Quest

Quest® MessageStats®for Outlook® Web Access (OWA) 7.6

User Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal.

Trademarks

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. Microsoft, Active Directory, ActiveSync, Excel, Lync, and Skype are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

MessageStats Report Pack for OWA User Guide
Updated - October 2019
Software Version - 7.6

Contents

1

MessageStats Report Pack for OWA Overview

About the Report Pack for Outlook Web Access (OWA)

Microsoft Outlook Web Access (OWA) is a webmail service for Microsoft Exchange Server that provides remote access to emails that are stored in an Exchange server and accessed through a web browser. In Exchange 2010 and later, the service is called Outlook Web App (OWA).

The MessageStats Report Pack for OWA provides webmail-specific reports that are integrated into the core MessageStats Reports interface. The report pack allows you to gather information about OWA logons and service delivery in large-scale Exchange organizations.

Architecture

The MessageStats Report Pack for OWA analyzes the servers in your Exchange organization and automatically discovers Outlook Web Access objects. The report pack locates and processes the IIS log files that contain information about these objects and writes the processed data to the MessageStats database. This information covers activity concerning the organization's Outlook Web Access.

In addition, the MessageStats Report Pack for OWA can gather log files from an archive on the local server or from a system-wide archive location, so you can gather information from archived log files that may no longer reside on the original production Exchange Server that generated the log files.

Report Pack Components

The MessageStats Report Pack for OWA contains the following component:

- Task Processors: Includes the IIS Logs Files gathering task which is shared between the Exchange ActiveSync and the OWA report pack. The OWA Task Processor must be installed on a server on which the MessageStats task processors reside.

Additionally, when you install the report pack, the installer extends the following core MessageStats components:

- MMC Client Console: The console is extended to allow you to create and manage the IIS Log Files gathering task, as well as to configure additional paths to the IIS log file repository.
- Database: The report pack extends the existing MessageStats SQL database by adding new tables and fields to store the data regarding OWA activity. The OWA Database Schema is installed on the server on which the MessageStats Database resides.
- Reports: The OWA reports are installed on the IIS server on which MessageStats Reports are installed.

Steps to Install and Configure the Report Pack

Before you can run the Report Pack for Outlook Web Access (OWA), you must perform the following functions in the following order:

1. Ensure that you meet the system requirements for the report pack.
2. Configure IIS Logging on your Exchange servers (see Configuring IIS Logging on the Exchange Server on page 8).
3. Install the Report Pack for OWA (see Installing the Report Pack for OWA on page 9).
4. Assign the OWA role to servers in the MessageStats console (see Assigning the OWA Server Role on page 10).
5. Create the OWA report pack gathering tasks (see Creating the IIS Log Files Gathering Task on page 12).

2

Installing the OWA Report Pack

System Requirements

Before you install the report pack, verify that you meet the MessageStats hardware minimum requirements. You must also have the MessageStats core product installed before you can install the report pack. For information about the MessageStats hardware requirements, see the *MessageStats Release Notes.*

For information about MessageStats required permissions, see the *MessageStats Quick Start Guide*.

Software Requirements

You install the report pack components on servers on which the core MessageStats components are already installed. You must meet the software requirements for MessageStats. The following table contains any additional software requirements for the report pack:

Table 1. Software minimum requirements

Component	Minimum Requirement
Task Execution Server (where the report pack task processors are installed)	• Microsoft PowerShell 2.0. **NOTE:** You can download the Windows Management Framework (which includes PowerShell 2.0) from Microsoft at http://support.microsoft.com/kb/968929.
Additional Software	• MessageStats 7.6 or later • .NET Framework 4.7.2
Exchange Servers	At least one server running Exchange 2010, Exchange 2013, Exchange 2016, or Exchange 2019. You must install the IIS Management Scripts and Tools on the Exchange server. The IIS Management Scripts and Tools are required to allow the report pack to gather the IIS log files.

Rights and Permissions

This section lists the rights and permissions required to install the MessageStats Report Pack for OWA.

Installation Rights

The following rights are required to install the report pack:

- Local Administrator rights of the computer on which you are installing MessageStats

Operational Rights

The following rights are required to configure the report pack and to run gathering tasks:

- MessageStats Admin rights on the server that houses the MessageStats database
- Local Administrator rights on the task execution server
- Local Administrators rights on all Exchange OWA servers
- Be a member of View-Only Organization Management and Public Folder Management groups

Configuring IIS Logging on the Exchange Server

Before you can use the MessageStats Report Pack for OWA, you must configure IIS logging on the Exchange server that has the OWA role installed.

The report pack supports one IIS log per site and requires the following log file format:

- W3C Extended Log File Format (set by default)

You must configure the extended properties. The default IIS logging configuration for the W3C Extended Log File Format is not sufficient for the report pack to gather the information required for reports.

Use the IIS Manager to configure the W3C Extended Log File Format for IIS logging on the Exchange server from which you want to gather data.

To Configure IIS logging on the Exchange server

1. Click **Start** and select **Administrative Tools | Internet Information Services (IIS) Manager**.

   - OR -

   In the Server Manager, select the **Web Server (IIS)** and open the **Internet Information Services (IIS) Manager**.
2. On the left, open the dropdown menu under the Start Page option.
3. Select the default Web Site.
4. Double-click **Logging**.
5. Under the One log file per: heading, ensure that **Site** is selected.
6. Set the Format to **W3C** and click **Select Fields**.
7. In the W3C Logging Fields dialog box, select the following options:
   - Date
   - Time

- Client IP Address (c-ip)
- User Name (cs-username)
- Method (cs-method)
- URI Stem (cs-uri-stem)
- URI Query (cs-uri-query)
- Protocol Status (sc-status)
- User Agent (cs(User-Agent))
- Cookie (cs(Cookie))
- Referer (cs(Referer))

8 Click **OK**.

For IIS 7 and later, the report pack supports all of the IIS log schedule options with the exception of the “Unlimited file size” option.

Installing the Report Pack for OWA

To install MessageStats Report Pack for OWA

1 Log on to your system using MessageStats service account.

2 Double-click the **autorun.exe** file and select the **Install** tab.

3 Select the **Outlook Web Access** link.

4 Read the license agreement and select the **I accept the terms in the license agreement** check box and click **Next.**

5 Select the features that you want to install and click **Next**.

6 Verify the folder in which the report pack is to be installed and click **Next**.

7 Verify the SQL instance (MessageStats database) on which you are installing the report pack database components and click **Next**.

8 Click **Next** to begin the installation.

9 When the installation is complete, click **Finish**.

3

Configuring the OWA Report Pack and Gathering Data

Assigning the OWA Server Role

Before you gather information from your Exchange OWA servers, you must assign each server the OWA server role in MessageStats.

In Microsoft Exchange, server roles identify the services that the server provides. Since the OWA reports provide information about activity on an Exchange OWA server, you must assign the OWA server role to identify your Exchange OWA servers.

To assign the OWA server role

1. In the MessageStats console treeview, expand the **Exchange Organizations** node and select an organization.
2. Expand the **Servers** node and right-click an Exchange OWA server.
3. Select **Properties**.
4. Select the **Server Roles** tab and click **Add**.
5. Select **OWA** from the list and click **OK**.

Discovered Roles and Assigned Roles

MessageStats retrieves the server role for the server from Active Directory and assigns the same server role in MessageStats. The server role is displayed in the Discovered Server Roles box. You cannot remove the server role value for a “discovered” server role.

You can add additional server roles to any Exchange server. You can remove a server role if the role is identified as being assigned.

Table 1. Available pre-defined server roles.

Predefined Exchange Server Roles	
Front End	Back End
OWA	Bridgehead
Public Folder	Client Access

Table 1. Available pre-defined server roles.

Predefined Exchange Server Roles	
Mailbox	Unified Messaging
Edge Transport	Hub Transport

To remove the OWA Server Role

1. From the MessageStats console, right-click an OWA Exchange server in the treeview and select **Properties**.
2. Select the **Server Roles** tab.
3. Select **OWA** from the list and click **Remove**.
4. Click **OK**.

Specifying an Alternate Location for IIS Log Files

In some situations, you may have custom-configured the location of the IIS log files on your Exchange IIS servers. You can use the IIS Log Folders property tab to indicate any alternate locations for the IIS log files.

To configure additional locations for the IIS log files

1. Expand the **Exchange Organizations** node, expand the Exchange organization you want, and select **Servers**.
2. Right-click the OWA Exchange server and select **Properties**.
3. Select the **IIS Log Folders** tab.
4. Click **Add** to add an IIS Log Folder.
5. Select an IIS Server Instance and enter or browse to the path where the log files are located.
6. Click **Apply**, then click **OK**.

To edit an IIS log file location

1. Select an existing IIS log file path and click **Edit**.
2. Enter or browse to the new path where the IIS log files for the server are located.
3. Click **OK**.

Gathering Information from IIS Log Files

MessageStats gathers information for reports through gathering tasks. Tasks specify which information is gathered and how often the gathering is repeated. To gather the data required for the MessageStats Report Pack for OWA, you must create an IIS Log Files/ OWA gathering task.

To populate the MessageStats Database with historical data, you should schedule a daily recurring IIS Log File gathering task. It is recommended that an IIS Log Files gathering task be run every 24 hours. You can schedule the gathering task to run any time you want. You may want to run the task at off-peak times.

If the Exchange IIS Log Files Are Not Scheduled Daily

Most Exchange servers are set to use the default W3C Extended Log File Format daily schedule for IIS log files. However, if you set the IIS log schedule to be weekly, monthly, or unlimited file size, you may notice that the IIS Log Files gathering task collects more data than the date range you specified.

For example, if you select a gathering date range to be a subset of the date range you set for your IIS log file schedule, the report pack gathers OWA statistics from the entire IIS log file, writes the data to the database, and reports on it.

If the MessageStats Report Pack for Exchange ActiveSync is also Installed

The MessageStats Report Pack for Exchange ActiveSync (previously Windows Mobile) also uses the information that is gathered by the IIS Log Files gathering task. If you have scheduled the Exchange ActiveSync Default Gathering task (which includes the IIS Log Files task) to run regularly, you do not need to schedule the IIS Log Files gathering task to run separately for the OWA report pack.

MessageStats Task Dependencies

The tasks that gather Outlook Web Access data have dependencies on data that is gathered by core MessageStats gatherings. To correctly populate the OWA reports, these core gathering tasks must be run in the following order:

1 Exchange Mailbox

2 Mailbox Account Properties

There is also one OWA report pack gathering tasks that must be run after the core tasks complete successfully:

3 IIS Log Files/ OWA

If you run a core MessageStats Default Gathering task on a regular schedule, the Default Gathering task includes the Exchange Mailbox and Mailbox Account Properties gathering tasks in the correct order.

Creating the IIS Log Files Gathering Task

To populate the OWA reports, you must create and run an IIS Log Files gathering task. You can create an IIS Log File gathering task at the Exchange organization level or at the Exchange server level.

The IIS Log Files gathering collects IIS log files from the Client Access Servers (CAS) for Exchange 2010 and 2013, and from the Exchange Mailbox server for Exchange 2016 and 2019.

If you have only the OWA report pack installed, it is recommended that you create a region that contains these servers and run the task against the region.

If Both OWA and Exchange ActiveSync Report Packs are Installed

The MessageStats Report Pack for Exchange ActiveSync also uses the information that is gathered by the IIS Log Files gathering task. If you have scheduled the Exchange ActiveSync Default Gathering task, which includes the IIS Log Files task, to run regularly, you do not need to schedule the IIS Log Files gathering task to run separately for the OWA report pack.

For Exchange 2013, if you have both the Exchange ActiveSync and the OWA report packs installed, you must collect from both Exchange CAS and Mailbox servers to ensure the ActiveSync data is complete. For Exchange 2016 or 2019, you must collect from the Exchange Mailbox server.

Prerequisites

Before you create an IIS Log Files gathering task, ensure that the MessageStats Default Gathering task for the organization has completed successfully.

If you have not already done so, assign the OWA server role to the appropriate OWA servers in the MessageStats console. For more information, see Assigning the OWA Server Role on page 10.

If your OWA Exchange server is protected by firewall software from the internal network that includes the MessageStats server, you may need to open certain ports on your firewall and modify the RPC configuration on your Exchange server to grant MessageStats access to the server. See Appendix B: Configuring RPC Through a Firewall on page 24.

To create an IIS Log Files gathering task

1. Expand the **Exchange Organizations** node and select the Exchange organization you want.
2. Right-click and select **Create Task**.
3. Enter a name for the task (for example, OWA Daily Task), select **IIS Log Files/ OWA** as the task template, and click **Next**.
4. Select **Most Recent** as the date range to indicate the last number of days from which to gather the IIS log files and click **Next**.

   In some situations, you can choose the Custom option if you want to select a specific date range to indicate the time frame from which to gather log files.
5. Review or change the default task execution server and click **Next**.
6. Clear the **Use Default Configuration** check box, specify a schedule for the gathering task and click **Next**.

   MessageStats provides two types of schedules: schedules that run once (at specific times such as December 31 or Now), and schedules that repeat for a defined period (such as daily, weekly, or monthly).
7. Verify the logging level for the task log files and click **Next**.
8. Specify the account under which the gathering task is to run, and click **Next**.

   You can accept the default account that is displayed for Task Credentials or clear the Use Default Configuration check box to enter a different account.
9. Click **Finish** to save the gathering task.

To change the properties of an existing task

1. Browse the tasks in the Tasks Summary View.
2. Right-click the task you want to configure and select **Properties**.
3. Step through the wizard to change the settings.

4

Managing Your Database

About Database Management

During the installation of the MessageStats Report Pack for OWA, additional tables are added to the MessageStats database to store OWA-specific data. MessageStats allows you to manage the storage of OWA data.

In MessageStats, the database management functionality is extended to include database management functions specific to OWA data. Using Database Management, you can delete obsolete information and fine-tune your database.

The Database Management tool provides the following functionality:

- Database Aging. Use this to delete historical data.
- Database Maintenance. Use this to defragment your database and reindex database tables.
- Delete Data. Use this to delete object and report data.

IMPORTANT: Before you modify your database, ensure that no MessageStats consoles or task processors are currently writing information to the database. If you use Database Management while a MessageStats console is writing to the database, you risk corrupting your database.

For detailed information about using the Database Management tool, see the *MessageStats Administrator Guide*.

Configuring an OWA Aging Task

You can use the Data Aging function to delete the historical data from the OWA tables in the MessageStats database. Use the Outlook Web Access Configuration option under the Data Aging node to define a regularly scheduled task that deletes old data.

To define a data aging task

1. Expand the **Database Management | Data Aging** nodes in the treeview.
2. Click the **Outlook Web Access Configuration** node.
3. Select **Delete aged data**.
4. Select the **Age Statistics** check box and select the age (in number of days) at which data is to be deleted.
5. Select a Schedule Type (daily, weekly, or monthly) to indicate how often you want to delete the data.
6. Enter the Start Date and Start Time information.
7. Select the **Limit Job Execution Time** check box if you want to limit the time duration for an aging job, and enter an end time.
8. Enter the recurrence interval:

- Number of days between jobs for Daily schedules
- Day of the week for Weekly schedules.
- Day of the month for Monthly schedules.

9 Click **Deploy**.

Data Aging Job History

After you create an aging job, the interface changes to a three-tab format:

- The Schedule tab contains the same content as the Create Job tab contained before a job was created.
- The Properties tab describes the properties associated with the aging job, and is updated as new information becomes available.
- The History tab contains a log of past aging jobs.

Deleting OWA Report Data

You can use the Delete Data node to delete OWA-specific report data from the MessageStats database.

To delete OWA report data from the database

1 Expand the **Database Management | Delete Data** nodes in the treeview.

2 Click the **Outlook Web Access Report Data** node.

3 Select the **Servers** check box and select a server for the statistical data that you want to delete.

4 Click **Get Range** to select the date range for the data you want to delete.

5 Indicate the date range for the information you want to delete.

6 Click **Delete Data**.

7 Verify that you want to delete the data.

5

Using Outlook Web Access (OWA) Reports

Introducing OWA Reports

The MessageStats Report Pack for OWA reports are a collection of OWA-specific reports that are accessible from the MessageStats web-based reports console.

You must run an IIS Log Files gathering task for the reports to be populated.

The following features are included in MessageStats reports:

- The Web Report Wizard that allows you to configure and generate reports, and provides report parts that you can add to and arrange on reports.
- The Graph Wizard allows you to create custom graphs from the data sources that you select.
- Predefined role-based security settings allow you to control who can view reports and create custom reports.
- A subscription service allows you to deliver reports through email, web sites, file shares, or ftp (file transfer protocol) site.
- Tooltips that display when you hover over column headings or over items in graphs can reveal detailed information.

Using the console, you can perform the following tasks:

- Group, insert, append, remove, and sort fields on reports. Quick Filters allow you to change report parameters quickly and easily to focus your report.
- Display report data in bar graphs, line graphs, and pie charts.
- Export or email entire reports in Microsoft Excel, text (as either comma-separated values or tab-separated values), XML, as a Word file, in HTML, or MHTML.
- Select portions of reports, such as columns or rows, and export the selections or send by email. You can also select a graph or chart to export it or send it by email.

For more information about how to use these features, refer to the *MessageStats Reports User Guide* and *MessageStats Administrator Guid*e.

Viewing the OWA Reports

On gathering completion, you can view reports based on the gathered information using the web-based MessageStats Reports component.

To access the OWA reports

1 Click **Start | Programs | Quest | MessageStats | MessageStats Reports.**

- OR -

From the treeview in the MessageStats Console, select **MessageStats Reports**.

- OR -

Open the web site where the MessageStats Reports reside using Internet Explorer.

2 In the reports treeview, select **Report Packs** | **Outlook Web Access**.

3 Select the report that you want to view.

4 Select the report filters, if required, and click **Apply Filter** to view the report.

NOTE: MessageStats reports can only be viewed using Internet Explorer (version 9 or later) browser.

OWA Report Descriptions

OWA Reports display successful and unsuccessful OWA logons. However, MessageStats can only report unsuccessful OWA logons that are detected by the Exchange CAS or Mailbox server.

If you use a component in your environment that performs authentication before logons reach the Exchange server, unsuccessful logons will not be reported. Internet Security and Acceleration (ISA) servers and the Forefront Threat Management Gateway are examples of such components.

The following table describes the reports found in MessageStats Report Pack for OWA:

Table 1. OWA User Logon reports.

Reports	Description	Filters
Logons by User Account	Lists the user accounts that performed OWA logons and shows the number of successful or unsuccessful logons performed.	• Date • Detail Level • Display Options • Trend and Forecast Options • Logon Result • User Account • Organization
Logons by Mailbox	Lists the mailboxes that were accessed using OWA and the number of times they were accessed, successfully or unsuccessfully. **NOTE:** The report will be empty unless the Exchange Mailboxes and the Mailbox Account Properties gathering tasks have run successfully. For more information, see the *MessageStats Administrator's Guide.*	• Date • Detail Level • Display Options • Trend and Forecast Options • Logon Result • Display Name • Organization

Table 1. OWA User Logon reports.

Reports	Description	Filters
Logons by Source IP	Displays the IP addresses of hosts from which users performed OWA logons and the number of successful or unsuccessful logons performed.	• Date • Detail Level • Display Options • Trend and Forecast Options • Logon Result • IP Address • Organization
Logons by Server	Lists the number of times users have logged onto their mailboxes using OWA during the time period specified in the report filter,.	• Date • Detail Level • Display Options • Trend and Forecast Options • Logon Result • Server • Organization
Logons by Department	Lists the departments of mailboxes that were accessed using OWA and the number of times those mailboxes were accessed. **NOTE:** The report will be empty unless the Exchange Mailboxes and the Mailbox Account Properties gathering tasks have run successfully. For more information, see the *MessageStats Administrator's Guide.*	• Date • Detail Level • Display Options • Trend and Forecast Options • Logon Result • Department • Organization
Logons by Virtual Directory/Web Site	Lists the virtual directories and web sites that handled OWA logons.	• Date • Detail Level • Display Options • Trend and Forecast Options • Logon Result • Server • Web Site • Virtual Directory • Organization

Table 1. OWA User Logon reports.

Reports	Description	Filters
Logons by Internet Browser and Version	Lists the names and versions of internet browsers that were used to perform OWA logons.	• Date • Detail Level • Display Options • Trend and Forecast Options • Logon Result • Internet Browser • Internet Browser Version • Organization
Server Uptime	Identifies which Exchange servers and associated services were available and running on the network for a full day, and also identifies the ones that were not available. For each date, the report lists the specific server, and whether the server was available for the duration of that day. By default, this report includes only Exchange servers that have been assigned the OWA server role.	• Date • Server • Server Roles • Region • Organization

Report Filter Definitions

The Report Filter glossary provides information about the various filter settings that you can use to define the information that appears in reports.

D

Date

Restricts the report content to the date range that you specify.

Date/Time Display

Used to determine whether you want date and time data to appear in UTC or local server time.

Department

Restricts the report content to the business department that you specify.

Note: Ensure that the Department attribute is defined for each mailbox account. If the attribute is not defined, null or blank record sets appear in the report and aggregated departmental information may not be accurate. The Department attribute must be defined using Microsoft Exchange.

Detail Level

Restricts the report content to the detail level that you selected:
Summary includes only the aggregated data.
Daily shows the detailed records grouped by day.
Hourly shows the detailed records grouped hourly.

Display Name

Restricts the report content to the Display Name that you specify.

Display Options

Display Options define the components you want to include on the report:

Data and Graph presents a graph at the top of the report followed by a corresponding data table.

Data Only presents data table and suppresses the graph view.

Graph Only presents a graph and suppresses the corresponding data table.

I

Internet Browser

Restricts report content to specific types of internet browsers used to access mailboxes through Outlook Web Access (OWA). Examples include Internet Explorer, Mozilla, Firefox, and so on.

Internet Browser Version

Limits the report content to the specified internet browser versions in reports about the browsers used to access mailboxes through OWA.

IP Address

Allows you to select the IP addresses from which users logged into the mailboxes through OWA.

L

Logon Result

The logon result is based on the user logons that are recorded in the IIS logs of the web site that is hosting OWA.

Successful Logons
Restricts the report content to successful logons to a mailbox through OWA. A successful logon occurs when a person or an entity (such as Internet Explorer itself) sends credentials in response to an authentication request from IIS, and IIS accepts those credentials.

Unsuccessful Logons
Restricts the report content to unsuccessful logons to a mailbox through OWA. An unsuccessful logon occurs when the credentials that are sent are not approved by the server.

O

Organization
Restricts the report content to the Exchange organization that you specify.

R

Region
Restricts the report content to the region that you specify.
Note: Regions must be defined in the MessageStats Console. For information about regions, please see the *MessageStats Administrator Guide*.

S

Server
Restricts the report content to the servers you specify.

Server Roles
Restricts the report content to the server roles you specify. By selecting a Server role filter, you can ensure that the reports contain comparable servers or comparable data. The report content is not skewed by a single server that is not comparable to other servers.
Note: You must manually identify server roles in the MessageStats Console using the Server Roles tab of the Server Properties dialog box. For more information, please see the *MessageStats Administrator Guide*.

T

Trend and Forecast Options
Indicate your graph display preference for the report.
Display Neither suppresses both trend lines and forecasts.
Trend Only includes trend lines, but not forecasts.
Trend and Forecast includes both trend lines and forecasts.

U

User Account
Restricts the report content to the Outlook Web Access logons that used the user accounts that you specify.

V

Virtual Directory
Restricts the report content to the Outlook Web Access logons that were handled by the virtual directories that you specify.

W

Web Site
Restricts the report content to the Outlook Web Access logons that were handled by the web sites that you specify.

Appendix A: Types of Installations

Complete Installations

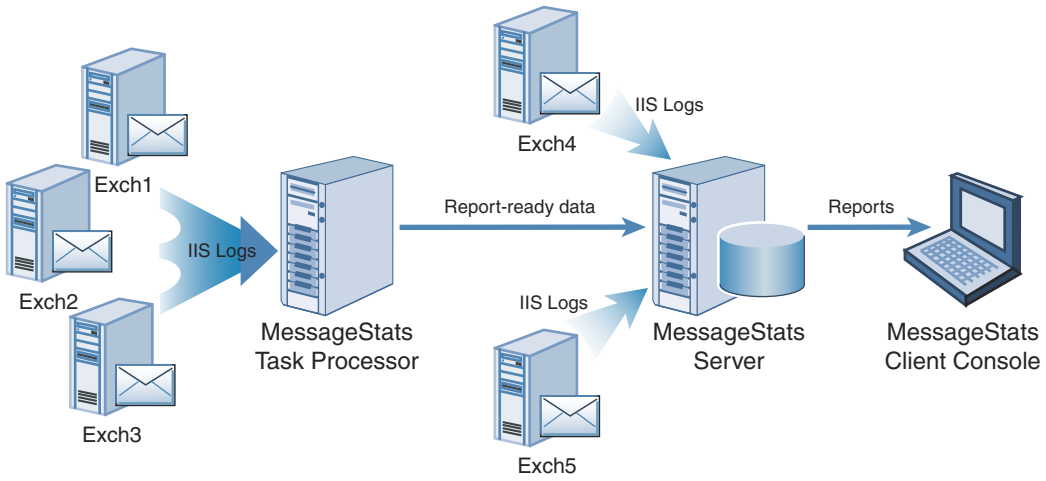
In a typical environment, all of the MessageStats components (or features) are installed on the same physical server using a complete installation. This type of installation is recommended for small enterprises.

Before installing the MessageStats Report Pack for OWA components, ensure that the review the minimum requirements and ensure they are met:

- All MessageStats Report Pack for OWA minimum requirements are met. See System Requirements on page 7.
- All the MessageStats Report Pack for OWA rights and permission requirements are granted to the appropriate accounts. See Rights and Permissions on page 8.
- IIS logging is properly configured. See Configuring IIS Logging on the Exchange Server on page 8.

Custom Installations

In some large enterprises, Database and Web Servers may be managed by a central resource. In order to install MessageStats in these environments, you can distribute the components onto appropriate machines using a Custom Installation. The most common scenario is to use a separate MessageStats Server and additional Task Processor servers.



In this type of deployment, data from the remote Exchange servers is processed by the local task processor. Then the report-ready data is transferred to the MessageStats Server and stored in the database. This minimizes network traffic by eliminating the need to copy all the data from the remote servers.

The MMC Client Console is installed on a MessageStats administrator's workstation or laptop. The administrator can create tasks and view log files, but task scheduling and gathering are carried out at another location with more robust resources.

To install the Report Pack for OWA onto an existing distributed MessageStats environment, use a Custom installation and install according to the following table.

Table 1. Distributed installation location of components

Core MessageStats Components	Report Pack Components	Function
MMC Client Console	OWA MMC Client Console	Adds the OWA components to the existing MessageStats MMC client console
Scheduler Service/Task Processors	OWA Task Processors	Adds the OWA task processor to the existing MessageStats Task Execution Server
Database	OWA Database	Extends the existing MessageStats database schema in order to store OWA Statistics
Reports	OWA Reports	Adds the OWA Reports to the existing MessageStats Reports site

B

Appendix B: Configuring RPC Through a Firewall

Configuring RPC Through a Firewall

To configure MessageStats to gather OWA data from an Exchange server, the console must be able to enumerate the IIS virtual directories on the Exchange server. This is done by making Remote Procedure Calls (RPC) to the IIS Management API on the server.

If your OWA Exchange server is protected by firewall software from the internal network that includes the MessageStats server, you may need to perform some RPC configuration on your Exchange server. You may also need to open certain ports on your firewall to grant MessageStats access to the remote API.

This appendix provides a procedure that you can use to configure your OWA server and firewall. The procedure assumes that you are using a Microsoft ISA Server as your firewall software. If you are using another firewall solution, the concepts behind the procedure are still valid.

IMPORTANT: This procedure requires that you manually edit the contents of the Windows registry. Serious problems can occur if you modify the registry incorrectly using Registry Editor or using another method. These problems might require that you reinstall the operating system. Quest cannot guarantee that problems can be solved. Modify the registry at your own risk.

Be sure to back up the registry before you modify it. Ensure that you know how to restore the registry if a problem occurs. For information about how to back up, restore, and modify the registry, see the Microsoft knowledgebase..

There are two parts to the process:

- Configuring RPC
- Configuring the ISA Server

Configuring RPC for OWA Access

In a default Windows installation, RPC is configured to randomly assign server ports to any port above 1024. It is unwise to open every port over 1024.

The recommended procedure is to configure RPC to use a specific range of ports. Microsoft recommends using ports 5000 and up since ports less than 5000 may be reserved.

Microsoft also recommends that a minimum of 100 ports be opened. Therefore this example shows how to configure RPC on the OWA server to use ports 5000 to 5100.

Example: To configure RPC to use ports 5000 to 5100

1 Create the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Internet

2 Under the Internet key, add the following values:

- Ports (MULTI_SZ)
- PortsInternetAvailable (REG_SZ)
- UseInternetPorts (REG_SZ)

3 Set the new values as follows:

Table 1. Settings for the new key values

Name	Type	Value
Ports	MULTI_SZ	5000-5100
PortsInternetAvailable	REG_SZ	Y
UseInternetPorts	REG_SZ	Y

4 Reboot the OWA server.

Configuring the ISA Server

Once you have configured RPC to use a specific set of ports on the Exchange server, you must make those ports available to the MessageStats server. You do this by opening the required ports on the firewall.

In addition to opening the dynamically-assigned ports, you also must open port 135. Port 135 provides access to the RPC Endpoint Mapper. The port must be available for proper operation of RPC.

Opening the proper ports on an ISA server

1 Open the ISA Server Management console.

2 Select the Firewall Policy node for your OWA server.

3 Under the Action menu, select **New/Access Rule**.

4 Enter a name for your access rule (for example, MessageStats RPC).

5 Click **Next**.

6 Select the **Allow** option and click **Next**.

7 On the Protocols page, add the **RPC (all interfaces)** protocol.

Make sure you do not add the **RPC Server (all interfaces)** protocol.

8 Create a new protocol for the range of RPC ports to be used. Set the protocol properties as follows:

- Protocol Type - TCP
- Direction - Outbound
- Port Range - 5000 to 5100

9 Add the newly created protocol type and click **Next**.

10 In the Access Rule Sources page, add the **Internal** network.

- OR -

Define the MessageStats server as a network identity and add it.

11 Click **Next**.

12 In the Access Rule Destinations page, add the Exchange server.

- OR -

Add Local Host if the ISA Server software is installed on the Exchange server.

13 Click **Next**.

14 On the User Sets page, click **Next**.

15 Click **Finish** to close the wizard and create the access rule.

16 In the console, click **Apply** to apply your changes.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.

Index

S

T

V

W