the **Message of the Day** field.
 3. Click **Submit Changes**.
When users go to the Web Client user Logon page, the message you specify displays at the top of the page.
-

Related topics:

[Options and Settings page field descriptions](#) on page 39

Creating a callback number hint


You can provide users with a hint about the required format for callback numbers, for example, dialing 9 for an external number. The hint that you create displays below the **Callback Number** field in the Web Client user interface.

-
1. Go to **Administration > Options and Settings** .
 2. On the Options and Settings page, complete the **Callback Number Hint** field.
 3. Click **Submit Changes**.
-

Related topics:


[Options and Settings page field descriptions](#) on page 39

Options and Settings page field descriptions

Name	Description
Web Server Timeout	<p>Specify the number of minutes of user inactivity that occur before the system times out the user. When a user takes an action after the timeout is reached, the system drops the session and logs out the user.</p> <p>The default for this field is 480 minutes. The minimum is 5 minutes, and the maximum is 720 minutes.</p> <p> Note:</p> <p>You can also change the server timeout from IIS. To change the server timeout from the IIS, go to IIS Manager > WebClientAppPool > Shutdown worker processes after being idle for (time in minutes). The server timeout in the IIS is effective only after all users on the system are idle for the time defined in the IIS.</p>
Choose Corporate Logo	<p>Specify whether you want to display your own corporate logo or you do not want to display any logo. If you want to display a custom corporate logo, you must replace the default file, named <code>CorporateLogo.gif</code>, with your own logo file.</p>
Edit the Web Link Control/Assign URL Link	<p>To add an intranet or Internet URL to the Web Client user interface for quick access, enter the URL of the site to which you want to provide a link.</p>
Edit the Web Link Control/Assign Web Link Label	<p>If you entered a URL in the Assign URL Link field, type the text that you want to appear in the menu bar.</p>
Feature Options/Enable new message notification	<p>Allows users to set message notification options in the Web Client user interface. For example, users can configure Web Client to display an alert box or pop-up window when they receive new voice messages. Enabling message notification can affect system performance.</p> <p>By default, this feature is disabled.</p>
Feature Options/Enable subject edit	<p>Allows users to edit the subject line of messages that they receive in their Web Client Inboxes. For example, users might want to create new message subjects to help them organize their messages more easily.</p> <p>By default, this feature is disabled.</p>
Message Creation Options/Allow Cc	<p>Allows users to send a carbon copy (Cc) of a message when they create, reply to, or forward a message using Web Client.</p> <p>By default, this feature is enabled.</p>

Name	Description
Message Creation Options/Allow Bcc	Allows users to send a blind carbon copy (Bcc) of a message when they create, reply to, or forward a message using Web Client. By default, this feature is enabled.
Message Creation Options/Allow Subject	Allows Web Client users to specify a message subject when they create a message, or modify a message subject when they respond to a message. By default, this feature is enabled.
Message Creation Options/Allow Message Text	Allows Web Client users to specify message text when they create a message, or modify message text when they respond to a message. By default, this feature is enabled.
Message Creation Options/Allow Attachments	Allows Web Client users to add attachments when they create, reply to, or forward a message. By default, this feature is enabled.
Message Creation Options/Allow email addresses in To	Allows Web Client users to specify email addresses (addresses that are not for a Modular Messaging mailbox) as recipients when they create, reply to, or forward a message. By default, this feature is enabled.
Message Options/Allow message copy/paste	Allows Web Client users to: <ul style="list-style-type: none"> • copy message text, voice, fax, and binary attachments to the clipboard. • paste clipboard contents to any message-related fields. By default, this feature is enabled.
Message Options/Purge messages on exit	Specify to have the system purge messages from the Deleted folder of each user when a user logs off or the user's Web Client session times out. By default, this feature is disabled.
Message Options/Allow Reply All	Allow users to reply to all when they reply to a message. If this feature is disabled, Web Client does not display the Reply All option in the message detail window or the right-click message menu. By default, this feature is enabled.
Search Options/Allow search by attachment type	Allows Web Client users to search their mailbox folders for messages that have a particular type of attachment, for example, voice or fax. By default, this feature is enabled.
Voice Player Options/Enable Voice Player	Allows Web Client users to use different voice players to play back and record voice messages and attachments. Voice player options include Avaya Voice Player or another local player, such as Windows Media Player. If you enable the voice player feature, you must specify at least one of the following voice player options.

Name	Description
	By default, this feature is enabled.
Voice Player Options/Allow AVP for Audio Playback	Allows Web Client users to use Avaya Voice Player to play back voice messages and voice attachments. You can enable this field only if you have enabled Voice Player. By default, this feature is enabled.
Voice Player Options/Allow Local Player for Audio Playback	Allows Web Client users to use a soundcard and an associated local player, such as Windows Media Player, to play back voice messages and voice attachments. You can enable this field only if you have enabled Voice Player. By default, this feature is enabled.
Voice Player Options/Allow AVP for Audio Record	Allows Web Client users to use Avaya Voice Player to record voice messages and voice attachments. You can enable this field only if you have enabled Voice Player. By default, this feature is enabled.
Voice Player Options/Allow Save/Save As/Export from AVP	Allows Web Client users to use the Save , Save As , and Export options in Avaya Voice Player. You can enable this field only if you have enabled Voice Player. By default, this feature is enabled.
Voice Player Options/Choose a Voice Player location	<p>If you have enabled Voice Player, choose one of the following options:</p> <ul style="list-style-type: none"> • If you want users to be able to use the Avaya Voice Player but not download it from the Web Client, select The Voice Player is already installed on client desktop(s). In this case, you manage the voice player installation. • If you want users to be able to download and use Avaya Voice Player, select The Voice Player will be downloaded by the individual user. In this case, users can download the voice player from Web Client to their own computers. <p>If Voice Player is enabled, the second option is the default.</p>
UI Text Options/Use Secure Web Client (English) string set	Specify to change the Web Client user interface so that it displays an alternate set of English strings. This alternate form of English is focused on voice mail. For example, if you enable this option, the users' primary mailbox folder is labeled Voicemail instead of Inbox. If you enable this option, users cannot select a language from the user Logon page. By default, this option is disabled.
UI Text Options/Message of the Day	Allows you to display a message on the Web Client Logon page. For example, you can type a message that alerts users to upcoming server maintenance.
UI Text Options/Callback Number Hint	Allows you to specify a hint that the system displays below the Callback Number field in the Web Client user interface. For example, if users' callback numbers must begin with 9 (to

Name	Description
	get an outside line), you can enter the following tip in this field: Type 9 plus the 10-digit number.
UI Text Options/ Enable executable scripting in text messages	<p>Allows the system to execute scripts embedded in text messages on the client desktop. For example, if you enable this option, the system can execute Javascript embedded in an HTML message.</p> <p> Warning:</p> <p>Enabling executable scripting can threaten system security by opening the user computer to cross-site scripting attacks by hackers. By default, executable scripting is disabled. If executable scripting is disabled, users can still view HTML messages without the scripting.</p>

Related topics:

- [Setting a timeout for inactive users](#) on page 29
- [Displaying a corporate logo in Web Client](#) on page 29
- [Adding a Web link to the Web Client menu bar](#) on page 30
- [Enabling notification of new messages](#) on page 31
- [Enabling message subject line editing](#) on page 31
- [Enabling executable scripts in text messages](#) on page 31
- [Enabling users to send carbon copies of messages](#) on page 32
- [Enabling users to send blind carbon copies of messages](#) on page 32
- [Enabling message subject creation](#) on page 33
- [Enabling users to create message text](#) on page 33
- [Enabling users to add message attachments](#) on page 34
- [Enabling users to send messages to email recipients](#) on page 34
- [Enabling users to copy and paste within messages](#) on page 35
- [Setting message purge on user exit](#) on page 35
- [Enabling users to reply to all](#) on page 36
- [Enabling message search by attachment type](#) on page 36
- [Enabling voice player use](#) on page 36
- [Using alternate Web Client English](#) on page 37
- [Creating a message of the day](#) on page 38
- [Creating a callback number hint](#) on page 38

Chapter 8: Backing up and restoring settings

Backing up Web Client settings

The Message Servers, User List, and Options and Settings pages allow you back up the page settings. Backing up page settings allows you to restore settings if you experience a loss of data.

-
1. Go to the page for which you want to back up data.
 2. Click **Backup**, and then click **OK** when prompted to confirm.
 3. When the message displays that the backup is complete, click **OK**.
-

Related topics:

[Message Servers page field descriptions](#) on page 11

[User List page field descriptions](#) on page 22

[Options and Settings page field descriptions](#) on page 39

Restoring Web Client settings

The Message Servers, User List, and Options and Settings pages allow you restore data if you experience a loss of system data. If a backup for the page is not available, the system defaults are restored.

-
1. Go to the page for which you want to restore data.
 2. Click **Restore**, and then click **OK** when prompted to confirm.
 3. When the message displays that the restore is complete, click **OK**.
-

Related topics:

[Message Servers page field descriptions](#) on page 11

[User List page field descriptions](#) on page 22

[Options and Settings page field descriptions](#) on page 39

Chapter 9: Viewing administration and maintenance history

Viewing the Administration History/Maintenance log

You can view Web Client administration and maintenance activities in the Administration History/Maintenance log.

Go to **Administration > Administration History/Maintenance Log** .

Related topics:

[Administration History/Maintenance log field descriptions](#) on page 45

Administration History/Maintenance log field descriptions

The Administration History/Maintenance log, which tracks Web Client administration and maintenance activities, contains the following columns.

Name	Description
Login name	Displays the log-in name that performed the administrative action. <ul style="list-style-type: none">• Admin: Indicates changes made by the system administrator• Services: Indicates changes made by technical support personnel• wmDaemon: Denotes the Daemon process that runs maintenance tests on the server
Date	Displays the date, in mm/dd/yy format, on which the administrative action was performed. The most recent entries are listed at the end of the log.
Time	Displays the time, in hh/mm/ss format, on which the administrative action was performed. The most recent entries are listed at the end of the log.

Name	Description
Action	Describes the administrative action performed. Logged activities include test results and configuration changes to the user list, message servers, and other settings. Successful tests are logged in green, and failed tests are logged in red. The system logs failed tests only once, until the tests succeed, with the exception of the Connect test. The system logs failures for the Connect test every 15 minutes since different servers can fail. The system only logs successful tests if the last test failed.

Related topics:

[Viewing the Administration History/Maintenance log](#) on page 45

Chapter 10: Performing maintenance

Web Client maintenance tools and tests

Web Client includes the following maintenance tools and tests. You can schedule the execution of tests or run tests or tools manually.

If you are working from the local computer that is the Web server, you can access some of the test tools from the Modular Messaging Web Client program group by clicking **Start > Programs > Avaya Modular Messaging Web Client Tools** .

CPU Availability

Use the CPU Availability test to monitor the number of times in a row that the Central Processing Unit (CPU) of the server is at or near 100% usage. If the system reaches a specified number of times, the system automatically reboots. You can view the status of this test on the Schedule Maintenance page.

IIS test

Use the IIS test to monitor the Internet Information Services (IIS) to ensure that it is functioning properly. If an IIS problem is found, the system can perform an IIS restart or system reboot to attempt to correct the problem. You can schedule this test on the Schedule Maintenance page.

Connectivity

Use the Connectivity test to verify the connection between the Web Client and the message servers that you administer for Web Client. The test also verifies the following:

- The name and IP address of the Web Client server is valid.
- The Web server is configured for network access.
- IIS is running on the Web server.
- A connection to the message servers exists.

You can run this test manually from the Tools page or from the desktop of the Web Client Web server. You can also use the Schedule Maintenance page to set an interval for executing this test automatically. The system executes this test every 15 minutes by default but you can change the frequency.

Running the test repeatedly could produce different results due to possible intermittent network problems.

Note:

If the Connectivity test fails for some but not all message servers, run the Ping test for each message server to determine if a problem exists with the network connection of the message

server. If the Connectivity test fails for all message servers, check the network connection of the Web Client server.

Install Verify (Ivy)

Use the Ivy test to verify that all necessary files are installed. Verification takes several minutes. You can run this test manually from the Tools page or from the desktop of the Web Client Web server. You can also schedule the test to run automatically on the Schedule Maintenance page.

If you run the test from the Tools page, you can create a baseline, which records the current warnings and errors. The next time you run the test, you can choose to view only the new warnings and errors that have occurred since you last ran the test.

Caution:

Your Web Client Web server must use the date format of mm/dd/yyyy in order for the Ivy tool to correctly display errors.

Ping

Use the Ping test to verify connections between the Web server and its desktop clients. The Ping test can also test for connections between the Web server and any other computer. The Ping test can fail for the following reasons:

- Incorrect domain name server (DNS) entry
- TCP/IP problems
- Network problems

You can run this test from the Tools page.

Note:

If the Ping test fails for a computer, you can run the test again for another computer to determine if the problem exists with the computer or the Web server. You can also run the Ping test using the IP address rather than the name of a computer. If the test with the IP address succeeds, the DNS settings are wrong for the computer. If the test with the IP address fails, a problem exists with the computer or with the network. Contact the appropriate administrator for assistance.

Web Server Control tool

Use the Web Server Control tool to block users from logging on to the Web Client server for a specified period of time or to reset the Web server, which logs off all users from the system immediately. This tool is useful when you want to shut down the system to perform maintenance tasks, such as upgrading the server.

A reset typically takes 1 or 2 minutes. Any attempts to access this page while the server is in the process of resetting causes an error to be displayed until the reset is complete. When Web Client and Web Subscriber Options are installed on the same server, resetting the Web server also blocks users from logging on to Web Subscriber Options.

You can access this tool from the Web Server Control page.

**Note:**

You can also log off all users by going to **Programs > Avaya Modular Messaging Web Client Tools > Reset Web Server** on the Web Client server.

Services Log tool

Use the Services Log tool to document general information about services and maintenance activities. The information you enter is written to a text file named `wmService.log`, located in the Data directory.

You can access this tool from the Services Log page.

Related topics:

[Running a Connectivity test](#) on page 52

[Running a Ping test](#) on page 52

[Verifying installation results](#) on page 53

[Blocking Web Client user logins](#) on page 54

[Using the Services Log page](#) on page 56

Scheduling maintenance activities

Scheduling Web Client test execution

You can schedule certain Web Client tests to run automatically at intervals that you specify. These tests include the CPU Availability, IIS, Connect, and IVY tests. You can also run most of these tests manually from the Tests page.

-
1. Go to **Administration > Schedule Maintenance** .
 2. On the Schedule Maintenance page, complete the fields necessary to schedule the test that you want the system to execute automatically.
 3. Click **Submit**.
-

Related topics:

[Web Client maintenance tools and tests](#) on page 47

[Schedule Maintenance page field descriptions](#) on page 50

Scheduling regular server reboots

If you are experiencing system problems on a regular basis, you can have the system periodically reboot the Windows 2003 server. Automatically rebooting the server is not required for normal server usage.

-
1. Go to **Administration > Schedule Maintenance** .
 2. On the Schedule Maintenance page, complete the **Select Interval** field next to **Periodic Server Reboot**.
 3. Click **Submit**.
-

Related topics:

[Schedule Maintenance page field descriptions](#) on page 50

Changing the start time of a scheduled test

-
1. Go to **Administration > Schedule Maintenance** .
 2. On the Schedule Maintenance page, click the **Next Run Time** of the test that you want to reschedule.
 3. In the Set Next Run Time dialog box, complete the fields on the page.
 4. Click **OK**.
-

Related topics:

[Web Client maintenance tools and tests](#) on page 47

[Schedule Maintenance page field descriptions](#) on page 50

Schedule Maintenance page field descriptions

The Schedule Maintenance page contains the following fields, which allow you to schedule and view the status of each maintenance test and activity. You can also perform many of these tests manually from the Test page.

Name	Description
Test	Lists the tests and activities that you can schedule.

Name	Description
Select Interval	<p>Select the frequency with which you want the system to perform the activity. This field is not available for the CPU Availability test because the system constantly monitors the activity of the server Central Processing Unit (CPU).</p> <p>The available intervals depend on the test. The following intervals are the defaults and the recommended values for each test:</p> <ul style="list-style-type: none"> • IIS test: 2 minutes • Connect test: 15 minutes • Ivy test: 24 hours <p>Select Never if you do not want the system to perform the activity automatically.</p>
Next Run Time	<p>Indicates the next time the system is scheduled to run the activity:</p> <ul style="list-style-type: none"> • Running: Indicates that the test is currently being executed • Not Running: Indicates that the test is not scheduled to run • Pending: Indicates that the test is in the process of starting <p>If a date and item are shown, you can change the next scheduled run of the activity.</p>
Last Executed	<p>This read-only field indicates the last time that the system executed the activity.</p>
Notify Locally	<p>For the IIS test, Connect test, and Ivy test, place a check in the Write to Event Log check box if you want the system to write the test results to the Windows Event Log.</p>
Last Result	<p>This field indicates whether a test passed or failed the last time that the system executed the test. Failures are indicated by a red Failed link. For the Connect test, click the Failed link to go back to the test.</p>
Last Failure	<p>This field provides the date and time for the last failure of a test that the system executed. If you click the date and time of the failure, you can view the failure in the Administration History/ Maintenance log. Click Reset to clear the failure information from the page. Resetting allows you to determine if you have fixed the problem, depending on whether the same failure occurs again.</p>
Select Number of Failed Tests to Perform Action/ Restart	<p>For the IIS test, specify the number of times the test fails before the system restarts the Web server. Select a number from 1 to 10, or select Never to specify that you do not want the system to restart Internet Information Services (IIS).</p>
Select Number of Failed Tests to Perform	<p>For the CPU Availability test and IIS test, specify the number of times the test fails before the system reboots the Web server. Select a number from 1 to 10, or select Never to specify that you do not want the Web server to be rebooted because the test failed.</p>

Name	Description
Action/ Reboot	

Related topics:

[Web Client maintenance tools and tests](#) on page 47

[Scheduling Web Client test execution](#) on page 49

[Changing the start time of a scheduled test](#) on page 50

[Scheduling regular server reboots](#) on page 50

Using test tools

Running a Connectivity test

-
1. Go to **Maintenance > Tools > Connectivity Test** .
 2. Complete the **Message Server** field, and click **Run Test**.
The system tests connectivity to each of the selected message servers and displays the test results, indicating whether each test passed or failed.

Related topics:

[Web Client maintenance tools and tests](#) on page 47

Running a Ping test

Use the Ping test to verify connections between the Web server and its desktop clients. You can also test the connection between the Web server and any other computer.

-
1. Go to **Maintenance > Tools > Ping Test** .
 2. Complete the **Enter host name or IP address** field.
 3. Click **Run Test**.
The system displays the results of the test, including packets sent and received.
-

Related topics:

[Web Client maintenance tools and tests](#) on page 47

Verifying installation results

1. Go to **Maintenance > Tools > Verify Installation** .
2. On the Verify Installation page, if you already have a baseline of the previous warnings and errors, specify whether you want to show only new warnings and errors or if you want to display them all.
3. Click **Run Test**.
4. If you want to save a record of the warnings and errors captured in the report, click **Build Baseline**.
The next time you run the test, you can filter out the existing warnings and errors and display only new warnings and errors.

Related topics:

[Web Client maintenance tools and tests](#) on page 47

[Verify Installation results page field descriptions](#) on page 53

Verify Installation results page field descriptions

The Verify Installation tool checks each Modular Messaging Web Client file on the server against the files stored in the Verify Installation database. The Verify Installation results page highlights any differences between the files on the server and the files in the database. For example, the test displays an error when the date and version of a file on the server is older than what displays in the database. Warnings are highlighted in yellow, and errors are highlighted in red. The error information is separated into different tables based on file type, such as images, system files, and tools.

 **Caution:**

If the test displays an error because files on the server are older than files in the database, you might need to reinstall the Web Client server software.

The following table describes the specific file information that the Verify Installation tool checks.

Name	Description
Name	Displays the name of the file required on the server.
Location	Displays the location where the required file should reside on the server, for example <code>C:\WINDOWS\system32</code> .
Size	Displays the size (in bytes) of the file required on the server.

Name	Description
Date	Displays the build date for the file required on the server.
Version	Displays the most recent version of the file required on the server.
Registered	Displays whether a required file should have a Windows registry entry. True indicates that the file should be registered, and false indicates that the file should not be registered.

Related topics:

[Verifying installation results](#) on page 53

Blocking Web Client user logins

1. Go to **Maintenance > Web Server Control** .
2. On the Web Server Control page, specify the time period (in days, hours, and minutes) for which you want to block user logins.
3. Click **Block Logins** to block future logins for the specified interval.



Note:

If you want to unblock logins before the specified time period expires, access this page again, and click **Clear Blocking**.

Related topics:

[Web Client maintenance tools and tests](#) on page 47

[Web Server Control page field descriptions](#) on page 55

Resetting the Web Client server

Go to **Maintenance > Web Server Control** , and click **Reset Web Server** to immediately log off all users.

Related topics:

[Web Client maintenance tools and tests](#) on page 47

[Web Server Control page field descriptions](#) on page 55

Unblocking Web Client user logins

Go to **Maintenance > Web Server Control** , and click **Clear Blocking** to allow users to log on to Web Client.

Related topics:

[Web Client maintenance tools and tests](#) on page 47

[Web Server Control page field descriptions](#) on page 55

Web Server Control page field descriptions

Use the Web Server Control tool to shut down the Web server, reset the Web server, and block new users from logging in for a specified time.

Name	Description
Block New Logins For/Days	Specify the number of days for which you want to block user logins. Leaving the value of this field at 0 indicates the current day.
Block New Logins For/Hours	Specify the number of hours for which you want to block user logins.
Block New Logins For/Minutes	Specify the number of minutes for which you want to block user logins.

Related topics:

[Blocking Web Client user logins](#) on page 54

[Resetting the Web Client server](#) on page 54

[Unblocking Web Client user logins](#) on page 55

Using the Services Log page

Use the Services Log page to record maintenance activity.

-
1. Go to **Maintenance > Services Log** .
 2. On the Services Log page, enter any information about service or maintenance activities in the text box.
 3. Click **Submit Comments to the Log** to save the entered comments to the `wmService.log` file in the Data directory.
-

Related topics:

[Web Client maintenance tools and tests](#) on page 47

[Web Client maintenance tools and tests](#) on page 47

Chapter 11: Viewing statistics

Web Client statistic types

You can view the following Web Client statistics.

Login statistics: Log-in statistics include data about user log-in activities during specific time periods. This data helps identify trends, such as peak usage times.

Data transfer statistics: Data transfer statistics provide data about the messages sent and received by Web Client.

Message event statistics: Message event statistics provide data about the types of messaging events performed by Web Client users.

Related topics:

[Viewing log-in statistics](#) on page 57

[Login Statistics page field descriptions](#) on page 58

[Viewing data transfer statistics](#) on page 58

[Data Transfer Statistics page field descriptions](#) on page 59

[Viewing message event statistics](#) on page 58

[Message Event Statistics page field descriptions](#) on page 61

Viewing log-in statistics

1. Go to **System Usage > Login Statistics** .
2. On the Login Statistics page, use the display options to specify how you want to view the data.
3. Click **Display Data**.

Related topics:

[Web Client statistic types](#) on page 57

[Login Statistics page field descriptions](#) on page 58

Viewing data transfer statistics

-
1. Go to **System Usage > Data Transfer Statistics** .
 2. On the Data Transfer Statistics page, use the display options to specify how you want to view the data.
 3. Click **Display Data**.
When you exit the Data Transfer Statistics page, the system restores the default display options.

Related topics:

[Web Client statistic types](#) on page 57

[Data Transfer Statistics page field descriptions](#) on page 59

Viewing message event statistics

-
1. Go to **System Usage > Message Event Statistics** .
 2. On the Message Event Statistics page, use the display options to specify how you want to view the data.
 3. Click **Display Data**.

Related topics:

[Web Client statistic types](#) on page 57

[Message Event Statistics page field descriptions](#) on page 61

Login Statistics page field descriptions

The Login Statistics page displays data about user log-in activities during specific periods of time. Information provided on this page helps in identifying certain trends, such as peak times,

for these log-in activities. When you exit the Login Statistics page, the system restores the default display options.

Name	Description
View	Specify the format in which you want to display the data: <ul style="list-style-type: none"> • Graph: Displays the data in a graph format • Raw: Displays the data in a tabular format
Data	Specify how you want to display the data: <ul style="list-style-type: none"> • New Logins: Displays only the new logins during the specified period • Peak Concurrent Logins: Displays the maximum simultaneous logins over the specified period <p>For example, assume that no users are logged in to the system. One user logs in at 1 p.m. and uses the system until 3 p.m. If you display New Logins, the data displays a single new login at 1 p.m. If you display Peak Concurrent Logins, the data displays one concurrent login at 1 p.m., 2 p.m., and 3 p.m.</p>
Statistics	Specify the time period for which you want to view log-in data: <ul style="list-style-type: none"> • Hourly Statistics For: Displays the log-in data for a selected date • Hourly Averages for the Last 30 Days: Displays the hourly average logins each day for the last 30 days, for the selected log-in type • Daily Totals for the Last 30 Days: Displays the total log-in data for each day for the last 30 days, for the selected log-in type

Related topics:

[Web Client statistic types](#) on page 57

[Viewing log-in statistics](#) on page 57

Data Transfer Statistics page field descriptions

The Data Transfer Statistics page provides statistical data about the ways in which Web Client sends and receives messages.

Name	Description
View	Specify the format in which you want to display the data: <ul style="list-style-type: none"> • Graph: Displays the data in a graph format • Raw: Displays the data in a tabular format

Name	Description
Message Type	Specify the message type for which you want to view data: <ul style="list-style-type: none"> • Voice: Displays voice message data • Fax: Displays fax message data • Text: Displays text message data • Attachment: Displays message attachment data
Transfer Type	Specify the transfer data you want to view: <ul style="list-style-type: none"> • Files Downloaded: Displays the number of files of the selected message type downloaded from the message server (through the Web Client server) to the client • Files Uploaded: Displays the number of files of the selected message type uploaded from the client to the message server (through the Web Client server) • Size Downloaded: Displays the amount of message data (in kilobytes [KB]) downloaded from the message server (through the Web Client server) to the client • Size Uploaded: Displays the amount of message data (in KB) uploaded from the client to the message server (through the Web Client server)
Statistics	Specify the time period for which you want to view data: <ul style="list-style-type: none"> • Hourly Statistics For: Displays the data for a selected date • Hourly Averages for the Last 30 Days: Displays the hourly average for each day for the last 30 days, for the selected data type • Daily Totals for the Last 30 Days: Displays the total transfer data for each day for the last 30 days, for the selected data type

Related topics:

[Web Client statistic types](#) on page 57

[Viewing data transfer statistics](#) on page 58

Message Event Statistics page field descriptions

The Message Event Statistics page indicates the type of messaging events that are performed by Web Client users.

Name	Description
View	Specify the format in which you want to display the data: <ul style="list-style-type: none"> • Graph: Displays the data in a graph format • Raw: Displays the data in a tabular format
Data	Specify the type of message event for which you want to view data: <ul style="list-style-type: none"> • Play Voice Events: Displays data about how often users display voice messages • Record Voice Events: Displays data about how often users record voice messages • Send Message Events: Displays data about how often users send messages • Delete Message Events: Displays data about how often users delete messages • Outcall Events: Displays data about how often outcall events, for example message playback through the telephone, occur
Statistics	Specify the time period for which you want to view data: <ul style="list-style-type: none"> • Hourly Statistics For: Displays the data for a selected date • Hourly Averages for the Last 30 Days: Displays the hourly average for each day for the last 30 days, for the selected data type • Daily Totals for the Last 30 Days: Displays the total data for each day for the last 30 days, for the selected data type

Related topics:

[Web Client statistic types](#) on page 57

[Viewing message event statistics](#) on page 58

Viewing statistics

Chapter 12: Send us your comments

Avaya appreciates any comments or suggestions that you might have about this product documentation. Send your comments to the [Avaya documentation team](#).

Send us your comments

Index

A

adding	
LDAP server	25
message server	9
syslog server	15
Administration History log	
description	45
administration history, viewing	45
administrator login ID, changing	17
administrator password, changing	17
alternate English, setting	37
attachment type search, enabling	36

B

backing up Web Client settings	43
blind carbon copies, enabling for messages	32
blocking user logins	54

C

callback number hint	
creating	38
carbon copies, enabling for messages	32
changing	
administrator login ID	17
administrator password	17
test schedule	50
creating	
callback number hint	38
creating message of the day	38
customizing corporate logo	29

D

Data Transfer Statistics field descriptions	59
deleting	
LDAP server	26
message server from Web Client	10
syslog server from Web Client	15
users	19
downloading server certificate	11

E

email recipients, enabling	34
enabling	
a	31

attachment type search	36
blind carbon copies for messages	32
carbon copies for messages	32
email recipients	34
message attachments	34
message copy and paste	35
message notification	31
message subject creation	33
message subject line editing	31
message text	33
reply to all	36
search by attachment type	36
voice player	37
executable scripts, enabling	31

I

inactive servers, timeout	29
installation results, verifying	53

L

LDAP	
adding server	25
deleting server	26
LDAP Administration field descriptions	26
modifying LDAP server profile	25
legal notices	2
Login Statistics	
field descriptions	59
logo, customizing	29
logs	
Administration History	45

M

message attachments, enabling	34
message copy and paste, enabling	35
message event statistics	
field descriptions	61
message notification, enabling	31
message of the day, creating	38
message purge, setting	35
message servers	
adding	9
deleting from Web Client	10
field descriptions	11
modifying	10
message subject creation, enabling	33

Index

message subject line editing, enabling	31
message text, enabling	33
modifying	
LDAP server profile	25
message server	10

N

notices, legal	2
----------------------	-------------------

O

Options and Settings field descriptions	39
---	--------------------

P

password	
Change Password field descriptions	18
changing administrator	17
Ping test	52

R

reboots, scheduling	50
recording maintenance activities	56
removing user restrictions	22
reply to all, enabling	36
resetting Web Client server	54
restoring Web Client settings	43
restricted users, viewing list of	20
restricting users	20 , 23
Restricted User Mailbox field descriptions	23

S

Schedule Maintenance field descriptions	50
scheduling server reboots	50
scheduling tests	49
server certification, downloading	11
services log, updating	56
setting	
alternate English	37
message purge	35
statistics	57–59 , 61
data transfer	59
login statistics	59
types of statistics	57
viewing data transfer statistics	58
viewing log-in statistics	57
viewing message event statistics	58
syslog servers	
adding	15
deleting from Web Client	15

T

testing connectivity to desktop clients	52
tests	
changing schedule	50
overview of tools and tests	47
Ping test	52
Schedule Maintenance field descriptions	50
scheduling	49
Verify Installation	53
Web Client, message server connection	52
timeout for inactive servers	29
tools	
overview of tools and tests	47
Web Server Control Tool	55

U

unblocking user logins	55
updating restricted user list	21
updating user access list	20
User List field descriptions	22
user logins	
blocking	54
unblocking	55
users	
deleting	19
removing restrictions	22
restricting	20
unblocking logins	55
updating restricted list	21
updating user access list	20
User List field descriptions	22
viewing list of	19
viewing list of restricted users	20

V

verifying installation results	53
viewing	
administration history	45
data transfer statistics	58
login statistics	57
message event statistics	58
restricted user list	20
user list	19
voice player	
enabling	37

W

Web Client server, resetting	54
------------------------------------	--------------------

Web Client URL, adding[30](#) Web Server Control field descriptions[55](#)

