Microsoft

Microsoft® Exchange Server

Messaging and Collaboration for Demanding Business Needs

Outlook Web Access Deployment and Troubleshooting Guide

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

1197

CONTENTS

Overview

Microsoft® Outlook™ Web Access for Microsoft® Exchange Server provides secure access to e-mail, personal calendar and group scheduling, and collaboration applications on Microsoft Exchange Server with only a Web browser. Microsoft's family of Outlook e-mail and collaboration clients effectively meets the needs of a broad range of users; Outlook Web Access is a good solution if you have the following type of users:

- **Roaming or remote access**. Users who are away from their personal computers, as well as users who share a computer can take advantage of Outlook Web Access to access their Microsoft Exchange Server information securely from any browser. Because Outlook Web Access does not download mail to the client, there is no risk of users accidentally copying messages to another user's hard disk drive.

- **UNIX clients and personal computers with hardware limitations**. Users running UNIX workstations or users whose personal computers lack the RAM or hard disk space for a more full-featured Outlook client, can use Outlook Web Access. Outlook Web Access is not intended to be a replacement for the full-featured Outlook messaging client for the 16-bit Windows® operating system or Macintosh computer.

- **Lowest common denominator cross-platform system**. Outlook Web Access can meet the needs of organizations that want to have identical clients on all platforms and require only simple, baseline e-mail, scheduling, and collaborative application functionality.

- **Extranet applications**. Corporations that want to deploy mail, discussion, or collaborative applications to vendors, suppliers, or customers can use Outlook Web Access to distribute these applications easily, inexpensively, and efficiently over the Internet.

Features

With Outlook Web Access, users can do the following:

- **Basic e-mail**. Address messages using Microsoft Exchange Server's global address book, send and receive file attachments and hyperlinks, set message priority, request delivery and read receipts, use hierarchical folders and the Outlook bar, and group and sort messages in a folder based on standard fields or conversation thread.

- **Basic calendar and group scheduling**. Create a one-time or recurring appointment in the personal calendar, access day and week views of the calendar, view free and busy times of multiple users and resources when you schedule a meeting, and automatically send and respond to meeting requests in e-mail.

- **Basic public folder access**. Access custom table views on public folders, or group and sort messages in a folder based on standard fields or conversation thread.

- **Collaboration applications**. Along with basic public folder support, develop custom forms for display in Outlook Web Access using the Microsoft® Visual InterDev™ development system.

Limitations

Although Outlook Web Access is a great solution for the preceding customer scenarios, it is not intended to satisfy advanced e-mail and collaboration requirements addressed by the other products in the Outlook client family. Outlook Web Access does not include the following advanced features:

- **General**. Offline use (users must connect to a Microsoft Exchange Server computer to view information); the user interface varies slightly from the rest of the Outlook client family, in which optimizations to work inside a Web browser are required.

- **E-mail**. Personal address book, spelling checker, send and receive rich text or HTML messages, auto-resolve addressees, Microsoft Exchange digital encryption or signature support, S/MIME support, replied and forwarded flags in list view, message flags and Inbox rules, three-pane view, drag to folder, search for messages, and WordMail and Microsoft® Office integration.

- **Calendar and group scheduling**. Monthly view and other customized views of the calendar, display discontinuous days side by side, appointment list views, view free and busy times, drag and drop to move an appointment, track acceptance of meeting attendees, all-day or multiple-day event, task lists and task management, and export to Timex DataLink Watch or other devices.

- **Public folder access**. Nontabular Outlook views, Outlook 97 forms.

- **Collaboration applications**. Outlook 97 forms, Microsoft Exchange digital encryption and signatures, synchronize local offline folders with server folders.

- **Server performance**. If the Web server hosting Outlook Web Access is on the same computer as Microsoft Exchange Server and Outlook Web Access is the client for all users, the number of users supported per Microsoft Exchange Server computer is reduced significantly. There are various options for running a Web server hosting Outlook Web Access on separate computers from Microsoft Exchange Server if no increase in the number of Microsoft Exchange Server computers is desired.

Active Server Components and Outlook Web Access Comparison Chart

Active Server Components (ASC): Component of the Web-based messaging client in Exchange Server 5.0

Outlook Web Access (OWA): Component of the Web-based messaging client in Exchange Server 5.5

E-mail Features	ASC 5.0	ASC 5.0 Sp1	OWA 5.5	OWA 5.5 Sp1
Message creation				
Receive rich text messages			X	X
Send attachments		X	X	X
Receive attachments		X	X	X
Hyperlinks	X	X	X	X
Set message importance	X	X	X	X
uest read or delivery receipt	X	X	X	X
Message addressing				
Access to global address list	X	X	X	X
Check names				X
Message folder viewing				
Sort by standard fields			X	X
Optionally view folder hierarchy in a pane			X	X
Outlook navigation bar			X	X
Message management				
Out of Office Assistant			X	X
Create folders on the server	X	X	X	X
Calendar				
Create a single appointment			X	X
Create recurring appointments			X	X
Day and week views of calendar			X	X
View free and busy time			X	X
Collaboration Applications/Other				
Custom HTML forms				X
Change Windows NT domain password				X
Access to personal contacts				X

Outlook Web Access Architecture

Outlook Web Access is implemented by a combination of Microsoft® Active Server Pages technology on the Web-server side and Java controls and scripts downloaded on demand to the user's Web browser.

Server Requirements

The following components are required for a successful installation of Outlook Web Access:

- Microsoft® Windows NT® 4.0

- Microsoft Windows NT 4.0 Service Pack 3 (SP3)

- Microsoft® Internet Information Server (IIS)
  Exchange 5.0 is supported *only* with IIS 3.0 (regardless of the service pack). You may be able to upgrade to IIS 4.0 if the Exchange 5.0/IIS 3.0 server is functioning correctly, but this configuration is not supported by Microsoft.
  Exchange 5.5 is supported with IIS 3.0 or IIS 4.0.

- Active Server Pages (ASP)
  ASP can be set up from the Windows NT 4.0 SP3 compact disc, or you can download SP3 and the ASP components from http://www.microsoft.com.

- Active Server Components or Outlook Web Access components
  The Active Server Components are included with Exchange Server 5.0. It is recommended that you install Exchange Server 5.0 SP1 or Exchange Server 5.5, because they include the enhanced Outlook Web Access components.

Client Requirements

You must have a compatible browser to connect to the Active Server Pages on the OWA server.

- Internet Explorer 3.02 with Rfc1867.exe installed to allow attachments (available from http://www.microsoft.com/ie)

- Internet Explorer 4.0 or later

- Third-party Internet browser software that supports frames, for example, Netscape Navigator.

Outlook Web Access (OWA) allows users to access their Exchange Server computer with only a Web browser. To give you a better idea of how this works, let's look at the following steps of an OWA client connecting:

1. A Web browser sends a request to a computer running Internet Information Server (IIS) with OWA components installed. This request includes a cookie from the Web browser that uniquely identifies the Web browser or user.

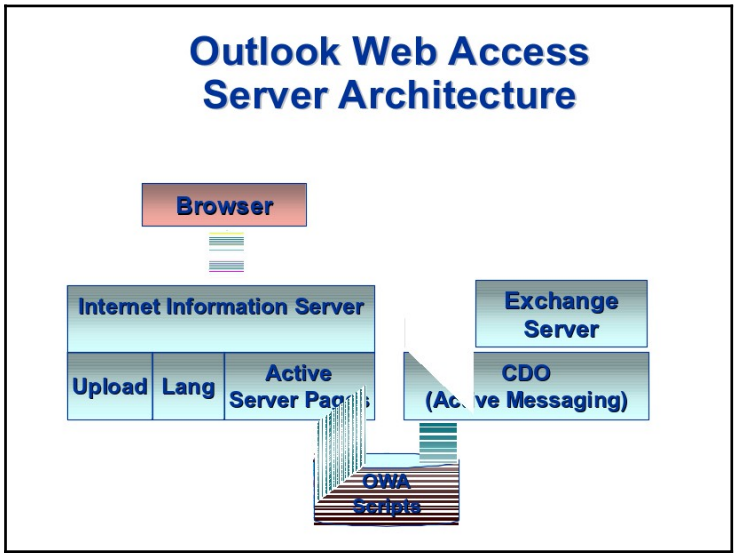
2. IIS forwards the request to Active Server Pages (ASP) for processing. ASP verifies that the cookie points to a valid ASP session, and that the user has already logged on. If not, the user is prompted to log on.

3. ASP opens the script file named in the URL and executes any server-side VBScript it contains. These scripts use Collaborative Data Objects (CDO) to open the message from the user's Exchange Server store. The message's globally unique identifier (GUID) is passed in on the query string of the URL.

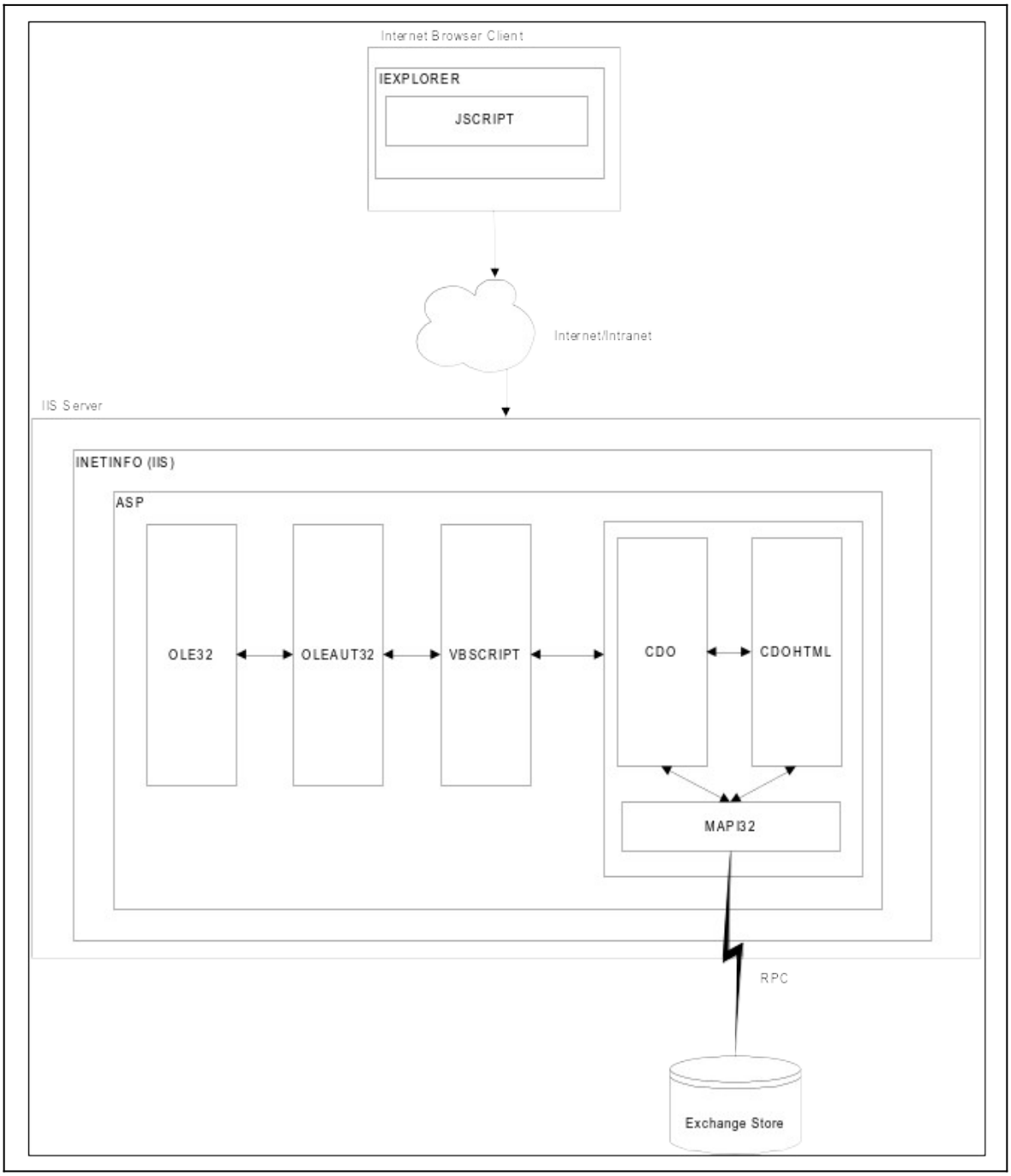
4. The CDO rendering library (Cdohtml.dll) converts the message requested into HTML, and then IIS returns the message to the browser.

5. The Web browser renders the HTML (which includes rendering the embedded JScript®).

OWA Architecture – Figure 1



OWA Components – Figure 2



OLE32 and OLEAUT32: Expose COM objects, libraries, and automation objects used by ASP, MAPI, CDO, and CDOHTML.

VBScript and JScript: ASP scripting engines (ASP provides native support for VBScript and JScript). By default, all ASPs use VBScript as their native language, but ASPs can also be written using JScript. For OWA, ASPs are written in VBScript and JScript. The VBScript is compiled or interpreted on the IIS computer and JScript is served to the

client. In OWA, VBScript is the server-side scripting engine, and JScript is the client-side scripting engine.

CDO (version 1.2): A library called by the server-side scripting engine (in this case, VBScript) to manipulate messaging objects in Exchange Server. The CDO object model is organized in two collections of objects: InfoStores and AddressLists. Each of these objects contains other objects and collections of objects, properties, and methods. CDO is COM based and thus uses OLE32 and OLEAUT32. CDO is an interface into MAPI, which is also COM based. In using CDO's interface into MAPI, remote procedure calls (RPCs) are used to communicate to the Exchange Server computer. Because of this, CDO must use a MAPI session. This session is stored as a state variable in the ASP session, which means that a user does not need to log on to MAPI for each request. The CDO library can be used to build both client and server applications.

CDOHTML (version 1.2): An HTML rendering library used to generate displayable output from CDO objects and properties. When the HTML has been rendered, it is sent to the Web browser and is generated from objects and properties referenced in a .asp file invoked by the browser. CDOHTML is COM based and is an interface into MAPI. Just as with the CDO library, CDOHTML must use a MAPI session. The CDOHTML object model is organized in two collections of objects: RenderingApplication and ObjectRenderer. Each of these objects contains other objects and collections of objects, properties, and methods. CDOHTML can only be used by server applications.

MAPI32: A COM-based messaging application interface.

Outlook Web Access with Security (NTLM, Basic, or SSL)

Security configurations may vary depending upon the installation of OWA. Security can be configured to use Anonymous, Basic (Clear Text), Windows NT Challenge Response (NTLM), Secure Sockets Layer (SSL), or a combination of these.

If IIS and Exchange Server are on the same computer, then you can use any of the above authentication methods. If IIS and Exchange Server are on separate computers, you will not be able to use NTLM authentication; however, because security may be an issue, implementing SSL will ensure that all information passing through the IIS computer is encrypted.

The following brief descriptions of each of the usable authentication methods may help in deciding which is right for a particular OWA installation.

Allow Anonymous

When a user establishes an anonymous connection, your server will log on the user with an anonymous or guest account, which is a valid Windows NT user account. This account has security restrictions that limit the type of Web content that anonymous users can access.

Basic Authentication

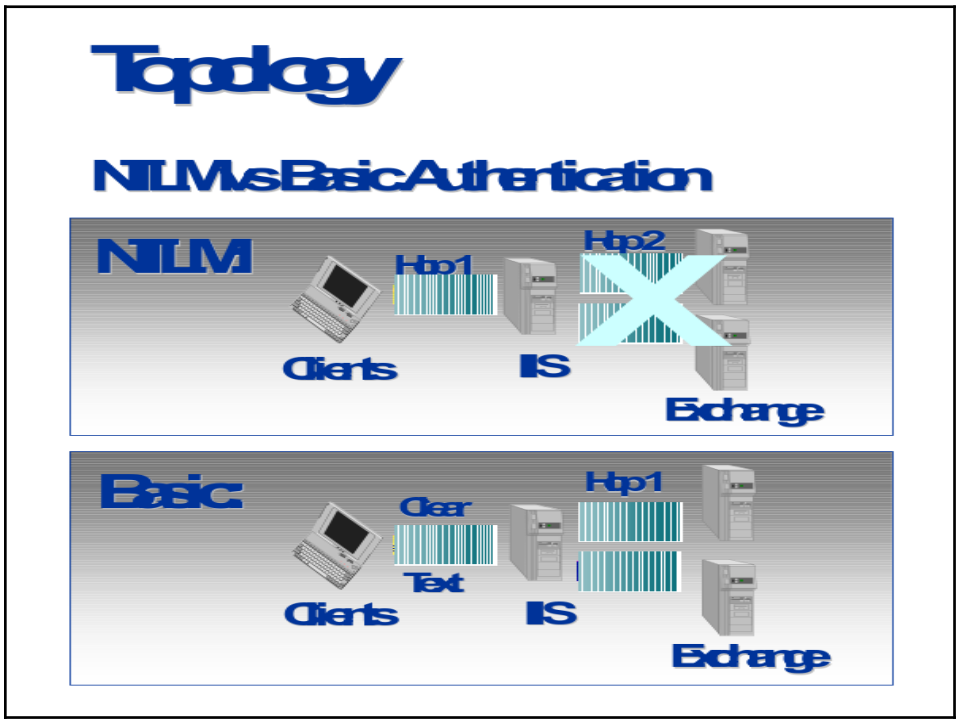
During the Basic authentication process, the user's Web browser prompts the user to enter a valid Windows NT account username and password.

Warning: Basic authentication results in the transmission of passwords across the network in an unencrypted form. A determined computer vandal equipped with a network-monitoring tool could intercept usernames and passwords.

Windows NT Challenge Response (NTLM)

The Windows NT Challenge/Response (NTLM) authentication method is much more secure because it uses a randomization algorithm and an encrypted password to authenticate users.

OWA Security – Figure 3



When a browser accesses a page through the Web, IIS determines which authentication to use in the following order:

1. If you select **Allow Anonymous**, all users assume the anonymous identity. The anonymous identity is determined by clicking the **Edit** button next to **Allow Anonymous**, modifying the username, and providing the password for that account. By default, the anonymous account is "IUSR_ComputerName."

2. If you do not select **Allow Anonymous** or if there is a problem with the settings for the anonymous account, IIS determines if Windows NT Challenge Response (NTLM) is selected. If NTLM is selected, then IIS attempts to use NTLM to authenticate the user. If the authentication is successful, the user assumes the security context of the account the user is logged on to on the Windows NT domain. If NTLM authentication fails, IIS determines if Basic authentication is allowed.

3. If you select **Basic Authentication**, IIS challenges the browser, which in turn presents a logon box to the user. The user must supply their DOMAIN\UserID and password, which are sent to the IIS computer using clear text.

Whether you use **Allow Anonymous** or **Windows NT Challenge Response** depends on whether you want your application (OWA) to identify the sender.

- If you want to identify the sender, use **Windows NT Challenge Response**.
- If you do not want to identify the sender or you want the message to be sent from a common mailbox, use **Allow Anonymous**.

If IIS and Exchange Server are on different computers, you must use either **Allow Anonymous** or **Basic Authentication**. The one you choose depends on whether you want to identify the sender.

- If you want to identify the sender, you must use **Basic Authentication**, which prompts the user for their DOMAIN\UserID and password. Both the username and password transmit as Clear Text over the network. In this case, you must prompt the user for their password because IIS needs the password to authenticate the user to Exchange Server.

If you do not want to identify the sender, or you want the mail to be sent from a common mailbox, then use **Allow Anonymous**. In this case, you must enter the anonymous user's password in the appropriate Microsoft Management Console (MMC) dialog box described below.

In either case, if you want to use the **Allow Anonymous** option, you must do the following:

1. Create a Windows NT Domain account and an Exchange Server mailbox for the anonymous user.

2. Enter the anonymous user's Windows NT password into the MMC anonymous user section. Clear the **Enable Automatic Password Synchronization** option.

3. Grant the anonymous user the right to "Log on Locally" to the IIS computer. You grant rights in the Windows NT User Manager.

Secure Sockets Layer

The Secure Sockets Layer (SSL) authentication method uses public or private key technology to ensure privacy. The SSL protocol resides at the Open Systems Interconnect (OSI) presentation layer and moves data from the application layer to the Transmission Control Protocol (TCP) transport layer. It is responsible for authentication, encryption, and verification of data integrity.

The authentication function assures that the data is being sent to the correct server and that the server is secure. Encryption ensures data cannot be read by anyone other than the target server. Data integrity ensures the data has not been corrupted or altered in transit. All client/server communication occurs on an SSL-encrypted channel on port 995.

The following steps describe the SSL process:

1. Client obtains the server certificate: The client and server introduce themselves to each other with HELLO messages and exchange information containing the encryption method to use, session information, server certificate (containing the server's public key), and random data.

2. Client verifies server: The client verifies the server certificate is from a certifying authority and then uses it to send a message to authenticate the server (to verify it is the server it claims to be). If the server does not pass the authentication, the client typically informs the user that the server is not the server it claims to be and could be a "trojanhorse" server.

3. Client/server determines the encryption key to use for this session: If the server replies back successfully, the client and server create a random secret key (referred to as a Master Key in the SSL specification) from the random data exchanged and the encryption method specified (such as RSA).

4. Data encrypted with agreed-upon key: All data sent over the SSL channel is encrypted with the secret key. Access to the Microsoft Exchange Server computer through the Internet is provided by logging on with a secure connection as a validated user or as an anonymous user. SSL must be enabled on the Microsoft Internet Information Server computer.

Using an Internet browser, such as Internet Explorer or Netscape Navigator, a user accesses the logon page and logs on to a Microsoft Exchange Server computer.

During the logon process, an authenticated and encrypted session is established between the browser and the Microsoft Internet Information Server computer. To gain access to the Microsoft Exchange Server computer, the user's Microsoft Windows NT domain account password must be validated before permission is granted to use the program and its data.

Validated User

The Active Server Component uses Microsoft Windows NT authentication to grant access to users mailboxes. To log on, users must enter their Microsoft Windows NT account name, their password, and their mailbox name. After validation is successfully completed, users have the same permissions in their mailbox as they have when they log on to a computer directly connected to the network.

Anonymous User

An anonymous user is a non-validated Web user who is not recognized by Microsoft Exchange Server. Users can log on to a Microsoft Exchange Server computer anonymously but are restricted to viewing and accessing only the published public folders and address lists. The administrator can specify which folders and address lists to publish using the Microsoft Exchange Server Administrator program.

Outlook Web Access Capacity Planning Analysis

Overview

This section is devoted to planning information for Exchange Server 5.5 Outlook Web Access (OWA). Deployment suggestions for specific user profiles on a given class of computers are provided, as well as general information on the performance characteristics of OWA. Also an overview of the message flow is provided to clarify the roles that the Web browser, IIS, and Exchange Server play.

OWA is a set of binaries, HTML and script files (ASP) that is installed as an Active Server application and integrated with IIS. The script files use Collaborative Data Objects (CDO), allowing users to send, edit, and view items in the Exchange Server public and private information stores with a Web browser. Although much of Outlook's rich functionality exists, no other client software is required. The Web browser performs a small amount of processing, using JavaScript. The OWA server handles most of the processing normally done by the client; this includes MAPI sessions, client logic, address resolution, rendering, content conversion, and RPC communications with the Exchange Server computer. The Exchange Server computer receives requests from OWA that look much like those coming from any MAPI client and processes them accordingly.

Because of this configuration, the OWA server handles all the user load of the active client sessions and therefore must be capable of running a number of active MAPI sessions to the Exchange Server computer. Although the browser has a small footprint on the user's computer, the sessions the user establish to the OWA server to connect to Exchange Server will consume some resources on the OWA server, and this needs to be planned for.

Performance Analysis

The key scaling bottleneck for an OWA server is the number of active ASP requests, which can be monitored with Performance Monitor by looking at the ASP process and Request/Sec counter. When this counter exceeds 10 to 15 ASP Requests/Sec, the server is slower to respond and your OWA users may see ASP page failures. There are several other things that can cause this same behavior, so do not confuse this bottleneck with a setup, configuration, or network problem. Both end-user response times and message throughput will improve slightly as you upgrade hardware; however, the number of concurrent sessions stops scaling as you approach a high number of ASP Requests/Sec. Unfortunately, this means that upgrading your hardware beyond the maximum specifications listed below will not allow you to significantly increase the number of OWA users you can fit on one OWA server.

ASP requests are created by each unique instance of a Web browser, so as a user requests the OWA logon page ASP requests are generated, as well as with each action the user performs in the Web client. ASP sessions expire after exceeding an idle timeout period (the default is one hour), or when a user explicitly ends the session by clicking the Logoff icon on the navigation bar. Reducing the session timeout (described in How to Change OWA's ASP Session Timeout below) reduces the active sessions and may allow more users to be hosted on one OWA server. Be aware that lowering this timeout will cause users to be redirected to the logon page more frequently.

User Per Server Testing

In an Exchange Server environment, the load placed on the IIS server by OWA clients is determined by the number of ASP requests per second that are processed on behalf of each user. OWA clients perform a number of tasks, each requiring the server to process ASP requests (for example, reading, deleting, and sending messages, along with scheduling activities). The challenge of planning the number of users per server is to characterize your user workload and then to monitor test users against an Exchange Server computer. The details in the following paragraphs will provide you with some ideas on building your own usage patterns. If you are planning to deploy OWA in your company, the following pages of information will help provide you some insight on how to monitor your users and fine-tune your OWA installation. Use of a performance-monitoring tool such as Windows NT Performance Monitor (PerfMon) will assist in the overall measurement of the number of ASPs processed per second. Additionally, your local Microsoft Consulting Services office can assist you in planning and modeling for large OWA deployments.

When you plan for an OWA deployment, you should gather data about how often your users will access the Exchange Server computer and what actions they will perform, such as how many logons per day, messages sent, read, deleted, and calendar actions per day. Organizations vary as to what features their users need in the OWA client, some simply need a means for checking e-mail messages, others may have very active users who send large messages, use their calendar heavily as well as read and delete a large number of messages. The type of user is an integral part of planning and servicing your OWA server. Companies who have very heavy users may need more OWA servers for the same number of Exchange Server mailboxes than an organization that uses the client to simply check e-mail occasionally over the Web. Also, keep in mind the work schedule of your users, if they work a 9 to 5 shift, or if you have users accessing the server all hours of the day equally.

After you have decided what features your users use, you will then want to take a sampling of some normal users and ask them to start using the OWA client from their workstations while you monitor the performance of the OWA server with Performance Monitor. By looking at the ASP requests your users are generating, you can estimate as to the best number of users per OWA server. The Performance Monitor counters you will want to watch are mentioned in the next section.

By investigating the trends of your test group, you will be more prepared for a larger deployment of OWA clients. The best method is to monitor your usage and add additional OWA servers when you see that the PerfMon counters listed below in the IIS and ASP Performance Monitor Counters section are consistently too high and users are frequently getting the "server too busy" error.

Recommendations on Capacity Planning

As a rule of thumb, keep the number of ASP Requests/Sec under 10. If the OWA server is driven beyond 10 to 15 ASP Requests/Sec, the server can context switch heavily, causing the performance of other applications on that server to degrade. For this reason, for a large deployment, we strongly suggest deploying OWA on one or several stand-alone servers separate from the Exchange Server computer. Because of the ASP Requests/Sec limit, OWA is best deployed on a two-processor server. Adding more processors will be unlikely to provide a performance benefit.

ASP memory cleanup happens on a background thread. If a server is very busy, it will consume memory throughout the day. After initial deployment, the server should be monitored in Performance Monitor to ensure that it has been configured with sufficient memory.

You can set the registry setting for RequestQueueMax (described below in the IIS and ASP Registry Changes and Optimizations section) to a lower number to prevent the server from context switching. By setting RequestQueueMax to a lower value, such as 15 to 20, you can prevent the server from queuing up too many ASP requests, which will overload the server. The lower you set this value, the more likely your users will see a "server too busy" error when trying to access a page. However, it is better to set this value lower so users will see the "server is busy" error rather than trying to overload the server. You can monitor this counter in Performance Monitor to see if you constantly hit these marks; if you do, you may need to consider adding more OWA servers to your organization.

Users Per OWA Server Results

The number of users per OWA server is difficult to determine because you will need to run tests on your own OWA servers for your own environment. The primary reason for this is that each user population has a different profile or usage characteristics. The best method is to do a test deployment and monitor your pilot users with PerfMon, and then add additional OWA servers when you see the ASP Requests/Sec limit on the server is being reached.

Users Per Exchange Server Results

When you determine how many users to place on each OWA computer, you need to determine how many Exchange Server computers are required to handle the traffic from all users. Much as a POP3 client generates a different server load than does a MAPI client, an OWA client also differs from a MAPI client.

A single OWA user places more load on an Exchange Server computer than does a single MAPI user (for example, Exchange client or Outlook97 users). There are several reasons for this, most of which revolve around OWAs middle-ware architecture. All user action is driven by HTTP requests, which is a very simple protocol. This limits OWA's ability to batch commands and perform other optimizations that are commonly done in a desktop client. The result is that an Exchange Server computer can support fewer OWA users than MAPI users.

OWA, IIS, and ASP Performance Tuning

How to Change OWA's ASP Session Timeout

Reducing the session timeout can reduce the average number of active sessions, and therefore decrease the resources required by ASP. The drawback is that a user's session will time out sooner, and users will be forced to log on after a shorter amount of idle time. This setting is set globally for ASP and is overridden by OWA for its sessions. The instructions below only affect the ASP sessions that are from OWA. Other ASP applications are not affected. Follow the steps below to modify OWA's session timeout:

1. Make a backup of the following file because you will need to modify it:

   \Exchsrvr\Webdata\<Lang>\Lib\Logon.inc

2. Open Logon.inc with notepad.

3. On the **Search** menu, click **Find**. Type "itimeout" and click **Find Next**.

   Note: The variable name "itimeout" appears eight times in this file. The first four refer to Authenticated access; *this is the section that should be modified*. The references in the Logon.inc are nearly identical, but all refer to Anonymous access.

4. Locate the following code fragment and modify only the number of minutes (as shown in bold below):

```
iTimeout = objRenderApp.ConfigParameter("AuthenticatedSessionTimeout")
If iTimeout = 0 Then
        ITimeout = 60 'minutes
End If
Session.Timeout = iTimeout
```

5. Save Logon.inc. Any sessions created after this point will reflect the changes made; there is no need to restart the Web service.

IIS and ASP Registry Changes and Optimizations

WARNING: Using the Registry Editor incorrectly can cause serious problems, including corruption that may require reinstalling Windows or Active Server Pages. Using the Registry Editor to edit entries in the registry is equivalent to editing raw sectors on a hard disk. If you make mistakes, your computer's configuration could be damaged. You should edit registry entries only for settings that you cannot adjust through the user interface, and be very careful whenever you edit the registry directly.

Registry path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services..\W3SVC...
\ASP ....\Parameters

ProcessorThreadMax REG_DWORD Range: 1 - 0x000000C8
Default: 10. This value specifies the maximum number of worker threads to create per processor. Generally, it is not advisable to create more than 20 threads per processor. If this value is changed, the Web server must be stopped and restarted for the change to take effect.

RequestQueueMax REG_DWORD Range: 1 - 0xFFFFFFFF
Default: 500. This value specifies the maximum number of .asp file requests to maintain in the request queue available for each thread. When the limit is reached, clients are sent the value from the registry value **ServerTooBusy**. If this value is changed, the Web server must be stopped and restarted for the change to take effect.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo
Parameters

UserTokenTTL : REG_DWORD Range: 0 -0 x7FFFFFFF
Default: 600 (10 Minutes). When a request is made to the server, the security credentials for the request (or the configured anonymous user) are used to create a user token on the server, which the server impersonates when accessing files or other system resources. The token is cached so the Windows NT logon only takes place the first time the user accesses the system or after the user's token has fallen out of the cache. NTLM authentication tokens are not cached. Units are in seconds.

MaxPoolThreads : REG_DWORD Range: 0 - 0xFFFFFFFF
Default: 10. **MaxPoolThreads** specifies the number of pool threads to create per processor. Each pool thread watches for the network request and processes the same. Generally, it is not recommended that you create more than 20 threads per processor.

MaxConnections : REG_DWORD Range: 0 - 0xFFFFFFFF
Default: 1000. This value specifies the maximum number of simultaneous connections that the server allows at any given time. When the number of current connections exceeds this value, the service rejects the request. It sends a friendly message if possible.

IIS and ASP Performance Monitor Counters

When you test for performance, the following performance counters are monitored and seem to be sufficient for identifying the majority of issues:

Object	Counter
Requests/Sec	Active Server Pages
Requests Executing	Active Server Pages
Requests Queued	Active Server Pages
Requests Total	Active Server Pages
Current Anonymous Users	Web Service
Connection Attempts/Sec	Web Service
% Committed Bytes In Use	Memory
Available Bytes	Memory
Private Bytes (inetinfo "IIS Process")	Process (see below for explanation)
Thread Count (inetinfo)	Process (see below for explanation)
% Processor Time	Processor

Private Bytes (inetinfo): This counter is extremely helpful when you are determining memory leaks in custom objects that are running In-Process (W3SVC).

Thread Count (inetinfo): This counter is extremely helpful when you are tracking down a badly behaved application running In-Process (W3SVC) that spawns multiple threads.

Recommendations for Performance Tuning

You need to monitor the ASP Requests/Sec counter to ensure the server is not receiving too many requests; this number should not exceed 10 to 15 ASP Requests/Sec.

RequestQueueMax registry setting: Set this to a value between 10 and 20 to prevent the request queue from growing during peak time. With the RequestQueueMax value set lower, users will get a "server to busy" error when accessing the OWA server if

there is heavy load on the server at the time. This will assist in keeping the queue size under control and from accepting requests that may not get processed for quite some time.

UserTokenTTL registry setting: Do not set this value too low. Monitor how your users use the OWA client. You do not want to force additional logons to the OWA computer because of the number of ASP requests a logon creates; however, you do not want this number to be too high, because the token will be cached much longer than needed.

MaxPoolThreads registry setting: Do not exceed 20 max threads per processor.

For more information about tuning IIS and ASP performance, see the following white papers:

- Server Performance Optimization on Microsoft's Web Site
  http://www.microsoft.com/workshop/server/feature/serveroptms.asp

- Tuning Internet Information Server Performance
  http://www.microsoft.com/isn/techcenter/tuningiis.asp

Outlook Web Access with Firewalls

Connecting an Outlook Web Access client to an Exchange Server computer over an existing connection to the Internet through a firewall requires adding some entries to the registry so that static ports can be mapped to connect to the Exchange Server computer.

A packet filter (or firewall) denies connection attempts made to any port for which you have not explicitly allowed connections. Exchange Server uses a well-known static port (port 135) to listen for client connections to the RPC Endpoint Mapper Service. However, after the client connects to this socket, Exchange Server reassigns the client two random ports to use when communicating with the directory and the information store. This makes it impossible to allow these ports to communicate through the firewall without forcing them to be statically assigned. Though port 135 is not necessary to be configured in the firewall filter settings for OWA, it is sometimes configured in addition because other client connections may be made in the future. Port 80 (for HTTP traffic) must be enabled on the firewall to allow OWA traffic to flow.

The following steps describe the registry information that must be added to allow the mapping of static ports to make this connection:

Note: DO NOT assign ports immediately above the 1023 range, because other problems such as directory replication failures may occur on your Exchange Server computer.

1. Start the Registry Editor (Regedt32.exe).

2. Under the HKEY_LOCAL_MACHINE subtree, and go to the following subkey:

   System\CurrentControlSet\Services\MSExchangeDS\Parameters

3. Add the following entry for the Microsoft Exchange Server directory service:

TCP/IP port REG_DWORD
DATA: <port number to assign>

Example: "TCP/IP Port"=dword:000004C9(1225)

The decimal number 1225 is used for the Directory Service, which is 4C9 in hexadecimal.

4. Go to the following subkey:

System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem

5. Add the following entry for the information store:

TCP/IP port REG_DWORD
DATA: <port number to assign>

Example: "TCP/IP Port"=dword:000004CA(1226)

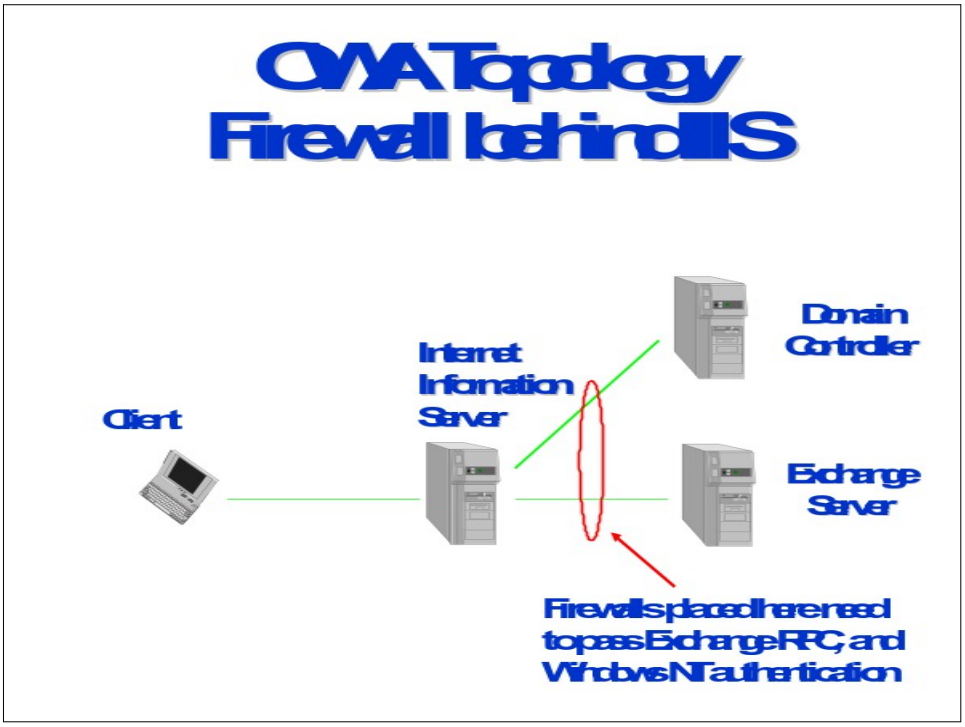
The decimal number 1226 was used for the information store, 4CA in hexadecimal format.

6. Quit the Registry Editor.

After setting these entries in the registry, you will need to configure the packet filter (or firewall) to allow TCP connections to be made to these ports, as well as to port 80 (with port 135 optional for other client connections).

The following diagram shows this configuration, where a firewall is located between the IIS computer and the Exchange Server computer. Therefore, follow the above steps 1 through 6 to statically map ports for the directory and information store, and then open those ports on your firewall. In the above example, you will need to open the following ports on the firewall: 135, 1225, and 1226.

OWA with Firewall (option 1) – Figure 4

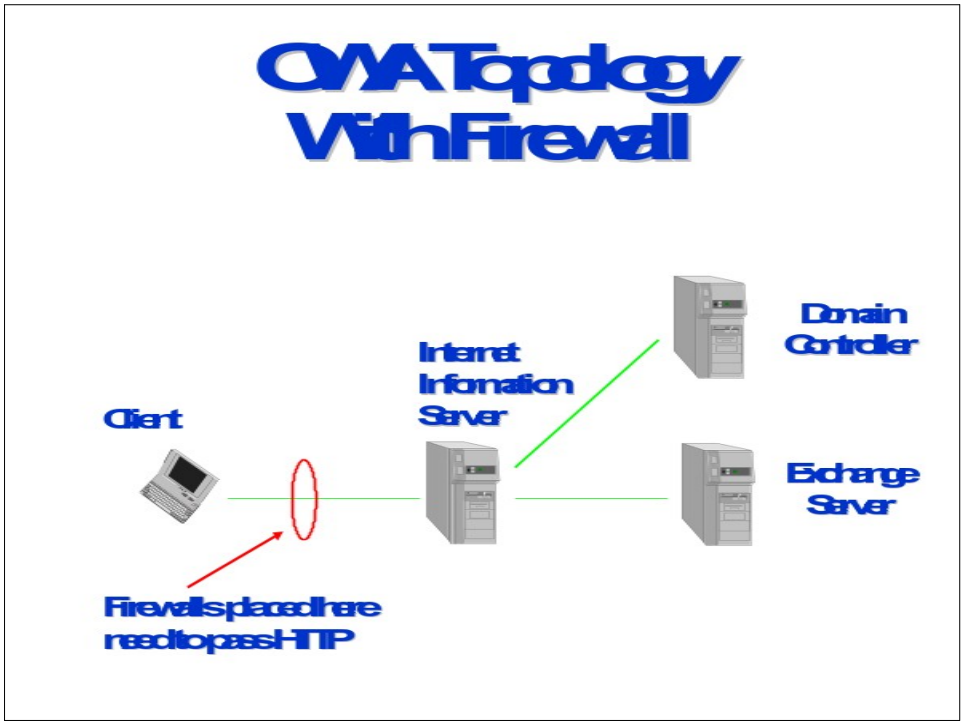


You can also configure your environment so that a firewall is located before the IIS computer. When configuring a firewall to hide all of your organization you will only be required to set the firewall to pass HTTP traffic over port 80 to connect to the OWA server via the Internet.

In this scenario, the client connects to port 80 on the IIS computer and the IIS computer communicates with the Exchange Server computer(s) to get the Exchange Server data. The IIS computer renders the data back into HTML for the OWA client, sending the data over the Internet on port 80 (HTTP). If you want to use the Windows NT Challenge Response (NTLM) authentication method, enable port 135 on the firewall as well so that the client over the Internet can connect directly over RPC to the IIS computer. (Note: for NTLM to authenticate the user, IIS or OWA and Exchange Server must be installed on the same server).

One other note, if you are using SSL, you will need to open the port you are using for SSL on the firewall. The default port for SSL is 995.

OWA with Firewall (Option 2) – Figure 5



Troubleshooting Outlook Web Access Problems

This section is intended to assist administrators with configuring Microsoft Exchange Server 5.0 Active Server Components and Microsoft Exchange Server 5.5 Outlook Web Access, and with troubleshooting error messages.

Server Configuration Checklist

This section covers the basic settings to ensure proper configuration of the Outlook Web Access components on the Exchange Server or IIS computer. Before troubleshooting a specific error message, see the following checklist for items that may be missing from your installation.

- The Log on Locally right: Each Windows NT account that will be accessing the Exchange Server computer through the Outlook Web Access client must have the Log on Locally right assigned on the IIS computer. The administrator can assign this right to the **Everyone** group or to specific groups if access restriction is needed. To assign this right to an account, follow these steps:

  1. Start User Manager for Domains.

  2. On the **Policies** menu, click **User Rights**.

  3. In the **Right** list, click **Log on Locally**.

4. Click the **Add...** button.

5. In the **Add Users and Groups** dialog box, click the **Show Users** button and choose one or more user or group accounts from the **Names** list.

6. Click the **Add** button and then click **OK** when you are finished.

7. Click **OK** again and exit User Manager for Domains.

Note: If the IIS computer is a Member server in a Windows NT domain, you must grant the Log on locally right to the appropriate Windows NT account using the local computer's accounts database, not the domain's accounts database. To do this, start User Manager for Domains in one of the following ways before you grant the Log on Locally right to the user account:

- Log on to the IIS computer using the local computer's Administrator account and start User Manager for Domains.

  -or-

- If you are logged on to the IIS computer with a domain account that is a member of the Local Administrator's group, start User Manager for Domains and click **Select Domain** on the **User** menu. Enter the local computer's name as \\ *servername*.

  -or-

- Start User Manager for Domains using the following command-line:

  usrmgr *servername*

  where *servername* is the name of the IIS computer. The end result is that the local computer's name will appear in the title bar of User Manager for Domains, instead of the domain name.

- Password authentication methods: The WWW service on the IIS computer must be configured for the appropriate password authentication method. This is dependent on how you intend to set up your Exchange Server and IIS computers. If both Exchange Server and IIS are installed on the same computer, you can use any of the three supported authentication methods. If Exchange Server and IIS are on separate computers, *only* Basic (Clear Text) and Anonymous authentication can be used. Windows NT Challenge Response (NTLM) authentication cannot be used if a browser other than Internet Explorer will be used for Web access. If you plan to use Basic (Clear Text) authentication and you want to have a more secure environment, configure Secure Sockets Layer (SSL) support on the IIS computer. For more information about setting up SSL, see your IIS documentation.

- Required components: The following components are required for a successful installation of Outlook Web Access:

  - Microsoft Windows NT Server 4.0

- Microsoft Windows NT Server 4.0 Service Pack 3 (SP3)

- Microsoft Internet Information Server (IIS)
  Exchange Server 5.0 is *only* supported with IIS 3.0 (regardless of the service pack).
  Exchange Server 5.5 is supported with IIS 3.0 or IIS 4.0

- Active Server Pages (ASP)
  ASP can be set up from the Windows NT Server 4.0 SP3 compact disc, or you can download SP3 and the ASP components from http://www.microsoft.com.

- Active Server Components or Outlook Web Access components
  The Active Server Components are included with Exchange Server 5.0. It is recommended that you install Exchange Server 5.0 SP1 or Exchange Server 5.5, because they include the enhanced Outlook Web Access components.

- Internet browser (use one of the following):

  - Internet Explorer 3.02 with RFC1867.exe installed to allow attachments (available from http://www.microsoft.com/ie)

  - Internet Explorer 4.0 or later

  - The latest version of any other third-party Internet browser software that supports frames (for example, Netscape Navigator)

- The IUSR_ *servername* Account: Make sure that the IUSR_ *servername* account has been assigned the Log on Locally right on the IIS computer. Also, make sure the password for this account is the same in both User Manager and the Internet Service Manager. These passwords can be changed independently and differences will cause access problems. By default, the IUSR_*servername* account is given a random password when IIS is installed.

- Use the following steps to set up anonymous access:

  1. On the Windows NT Start menu, point to **Programs**.

  2. Select **Microsoft Exchange**, and then select **Microsoft Exchange Administrator**.

  3. Select the server you are configuring, and then open the Configuration container.

  4. Choose **Protocols**, and then double-click **HTTP (Web) Site Settings**.

  5. Select the **Allow anonymous users to access the anonymous public folders** check box.

  6. Click the **Folder Shortcuts** tab.

  7. Click **New** to add folders for anonymous viewing, and then select an existing folder in the **Public Folders** dialog box.

8. Click **OK**.

Published folders must have at least **Read** permission granted to the Anonymous account. This is set on the **Permissions** tab for the specified folder. Folder permissions can be accessed from either the Microsoft Exchange Server Administrator program or from the client.

1. In the Microsoft Exchange Server Administrator program, browse to find the public folder for which you created a shortcut.

2. On the **File** menu, click **Properties**.

3. Click **Client Permissions**.

4. In the **Client Permissions** dialog box, select **Anonymous** and change its role from **None** to the desired level of access.

5. If you want to publish all subfolders of this folder for anonymous access, select the **Propagate these properties to all subfolders** check box.

6. Click **OK**.

Additional Information

A single Exchange Server computer running OWA can connect to many Exchange Server computers. The OWA computer must be configured to point to a specific Exchange Server computer during installation of the OWA component from the Exchange Server compact disc. It then uses the directory service on that Exchange Server computer to look up the home private store server for each user and automatically makes a connection to that server. When you log on to the correct mailbox name or alias on the OWA login screen, your request is checked using the directory service and directed to the correct home server. This capability prevents having to install multiple OWA servers in an organization.

However, if you will be using OWA for a large number of users, you may want to install multiple OWA servers in your organization. This will allow load balancing to prevent deterioration of performance on the OWA server. The number of users per OWA server may vary and should be considered when you select the number of OWA servers to deploy. The total number of users per server may vary depending on the amount of traffic generated by each user. Measuring the load can be determined using the Performance Monitor for the ASP Requests/Sec counter. This traffic should be limited to approximately 15 ASP Requests/Sec. More than this can effectively bring down the server or severely hinder its performance.

When the approximate number of users per OWA server has been determined, you can more appropriately plan for the number of OWA servers to deploy in your organization. Users can be assigned to log on to a specific OWA server. As mentioned above, the directory service on the Exchange Server computer looks up the home private store for each user's mailbox.

Troubleshooting Error Messages

This section covers the most common issues with the Microsoft Exchange Server 5.0 Active Server Components and Microsoft Exchange Server 5.5 Outlook Web Access.

If the error message that you are receiving is not listed here, or you are still having problems with Outlook Web Access after reading this troubleshooting guide, please search for additional answers in the Microsoft Knowledge Base at http://support.microsoft.com/support.

Note: To perform most of these procedures, you must have administrative privileges on either the Exchange Server or the Internet Information Server (IIS) computer. If you do not have these rights, please contact your administrator.

"Failed to Get Inbox" Error Message During Log On

One of the most common error messages that you can receive when you attempt to log on to a Microsoft Exchange Server mailbox using the Outlook Web Access client is the "Failed to Get Inbox" error message. Use the following steps to troubleshoot this error:

1. You may have typed the mailbox incorrectly. Try entering the alias again.

2. Confirm that the mailbox alias name does not contain any spaces. If it does, rename the mailbox alias by removing the spaces.

3. If you are prompted for a username and password, enter the domain and username in the Windows NT Authentication dialog box as *Domain**Username*.

4. Access another Web page to ensure that the browser is not the problem.

5. If you log on to a mailbox with one alias, log off and try to log on to another mailbox, the "Failed to Get Inbox" error may occur because the browser has cached the previous user's credentials. Close the browser and try again.

6. If you are logging on as an Anonymous user to access public folders, verify that you have given sufficient permissions for the Anonymous account to access public folders.

7. Log on to the mailbox from an Exchange or Outlook client to verify that the mailbox is accessible. This may determine whether there is a problem with mailbox corruption or a problem specific to the Outlook Web Access components.

8. Try to log on from another computer. If this works, the password file of the user on the original computer may be corrupted if this is a Windows 95 system. Try deleting your *.pwl file, log off, and then log back on to Windows 95. This creates a new *. pwl file.

9. To ensure that the IIS computer on which you are attempting to access your Exchange Server mailbox is not the problem, try connecting to the default page of that server at http://*servername*.

10. Create a new mailbox and Windows NT account. Try accessing this mailbox to ensure that there is no problem with a specific user's account.

11. Check the password authentication method being used by the WWW service on the IIS computer. To do this, follow these steps:

    a. Open Internet Service Manager.

b. Double-click the WWW Service.
c. Under Password Authentication, make sure that:

- The **Allow Anonymous** check box is selected.
- The **Basic (Clear Text)** check box is selected.
- The **Windows NT Challenge Response** check box is *not* selected.

Note: Windows NT Challenge Response can be enabled if the Web server is on the same computer as Exchange Server. The **Basic (Clear Text)** check box can be cleared if you are only using Internet Explorer *and* your Web server is on the same computer as Exchange Server.

12. If you are using NTLM authentication on the IIS computer, verify that the **Do not use Proxy server for local addresses** option has been selected on the client's Web browser.

13. If you are using NTLM authentication, verify that you are logged on to the domain with the Windows NT account that has permissions on the Exchange Server mailbox. If the user can log on from the IIS computer but not from a client workstation, verify that the user has the Log on Locally right assigned on the IIS Server.

    Note: If the IIS computer is a Member server in a Windows NT domain, you must grant the Log on Locally right to the appropriate Windows NT account using the local computer's accounts database, not the domain's accounts database. To do this, start User Manager for Domains in one of the following ways before you grant the Log on Locally right to the user account:

    - Log on to the IIS computer using the local computer's Administrator account and start User Manager for Domains.

      -or-

    - If you are logged on to the IIS computer with a domain account that is a member of the Local Administrator's group, start User Manager for Domains and click **Select Domain** on the **User** menu. Enter the local computer's name as \\ *servername*.

      -or-

    - Start User Manager for Domains using the following command line:

      usrmgr *servername*

      where *servername* is the name of the IIS computer. The result is that the local computer's name will appear in the title bar of User Manager for Domains, instead of the domain name.

14. If you are prompted with a dialog box requesting the username and password when you log on to the mailbox, but you still get the "Failed to Get Inbox" error message, enable **Allow Anonymous** and **Basic (Clear Text)** password authentication on the IIS computer through IIS Manager.

15. Verify the home server of the mailbox. If you are trying to log on to an Exchange Server computer other than your home server, allow adequate time for your mailbox to replicate to the server that you are trying to log on to.

16. Verify that you can log on to Exchange Server through a Web browser located on the IIS computer. If you are unable to log on from the IIS computer, check for a problem in the user's Windows NT account or password.

17. If the Exchange Server computer is on an NTFS partition, share it out with the same name and give Full Control access to the Everyone group.

18. If you are replicating directories between two recently connected sites, you must ensure that no two mailboxes contain the same alias. If they do, you must either rename or remove the duplicate alias.

For more information on troubleshooting this error message, see the following articles in the Microsoft Knowledge Base: Q167003, Q173451, Q173676, Q175122, Q189654, Q175698, Q174352, Q173470, Q165661, Q166994, Q165987

Sorry! The Exchange Server Is Down or the HTTP Service Has Been Disabled by an Administrator

This is another common error message that you may see when you log on to a mailbox. The following steps can be used to troubleshoot this error message:

1. The **HTTP** protocol may be disabled. Open the Microsoft Exchange Server Administrator program, select the **Protocols** container, and then open the **HTTP (Web) Site Settings** object. Make sure that the **Enable Protocol** option is selected. Open the properties for the mailbox and click the **Protocols** tab. Select the **HTTP** protocol, and then click **Settings**. Make sure that **Enable HTTP for this recipient (HTTP is enabled on this server)** is selected.

2. Anonymous access may be disabled in **LDAP.** Open the Exchange Server Administrator program, select the **Protocols** object, and then open the **LDAP (Directory) Site Defaults** object. Click the **Anonymous** tab and make sure that the **Allow anonymous access** option is selected.

3. This error may also occur if the Anonymous access account defined in the DS Site Configuration object in the Microsoft Exchange Server Administrator program does not have Search permissions at the Configuration container level. This Search feature is only available in Exchange Server 5.5 or later.

4. Verify that the Microsoft Exchange Server Information Store service on the Exchange Server computer is started.

5. Verify that the **MSExchangeWeb** registry key shown below contains the correct values for the Organization, Site, and Server names of the Exchange Server computer to which you are connecting. Open the Microsoft Exchange Server Administrator program. Note the organization, site, and server names displayed for the server to which you are connecting. Start the Registry Editor (Regedt32.exe) on the Microsoft Exchange Server computer and select the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \MSExchangeWeb\Parameters

Verify that the following values match:

- Enterprise - Must match the Organization name.
- Site - Must match the Site in which the server is located.
- Server - Must match the server to which you are connecting.

If any of the above values are incorrect, change them to match the names displayed in the Exchange Server Administrator program. These values are not case sensitive.

6. Verify that the IUSR_*servername* account has at least **Change** permissions on the directory that contains the temporary .mmp files. This directory is specified in the following registry key:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Messaging Subsystem\ProfileDirectory

For more information about changing this key, see the "Failed to Connect to the Microsoft Exchange Server *Servername*" section.

For more information on troubleshooting this error message, see the following articles in the Microsoft Knowledge Base: Q165712, Q173455, Q180417, Q174709, Q167003

Access Is Denied

When you log on and try to enter authentication credentials, you may be repeatedly prompted with Windows NT Authentication dialogs, or you may get the immediate error message "Access is Denied." Perform the following steps to troubleshoot this error message:

1. The password may have been typed incorrectly. Retype the password and double check the spelling, being sure to check capitalization and so forth.

2. The username may have been typed incorrectly. Retype the username, double checking capitalization, and so forth. Use the *Domain**Username* format.

3. You may not have the Log on Locally right on the IIS computer. To correct this, perform Step 1 in the "Server Configuration Checklist" section at the beginning of this section.

For more information on troubleshooting this error message, see the following articles in the Microsoft Knowledge Base: Q169649 and Q173470

Failed to Connect to the Microsoft Exchange Server S*ervername*

This is another error message you may receive when you attempt to log on to a mailbox through the Outlook Web Access client. Use the following checklist to troubleshoot this error:

- Check the permissions set on the *Winnt* directory and all of its subdirectories. Also, check the permissions on the *Exchsrvr*\Webdata and *Exchsrvr*\Webtemp directories and all of their subdirectories. If you are using Exchange Server version 5.0, the *Winnt* directory and all of its subdirectories must have **Change** permissions set on them for the Domain Users group. The *Winnt*\System32 directory must have at least **Read** permissions set for the Domain Users group.

- When you use Microsoft Exchange Active Server Components to access information on a computer running Microsoft Exchange Server, files with an .mmp extension are created in your *Winnt* directory by default. The .mmp file is a temporary file used by Active Messaging to store certain profile information during the active session. This file should be deleted after the user logs off and the session is closed. Because these files must be created dynamically, the Microsoft Internet Information Server (IIS) Anonymous Log on account (IUSR_*servername* by default) needs to have **Change** permissions on the *Winnt* directory.

- After you install Microsoft Exchange Server 5.0 Service Pack 1, you can change the directory in which the temporary .mmp files are created.

  WARNING: Using Registry Editor incorrectly can cause serious problems that may require you to reinstall Windows 95. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

  If the following registry key is present, the .mmp files will be created there instead of in the *Winnt* directory:

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Messaging Subsystem

  To create this registry entry, perform the following steps:

  1. Start Registry Editor (Regedt32.exe) and go to the following key:

     HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Messaging Subsystem

  2. On the **Edit** menu, click **Add Value** and type the following values:

     - Value Name: ProfileDirectory
     - Data Type: REG_SZ
     - Value Data: Path to the directory in which the temporary files are created. (for example: C:\WEBTEMP)

     If the registry value is not present, the .mmp files are created in the *Winnt* directory.

     Note: The IIS Anonymous Log on account (IUSR_*servername* by default) must have **Change** permissions for the directory specified for ProfileDirectory.
     If using Exchange Server 5.0 SP1 or later, verify that the *Winnt* directory and all of its subdirectories have at least **Read** permissions set on them for Domain Users group. Verify that the *Winnt*\System32 directory has at least **Read** permissions

set for the Domain User group. If you are using Exchange Server version 5.5 or later, no special permissions have to be set on the *Winnt* directory.

You may need to change the permissions on the Exchsrvr\Webdata directory and all of its subdirectories to **Read**. Verify also that the Exchsrvr\Webtemp directory and all of its subdirectories are set to **Change**.

For more information on troubleshooting this error message, see the following articles in the Microsoft Knowledge Base: Q176240 and Q178511

VBScript Error Accessing Outlook Web Access Server

You may receive the following VBScript error on your Web browser when you attempt to connect using Outlook Web Access. The script name and line number may not necessarily be identical, but the error code will remain the same.

```
Microsoft VBScript runtime error '800a03e3'
Unknown runtime error
/exchange/USA/lib/session.inc, line 300
```

This error may have more than one cause. Check the following:

- Anonymous access is not enabled on the LDAP protocol in the Exchange Server Administrator program and/or the anonymous account has not been assigned the correct permissions. Trying to connect to a mailbox that does not exist or no longer exists will generate this error. Verify the mailbox alias to which you are trying to connect.

- Open the Exchange Server Administrator program to check the LDAP protocol and anonymous account permissions. View the properties of the LDAP protocol and ensure that **Allow Anonymous** is checked. View also the properties of the DS Site Configuration container and ensure the account designated for the anonymous access is correct and that the password for this account is correct. (Note that the IUSR_*servername* account is normally used for anonymous access; however, it is possible to use a different account name.)

- View the properties of the Configuration container and click the **Permissions** tab. Ensure that the IUSR_*servername* or anonymous account has **Search** permissions.

If you make any of the above changes, you must stop and restart the World Wide Web Publishing service (WWW) through Control Panel Services or through IIS Manager.
This runtime error message can also occur when the server is very busy or when you try to connect to a mailbox that does not exist but is authenticated as a real user. Also, this problem may occur if the incoming message is larger than the input buffer of the Internet Web browser (usually around 16 KB). A hotfix for this problem is available.

Note: This hotfix should only be used in specific cases where installation of the hotfix is warranted. This hotfix is only for use with Exchange Server and IIS 3.0. The hotfix is available on the Microsoft anonymous FTP server site ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/ASP/asp-memfix/.

For more information on troubleshooting this error message, see the following articles in the Microsoft Knowledge Base: Q178656, Q183533, Q176245

"Unable to Get Published Folder List" Error or "No Public Folders" When You Log on Anonymously

- Verify that the IIS server's WWW service is running and handling ASP requests. This can be done by running some of the sample scripts available with IIS.

- If no public folders are published, go to the Microsoft Exchange Administrator program to confirm that the **HTTP** protocol is enabled and allows anonymous access to public folders. Use the following steps to confirm whether the protocol is enabled:

    1. Open the Exchange Administrator program.

    2. Open the **Protocols** object.

    3. Double-click **HTTP** and click the **General** tab. Click the **Folder Shortcuts** tab. Verify that the folders for anonymous access are available in the **Public Folder Shortcuts** list.

        Note: Including only the Public Folder tree object will not provide anonymous access to any of the top-level public folders.

- Verify that access permissions for the folder are correctly set. Make sure that the default permissions for the anonymous account are set to a minimum of **Reviewer**.

- Verify that the public folders you are trying to open are available from the Microsoft Exchange or Outlook client. This should ensure that the public folder is accessible.

- Set up a test folder, add it to the list of public folders, and assign the appropriate permissions. Remember to quit and restart the browser before you attempt to access the test public folder.

- Make sure that the IUSR_*servername* account has **Log on Locally** rights on the IIS server.

- Make sure that the IUSR_*servername* account's password in User Manager is the same as in the Internet Service Manager.

- Check to ensure that the **Guest** account on Exchange Server has not been disabled. Perform these steps to confirm the information:

    1. In Exchange Server, select **User Manager for Domains**.

    2. Select the **Guest** account and double-click to view the properties.

    3. Make sure that **Account Disabled** check box is cleared (not selected).

For more information on troubleshooting this error message, see the following article in the Microsoft Knowledge Base: Q169183

Unable to Render View 424Object Required

This error message will occur if some of the Outlook Web Access files located on the Microsoft Exchange Server computer are corrupted or missing.

To correct this behavior, remove and reinstall the Outlook Web Access components from the Microsoft Exchange server using the following steps:

1. Back up the Exchsrvr\Webdata directory on the Microsoft Exchange Server computer.

2. Run the Microsoft Exchange Server Setup program and choose the **Add/Remove** option.

3. Cancel the selection of the Outlook Web Access components and continue with the Setup program to remove the Outlook Web Access components.

4. Delete the Webdata directory.

5. Run the Setup program again and select the Outlook Web Access components.

6. Continue the Setup program to perform a clean installation of the Outlook Web Access components.

For more information on troubleshooting this error message, see the following article in the Microsoft Knowledge Base: Q178154

Unable to Render View

This error message will occur if the following registry keys on the computer running the OWA components have incorrect security permissions:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \MSExchangeWEB

-and-

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC

To set the correct permissions for the above listed registry keys, follow these steps:

1. Start the Registry Editor (Regedt32.exe) on the OWA server.

2. Select the first key listed above.

3. On the **Security** menu, select **Permissions**.

4. Click the **Add** button and select the **Everyone** group.

5. Change the **Type of Access** to **Full Control** and click **OK**.

6. Select the **Replace Permissions on Existing Subkeys** check box and click **OK**.

7. Repeat steps 2 through 6 for the second key listed above.

8. Shut down the OWA services and restart the computer.

For more information on troubleshooting this error message, see the following article in the Microsoft Knowledge Base: Q184304

VBScript Runtime Error '800A01A8' Object Required: 'Application (...)' \ exchange\USA\logon.asp, Line12

This runtime error may be caused by file corruption in the Exchange Active Server Components. A failed installation followed by a successful installation can also cause the errors. The failed installation can cause the reinstallation process to not proceed as expected.

Occasionally, when you try to remove the Active Server Components (ASC) from Exchange Server Setup using **Add/Remove**, the check box for this option cannot be cleared. You may not be able to uninstall just the **Active Server Components** option by using **Add/Remove**.

Modifying the related registry key will allow ASC the to be reinstalled. To make the correct modification, locate the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\Setup

and remove the *String Value* **Web Connector** from the key. This action clears the **ASC** option from the Exchange Server CD Setup program. You should then be able to reinstall the **ASC** option.

For more information on troubleshooting this error message, see the following articles in the Microsoft Knowledge Base: Q186155 and Q178280

HTTP Error 401 401.1 Unauthorized: Log On Failed

This error will occur when you try to access your mailbox through the Active Server Logon page if Internet Information Server (IIS) version 4.0 has been installed on a Microsoft Exchange 5.0 Web Access Server. Exchange Server version 5.0 Web Access is not supported with IIS version 4.0. The only alternative in this situation is to remove IIS version 4.0 and reinstall IIS version 3.0.

For more information on troubleshooting this error message, see the following article in the Microsoft Knowledge Base: Q176587

<Script language="JavaScript">top.location='/exchange/logon.asp'</script>

When you attempt to open a Microsoft Excel or Microsoft Word attachment that is in a public folder or in an e-mail message from within the Outlook Web Access client using Internet Explorer 3.02 or 4.*x*, Internet Explorer starts Excel or Word in the browser. Internet Explorer also inserts this error.

For Internet Explorer 3.02 build 1300, the fix is to install Rfc1867.exe by installing the Internet Explorer 3.02 File Upload Add-On from the Microsoft Web site at http://www.microsoft.com/ie/download/.

Internet Explorer 4.0 does not show this problem. For Internet Explorer 4.01, you must be running build 4.72.3110.8.or later, which is Internet Explorer 4.01 SP1. This is publicly available from http://www.microsoft.com/ie.

For more information on troubleshooting this error message, see the following articles in the Microsoft Knowledge Base: Q178761 and Q170633

ASP 0115 Error in the Browser and Event ID 5 in the Event Log

When you try to access an Exchange Server 5.5 computer using Outlook Web Access (OWA), you may see some of the following symptoms:

- The Internet browser stops responding.
- The Internet browser returns an ASP 0115 error.
- An Event ID 5 is logged in the application event log on the Internet Information Server (IIS) computer. Note that the server is still available, but the ASP page for the Outlook Web Access (OWA) client is unresponsive.

Microsoft has confirmed this to be a problem in Microsoft Outlook Web Access version 5.5. This problem has been corrected in the latest U.S. Service Pack for Microsoft Exchange Server version 5.5. For more information on troubleshooting this error message, see the following article in the Microsoft Knowledge Base: Q184841

HTTP Error 404 File Not Found

After applying Microsoft Exchange Server 5.5 SP 1, you may receive the following error when you try to open messages using the Outlook Web Access client:

> HTTP Error 404 File Not Found. The Web server cannot find the file or script you asked for. Please check the URL to ensure that the path is correct. Please contact the server's administrator if this problem persists.

This is caused by an incorrect URL for the messages. There is a calculation and check performed on the files in the Webdata directory to determine if the object is a file or a directory. If some flags (such as Archive or Compressed) are set on the directory, it may cause the calculation routine to be incorrect and produce the wrong URL.

Microsoft has confirmed this to be a problem in Microsoft Outlook Web Access 5.5. This problem will be corrected in the next U.S. service pack for Microsoft Exchange Server 5.5. For more information on troubleshooting this error message, see the following article in the Microsoft Knowledge Base: Q192930

Server and Registry Settings

Setting the Session Timeout

Use the following steps to set timeout values:

1. Open the Exchsrvr\Webdata*Lang*\lib\logon.inc file using a text editor such as Notepad.

2. Search for the Session.Timeout string. The first occurrence is for authenticated access and the default value is 60 minutes. The second occurrence is for anonymous access and the default value is 20 minutes.

3. Change either or both of the values as appropriate to your situation.

The MSExchangeWeb Registry Key

The Outlook Web Access settings are stored in the following registry key on the IIS computer:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb

This registry key has four subkeys: AcceptLanguage, Applications, Parameters, and Performance.

- AcceptLanguage: This key contains subkeys for all possible accepted languages and a default key. Every key points to United States settings by default, unless you are running JPN, FRN, or GER setup, in which case the key for that language is localized. Each key contains the following values:
    - **CodePage**: The code page to use for this language.
    - **Directory**: The directory in which the localized scripts are located in Webdata.
    - **LCID**: The locale ID, used for things such as date format.
- Applications: Every subkey under Applications is the name of a virtual root that the Exchfilt.dll file uses to determine if it needs to insert a language directory into the URL.
- Parameters: This key contains the following values:
    - **Enterprise**: The enterprise of the computer running Exchange Server.
    - **HTMLQuoting**: Used by RTF-HTML. May not be in use.
    - **Language Pack Directory**: Tells Outlook Web Access where to search for langpack DLLs.

- **RFC1867NoCleanupAtUnload**: Whether Exupload.dll should delete items in the SaveDirectory when it loads.
- **RFC1867SaveDirectory**: Directory to save temporary files in when uploading.
- **RFC1867Trace**: If 0 (zero), there is no trace. Otherwise, put a location of the form the browser submits when uploading a file. The trace goes in the SaveDirectory.
- **Server**: The name of the Exchange Server computer.
- **Site**: The site where the Exchange Server computer is located.
- **Debug**: Adds debug information to JavaScript dialogs.
- **AuthenticatedSessionTimeout**: Authenticated Session Timeout, in minutes.
- **AnonymousSessionTimeout**: Anonymous Session Timeout, in minutes.

- Performance: This key contains standard Performance Monitor (PerfMon) counter information.

Additional Information from Exchange 5.5 Release Notes

Installing the Windows NT Hotfix for Outlook Web Access

When you install Outlook Web Access, you should install the Windows NT hotfix that addresses problems with Secure Sockets Layer (SSL) and memory leaks. This hotfix is for use only with Exchange Server using IIS 3.0. For more information, see the Microsoft Knowledge Base at the Microsoft Technical Support Web site: (http://support.microsoft.com/support).

You can download the hotfix from the Microsoft anonymous FTP server site:

ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/ASP/asp-memfix

The self-extracting zip file is called ASP-Memfix.exe.

Installing Internet Explorer 4.0 after Installing Microsoft Exchange Server

In many cases, you may want to install Internet Explorer 4.0 on your Outlook Web Access server for troubleshooting and setup. If you need to run Internet Explorer and Microsoft Exchange Server on the same computer, it is strongly recommended that you install Internet Explorer 4.0 before installing Microsoft Exchange Server. If you install Internet Explorer 4.0 after installing Microsoft Exchange Server, Internet Explorer modifies the Multipurpose Internet Mail Extensions (MIME) registry database. This results in problems for international mail, especially mail with double-byte character content. If you install Internet Explorer 4.0 after installing Microsoft Exchange Server, complete the

following procedure to correct this problem. You can perform these steps without stopping any Microsoft Exchange Server services.

Note: This procedure is *not* required if you install Internet Explorer 4.0 before you install Microsoft Exchange Server.

1. Copy the Reset.inf file in the Server\Support\Mimedb directory from the Microsoft Exchange Server compact disc to a local hard disk drive.

2. Right-click the file name and click **Install**.

Web Browser Exception Errors When Using 128-bit SSL Authentication

When 128-bit SSL authentication is enabled for IIS, some Web browsers such as Internet Explorer versions earlier than 3.02 build 1310, can quit because an exception error occurs when users access Web documents using Microsoft Outlook Web Access.

To eliminate these types of Web browser exception errors, you can add the following registry key to the IIS computer:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\w3svc\asp \parameters\BufferingOn=1

This enables buffering on the IIS computer. When buffering is enabled, Active Server Pages are parsed completely before any data is sent to Web browsers. Buffering is not enabled for servers by default.

In addition to modifying the registry, you can also control buffering on a per-page basis by inserting <%Response.Buffer = TRUE %> at the top of a page.

Caution: With buffering enabled, more server memory is used to parse Active Server Pages and server performance is slower. Be sure to monitor the server to evaluate the impact of buffering on server performance. You may need to upgrade the server's processor or memory to maintain optimum performance.

For optimum performance of Outlook Web Access when you use 128-bit SSL authentication, consider upgrading your users' Web browsers to versions that have the enhanced ability to handle 128-bit SSL authentication. Internet Explorer 3.02 build 1310 and later versions have enhanced 128-bit SSL authentication capability. For more information about obtaining the latest version of Internet Explorer, use your Web browser to visit http://www.microsoft.com/ie.

Installing Microsoft Outlook 8.03 on an Exchange Server 5.5 Computer

If you install Outlook 8.03 on a Microsoft Exchange Server 5.5 computer, Outlook Web Access does not perform as expected. To solve this problem, run Regsvr32a.exe after installing Outlook. This utility resets the affected registry settings by re-registering Cdo.dll. You can download Regsvr32a.exe from the Microsoft Web site at:

http://support.microsoft.com/support/downloads/dp2439.asp

Run Regsvr32.exe from the command line using the full path to Cdo.dll as the argument. For example, the following command changes the registry settings by re-registering Cdo.dll:

regsvr32.exe *systemroot*\system32\cdo.dll

(where *systemroot* is your Windows NT directory)