CHAPTER 10

Exchange 2003 Tips and Tricks

Now that we have explored the new features in Exchange 2003 along with some of the new features in Outlook 2003 and Windows 2003, I wanted to share with you some of the knowledge and experience I gained as a result of working with Exchange 2003 for the last couple of years. To use a comparison, in this chapter I am going to not only give you a few fish but also teach you how to get more on your own.

I have divided this chapter into several sections. First I'll provide an overview of tuning Exchange 2003. Then I'll discuss some tuning parameters that have been deprecated from Exchange 2000. These are settings you may have added to Exchange 2000 that are no longer needed for Exchange 2003. In addition, I'll cover some new tuning parameters and other settings you can use in Exchange 2003 to control certain aspects of its behavior.

In the sections on tools and resources, I'll show you how to find the latest information on Exchange 2003 and how to use the new Exchange Technical Documentation Library. In addition, I'll cover the package of Exchange tools you can download for free and use to manage, configure, and administer your environment. I'll share with you some great third-party Web sites, forums, communities, and other resources provided by many other Exchange experts and used by countless numbers of Exchange administrators around the world. No one mind can hold it all, but don't let that stop you from trying.

One caveat first: Information in this chapter, including any URLs or other Internet Web site references provided, may change without notice. I have tried to include only those references that I believe will not change anytime in the near future. Unfortunately, because I have no control over these sites, I cannot prevent them from changing. However, if they do change (or if any of the links mentioned anywhere in this book change),

there is a good chance that you will be able to find their new locations. First, it's possible that a moved link will automatically redirect you to the new site. Second, you may be able to search the parent site of some of the provided links to find the new home for the content. Third, your favorite search engine is your friend. For example, you may be able to "refind" any moved or changed content using Google, Yahoo, or one of the many other search engines on the Internet that cache indexed content. Finally, when all else fails, you might try traveling back through time to see the referenced link in its original form. Seriously! You can use the Internet to do this.

One of my favorite Web sites is the Internet Archive at http://www.archive.org. The Internet Archive is a public nonprofit corporation that was founded to build an "Internet library." The library is intended to offer permanent access for researchers, historians, and scholars to historical collections that exist in digital format. But that's not why I like this site so much. I like it because of its *Wayback Machine,* a virtual time-travel machine that enables you to access and browse stored archives of Web pages and sites. The Wayback Machine was born in 1996, when the Internet Archive first began archiving the Web. Since then it has accumulated more than 100 terabytes worth of archived Web sites (about *30 billion!*), which are available for access by the public for free. Here's how it works.

1. Point your Web browser to http://web.archive.org. This is the Wayback Machine home page.
2. In the Wayback Machine field, enter the URL of the Web site you want to access. You can use any valid Web address, including ones that no longer exist.
3. Click the Take Me Back button to start your journey back through time. This will produce a table of search results organized by date.
4. In this table, under the date columns are hypertext links of other dates. You simply click on one of the date links to open the URL you entered as it appeared on that date.

Pretty cool, huh? An asterisk next to a date indicates that the page was changed on that date. For example, if you see "10/15/1999 *" below "10/05/1999," it means that on October 15, 1999, the URL was changed from how it looked on October 5, 1999. Most of the content from the Web sites should be available; however, many images (especially those from before 1999) will likely not be present. But otherwise, the Wayback Machine will show you the site as it appeared on the date whose link you click.

Tuning Exchange 2003

For the most part, Exchange 2003 is self-tuning. In Exchange 5.5 and earlier versions, Exchange shipped with a wizard-based tool called the *Performance Optimizer*. An administrator would launch this tool and answer a series of questions about the server's role, the number and type of users on the server, and what disks were available for use by Exchange. Behind the scenes, the Performance Optimizer would examine available resources and, based on all of this gathered information, it would make some adjustments to the Exchange configuration to tune Exchange properly for each server.

The Performance Optimizer could be used to move databases and transaction log files to different (presumably faster) disks, and it could also be used to limit the amount of memory that the information store (STORE.EXE) could consume. The Performance Optimizer was removed from Exchange starting with Exchange 2000, and it remains missing from Exchange 2003. It was removed because Exchange 2000 (and now Exchange 2003) was made to be self-tuning. If you need to move the databases and transaction logs, that functionality is now found in ESM; however, if you want to limit the amount of memory used by Exchange, you are out of luck—there is no longer any supported way to do this.

There are, however, plenty of opportunities to tune and/or control Exchange's behavior. Some of these settings have already been discussed in previous chapters. For example, in Chapter 2, I wrote about using some new BOOT.INI switches to tune memory allocation on your Exchange server. Chapter 4 covered how to tune ESE buffers, and in Chapter 9, I showed you how to use OWA spell-check throttling to prevent spell-check requests from overwhelming your Exchange server. In this chapter, I'll continue down that path with various settings and other practices you can employ to change and tune how Exchange behaves.

Generally speaking, the goal of performance tuning is to decrease server response time while supporting more users. Most of the tuning and performance boosts you can get from Exchange come from choosing appropriately sized hardware and from employing best practices for the design and deployment of Exchange. Because this was covered in Chapter 2, I won't repeat that information here. Instead, we'll focus on tuning other areas of Exchange. Because many readers are already using Exchange 2000, I'll start by reviewing Exchange 2000 tuning parameters that are no longer necessary in Exchange 2003.

Deprecated Exchange 2000 Tuning Parameters

Although Exchange 2000 did not include the Performance Optimizer, there were still a variety of registry settings and other changes you could make to tune Exchange or change its behavior.[1] Any changes you made to tune or alter the behavior of Exchange 2000 need to be reviewed before implementing Exchange 2003. Indeed, most of them are no longer needed in Exchange 2003, but more importantly some of them can cause problems when used on an Exchange 2003 system. Therefore, before upgrading any Exchange 2000 servers to Exchange 2003, you should review the following information.

Exchange 2000 Clusters

Exchange 2000 included two tuning registry parameters specific to EVSs running in a cluster. Both parameters were designed to prevent a very busy SMTP resource in an EVS from starving other resources in the EVS such as IMAP4 and POP3. The tuning parameters were the *SMTP % of threads* and *Additional threads per processor* values, which were represented in the registry as follows.

```
Location: HKLM\System\CurrentControlSet\Services\SMTPSVC\Queuing
Value: MaxPercentPoolThreads

Location: HKLM\System\CurrentControlSet\Services\SMTPSVC\Queuing
Value: AdditionalPoolThreadsPerProc
```

`MaxPercentPoolThreads` was used to control the percentage of threads used by the SMTP service, and `AdditionalPoolThreadsPerProc` enabled you to control the number of additional threads that could be spawned on a per-processor basis. If you added either of these registry entries to your Exchange 2000 cluster, you should remove them prior to upgrading your EVSs to Exchange 2003.

1. Many of the Exchange 2000 tuning parameters were documented in a Microsoft white paper titled "Microsoft Exchange 2000 Internals: Quick Tuning Guide." If you used this guide to tune your Exchange 2000 server, you likely need to remove some tuning parameters before upgrading to Exchange 2003.

Directory Service Access Cache

As the name suggests, Directory Service Access (DSAccess) is an internal component in Exchange that controls how all Exchange components access Active Directory. The primary function of DSAccess is to keep tabs on various directory-related things. For example, DSAccess discovers the Active Directory topology and detects the state of domain controllers and global catalog servers (up or down). In addition, all directory queries are routed through DSAccess, such as recipient resolution, configuration setting look-ups, and others. As part of its job, DSAccess maintains an in-memory cache of the results of some of these queries so that if the same information is requested twice, it can be retrieved from the DSAccess cache instead of through another LDAP query against Active Directory. The size of the in-memory cache is configurable, in that you can set a maximum size for various cached items.

Many administrators found that on larger Exchange 2000 servers, the out-of-the-box values for the maximum cache size for recipient look-ups and the maximum cache size for configuration look-ups were not always optimized for their servers. On systems with an undersized DSAccess cache, it was common for local message delivery and/or address book resolution to be slow. Once the maximum size of the recipient cache was increased and the size of the configuration cache was decreased, performance would improve. The DSAccess cache tuning parameters for the configuration data cache and the user object cache were represented in the registry as follows.

```
Location:
HKLM\System\CurrentControlSet\Services\MSExchangeDSAccess\Instance0
Value: MaxMemoryConfig

Location:
HKLM\System\CurrentControlSet\Services\MSExchangeDSAccess\Instance0
Value: MaxMemoryUser
```

In Exchange 2000, each cache pool (e.g., the configuration cache, the recipient cache, and so on) was initially set at 25MB in size. To improve performance, the default values for the configuration and recipient caches have been optimized in Exchange 2003. The configuration data cache, which more often than not never needed anywhere near 25MB, now

defaults to 5MB. The user object cache, which was often undersized for larger systems, now defaults to 140MB. Therefore, you should remove the `MaxMemoryConfig` and `MaxMemoryUser` registry entries prior to upgrading from Exchange 2000 to Exchange 2003.

Extensible Storage Engine Heaps

Like other operating systems, Windows includes a process-wide heap manager that handles memory operations for all processes. Each time a process instantiates, a default heap (called the *process heap*) is created for that process. Programs or modules loaded in that process can also create additional heaps if needed. Exchange is one program that does this.

In Exchange 2000, each time the Exchange information store was started, the STORE.EXE process got its initial process heap. Then, a module loaded in the information store process—ESE.DLL—allocated four JET heaps for each processor present in the system. Although these heaps were separate pools of memory in the information store process, they were collectively referred to as the *ESE multiheap.* On a single CPU system, ESE allocated four JET heaps. On a dual CPU system, it allocated eight; on a quad system, it allocated sixteen; and so forth. When Exchange 2000 was installed on systems with four or more CPUs, it was found that the ESE multiheap caused excessive virtual memory consumption, which in turn led to performance problems. Ironically, the problem was worse on systems with a large amount of resources installed (multiple CPUs and multiple gigabytes of memory).

To correct this problem, Microsoft recommended that customers with large Exchange 2000 servers add the following registry entry to their systems.

```
Location: HKLM\Software\Microsoft\ESE98\Global\OS\Memory
Value: MPHeap parallelism
Type: REG_SZ
```

The value data setting depended on the number of CPUs present in the system, and if you added or removed CPUs to the system in scale-up or scale-down procedures, you had to manually readjust this setting. Exchange 2003 now automatically calculates the optimum number of heaps to allocate based on the unique specifications of each system. Therefore, you should remove the `MPHeap parallelism` registry entry from Exchange 2000 servers prior to upgrading to Exchange 2003.

Initial Memory Percentage

In Chapter 7, I wrote about virtual memory and the importance of monitoring it on an Exchange server. It is especially important to watch on Exchange servers for two reasons: (1) the more virtual memory available, the greater the load that can be handled; and (2) performance problems can occur (especially on Exchange clusters) when virtual memory becomes too fragmented. When virtual memory becomes too fragmented, Exchange logs the following event in the Application event log.

```
Event Type: Error
Event Source: MSExchangeIS
Event Category: Performance
Event ID: 9582
Date: 10/10/2003
Time: 3:42:38 PM
User: N/A
Computer: EX2K3
Description: The virtual memory necessary to run your Exchange
server is fragmented in such a way that normal operation may begin
to fail. It is highly recommended that you restart all Exchange
services to correct this issue.
```

As this event log entry indicates, restarting all Exchange services was needed in order to correct the problem. If this happened regularly, you ended up restarting Exchange frequently, and both your users and management probably wondered why their e-mail server was so unreliable.

To combat the virtual memory fragmentation problem, Microsoft introduced the following registry entry and recommended value in Exchange 2000 that hard-coded Exchange's initial memory allocation to 10% of the total amount of physical memory in the system.

```
Location:
HKLM\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem
Value: Initial Memory Percentage
Type: REG_DWORD
Value Data: 0xa (hex)
```

By starting out with this initial allocation and then growing from there, virtual memory fragmentation would not occur as often. As I mentioned in

Chapter 7, Exchange 2003 includes support for special startup switches in Windows 2000 Advanced Server and Windows Server 2003 that help reduce virtual memory fragmentation, and Microsoft made additional changes to help prevent virtual memory fragmentation in Exchange clusters. As a result, the `Initial Memory Percentage` registry value is no longer needed. Moreover, because it does not work on an Exchange 2003 server, you should remove this value from all Exchange 2000 servers prior to upgrading to Exchange 2003.

Log Buffers

As a database that passes the ACID (Atomic, Consistent, Isolated, and Durable) test for transaction-based activity, Exchange first writes all activity to transaction logs and then commits the transactions to the database file. But before Exchange writes anything to a transaction log, it first holds the information in memory in an area called *log buffers.* Unlike the settings mentioned so far, which are registry values, the size of the log buffers is controlled by an attribute of the information store object in Active Directory—`msExchESEParamLogBuffers`.

Throughout the product life of Exchange 2000, the recommended best practice setting for the `msExchESEParamLogBuffers` attribute changed a few times. Out of the box, it was set to `84`, which was determined to be too low for heavily used servers, especially clustered back-end servers. When Service Pack 2 for Exchange 2000 was released, Microsoft recommended that customers adjust this value from `84` to `9000`. When Service Pack 3 was released, Microsoft recommended that customers readjust the value down from `9000` to `500`. Because the out-of-the-box value for `msExchESEParam LogBuffers` in Exchange 2003 is `500`, you will want to use the ADSI Edit tool to delete any manual tuning entries (even if set to `500`) and return the value for this attribute back to `<Not Set>`.

Maximum Number of Open Tables

Although it typically provided little bang for the buck, another way to combat memory fragmentation and allocation issues in Exchange 2000 was to reduce the maximum number of open tables that can be used by Exchange. Exchange 2000 cached data about folders that were not currently accessed, a behavior that in some cases contributed to virtual memory fragmentation. To reduce the cache's impact on virtual memory fragmentation, the `msExch ESEParamMaxOpenTables` attribute in Active Directory would be lowered.

Typically this change was made only at the direction of Microsoft PSS; however, it was a documented value, so many administrators have made this change. Certainly you'll want to check your own storage groups to see if the value exists. It was often used in tandem with the /3GB switch in the Windows BOOT.INI file, so it's a pretty safe bet that if you are using /3GB, you probably also have this value set.

`msExchESEParamMaxOpenTables` is an attribute of storage groups. The recommended value for this attribute also changed periodically throughout the life of Exchange 2000. In Service Pack 2, the default value was automatically set to `42500` on four-way systems and `85000` on eight-way systems. In Service Pack 3, this was changed to `13800` and `27600`, respectively. If you do find a value set for `msExchESEParamMaxOpenTables` on any Exchange 2000 storage group, regardless of its value you will want to return the value for this attribute back to `<Not Set>` prior to upgrading to Exchange 2003.

Outlook Web Access—Content Expiry

Like Exchange 2000 OWA, the Exchange 2003 version of OWA is comprised partially of static files (such as image files, scripts, and so forth). Typically these files were changed only when administrators either customized one or more OWA files or installed an Exchange service pack. Despite the fact that the files remained unchanged for long periods, they were marked as expiring one day after being fetched by the Web browser. Because the files expired each day instead of being retrieved from the browser cache, they were pulled down every day by every user from the OWA server—the same file, the same user, different days. To stop this insanity, Microsoft recommended that the virtual directory that served the static files—Exchweb—be configured with a much longer content expiry (a year or so).

While this method worked to reduce the load on your network and your OWA server in Exchange 2000, it doesn't work in Exchange 2003. In fact, on Exchange 2003 servers, the Exchweb virtual directory should *always* have its content expiration set to 1 day. It should not be disabled, and it should not be set to anything greater than 1 day.

SMTP Service Tuning

On busy Exchange 2000 systems that sustained large SMTP message queues (e.g., an average of 1,000 or more), performance constraints were encountered because of a default setting on the SMTP service of a maximum of

1,000 file handles. Each time the SMTP transport stack on an Exchange 2000 (or Exchange 2003) server receives a message, it is streamed out to the file system, where it waits to be routed to its destination. To write it to the file system, the SMTP transport stack obtains a file handle and then passes the message into that handle. Because Exchange 2000 defaulted to a maximum of 1,000 file handles, the SMTP service could write only 1,000 simultaneous messages to the file system.

To improve performance for these large systems, three registry entries were often simultaneously adjusted to increase the maximum number of file handles that could be opened by the SMTP service (so that more messages could be processed) and to decrease the number of open file handles for the installable file system, another Exchange component (to avoid running out of memory when the queue is large). These registry values, which did not exist by default and therefore needed to be added manually, are listed here.

```
Location: HKLM\System\CurrentControlSet\Services\SMTPSVC\Queuing
Value: MsgHandleThreshold
Type: REG_DWORD

Location: HKLM\System\CurrentControlSet\Services\SMTPSVC\Queuing
Value: MsgHandleAsyncThreshold
Type: REG_DWORD

Location: HKLM\System\CurrentControlSet\Services\Inetinfo\Parameters
Value: FileCacheMaxHandles
Type: REG_DWORD
```

The `MsgHandleThreshold` and `MsgHandleAsyncThreshold` entries would be set to the same value (some value greater than `1000`), and the `FileCacheMaxHandles` entry would be reduced from `800` to `600`.

Exchange 2003 dynamically calculates the appropriate settings for SMTP files handles, so these settings are no longer needed. Therefore, before upgrading any Exchange 2000 servers with these settings to Exchange 2003, you should delete the entries from the registry.

Exchange 2003 Tuning Parameters

Now that we have gone over the legacy tuning parameters from Exchange 2000 that need to be removed, let's dive into the new tuning parameters in Exchange 2003. Some of these parameters (e.g., the BOOT.INI switches, the OWA spell-check throttling, and so on) have been mentioned in previous chapters, so those won't be duplicated here. I have listed the Exchange 2003 tuning parameters in the following subsections.

Outlook Web Access Parameters

OWA is highly configurable. We've discussed in earlier chapters some features (such as themes and spell-check management) that demonstrate this. You can also configure or enable other settings that provide even more control over the OWA experience, such as attachment blocking, access to freedocs, control over the OWA cookie timeout, enhanced segmentation, and more.

Attachment Blocking

As part of Microsoft's Trustworthy Computing initiative, Exchange 2003 OWA automatically blocks attachments with certain extensions. OWA prevents the sending and opening of a superset of attachments and MIME types using a two-level blocking mechanism. Level 1 items are totally blocked. Level 2 items can be accessed, but only if first saved locally. The list of blocked Level 1 and Level 2 file extensions and blocked MIME types are configured through four registry entries, which are listed in the following registry entries showing their default values. As you can see, many of the default Level 1 entries for file extensions and MIME types are also default Level 2 entries. When the same entry is present for both levels, Level 1 takes precedence, and the attachment is blocked. You are free to edit any of these entries to suit your organization's specific needs. If you reinstall or update Exchange, your changes will remain.

```
Location: HKLM\System\CurrentControlSet\Services\MSExchangeWeb\OWA
Value: Level1FileTypes
Type: REG_SZ
Value Data:
ade,adp,app,asx,bas,bat,chm,cmd,com,cpl,crt,csh,exe,fxp,hlp,hta,
```

```
inf,ins,isp,js,jse,ksh,lnk,mda,mdb,mde,mdt,mdw,mdz,msc,msi,msp,
mst,ops,pcd,pif,prf,prg,reg,scf,scr,sct,shb,shs,url,vb,vbe,vbs,
wsc,wsf,wsh

Location: HKLM\System\CurrentControlSet\Services\MSExchangeWeb\OWA
Value: Level1MIMETypes
Type: REG_SZ
Value Data: application/hta,x-internet-signup,
application/javascript,application/x-javascript,
text/javascript,application/msaccess,application/prg,
text/scriptlet

Location: HKLM\System\CurrentControlSet\Services\MSExchangeWeb\OWA
Value: Level2FileTypes
Type: REG_SZ
Value Data:
ade,adp,asx,bas,bat,chm,cmd,com,cpl,crt,exe,hlp,hta,htm,html,htc,
inf,ins,isp,js,jse,lnk,mda,mdb,mde,mdz,mht,mhtml,msc,msi,msp,mst,
pcd,pif,prf,reg,scf,scr,sct,shb,shs,shtm,shtml,stm,url,vb,vbe,vbs,
wsc,wsf,wsh,xml,dir,dcr,plg,spl,swf

Location: HKLM\System\CurrentControlSet\Services\MSExchangeWeb\OWA
Value: Level2MIMETypes
Type: REG_SZ
Value Data: text/xml,application/xml,application/hta,text/html,
application/octet-stream,application/x-shockwave-flash,
application/futuresplash,application/x-director
```

In addition to this level of attachment blocking, OWA 2003 enables you to selectively block attachments for users based on how they are accessing OWA. For example, for security, bandwidth, or other reasons, you might wish to block attachments for users who access OWA from the Internet (e.g., via a front-end server) while allowing full access to attachments for users accessing OWA from your private network (e.g., directly via the back-end server). To do this, you need to add the following new entry to the registry(ies) of your OWA server(s).

```
Location: HKLM\System\CurrentControlSet\Services\MSExchangeWeb\OWA
Value: DisableAttachments
```

```
Type: REG_DWORD
Value Data: 0, 1, or 2 (dec)
```

If `DisableAttachments` is not present or is set to `0`, the standard Level 1/Level 2 attachment blocking is performed. When `DisableAttachments` is set to `1`, all attachments are blocked. If you set `DisableAttachments` to `2`, attachments not blocked by Level 1/Level 2 blocking are allowed on back-end servers but not on front-end servers.

Freedocs

While you may not have heard of freedocs, chances are you have used them before. If you have ever dragged and dropped a document or a file directly into an Exchange folder (as opposed to attaching it to a message or post), you have used freedocs. *Freedocs* is the term given to stand-alone data in the information store. Because the dropped file is not an attachment of a message, it is considered a "free document" or a freedoc.

Freedocs are not new to Exchange 2003; they were present in all prior versions of Exchange. For example, in Exchange 2000, freedocs became accessible via OWA URLs (e.g., http://ex2k3/public/training/exchange2003/intro_to_e2k3.doc). What is new to Exchange 2003 (as part of Secure by Default) is the ability to control access to freedocs through these OWA URLs. Here is a registry entry you can add to your OWA servers to control access.

```
Location: HKLM\System\CurrentControlSet\Services\MSExchangeWeb\OWA
Value: EnableFreedocs
Type: REG_DWORD
Value: 0, 1, 2, or 3 (dec)
```

If `EnableFreedocs` is not present or is set to `0`, freedocs are completely blocked in OWA. Because the value is not present by default, freedocs are blocked out-of-the-box in OWA. When `EnableFreedocs` is set to `1`, freedocs are accessible only when accessed directly via a back-end server; freedocs will not be accessible to OWA users connecting through a front-end server. If you set the value to `2`, freedocs will be accessible from back-end servers and from any front-end server configured with a Host Header entry that matches the following registry on the back-end server.

```
Location: HKLM\System\CurrentControlSet\Services\MSExchangeWeb\OWA
Value: AcceptedAttachmentFrontEnds
Type: REG_SZ
Value: comma-delimited list of FE servers, e.g.,
www.something.com,www.somethingelse.com
```

Finally, when `EnableFreedocs` is set to `3`, freedocs are accessible to all OWA users.

OWA Cookie Timeout

In Chapter 5, I described FBA, which makes using OWA more secure. FBA uses cookies authentication; that is, it stores the user credentials in a cookie that expires after a predetermined amount of time. In Chapter 6, I detailed the default session inactivity timeout settings for trusted (private) computers and shared (public) computers (the `TrustedClientTimeout` and `PublicClientTimeout` settings). In addition to idle timeouts, you can also specify a timeout value for the FBA cookie. To do this, add the following registry entry to the OWA server.

```
Location: HKLM\System\CurrentControlSet\Services\MSExchangeWeb\OWA
Value: KeyInterval
Type: REG_DWORD
Value Data: Timeout value (in minutes)
```

You can set `KeyInterval` to any value between `1` and `1440` (between 1 minute and 24 hours). If you add this registry entry, you will need to stop and restart the World Wide Web Publishing Service for the change to take effect.

Enhanced Segmentation

Exchange 2000 Service Pack 2 introduced a new feature called *OWA segmentation.* OWA segmentation, which is described in Microsoft Knowledge Base article 311154 (among other places), enables administrators to selectively enable and disable specific OWA features. OWA can be segmented or a per-user or per-server basis, with user settings taking precedence over server settings. There are a variety of reasons to segment OWA; for example, some organizations do not want users to have access to all OWA features because of security reasons or training concerns. Monetary

reasons also exist—application service providers that sell hosted Exchange services may want to segment OWA and sell both a lite version and a full-featured version of OWA. This is sometimes referred to as *tiered licensing* or *provisioning*.

Per-server segmentation is performed by adding a specific hexadecimal value to the registry of the mailbox server, as shown here.

```
Location: HKLM\System\CurrentControlSet\Services\MSExchangeWeb\OWA
Value: DefaultMailboxFolderSet
Type: REG_DWORD
Value Data: See Table 10.1
```

Per-user segmentation is performed by configuring the `msExchMailboxFolderSet` attribute in Active Directory. This is an attribute of all mailbox-enabled users. In Exchange 2000, this attribute did not exist prior to Service Pack 2. To segment OWA you had to manually extend the Active Directory schema using OWASCHEMA.VBS, which added this attribute. Because this was a manual process, it is possible that your Exchange 2000 forest does not contain this attribute. However, as soon as Exchange 2003 FORESTPREP is performed, this attribute will be added.

Both `DefaultMailboxFolderSet` and `msExchMailboxFolderSet` are decimal values based on the bit masks shown in Table 10–1. Each bit mask corresponds to an individual OWA feature. Create a list of the features you want to enable, and add together their bit mask values. Then enter this sum as the decimal value in the registry or in Active Directory. Many of these values existed in Exchange 2000 Service Pack 2 and later; values that are new to Exchange 2003 have a checkmark in the New to Exchange 2003 column.

Once you have added all of the hex values, enter the sum in the appropriate place. For example, if you want to enable access to only the Messaging and Calendar features, you would use the following formula:

```
  0x00000001 (Messaging)
+ 0x00000002 (Calendar)
------------
  0x00000003
```

You would then enter `0x00000003` in the registry or in Active Directory, depending on where you want to configure this.

Table 10–1 OWA Segmentation Values

Exchange Feature	Bit Mask Value (Hex)	New to Exchange 2003
All Features	0xFFFFFFFF	
Calendar	0x00000002	
Contacts	0x00000004	
Journal	0x00000010	
Junk E-mail	0x00010000	√
Messaging	0x00000001	
New Mail	0x00000100	
Notes	0x00000020	
Public Folders	0x00000040	
Reminders	0x00000080	
Rich Client	0x00000200	
Rules	0x00004000	√
S/MIME	0x00000800	√
Search Folders	0x00001000	√
Signature	0x00002000	√
Spell Check	0x00000400	√
Tasks	0x00000008	
Themes	0x00008000	√

Enabling Public Folder Replies

By design, unless you are accessing OWA through a front-end server (and not directly via a back-end server), you will not be able to use the Reply, Reply All, or Forward functions for messages contained in public folders. While you'll be able to reply to and forward all messages in your mailbox regardless of how you access OWA, unless you go through an Exchange 2003 front-end server, you will not be able to take these actions for public folder messages.

In addition to these restrictions, by default there is a 2MB limit for all messages sent via a reply or forward action. You can override this limit by adding the following registry entry to your front-end servers, which specifies the allowable maximum size.

```
Location: HKLM\System\CurrentControlSet\Services\MSExchange\OWA
Value: maxPFReplyForwardSize
Type: REG_DWORD
Value Data: X
```

For the `maxPFReplyForwardSize` entry, *X* is the maximum size you want to set in kilobytes.

Outlook Parameters

In previous chapters, I wrote about the new features in Outlook 2003 specifically targeted at Exchange users. Features such as RPC over HTTP (which is really RPC over HTTPS), Cached Exchange Mode, and others help to greatly improve the overall experience for Outlook users. In addition to these new features, a variety of administrative options can be set to improve the experience for both Outlook users and Exchange administrators, such as improved alias matching, the ability to disable MAPI compression, control of RPC over HTTPS polling, and improved behavior regarding the ability to restrict access to Exchange based on the version of Outlook that is running.

Alias Matching

If you enter an alias into the TO, CC, or BCC fields in Outlook, before the message can be sent the recipients must first be resolved. Outlook would look up the information in the Global Address List and/or in a personal address book or in Outlook contacts. By default, any partial name that you enter is checked against three naming fields: first name, last name, and alias. Consider the following entries in the Global Address List.

```
First Name        Last Name         Alias
John              Doe               JohnD
Johnny            Roe               JohnR
```

If you enter "John" on any of the address field lines, Outlook will match both entries and ask you to choose which entry to use. Previous versions of Outlook enabled you to bypass duplicate entries by appending an equals sign (=) to the beginning of your entry. For example, to bypass duplicate entries and specify Johnny Roe, you would enter "=JohnR" into the address field. Because Johnny Roe's alias is JohnR, it is instantly matched.

Outlook 2003 improves this behavior by eliminating the need to use the equals sign if you have added the following Outlook registry setting.

```
Location: HKLM\Software\Microsoft\Exchange\Exchange Provider
Value: OAB Exact Alias Match
Type: REG_DWORD
Value Data: 1 (dec)
```

If the `OAB Exact Alias Match` value is not present or is set to anything other than `1`, Outlook 2003 will behave like all other Outlook clients and will exactly match an alias only when the equals sign is used. If the value is present and set to `1`, Outlook will resolve the exact alias without providing a list of possible matches.

MAPI Compression Settings

In Chapter 2, I wrote about a new feature called *MAPI compression* (referred to internally as *AirMAPI*) that is available when you use Outlook 2003 and Exchange 2003 together. AirMAPI compresses all content at the Exchange server before sending it to Outlook, which decompresses it. When AirMAPI is enabled, another feature called *Buffer Packing* is also enabled. With Buffer Packing, information sent from Exchange to Outlook is packaged in bigger, optimized buffer packets, which reduces the number of packets that ultimately need to be sent.

While AirMAPI and Buffer Packing provide some impressive performance improvements, they can hinder some troubleshooting efforts. When troubleshooting client-server issues, a common practice is to use a network sniffer such as Network Monitor to capture network traffic for analysis. Because AirMAPI is enabled by default, it can make troubleshooting more difficult because all of the data in the trace is compressed and therefore not readily discernable. Fortunately, you can use the following server-side registry entries to control and/or disable AirMAPI and Buffer Packing if needed.

```
Location:
HKLM\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem
Value: Rpc Compression Enabled
Type: REG_DWORD
Value Data: 0 or 1
```

```
Location:
HKLM\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem
Value: Rpc Compression Minimum Size
Type: REG_DWORD
Value Data: X

Location:
HKLM\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem
Value: Rpc Packing Enabled
Type: REG_DWORD
Value Data: 0
```

None of these entries exist by default, and therefore they need to be manually added if you want to configure or disable AirMAPI. If `Rpc Compression Enabled` is not present or is set to `1`, AirMAPI compression is enabled. Any other value will disable it. The `Rpc Compression Minimum Size` entry is used to specify a minimum size for an RPC packet in order for AirMAPI to be used. If this value is not present, a default value of 1,024 bytes is used. In this example, *X* represents the desired minimum size in bytes.

Finally, you can selectively enable and disable Buffer Packing by using the `Rpc Packing Enabled` entry. If this entry is not present, a value of `1` is assumed and Buffer Packing is enabled. When this entry is set to `0`, Buffer Packing is disabled.

When changing any of these settings, you will need to stop and restart the Information Store service for the change(s) to take effect. Because of the benefits provided by AirMAPI and Buffer Packing, I recommend disabling these features for troubleshooting purposes only.

RPC over HTTPS Polling

When making an initial connection to an Exchange server, Outlook registers itself for new message notifications. Whenever a new message is received in an Outlook user's mailbox, Exchange sends a notification to Outlook using UDP. This notification is essentially a small flag to the client that a new message is present and needs to be displayed. When Outlook receives the UDP notification, it retrieves the message from the Exchange server and displays it in the appropriate folder (e.g., the Inbox).

New message notifications are intended for Outlook clients that are running in either online mode or Cached Exchange Mode, and they won't

work for Outlook clients using RPC over HTTPS. In fact, when using RPC over HTTPS, Outlook does not register for notifications (because it won't be able to receive them). Instead, Outlook clients using RPC over HTTPS use a polling mechanism to check for new messages. While polling is initiated by Outlook, the polling frequency is dictated by the Exchange server. Polling is not new to Outlook 2003; Outlook 2002 automatically reverts to polling if the UDP notification fails. However, new in Exchange 2003 is your ability to configure a polling interval for RPC over HTTPS clients.

By default, Outlook 2003 will poll every 60 seconds. You can change the frequency by adding the following registry entry to the Exchange server that contains the user's mailbox.

```
Location:
HKLM\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem
Value: Maximum Polling Frequency
Type: REG_DWORD
Value Data: X
```

For this value, *X* is the minimum number of milliseconds between polling intervals. If `Maximum Polling Frequency` is not present, a default value of 60 seconds (`60000` when set in milliseconds) is used. Again, this is the minimum number of milliseconds between polling intervals, which means that polling does not take place every 60 seconds. Instead, polling will occur any time between the polling frequency interval and twice that interval. For example, if you set `Maximum Polling Frequency` to 90 seconds, polling will take place between 90 and 180 seconds after the last poll.

When configuring this value, keep in mind the following important information. First, Microsoft does not recommend *lowering* this value because of the performance hit to Exchange, Outlook, and the network. Therefore, you should not use a polling frequency less than 60 seconds. Second, you may not need to adjust polling at all because many user actions will actually check for the new message flag as part of internal operations. For example, if you switch folders or open a message, new items on the server will be displayed. This occurs because when Outlook sends necessary RPC requests to Exchange to effect the user action, the new message flag is checked and, if present, the new message notification is included in the RPC response sent back to Outlook.

Outlook Version Blocking

Both Exchange 2000 and Exchange 2003 support a feature that enables administrators to prevent specific versions of MAPI clients from connecting to and using Exchange. For example, if you want to allow only Outlook 2003 users to connect to your Exchange server, you would configure the registry on the Exchange server as described in Microsoft Knowledge Base article 288894. You can also use this feature to disable all MAPI access to an Exchange server (by specifically blocking all known MAPI clients) or to block unpatched versions of Outlook 2003 (or any other Outlook client) from using Exchange until they have all required updates.

After adding the appropriate settings to the registry, Exchange 2000 required you to stop and restart the Information Store service for the change to take effect. New in Exchange 2003 is the ability to dynamically read this value from the registry and apply it without having to restart the store. A background thread checks this value every 15 minutes, so the most you'll ever need to wait for this change to take effect is 15 minutes. Because the 15-minute cycle for the background thread is hard-coded, if you want the change to take effect sooner, you still need to cycle the Information Store service.

Exchange Server Parameters

On an Exchange 2003 server you can configure a few additional parameters that provide you with additional levels of control. Some of these parameters have already been discussed in other chapters, such as the `Recovery SG Override` setting described in Chapter 8 and the OWA spell-check throttles described in Chapter 9. The additional parameters enable you to control out-of-office messages (OOFs)[2] and delivery status notification (DSN) messages, reenable the M: drive, and designate a specific system for backfilling public folders.

2. In case you are wondering why people use *OOF* for *out-of-office* instead of *OOO*, it has to do with the original implementation of the term. Instead of the term *out-of-office*, people used to use the term *out-of-facilities*. Thus *OOF* is actually an acronym for *out-of-facilities*, but now it is generally used to mean *out-of-office*. Special thanks to KC Lemson at Microsoft for sharing this interesting trivia bit (see http://blogs.gotdotnet.com/kclemson/CategoryView.aspx/Messaging%20Trivia).

Controlling Out-of-Office Messages

When an Outlook user enables the Out of Office Assistant to generate OOFs, an OOF is generated for messages sent to this user when his or her e-mail address is explicitly listed in the TO or CC fields or when he or she is a member of a distribution list (or mailing list) listed in the BCC field. For a variety of reasons, you may wish to limit OOFs to those cases where a user is specifically listed in the TO or CC fields and not in a BCC field. This feature is particularly useful in situations where users are members of mailing lists managed by foreign (i.e., non-Exchange) messaging systems.

To suppress the generation of OOFs for BCC'd distribution lists, add the following registry entry to the Exchange server that contains the mailbox(es) you want to affect.

```
Location:
HKLM\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem
Value: SuppressOOFsToDistributionLists
Type: REG_DWORD
Value Data: 1
```

If the `SuppressOOFsToDistributionLists` value is not present or is set to anything other than `1`, the behavior will remain unchanged. However, when set to `1`, this registry entry will suppress OOFs for BCC'd distribution lists. When you use this feature, keep in mind that an OOF will still be sent in cases where a message is sent to an individual recipient using the BCC field only (i.e., no recipients in TO or CC fields) even if `SuppressOOFs ToDistributionLists` is enabled. This applies only if the recipient is in the BCC field and the TO and CC fields are blank. If another recipient is present in the TO or CC fields, `SuppressOOFsToDistributionLists` will suppress the OOF.

Controlling Delivery Status Notifications

When an Exchange user sends a message to an external recipient whose messaging system is configured to use custom nondelivery reports (NDRs), the user may not receive the custom NDR and instead may receive a standard NDR similar to the following one.

```
From: System Administrator
To: <sender name>
Subject: Undeliverable: <subject>
```

```
Your message did not reach some or all of the intended recipients.

    Subject: <subject>
    Sent: <date> <time>

The following recipient(s) could not be reached:

    <recipient> <date> <time>

The e-mail account does not exist at the organization this message
was sent to. Check the e-mail address, or contact the recipient
directly to find out the correct address. <Domainname #5.1.1>
```

A standard NDR is received instead of the foreign system's custom NDR because the Exchange information store reformats the message as the message is converted to a MAPI message. When this happens, any customizations made to the NDR are lost. (Note though that this happens only with MAPI clients; if you access the message using a non-MAPI client instead, the custom NDR will be preserved.)

In Exchange 5.5 and earlier versions, the custom NDR was also preserved even when viewed by a MAPI client. Exchange 2000 added support for the *Report* content type as prescribed in RFC 1892, and this effectively broke custom NDRs. Based on feedback from its customers, Microsoft allowed this behavior to be modified by using a registry entry on the Exchange server for customers running Exchange 2000 Service Pack 3 plus the hotfix from Microsoft Knowledge Base article 812806 or later. The code changes in the hotfix have been rolled into Exchange 2003, enabling you to add the following registry entry to your Exchange server to override the conversion behavior and render the NDRs as intended by the foreign mail system.

```
Location:
HKLM\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem\
InternetContent
Value: RenderDSNsAsMessages
Type: REG_DWORD
Value Data: 1
```

If `RenderDSNsAsMessages` is not present or is set to anything other than `1`, the custom NDR will not be preserved. If the registry entry is set

to 1, the custom NDR is preserved and viewable by MAPI clients. This change takes effect dynamically so there is no need to restart the server or any services.

Reenabling the M: Drive

As I wrote in Chapter 3, Exchange 2000 shipped with a feature known as the Exchange Installable File System (ExIFS, often simply called IFS). ExIFS is a kernel-level driver that exposes some of the data from the Exchange information stores to the Windows file system through a drive letter mapping. By default, the drive letter used was M. If this letter was already in use for a drive mapping, the next available letter was used (e.g., N, O, and so on). The ExIFS drive mapping was not the same as a local or network drive, although it was widely misinterpreted as one. Many administrators treated the M: drive like a physical disk; some administrators scanned the drive with antivirus scanners or took backups of it, mistakenly believing they were backing up their Exchange data. Others set permissions on Exchange items through the file system. Unfortunately, these actions were not supported, and in most cases they actually *damaged* the information store databases.

Remember, the whole idea of product evolution is to design and evolve the product in a way that keeps support calls to an absolute minimum. With ExIFS, the exact opposite was happening; administrators with damaged databases posted frantic requests for help in Microsoft's newsgroups, while at the same time PSS was receiving a high volume of calls on this same issue. To address this problem, and more importantly to prevent it from happening again with Exchange 2003, Microsoft changed the default behavior for ExIFS and left it turned off. Whether you upgrade from Exchange 2000 or install a fresh copy of Exchange 2003, the drive mapping for ExIFS will not be present unless and until you enable it.

From a best-practice perspective, you should not enable the ExIFS drive mapping unless you have a very specific reason you need to do this. If you do reenable the M: drive (regardless of what drive letter is actually assigned), you should be aware of the following caveats.

- Only non-MAPI content should be accessed via this drive. Accessing MAPI data via ExIFS is not supported and could damage your store.
- You should not share out the M: drive or any folders under this drive. In other words, do not create a Windows file share for SMB-based

access. If you need to expose the non-MAPI data to network users, you can use Web Folders instead.

- If you enable the drive mapping, you will need to reboot Exchange every time you install an update or an upgrade (e.g., a new service pack).
- The same restrictions in Exchange 2000 still apply. Do not scan the M: drive; do not use backup software to back up the M: drive; and do not set any ACLs or other permissions on the M: drive.

If after reading this far you still want to reenable the M: drive, you can do so by adding the following registry entry to your Exchange server.

```
Location: HKLM\System\CurrentControlSet\Services\ExIFS\Parameters
Value: DriveLetter
Type: REG_SZ
Value Data: M
```

If you prefer to use something other than M for the drive letter, simply enter the desired letter for the value data. You will then need to reboot the Exchange Information Store service for this setting to take effect. Also, if you decide to later disable this drive mapping, simply removing the registry entry and cycling the information store may not be sufficient. You may also need to use the procedure documented in Microsoft Knowledge Base article 305145.

Backfilling the Public Folder

Whenever any update is made to an Exchange public folder, a change number (CN) is assigned to the folder, which is used by the replication engine to track folder updates. A set of CNs is called a *CNSet*. Whenever one Exchange server sends updates to another Exchange server, it includes its CNs. The receiving server reads the sending server's CNs to determine whether any changes have been made and whether the receiving server is missing any data as a result of the change(s). If it is missing data, backfilling will occur.

Backfilling provides a recovery mechanism in a variety of situations, such as when a public store has been restored from a backup or has been offline for some time, or when replication messages are somehow lost in transit. If a public folder store detects a gap in any folder's CNSet, it issues

a *Backfill Request* message. The server to whom the request is sent responds with a *Backfill Response* message that includes the missing data.

A new feature in Exchange 2003 is a setting that provides you with the ability to override the default public folder backfill algorithm and designate a preferred server for backfill requests. This setting can be implemented as an Active Directory attribute or as a registry setting on the Exchange server. Before an Exchange server sends a backfill request, the Active Directory attribute is checked first. If the attribute is null, the registry is checked. If the entry is not present, the default algorithm for public folder backfilling is used.

If you want to use the Active Directory attribute, enter the GUID of the desired backfill server to the `msExchPreferredBackfillSource` attribute on the Exchange server's public information store object (e.g., on the server sending the Backfill Request message, not on the one you want to use as the backfill server). If you prefer using the registry, add the following entry on the server sending the Backfill Request message.

```
Location: HKLM\System\CurrentControlSet\Services\MSExchangeIS
Value: Preferred Backfill Source
Type: REG_SZ
Value Data: Public Folder Store GUID of desired backfill server
```

Both the Active Directory attribute and the registry change take effect dynamically (they are checked as part of each backfill request), so there is no need to stop or start anything.

Exchange 2003 Tools

When managing Exchange environments, having a large and versatile set of tools is a must. When you consider that Exchange 2003 is a combination of very different technologies—some related to storage and others to transport—and that it is tightly integrated with Windows, IIS, and Active Directory and wholly reliant on healthy and correct name resolution services, it is easy to see why Exchange administrators need to be prepared for anything and everything. For example, if the Active Directory global catalog is not constantly available to Exchange 2003, it will break; if DNS is unavailable or configured incorrectly, Exchange 2003 will break; if a hardware fault occurs, it can corrupt your Exchange databases.

Some of the tools you may find yourself frequently using we've already covered, such as ESM, Internet Services Manager, Active Directory Users and Computers, ExDeploy, and the deployment tools (NetDiag, DCDiag, ExMerge, Jetstress, LoadSim, ESEUTIL, and ISINTEG), so I won't duplicate information on those here. Instead, I'll describe for you the additional tools you'll want to have on hand for all sorts of situations, such as the all-in-one Exchange 2003 tools and updates package and some useful Windows tools.

Microsoft has taken more than 20 tools, updates, and applications and packed them together into a single download package called EXALLTOOLS.EXE (ExAllTools). This package contains some of the tools discussed in earlier chapters, including the following:

- Exchange 2003 Management Pack Update
- Exchange Deployment Tools (ExDeploy)
- Exchange Server Stress and Performance (ESP) 2003
- Jetstress
- Load Simulator (LoadSim) 2003
- Mailbox Merge Wizard (ExMerge)

These tools help you size, deploy, and manage Exchange servers, as well as import and export Exchange mailbox data. Currently 15 other tools included in ExAllTools provide a wide variety of useful features to help you troubleshoot and configure several different aspects of your Exchange infrastructure.[3] Once again, for ease of reference I am describing them briefly in the following subsections.

Add Root Certificate Tool

The Add Root Certificate tool, ADDROOTCERT.EXE, is used to add an internal root certificate to a Pocket PC 2002 device to enable it to use SSL to communicate with Exchange features such as ActiveSync, which requires SSL. All Pocket PC 2002 devices come preloaded with root certificates from four certification authorities (CAs): Verisign, Cybertrust, Thawte, and Entrust. If you are using your own internal CA, you can use the Add Root Certificate tool to add a root certificate from your internal CA

3. You can download these tools individually or in the (currently 22MB) all-in-one package by visiting http://www.microsoft.com/exchange/updates or http://www.microsoft.com/exchange/tools/2003.asp.

to the Pocket PC 2002 device. The Add Root Certificate tool can be used to install only root certificates; it cannot be used to install any subordinate or intermediate certificates. In addition, this tool is meant for use only on Pocket PC 2002 devices. Pocket PC 2003 devices include their own mechanism for installing certificates.

To install your own root CA, export it to a .CER file, and then copy both ADDROOTCERT.EXE and the .CER files to your Pocket PC 2002 device. Execute ADDROOTCERT.EXE on the device and install the .CER file. For more information, consult the Read Me file included with this tool.

Address Rewrite Tool

The Address Rewrite tool, EXARCFG.EXE, is a tool you can use to rewrite P2 addresses on messages sent into Exchange from foreign messaging systems that are destined for and external or Internet address. P2 addresses, as defined in RFC 822, include the FROM, REPLY TO, and SENDER fields for a message. EXARCFG.EXE is very similar to the `RerouteVia Store` registry entry used in Exchange 5.0 and Exchange 5.5 to reroute all SMTP messages through the Exchange information store. It pushes the message into the information store, invalidates all existing MIME information, and forces a conversion of the message from MIME to MAPI. Converting from MIME to MAPI causes the address to be rewritten as configured. Once the rewrite is complete, the message is rerendered and sent off to its destination.

Before using this tool, you should understand its effects on your messages. First, all messages submitted via external SMTP will undergo the content conversion process, even if addresses do not need to be rewritten. Second, unless you route all of your internal messages through external SMTP servers, you cannot use this tool to rewrite internal addresses. EXARCFG.EXE is implemented as a command-line tool; Table 10–2 presents the command-line switches.

For more information on using the Address Rewrite tool, including details on how to also enable it by configuring an attribute in Active Directory, see the Read Me included with this tool.

Archive Sink

The Exchange 2003 Archive Sink is a combination of a Visual Basic script and a companion module (DLL) file used to enable message archiving. The Archive Sink is not new to Exchange 2003 (it was also available for Exchange

Table 10–2 Command-Line Switches for the Address Rewrite Tool

Switch	Description
`/?`	Displays the list of command-line switches.
`-d`	Disables address rewrite. Use with the `-s` (required) and `-v` (optional) switches. If `-v` is not specified, the first SMTP virtual server is used.
`-e`	Enables address rewrite. Use with the `-s` (required) and `-v` (optional) switches. If `-v` is not specified, the first SMTP virtual server is used.
`-l`	Lists the settings for all servers in the domain. Use with `-s` to list the settings for a specific server.
`-s: Server`	Specifies a specific server when used with other switches.
`-v: #`	Specifies the instance number of the SMTP virtual server you want to configure.

2000), but it has been improved in Exchange 2003. Specifically, it includes a new feature that can save all message envelope information, including BCC recipient information (which the Exchange 2000 version could not do). In addition, the updated version fixes a bug in the Exchange 2000 version that required you to remove the sink if you wanted it to stop working. In Exchange 2003, you can disable the sink without removing it.

The script is used to copy and register ARCHIVESINK.DLL on an Exchange server, and by default BCC archiving is disabled. Once the DLL has been registered, you need to configure a registry entry and then restart IIS on the mailbox store server for the change to take effect. To enable BCC archiving, check the box labeled "Archive all messages sent or received by mailboxes on this store" on the General tab of the Mailbox Store Properties dialog of the desired mailbox stores.

For more information on using the updated Archive Sink, see the Read Me included with this tool.

Authoritative Restore Tool

The Authoritative Restore tool, AUTHREST.EXE, is used to force a directory database that was restored from backup to replicate to other servers. It is used in Mixed Mode Exchange environments that run Exchange 5.5 and the Exchange 2003 Site Replication Service. AUTHREST.EXE is not new to Exchange 2003—it has also been available with all previous versions of Exchange—however, it has been updated for use with Exchange 2003.

This tool is generally needed only in a scenario where a directory server containing data older than the production directory needs to be restored and the missing data must be backsynchronized to the other production servers. This scenario happens if valid directory data is accidentally or intentionally deleted. If directory information does go missing from your organization, you have two choices. If you have a backup of the directory information, you can restore it and then use AUTHREST.EXE to backsync it (i.e., replicate the missing data back into the directory). If you don't have a backup, you will need to recreate all of the data.

For more information on using the updated version of the Authoritative Restore tool, see the Read Me included with this tool.

Disable Certificate Verification Tool

The Disable Certificate Verification tool, CERTCHK.EXE, is used to enable or disable certificate verification checking on Pocket PC 2002, Pocket PC 2003, and Smartphone devices for testing purposes. When verification has been disabled, the mobile device will still use SSL to communicate with Exchange; it just won't verify the root CA against the device's certificate trust list. Instead of providing you with any warnings about the certificate, the mobile device will simply use the certificate. This is particularly useful if you have not yet used the Add Root Certificate tool to add your organization's internal root certificate to a mobile device but you want to test SSL connectivity from the device to Exchange.

For more information on using CERTCHK.EXE, see the Read Me file included with it; however, do keep in mind that this tool is for testing purposes only and should not be used in production environments.

DNS Resolver Tool

The DNS Resolver tool, DNSDIAG.EXE, simulates the internal name resolution code inside the SMTP transport stack and provides diagnostic output regarding the DNS resolution process. This command-line tool, which can be used only on Exchange servers running on Windows 2003 or Windows 2003 systems running the IIS SMTP service, is designed to run on the system experiencing name resolution problems. Table 10–3 lists he command-line switches for DNSDIAG.EXE.

When the tool is executed, it will provide return codes that are set at the error level so that you can script this tool in batch files. For more information on using DNSDIAG.EXE, including a list of the error return codes, see the Read Me file included with this tool.

Table 10–3 Command-Line Switches for the DNS Resolver Tool

Switch	Description
`-a`	Specifies that all DNS servers should be queried in the test.
`-p <protocol>`	Specifies which protocol to use (TCP, UDP, or DEF). Cannot be used in tandem with `-v`.
`-s <server list>`	Specifies a list of IP addresses for the DNS servers you want to use. If you do not use this optional switch, the locally configured DNS servers are used. IP addresses can be delimited by using a space or a tab. Cannot be used in tandem with `-v`.
`-v <SMTP VS #>`	Specifies a particular SMTP virtual server in instances where more than one exists on the same server.

Error Code Lookup Tool

The Error Code Lookup tool, ERR.EXE, is used to translate errors reported by Windows and to provide you with an explanation of their meanings. ERR.EXE is another command-line tool, and it can resolve errors in a variety of formats:

- Hexadecimal (e.g., 0x31c or 31c)
- Numeric (e.g., 1723)
- String (e.g., UNKNOWN_FAILURE or INTERNAL_UNKNOWN_FAILURE)

Many of these same error messages can also be translated using the `NET HELPMSG` command found in Windows, as well as the Visual C++ Error Lookup tool that ships with Visual Studio; however, you may still find ERR.EXE to be useful. For more information on using ERR.EXE, see the Read Me file included with this tool.

GUIDGen

GUIDGen is a user interface–based tool that enables you to generate GUIDs you can use for anything that requires a GUID. GUIDGen can create GUIDs using several different formats, enabling you to create GUIDs for automation, programming, scripts, and other purposes. As shown in Figure 10–1, GUIDGen also includes a Copy button you can use to copy a

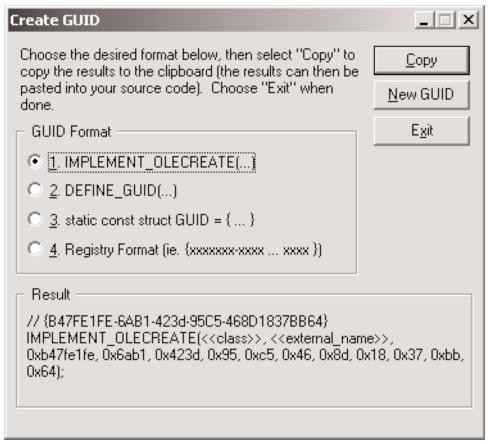

Figure 10–1 GUIDGen user interface

newly generated GUID to the Windows clipboard for quick pasting in your application, your source code, or wherever you want to insert the GUID.

GUIDGen is not new to Exchange 2003; previous versions of Exchange also included this tool. For more information on using GUIDGen, see the Read Me file included with this tool.

Importer for Lotus cc:Mail Archives

The Microsoft Importer for Lotus cc:Mail Archives, CCMARCH.EXE, is used to import data from Lotus cc:Mail archive (.CCA) files into an Exchange public folder or personal store (.PST) file. In addition, CCMARCH.EXE can also import cc:Mail addresses from a private directory (PRIVDIR.INI) to a personal address book (.PAB) file or to the Outlook Contacts folder.[4]

CCMARCH.EXE is a wizard-based tool that steps you through the import process. Before using it, I recommend reading its documentation, especially the compiled HTML help (.CHM) files included with it, which describe the tool's underlying concepts as well as how to use the tool.

4. Note, though, that Outlook 2000 and later clients can natively import Lotus cc:Mail data and therefore do not need this tool.

Information Store Viewer

The Information Store Viewer, MDBVU32.EXE, also known as the Message Store Viewer, is used to view and configure message storage files in a mailbox store, a public folder store, a .PST file, or an offline store (.OST) file. MDBVU32.EXE uses MAPI 1.0 calls to connect to a MAPI-based message store. As illustrated in Figure 10–2, you can use it to view or delete messages, folders, rules, and scripts; access system mailboxes; and change raw data.

When you encounter this tool, you might get a chuckle out of its icon, which is a flaming drum of toxic nuclear waste. This should be your first clue that this tool can be very hazardous to a message store. Because it provides write access to raw message store data, a wide variety of problems can occur if the wrong item is changed or deleted. More importantly, the tool has no "undo" feature, so you should make sure you have a current full backup of your message store(s) before using this tool.

For details on how to install and use MDBVU32.EXE, consult the Read Me file included with this tool.

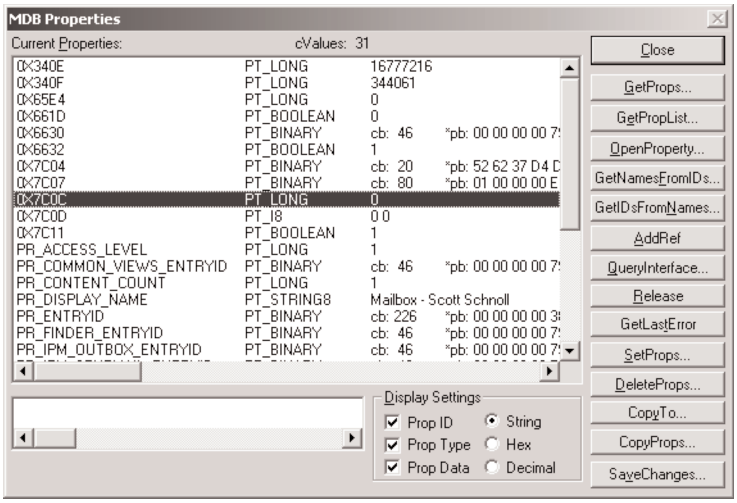

Figure 10–2 Message store database properties displayed in Message Store Viewer

Inter-Organization Replication Tool

This is another tool available in prior versions of Exchange that has been updated for use with Exchange 2003. This tool consists of two programs—the Replication Configuration program (EXSCFG.EXE), which is shown in Figure 10–3, and the Replication service (EXSSRV.EXE)—and is used to replicate public folder content and Free/Busy information between two Exchange organizations. It enables users in each organization to coordinate meetings and appointments and to share contact and public folder data.

This tool is very useful for companies undergoing mergers or acquisitions, for companies with separately administered Exchange organizations, or in any scenario in which you have two separate and distinct Exchange organizations. It can be used to replicate data between an Exchange 2003 organization and another Exchange 2003 organization, or with an Exchange 2000 or Exchange 5.5 organization. If you do plan to use this tool with Exchange 2003 and a legacy Exchange organization, be sure to use the Exchange 2003 version of this tool.

One of the advantages of this tool is that it does not need to run directly on an Exchange server. It can be used on any system running ESM.

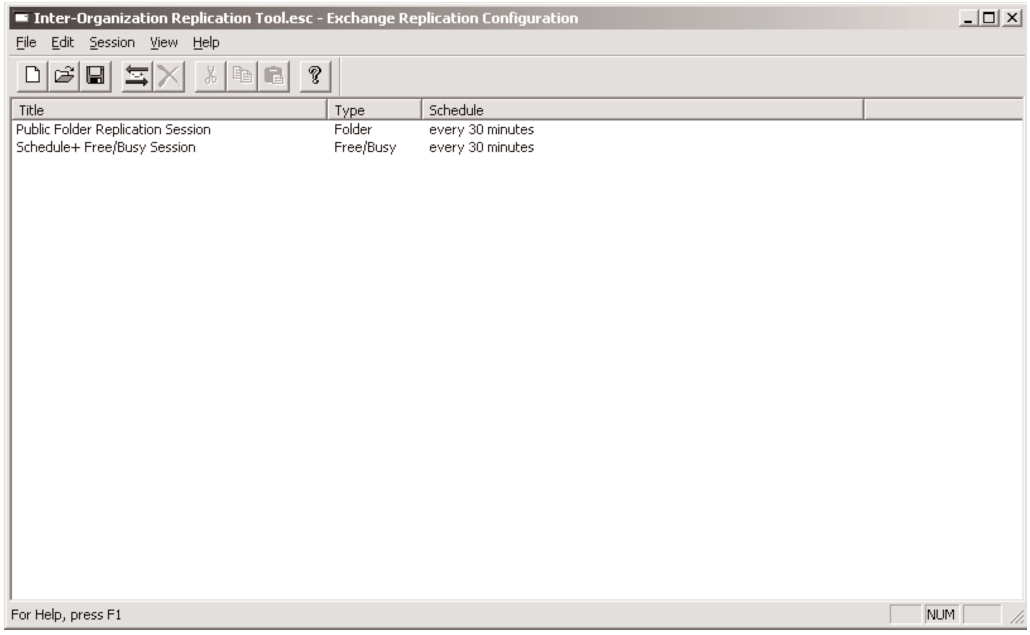

Figure 10–3 Replication Configuration program user interface

Note, though, that this tool may not be sufficient for everyone's inter-organizational replication needs. If you have complex replication needs, you may find Microsoft Identity Integration Server (MIIS) 2003 better suited to your needs.[5] For more information on using the Inter-Organization Replication tool, consult the Read Me file included with it.

MTA Check Tool

The Message Transfer Agent (MTA) Check tool, MTACHECK.EXE, is a command-line tool used to analyze and correct MTA database consistency problems. The MTA database is quite efficient and normally performs well. However, like any database it can become corrupt. When that happens, one of several events will be logged in the Application event log on the Exchange server. An example of such an event is shown here.

```
Event Type: Error
Event Source: MSExchangeMTA
Event Category: None
Event ID: 9405
Date: 10/18/2003
Time: 9:34:07 AM
User: N/A
Computer: EX2K3
Description: An unexpected error has occurred which may cause the
MTA to terminate. Error: <error code>
```

Several other possible events can be logged when the MTA is corrupt. This event is just one example. If you receive one of these events, or if you suspect corruption, you can use MTACHECK.EXE to verify database integrity and fix the problem. MTACHECK.EXE can be launched without any startup switches (in which case it runs with only minimal logging), or it can be launched using one of the command-line switches listed in Table 10–4.

A couple of important steps need to be performed before MTACHECK.EXE should be run. For more information on these steps and the MTA Check tool itself, consult the Read Me file included with this tool.

5. For more information on MIIS, see http://www.microsoft.com/miis.

Table 10–4 Command-Line Switches for the MTA Check Tool

Switch	Description
`/f <filename>`	Designates a file for logging output.
`/rd`	Deletes directory replication messages from the MTADATA directory.
`/rl`	Deletes link monitor messages from the MTADATA directory.
`/rp`	Deletes public folder replication messages from the MTADATA directory.
`/v`	Runs MTACHECK.EXE with verbose logging. Can be used in combination with `/f`.

SMTP Internet Protocol Restriction and Accept/ Deny List Configuration Tool

If you specifically block or allow computers to access your Exchange SMTP virtual server, this tool is for you. The SMTP Internet Protocol Restriction and Accept/Deny List Configuration tool is a combination of a Visual Basic script (.VBS) file and a companion module (.DLL) file that enables you to programmatically manipulate SMTP virtual server connection control and relay control settings, including the Accept and Deny List settings. Despite their names, the script file (IPSEC.VBS) and the DLL file (EXIPSEC.DLL) are not related to the IPSec protocol. It's just a naming coincidence.

You can use the script to add, delete, list, or completely clear IP address restrictions set on an SMTP virtual server or on the Global Accept or Global Deny lists. EXIPSEC.DLL can be used against Exchange 2000, but Global Accept and Deny List manipulation is supported only on Exchange 2003 servers. For more information, including the available command-line switches for IPSEC.VBS, refer to the Read Me file that ships with this tool.

Up-to-Date Notifications Troubleshooting

As I wrote in Chapter 9, Exchange includes a feature called Always Up-to-Date (AUTD), which notifies a user's mobile device that data has changed on the Exchange server. Exchange sends a control message to the device, which causes it to commence a data synchronization session, thereby keeping the device up-to-date. In a perfect world, these messages are *always*

correctly received and processed by every mobile device you have. However, in the real world, this is not necessarily true.

In cases where messages are not received, or when AUTD does not seem to be functioning properly, you can use the AUTD Troubleshooting tool to diagnose and resolve the problem. This tool is implemented as an ASP.NET application that includes some Web pages, a Javascript file, and some configuration setting files. These files are copied to a folder and then exposed as an IIS virtual directory. The tool provides a Web-based interface that enables an administrator to log on, specify the mailbox he or she wants to troubleshoot, and view the mobile device and AUTD message information described in Table 10–5.

Because many of the problems you may encounter will be the result of external issues (or other issues beyond your control), the AUTD Troubleshooting tool may not be able to solve every problem you encounter. However, it will help isolate and identify problems and let you know whether the problem is on your end (e.g., with Exchange) or external (e.g., with a mobile communications provider). For more information on the AUTD Troubleshooting tool, including how to install and use it, refer to the Read Me file included with this tool.

Table 10–5 Information Available from the AUTD Troubleshooting Tool

Information	Description
Address	Displays the IP address of the mobile device.
Carriers	Displays the number of carriers listed in Active Directory.
Delivery	Displays how notifications will be delivered to the mobile device.
Device	Displays the name of the mobile device.
Exchange server	Displays the name of the Exchange server that contains the user's mailbox.
Expires	Displays the expiration date/time for the device if it stops syncing. Once expired, AUTD notifications will no longer be sent to the mobile device.
Send mail	Sends a test message to the mobile device to verify message flow from Exchange to the mobile device.
User name	Displays the name of the Exchange user whose mailbox you are troubleshooting.

WinRoute

WinRoute is another tool available in prior versions of Exchange that has been updated for use with Exchange 2003. This tool, WINROUTE.EXE, is used to examine the link state routing information currently being used by the routing master in an Exchange site.

As shown in Figure 10–4, WinRoute is a user interface–based tool that displays link state routing information in three window panes.

1. The tree view pane displays the organizational routing table.
2. The address space pane displays all known address spaces, including type, cost, restriction, connector, and source Routing Group and Administrative Group information.
3. The raw routing data table pane displays (for information purposes only) the current routing information being used by Exchange.

As Microsoft states in the WinRoute documentation, this should be the first (or one of the first) tools you use when troubleshooting message

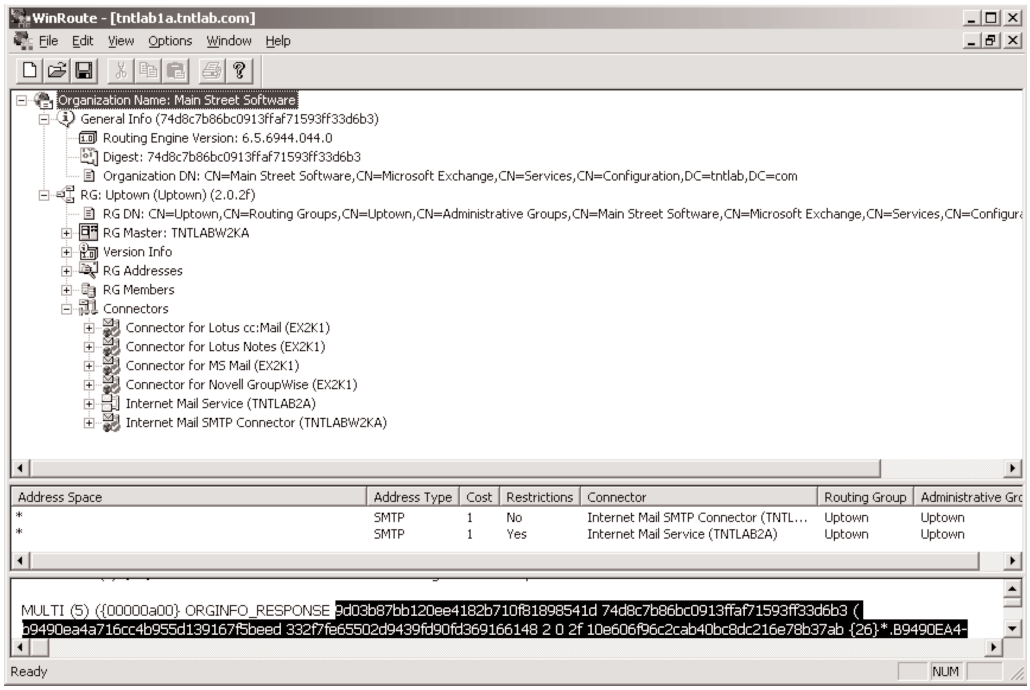

Figure 10–4 WinRoute user interface

routing problems. For more information on using this tool, refer to the Read Me file included with it, as well as Microsoft Knowledge Base article 281382.

Additional Tools and Updates

On the same pages[6] where you'll find the tools mentioned earlier and the all-in-one package, you will also find some additional tools and updates that can provide additional functionality or help diagnose and resolve problems that affect your Exchange infrastructure. For example, the .NET Framework Device Updates (DUs), which provide support for additional mobile devices for OMA and ActiveSync, will be available from those pages. At the time of the Exchange Server 2003 Launch (October 22, 2003), Exchange 2003 included DU2, and DU3 was available on those pages. DUs are anticipated to be released every six months.

The Microsoft Baseline Security Analyzer (MBSA) tool is also linked from the Exchange Tools page. MBSA is a free security sweep tool that can scan Windows NT 4.0 and later systems for configuration settings that are considered security risks. In addition, MBSA can check for missing security patches and updates for Windows NT 4.0 and later, IIS 4.0 and 5.0, SQL Server 7.0 and 2000, Internet Explorer 5.01 and later, Exchange 5.5 and 2000, and Windows Media Player 6.4 and later. As you can see in Figure 10–5, MBSA looks very similar to Microsoft Windows Update.

MBSA is one of the tools that can be used to implement Microsoft's Secure in Deployment strategy described earlier in this book. One of the many reasons that administrators struggle with the act of applying patches to all of their systems is that having too many systems and too many patches makes it difficult to tell what needs to be patched and why. MBSA is designed to cut right through the problem and identify which systems need to be patched (and what patches are needed) and which systems should be reconfigured (and how to do that). If you are not using MBSA already, I strongly encourage you to download it and give it a try.[7]

Finally, administrators and developers who build applications on top of or inside of Exchange will also find a link to the latest Exchange SDK. The

6. See http://www.microsoft.com/exchange/updates or http://www.microsoft.com/exchange/tools/2003.asp.

7. For questions, comments, and assistance with MBSA, I recommend visiting the microsoft.public.security.baseline_analyzer newsgroup on Microsoft's news server (msnews.microsoft.com).

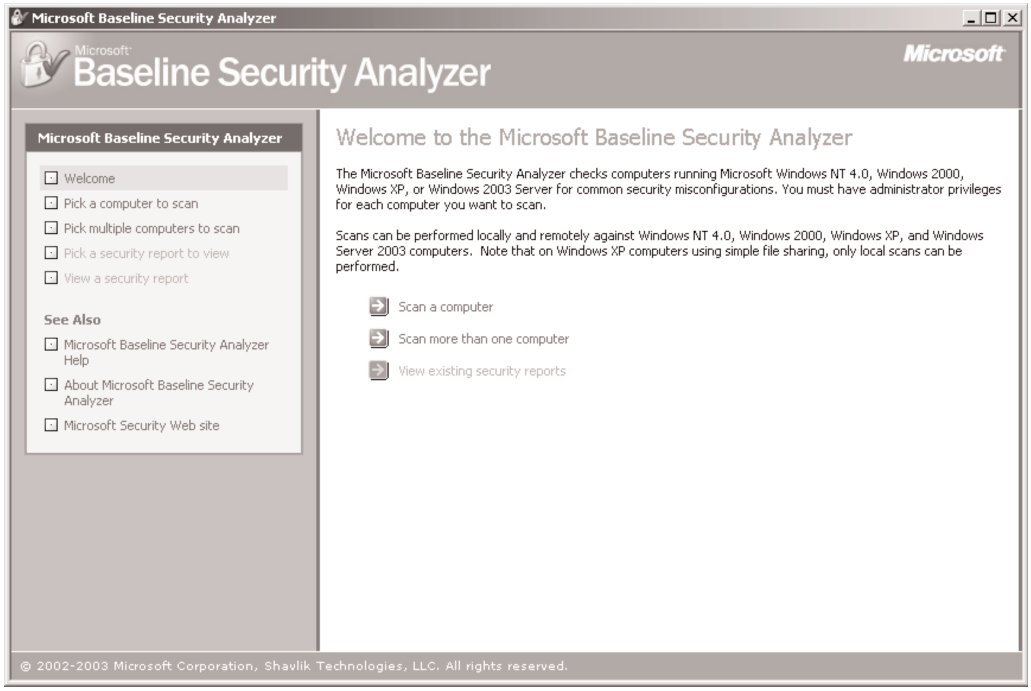

Figure 10–5 Microsoft Baseline Security Analyzer Welcome screen

SDK includes a wealth of information and sample applications that demonstrate how to programmatically access, use, and manipulate Exchange storage and transport resources.[8]

Resources and Links

Now that you have had a taste of the fish I offered in previous section, I thought I would share with you some great fishing holes on the Internet. Certainly microsoft.com is packed with a wealth of information, some of which I will detail in the following subsections. But there is also a large and thriving worldwide Exchange community made up of mailing lists, Web

8. The Exchange 2003 SDK is on a quarterly update schedule and is freely downloadable from http://msdn.microsoft.com/exchange.

site forums, newsfeeds, and blogs that contain and express a tremendous amount of experience and expertise on Exchange, including Exchange 2003. In fact, some of these resources are actually provided by the very people at Microsoft who *wrote* portions of Exchange!

Since Exchange is a Microsoft product, it's only fair that we start with Exchange-related resources that are available from Microsoft's Internet properties, including several Web sites with Exchange-specific content, public newsgroups, and technical chat rooms.

Microsoft Exchange Product Home Page

Obviously, the best place to start for Exchange-related content, information, tools, updates, and so on is the Exchange Server Product Home Page at http://www.microsoft.com/exchange. Here you can find links to anything and everything about Exchange 2003 (as well as Exchange 2000 and Exchange 5.5). You can download or request on CD a trial version of Exchange 2003, and unless Microsoft sends service packs to you on official CDs, this is the only place to obtain service packs for Exchange.

If you are outside the United States, you may prefer to use one of the other Exchange Product home pages throughout the world; there are more than 30 of them, many of which are in local languages (e.g., Chinese, German, French, and so on). You can find the complete list at http://www.microsoft.com/exchange/wwide.asp.

Regardless of which site you choose, the content should be pretty much the same and just localized for the site being browsed. However, it's a good idea to keep tabs on the U.S. site because it is often updated first with the most recent content. In addition, the U.S. site is also a springboard to all other Exchange-related sites at Microsoft, including the Exchange Developer Center Web site, the Microsoft TechNet site for Exchange (which also includes the Exchange Technical Documentation Library), the Exchange Server 2003 Support Center, Exchange 2003 Events and Errors, the Exchange public newsgroups, and the Exchange Server Community.

Exchange Developer Center Web Site

Even if you don't develop full-blown applications on Exchange, you still may be interested in the Exchange Developer Center Web site at http://msdn.microsoft.com/exchange. This site, which is primarily intended for developers, is the best place to go for the latest version of the Exchange 2003 SDK and a great place to browse the SDK documentation online

and check out sample code written in C#, C++, Visual Basic .NET, and VBScript.

In addition to the code samples, API documentation, and other content, this site also includes some development tools that get you started on building Exchange-based solutions, such as:

- Exchange Application Deployment Wizard
- Exchange Explorer
- Exchange Store Event Sink Wizard for Visual Basic 6
- Managed Exchange TreeView Control

Even if development isn't your forte, you may find the information on creating and using event sinks to be useful for your environment. An event sink is a piece of code (the sink) that executes (fires) when something (the event) happens. Exchange 2003 supports *protocol* event sinks and *transport* event sinks (for managing messages in the SMTP service) and *store* event sinks (for managing messages in the Exchange store). Protocol events occur at the SMTP command verb level between the client and the server, and protocol event sinks can be used to modify commands and responses to commands. Transport events occur as messages flow through the SMTP transport stack, and transport event sinks can be used to manipulate messages as they travel through SMTP. Event sinks are useful in all sorts of situations; they can be used to convert messages, scan for content, add disclaimers to outgoing messages, or reroute messages in a workflow environment. In addition, there is a Protocol Sink Template you can use to create an in-house antispam solution that accepts or rejects messages based on a spam confidence level. You can do with event sinks just about anything you would want to do with or to a message while in the SMTP transport stack or information store.

Microsoft TechNet Exchange Center

The TechNet Exchange Center at http://www.microsoft.com/technet/prodtechnol/exchange/exchange2003/default.asp is an excellent technical clearinghouse of resources and information related to Exchange 2003. Information on this site is conveniently broken down into the natural lifecycle categories for a product such as Exchange: evaluate, plan, deploy, support, and train.

While the TechNet Exchange Center is not new (it existed for Exchange 5.5 and Exchange 2000), what is new to the TechNet site is

the Exchange Server 2003 Technical Documentation Library (TDL). The TDL is a catalog of Exchange-related technical documents that have been reviewed and approved by the Exchange product team. You'll want to check this site frequently because there are some upcoming technical documents yet to be published. As of this writing, the following documents are scheduled for future release around the following estimated dates:

- Exchange 2003 Automation Guide (March 2004)
- Exchange 2003 Backup, Restore, and Disaster Recovery Guide (March 2004)
- Exchange 2003 Client Access Guide (March 2004)
- Exchange 2003 Interoperability and Migration Guide (March 2004)
- Exchange 2003 Message Security Guide (March 2004)
- Exchange 2003 Performance and Scalability Guide (March 2004)
- Exchange 2003 Reliability and Clustering Guide (March 2004)
- Exchange 2003 Security Guide (June 2004)
- Exchange 2003 Technical Overview (June 2004)
- Exchange 2003 Transport and Routing Guide (June 2004)
- Exchange 2003 Troubleshooting Guide (June 2004)
- Unsupported Exchange 2003 Deployments (June 2004)
- Welcome to Microsoft Messaging (March 2004)

All documents that have an expiration date will have a *checked book icon* next to them in the TDL. On or before the document's expiration date, a newer replacement document will be posted (often, although not always, with the same name). You may hear these referred to as *living documents* because they will grow and evolve along with Exchange 2003. The TDL can be accessed directly from http://www.microsoft.com/exchange/library. If you ever want to provide feedback to Microsoft about an Exchange 2003 technical document, you can do so by sending an e-mail to exchdocs@microsoft.com.

Exchange Server 2003 Support Center

The Exchange Server 2003 Support Center, also known as the PSS Exchange Center, can be found on the Web at http://support.microsoft.com/default.aspx?pr=exch2003. This site contains four primary areas of content.

1. *The Highlights and Top Issues area* changes to reflect the most frequently received support calls at Microsoft. If a lot of people are

experiencing the same problem or if something needs clarification based on real-world experiences, chances are it will become a Highlight and Top Issue.

2. *Step-by-Step Instructions and How-to Articles* provide detailed steps on how to configure various features, settings, and infrastructure components to provide the best experience for your environment.
3. *Support WebCasts* are live, online presentations from PSS support engineers, Exchange product team members, and Exchange community participants. Even if you miss a WebCast, you can still view it because they are all recorded using Windows Streaming Media technology. If you don't have time to sit for the entire WebCast, you can also download both the PowerPoint slides and a transcript of the WebCast for offline viewing and reading.
4. *The Additional Resources and Related Sites area* provides links to other Web sites that include Exchange or Exchange-related content (such as the Exchange sites previously listed), as well as the Microsoft Office Outlook 2003 Support Center.

If you encounter a problem with Exchange, before contacting Microsoft PSS for support (unless it is an extreme emergency and you don't have the time), I recommend browsing this site. You may actually find your problem and its resolution described here, saving your organization both time and money in the problem resolution process.

Microsoft Knowledge Base

The Exchange Support Center is one of many product support centers linked to Microsoft Help and Support Online (http://support.microsoft.com). This is Microsoft's primary online product support site for customers in the United States. Non-U.S. customers typically use one of the international support Web sites listed at http://support.microsoft.com/common/international.aspx. Regardless of which locale you choose, all Microsoft Help and Support sites include a link to the Microsoft Knowledge Base.

The Microsoft Knowledge Base Online is a Web front-end to Microsoft's database of Knowledge Base articles (sometimes referred to as KBs) that contain information that Microsoft wants the general public to know about its products and technologies. KBs range in content from specific how-to articles to errata to clarifications of Microsoft policies and so forth.

As you can tell by the several references to KBs throughout this book, the Microsoft Knowledge Base often supplements the knowledge about Exchange that has not yet made its way into other Exchange product documentation. This is one of the reasons that the Microsoft Knowledge Base is one of the first places I check when troubleshooting an issue with a Microsoft product. It is updated frequently and very easy to access. You can search the Microsoft Knowledge Base Online at http://support.microsoft.com/search, and if you use Internet Explorer to access the Web, you can go directly to any article if you know the article number. For example, if you want to view article 818474, you would enter "MSKB 818474" into the Internet Explorer address bar, which would then open that article from the Web. To make this work, you need to add the following registry entries to the computer you use to browse the Web. First create this new KEY:

```
Location: HKCU\Software\Microsoft\Internet Explorer\SearchURL\mskb
```

Then add the following values under this key (all are REG_SZ):

```
Value: Default
Value Data: http://support.microsoft.com/default.aspx?scid=kb;en-us;%s

Value: (space) ← note this is not the word space but a single space
Value Data: +

Value: +
Value Data: %2B

Value: %
Value Data: %25

Value: &
Value Data: %26
```

Figure 10–6 shows an example of how this looks in the registry editor.

Offline access to the Microsoft Knowledge Base is available via a monthly CD subscription called Microsoft TechNet. This is handy to have when online access is not available (which might even be the problem you need to fix). You can find pricing and information on Microsoft TechNet subscriptions at http://www.microsoft.com/technet/subscriptions.

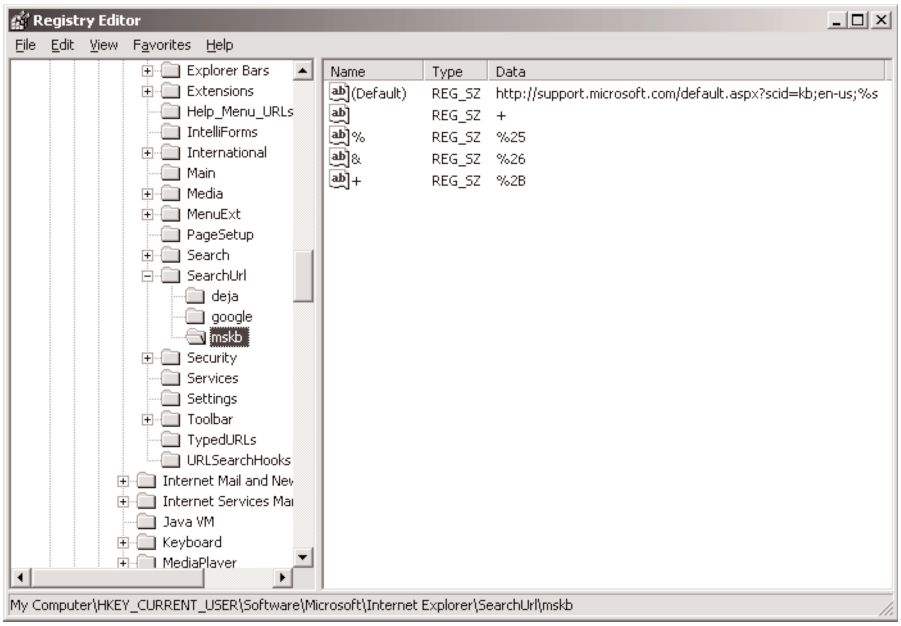

Figure 10–6 Internet Explorer custom search URL entry for the Microsoft Knowledge Base

Exchange 2003 Events and Errors

Like many Windows Server System applications, Exchange 2003 logs a variety of events to the Application event log in Windows. Several of the events that can be logged by Exchange have been discussed throughout this book. Unfortunately, Exchange is capable of logging thousands of different events, making it impossible to become familiar with all of them. Depending on the event and the diagnostic logging level you have configured, some Exchange events will be self-explanatory while others will appear to require a crack team of decoders to decipher the event's meaning. For example, does the following event mean anything to you?

```
Event Type: Error
Event Source: MSExchangeIS
Event Category: Database
Event ID: 9031
Date: 10/11/2003
Time: 7:34:04 AM
```

```
User: N/A
Computer: EX2K3
Description: Database resource failure error <error code> occurred
in function <function name> while accessing the database.
```

Fortunately, Microsoft has an Exchange 2003 Events and Errors Web site (http://www.microsoft.com/exchange/2003/events/default.asp) that you can use to search for information about events based on the Event Source and the Event ID. When you find a matching event, you can read an explanation of the event, along with any necessary or recommended actions and a list of related Knowledge Base articles. The search results will vary among events and not all events are available, but this is still a valuable resource for investigating new and unusual as well as familiar and common events. A search for the example event produced the results shown in Figure 10–7.

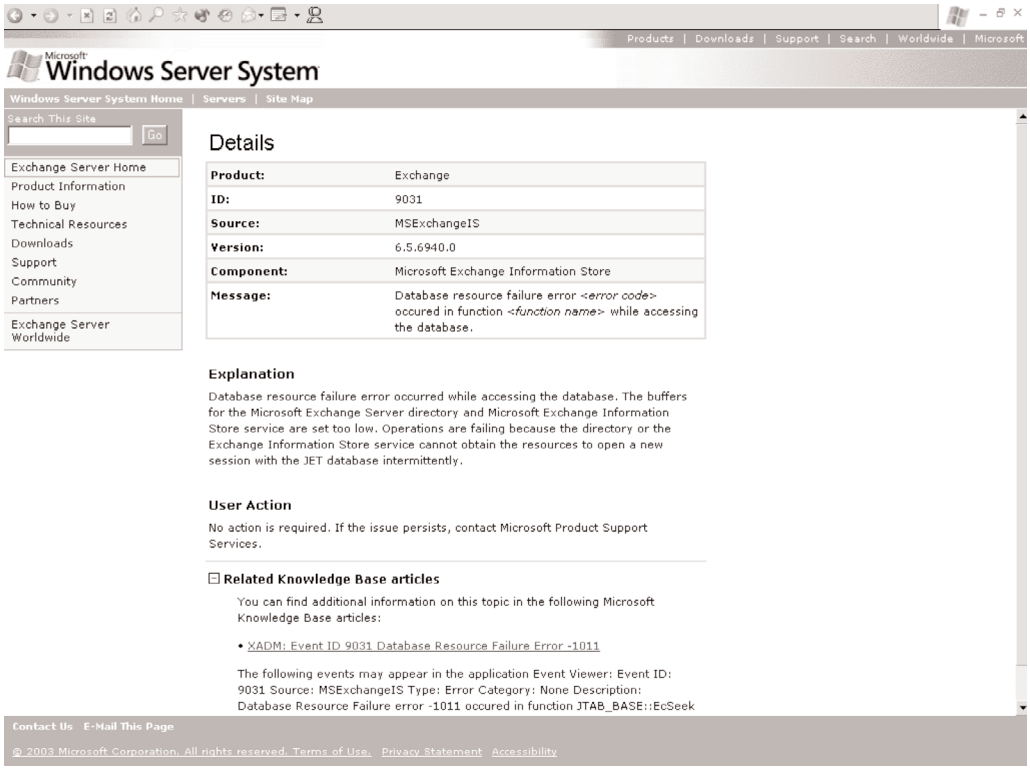

Figure 10–7 Exchange 2003 Events and Errors Web site search results

Exchange Public Newsgroups

Microsoft hosts a variety of newsgroups on a cluster of servers that are available to everyone free of charge around the clock every day of the year. By far, Microsoft's largest online community is the Microsoft public newsgroups. There are thousands of newsgroups covering a wide variety of Microsoft products and technologies, including several specifically for Microsoft Exchange Server.

The public newsgroups are accessible via an NNTP newsreader, such as Outlook Express (and many others), and via the Web with Internet Explorer 4.0 or later or Netscape 4.6 or later. In addition to the English-based newsgroups, there are Exchange newsgroups in several languages, including Arabic, German, Spanish, French, Korean, and others. Posts remain on the server for 90 days, after which they expire. You can find questions of all types posted by users with wide-ranging levels of experience. Newsgroup topics include installation, administration, clients, clustering, connectivity, design, development, and miscellaneous topics.

You can access the Web-based interface to the Exchange newsgroups by pointing your browser to http://support.microsoft.com/newsgroups/?pr=newsgexch2k. The newsreader can be used by pointing your NNTP client to msnews.microsoft.com. Microsoft does not provide official support for Exchange in the newsgroups. Instead, the company provides the newsgroups as a way to help people become part of the global community of Microsoft customers and product experts. The newsgroups do not have a Microsoft search interface; however, they are searchable through Google Groups (http://www.google.com/groups), formerly DejaNews (you can still get there using http://www.deja.com). You can use the same trick mentioned earlier for the Microsoft Knowledge Base to make Google and Google Groups easy to search through the Internet Explorer address bar. Use the following registry entries to add Google and Deja keywords to Internet Explorer.

To add Google, create this new KEY:

```
Location: HKCU\Software\Microsoft\Internet Explorer\SearchURL\google
```

Then add the following values under this key (all are REG_SZ):

```
Value: Default
Value Data: http://www.google.com/search?q=%s
```

```
Value: (space) ← note this is not the word space but a single space
Value Data: +

Value: +
Value Data: %2B

Value: =
Value Data: %3D

Value: &
Value Data: %26

Value: ?
Value Data: %3F

Value: #
Value Data: %23
```

To add Google Groups, create this new KEY:

```
Location: HKCU\Software\Microsoft\Internet Explorer\SearchURL\deja
```

Then add the following values under this key (all are REG_SZ):

```
Value: Default
Value Data: http://groups.google.com/groups?q=%s

Value: (space) ← note this is not the word space but a single space
Value Data: +

Value: +
Value Data: %2B

Value: %
Value Data: %25

Value: &
Value Data: %26
```

Microsoft MVP Program

Community is very important both to and within Microsoft, and because of that you'll find many experienced Microsoft employees participating in the Exchange newsgroups and sharing their expertise freely. Some of them actually write portions of Exchange, and many support Exchange at Microsoft for a living. Other top participants include individuals in the Microsoft Most Valuable Professionals (MVP) program.

The MVP program is a worldwide award and recognition program that makes an annual award of MVP status to outstanding members of Microsoft's technical communities. The MVP program exists to recognize the top contributors to various product communities to help build, promote, and improve the community experience. The award recipients—referred to as Microsoft MVPs—are the most active experts in technical communities recognized by Microsoft for their past quality participation, their demonstrated practical expertise, and their passion for technology. While MVPs have diverse backgrounds and professions, they all have three things in common: a passion for technology, strong expertise and experience, and a willingness to freely share both.

When it comes to Exchange knowledge outside of Microsoft, few people in the world know as much about Exchange as the Exchange MVPs, a group to which I am very proud to belong. As you'll read later in this chapter, many MVPs (including many Exchange MVPs) also maintain their own Exchange-related communities, which I encourage you to visit. For more information about Microsoft MVPs and the MVP program, visit http://mvp.support.microsoft.com.

Exchange Server Communities

The central hub in the general worldwide Exchange community is the Exchange Server Community Web site (the Community) at http://www.microsoft.com/exchange/community. This site is a Web-based portal for *living* Exchange information. The Community is designed to facilitate the sharing of technical information, current hot topics, and important announcements. It provides information on upcoming events, WebCasts, and TechNet Chats, plus a quick roundup of the most active newsgroups and newsgroup threads.

The Community isn't just about the Microsoft portion of the whole Exchange community; it's a portal to several other communities—some hosted by Microsoft, others by third parties—which can be found both on

the Community home page and at http://www.microsoft.com/exchange/community/relcommunities.asp. Some of these communities, as well as other communities that are not listed on these sites, are described in the following subsections. For ease of reference I have broken them down into the following categories: Web sites, blogs, and newsfeeds.

Exchange-Related Web Sites

When working with a product as widely used as Exchange, it is not surprising to find that some very good and useful information can be found in some interesting places. Microsoft definitely is not the only source of information on Exchange; in fact, in many cases you may prefer unbiased information about Exchange that can come only from a non-Microsoft source. Several third-party Web sites provide technical information and places to share real-world experiences with Exchange, and I want to share some of the best Web sites with you. Unfortunately I cannot list them all, so you'll want to browse the links on the sites I have listed because they likely link to sites I have not listed. I am listing them, with a very brief description of each site.

- *The Entourage Help Page* (http://www.entourage.mvps.org): This site is devoted to Microsoft Entourage:mac, the Macintosh-based Exchange client. You can find the homepage for Entourage at http://www.microsoft.com/mac/products/entouragex/entouragex.aspx?pid=entouragex.
- *Exchange Resource Center* (http://www.amrein.com/eworld.htm): This site is a clearinghouse of Exchange-related resources, such as books, articles, software, tools, and FAQs.
- *KBAlertz* (http://www.kbalertz.com): This site was developed by Dave Wanta, a network administrator and developer. To stay abreast of Microsoft technologies, Dave spent a weekend writing a notification service that is tied to the Microsoft Knowledge Base Online. The service was designed to notify him when a new Knowledge Base article was released by Microsoft. Dave turned his service into KBALertz, which provides free e-mail and RSS notification of new Knowledge Base articles as soon as Microsoft posts them.
- *The Mail Resource Center* (http://www.mail-resources.com): The Mail Resource Center includes messaging-related news and information plus tools. Its Web Links section in particular is worth a visit—it has more than 400 links in 61 different categories.

- *Microsoft Exchange Server Resource Site* (http://www.msexchange.org): This site provides articles and tutorials for configuring Exchange features, details on third-party add-on products, message boards, and discussion lists.
- *OutlookExchange* (http://www.outlookexchange.com): This site features more than 30 columnists writing articles on a wide variety of topics related to both Exchange and Outlook.
- *SearchWin2000/TechTarget* (http://searchwin2000.techtarget.com): SearchWin2000 is packed with tips, how-to's, discussions, WebCasts, and forums related to a wide variety of products and technologies, including Exchange. By the time you read this a new TechTarget site—http://www.SearchExchange.com—should also be available.
- *Simpler-Webb Exchange Resources* (http://www.swinc.com/resource/exchange.htm): In addition to developing products for Exchange, the creators of this site have maintained FAQs pages for Exchange 2003, Exchange 2000, and Exchange 5.5.
- *Slipstick Systems Exchange and Outlook Solutions Center* (http://www.slipstick.com): Slipstick Systems was Sue Mosher's Web site. Sue is a prolific author, journalist, Microsoft MVP, and all-around Exchange and Outlook guru, and this site is filled with lots of great Exchange and Outlook information. It has recently changed ownership and is now run by another Outlook guru (and fellow MVP)—Diane Poremsky.

Blogs

The term *blog* is short for *Weblog*. A blog is essentially a Web-based, diary-style journal. Blogs are updated at various intervals; some daily, others less frequently. These often-updated Web sites provide links to other interesting information on the Web, typically adding their comments and other information about the links. Blogs are a kind of personal community because the *bloggers*, those who write blogs, form pockets of communities with other bloggers and followers of their blogs.

You might be surprised to know that blogs are as old as the Web. In fact, Tim Berners-Lee, the father of the Web, also created the first blog (which you can still find on the Web at http://www.w3.org/History/19921103-hypertext/hypertext/WWW/News/9201.html) in 1992. It wasn't called a Weblog, though; that term wasn't coined until December 1997. As for sites that specifically considered themselves blogs, in the beginning of

1999, there were only 23. But throughout the beginning months of 1999, blogs began growing in numbers.

In July 1999, the first free do-it-yourself blogging tool was launched by Pitas. Within months there were many more freely available blogging tools that made it easy for anyone to blog. No HTML, no Web site code, no heavy lifting at all; just enter your thoughts, opinions, and links as if you were sending an e-mail to a friend and post it for your readers to consume. Blogs continue to grow in numbers and in popularity. A number of Exchange-related blogs are worth checking out—I've listed the ones I visit.

- *MS Exchange Blog* (http://www.msexchange.co.uk): This blog is the combined efforts of Chris Meirick, Neil Hobson, and William Lefkovics, three Exchange MVPs who share tips, news, and links related to Exchange.
- *Kase's Blog* (http://blogs.gotdotnet.com/kclemson/): This blog is kept by KC Lemson, a program manager on the Exchange Server product team at Microsoft. KC provides tips on Outlook, Exchange, and software development, as well as messaging trivia and an insider's view on what it's like to work on the Exchange team at Microsoft.
- *David Lemson—Exchange Guy* (http://blogs.gotdotnet.com/dlemson/): This blog is kept by David Lemson, another program manager on the Exchange Server product team at Microsoft. Like KC, David also provides tips on Exchange. David posts some great information on the transport components in Exchange 2003 (and since he has worked in the core transport group on the Exchange team since 1998, you know I mean *great!*).
- *E2K Security* (http://www.e2ksecurity.com): This blog is kept by Paul Robichaux, an author of 12 technical books and numerous Exchange-related articles, a noted Exchange guru and speaker, and an Exchange MVP. Paul's blog focuses primarily on Exchange security.
- *You Had Me at EHLO* (http://blogs.msdn.com/exchange): This is a brand new blog from the folks on the Exchange team at Microsoft. It will feature a rotating cast of participants from all areas of Exchange, including development, PSS, user education, SDK, and so forth. I highly recommend frequent visits to this blog.

Newsfeeds

A *newsfeed* is a Web site, newsgroup, or blog that is available via a feed mechanism (i.e., a mechanism that "feeds" the content to a newsfeed

client). One of more popular types of newsfeeds is RSS, which stands for different things depending on whom you ask. RSS can mean Rich Site Summary, RDF Site Summary, and Really Simple Syndication. RSS was first developed by Netscape in 1999 as a way to implement channels in its Web browser. Channels didn't last long, and Netscape abandoned RSS development. Others such as UserLand persisted, and now RSS is one of the most successful Internet-based implementations of XML to date.

Today there are a variety of both RSS creation programs and *news aggregators*, which are RSS clients that often provide access to newsgroups in addition to newsfeeds. Because RSS is designed for content that is updated often or continuously, static Web sites typically don't use it. However, RSS is gaining in popularity, in part due to the benefits it provides folks who do update their sites regularly, including bloggers. In fact, you'll find that many blogs are available through RSS feeds, enabling you to view all of your news and information in a single client instead of separate Web pages.

If you search the Web, you can find several RSS newsreaders, some of which are free, some shareware, and others commercial applications. They generally all work the same way.

1. You install the RSS client.
2. You subscribe to RSS feeds.
3. The RSS client checks your subscribed feeds periodically (e.g., hourly, daily, weekly, and so on).
4. Updated content is displayed using headlines.
5. You click the headline for the content you want to read.

RSS is a great way to have the news come to you for perusal and reading. If you have not yet experimented with RSS, I recommend that you do so; you should expect RSS feeds to continue to grow in popularity, and as mentioned previously, Exchange 2003 content is already available via RSS.

Summary

A plethora of Exchange-related resources on the Internet can help you plan, deploy, manage, and troubleshoot Exchange 2003. In this chapter, I discussed the settings that have been deprecated from Exchange 2000, as

well as some new settings for Exchange 2003 you can use to control certain aspects of its behavior.

In the sections on tools and resources, you learned where to find the latest information on Exchange 2003 and how to use Microsoft's new Exchange TDL. In addition, you learned about the free Exchange tools you can use to manage your Exchange infrastructure. There are several tools that can be used in a variety of situations, and all of the tools are worth checking out.

In addition to the Exchange product home page, Microsoft also has Exchange content on their TechNet Web site geared toward IT professionals and developer-related information on the MSDN Web site. In addition, Microsoft provides free peer-to-peer newsgroups that are available 24/7 and used by Exchange administrators all over the world. In addition, many Microsoft MVPs and some Microsoft employees regularly monitor these newsgroups, freely sharing their expertise and answering questions where they can. Finally, several third-party Web sites, blogs, newsfeeds, and other resources are provided by many other Exchange experts, including Microsoft employees who wrote Exchange.