Realtime publishers

"Leading the Conversation"

eJournal

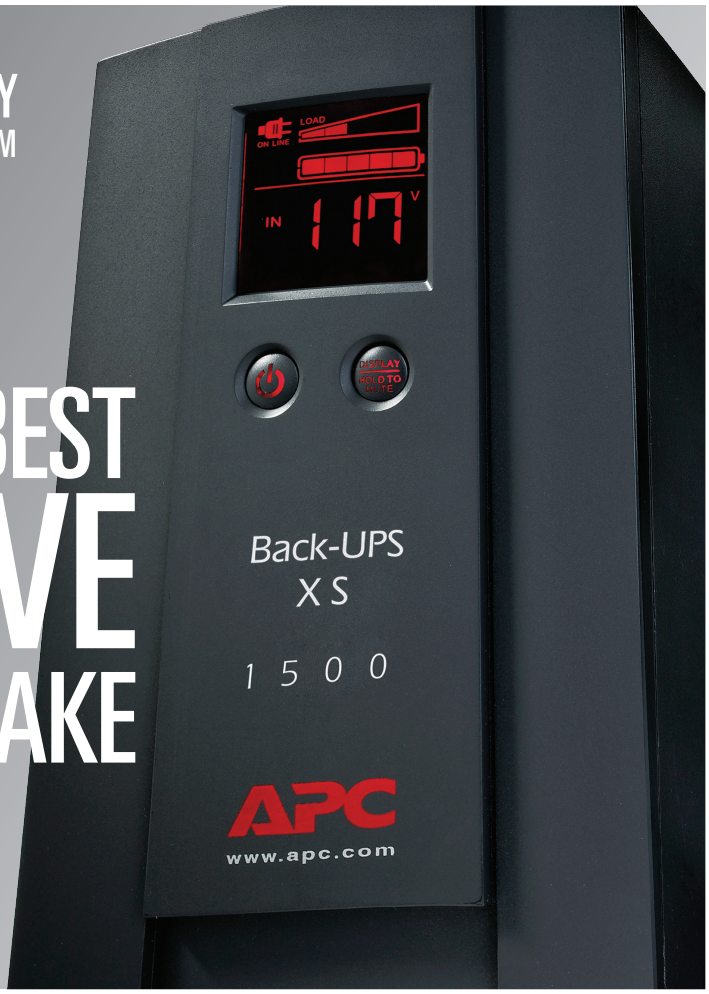
Windows Administration

in Realtime

February 2008

$150,000 INSURANCE POLICY
AGAINST HARDWARE DAMAGE TO YOUR SYSTEM

- SEE WEBSITE OR PRODUCT PACKAGING FOR MORE DETAILS -



INTRODUCING THE BEST POWER MOVE A BUSINESS CAN MAKE

Forget about acquisitions and mergers for a moment and think about your electricity and all that you rely on your computer for: personal and business files, financial information, broadband access, videos, photos, music, and more. Increasingly, computers are the hub for managing our lives. And more people rely on APC to protect their hardware and data than any other uninterruptible power supply (UPS) brand.

Why is APC the world's best selling power protection?

For 20 years, we have pioneered power protection technology. Our Legendary Reliability® enables you to save your data, protect your hardware, and prevent downtime. It also guards against a power grid that is growing less reliable every day.

According to the Department of Energy, electricity consumption will increase by 40% over the next 10 years. Yet today, investment in utilities is at an all-time low. It's a "perfect storm" for computer users, one that makes APC protection even more essential.

APC has a complete line of power protection solutions to suit a range of applications. Already an APC user? Get the latest replacement battery cartridge for your unit or upgrade to a newer model.

Find out why 30 million people don't need to worry about losing their data to power problems

APC power protection products are available at:

BEST BUY · CDW · Circuit City · Office DEPOT · STAPLES

that was easy.

APC Solutions for Every Level of Protection:

Home Starting at $59

Best value battery backup and surge protection for home computers.

Back-UPS® ES 550R

8 outlets, DSL protection, 44 minutes of runtime*

Home Office Starting at $99

Complete protection for home and small business computers.

Back-UPS® ES 750

10 outlets, DSL and Coax protection, 70 minutes of runtime*

Small Business Starting at $459

High-performance network power protection with best-in-class manageability for servers.

Smart-UPS® 1000

Register to win an APC 1500VA Battery Back-UPS® system (Model: BX1500LCD) a $199 Value!

Visit www.apc.com/promo Key Code a930w or Call 888.289.APCC x9432 or Fax 401.788.2797

APC® Legendary Reliability®

e-mail: esupport@apc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA • BK2B7EF-EN *Runtimes may vary depending on load. **Actual prices may vary

Inside This Issue

February 2008 • Volume I, Number I

Letter from the Editor

Welcome to the Conversation!

by Greg Shields

It has become cliché to refer to how the world of work is changing. At the same time, I find myself amazed at how far IT has come in such a short span of years. Becoming rare are the traditional brick-and-mortar establishments where work is done until 5:00pm and then employees head off to home. With many businesses, employees find themselves working from home, travelling abroad, having meetings in restaurants, and connecting to applications in Cincinnati through networks in Dubai.

This thought was particularly driven home as my laptop and I sat down for a burger in a place here in Denver called Stuben's Food Service. A replica of a 1950s diner of the same name, this new Denver establishment is the perfect combination of the old and the new. Stainless steel countertops, Yoo-Hoo, malted milkshakes, and, oddly enough, a publicly accessible wireless connection are all available for those who want it.

That dichotomy between old school and new explains a lot about the world of IT today. Though we need to keep looking to the future in serving the needs of our users, we at the same time must engage with the care and feeding of the servers and applications of yesteryear. Even as users travel the globe in search of new business opportunities, they still need access to applications that haven't seen updates in years or more.

In the same vein, the way we in IT get the information we need to do our jobs has changed as well. It can take months to get a print magazine out the door. A book can take half a year or more. Economies of scale and the desires for searchability and instant access have aged many (though not all) of our printed manuals.

You have demanded instant gratification. So we here at Realtime Publishers have provided it. As the editor of our first eJournal, I'd like to welcome you to our best effort towards providing some of the most timely IT information possible. This all-electronic publication gives us the opportunity to talk candidly with you about the topics, trends, and technology we see in IT today. With top-notch writers that you have demanded, you can expect some of the best and most interesting IT content available. Its electronic distribution grants us the capability to point you today towards what works today. And, above all, we can do it without the loss of a single tree.

So as I write this, sitting in this 1950s restaurant utilizing a network connection of the 2000s, it makes me happy to see how far we've come. It makes me even more excited to report to you on how we're doing it. Enjoy the eJournal. And if you're ever in Denver, stop by for the green chili cheeseburger and fries. As with the publication you're about to read, you won't be disappointed.

The Industry Outlook

Hot Topics in the IT Arena

by Don Jones

Free Vista?

Microsoft recently offered free copies of various editions of Windows Vista to people interested in having Microsoft track their computer usage for several months. Part of Microsoft's "Windows Feedback Program," data from the study will likely drive future Windows development, and may help Microsoft understand why so many people are so vocally not interested in the new operating system (OS), preferring instead to stick with good ol' Windows XP.

PowerShell Takeover

More and more companies are jumping on the "manage from the command-line" bandwagon. Newcomers to the party include Citrix, IBM, and VMWare, all of whom have instrumented key products (MetaFrame, WebSphere, and VMWare Server, respectively) in Windows PowerShell, enabling command-line administration and automation.

More Portable, Longer Power

The increased popularity of laptops over desktops is driving new technologies aimed at better portability and better battery life. LED backlighting and newer Intel chipsets (such as "Santa Rosa") are now joined by Toshiba's 128GB solid-state storage—a 128GB "hard drive" with no moving parts and lower power consumption than a spinning disk. Sized to replace 2.5" notebook drives, it's an exciting new development for ultra-portable, ultra-battery laptops.

Microsoft Adds Virtual Machine Management

With the release of System Center Virtual Machine Manager, Microsoft is making a play for the enterprise virtualization market. Sold for $500 (which lets you manage as many as five physical host servers), it offers centralized VM deployment and management, workload-balancing analysis, physical-to-virtual and virtual-to-virtual conversion, and more. It's also automated via Windows PowerShell. However, this product isn't filling what's widely believed to be Microsoft's "missing piece" of virtualization—performance. It remains to be seen whether the "hypervisor" portion of Windows Server 2008, not scheduled to ship until 6 months or longer after Win2008 itself ships, will bring much-needed performance improvements.

The Deep Dive

User Account Control: Why You Need It. Why You Don't.

by Greg Shields

Vista's User Account Control (UAC) has been making waves in the world of IT. Unfortunately, for many, they're not the good kind. UAC has become known as one reason why many admins are waiting on the move to Vista. In my conversations with administrators across multiple organizations, the changes made by UACs to the user's experience are one of a series of hurdles that make this OS upgrade one of the slowest yet.

But is all the weeping and gnashing of teeth actually worthwhile? What value does UAC provide for Vista? Is the added security worth the added annoyance? In this, my first column for Realtime Publishers' premier issue of eJournal, let's begin with a discussion about the pros and cons of UAC.

Are You Sure?

If you've had your head in the sand for the past year or you've made the conscious decision to ignore Vista entirely, you may not be familiar with UAC. Although it's most obvious element is the much-maligned *Windows needs your permission to continue* prompt, there's more to UAC than meets the eye.

In the background, UAC is actually quite a bit more than that prompt. More than anything, UAC was designed as a tool to force administrators to operate as standard users as much as possible. With previous OS versions, we were implored by Microsoft and security pundits everywhere to operate our desktops as standard users. When we needed to use our administrative powers, they suggested we elevate individual processes using tools such as the command-line "runas." By separating our standard operating environment from the one we need to accomplish god-like tasks, our actions were less likely to cause harm across the entire network. If we accidentally brought down a virus or malware, that bad software was less likely to be distributed everywhere compliments of our credentials.

UAC accomplishes its goal by separating our administrator "token"—the small piece of code that identifies our rights and privileges to the system—from that of our standard user token. When we're typing a document in Microsoft Word or surfing the Internet in Internet Explorer, we don't need to pull out our deity membership card for access. In fact, we shouldn't even want it for those standard activities.

But when a situation arises when we do, UAC can automatically elevate us without requiring a separate login. No log-out-and-log-back-in. No "runas" for each process. Simply a dialog box asking whether we're OK with elevating our rights for this particular task. It's a great concept that goes far in helping those who have traditionally done the right thing and run as standard users. For those who haven't, the prompts can become the bunt of a host of bad IT jokes.

There are other reasons behind UAC's prompting as well. By providing a visual indicator when something needs administrative access, users are enabled to make more informed decisions about the actions they're attempting to complete on the system. For administrators with vast and far-reaching privileges across the network, this prompt is also a kind of "wake up call." Its notification helps protect us when we might have attempted an action that could have bad and far-reaching results. If you've ever accidentally deleted a critical system file or reset a network connection, you're familiar with the occasional oops that even we trained professionals are guilty of from time to time.

The concern on the part of many administrators has to do with the persistence of UAC's reminders. Need to change an IP address? Cancel or Allow. Modify a user? Cancel or Allow. Install software? Cancel or Allow. As administrators, we're bombarded with constant reminders that we are indeed administrators and that we're attempting to do something administrative. It is that regular admission on the part of the OS that *we might not really want to do what we're about to do* that is the source of irritation for many who use UAC for any extended period of time.

Yes, I'm Sure!

Now, don't get me wrong. Even without the prompts, UAC is a valuable component of Vista's improved security model. With it, we get core system protection from malware. Running as a non-administrator, a malware infection is less likely to impact the system. Heck, a malware infection overall is less likely to occur due to UAC's integration with Windows Integrity Control (WIC). Using WIC, we divide all rights, NTFS permissions notwithstanding, into the "haves" and the "have nots." Users protected by UAC go into the "have" group, while nearly everything coming out of Internet Explorer goes into the "have not" bucket. Malware need not apply because in most cases it automatically arrives in-system as a "have not."

We also gain protection against dialog box spoofing. When malware attempts to install itself or begin running with nefarious intentions, UAC's prompt lets us know that a process is attempting to run that needs administrative rights. For administrative users who have a clue and are watching carefully, this prompt provides an extra, added protection against malware popping up windows asking for approval to install itself and begin running.

A tangential benefit is the pressure UAC puts on third-party software vendors. UAC's redefinition of which areas in the file system are copacetic for software to install helps enforce good software development practices onto vendors. Thanks to UAC, vendors are now stuck between the stick and the carrot of Microsoft forcing them to write better-secured software. If you've ever had to begrudgingly grant administrative privileges to "Stan in Accounting" because one minor piece of poorly written software he needs requires it, you'll be happy over the long haul when UAC's political pressure forces that application's vendor to recode it correctly.

ADD UAC

All of these are clear reasons why UAC is a good thing, and remains a good idea for Microsoft to have included in the OS. If it just weren't… so…persistent…in how often it presents itself on-screen. Now here's the catch. Even that persistence can be dialed down somewhat. If you're thinking about changing its default settings to get rid of it partially or completely, consider some of the following realities:

- *UAC is only enabled for administrators.* Standard users needn't necessarily be bothered by UAC prompts whatsoever. If you're a standard user, you're less likely anyway to truly understand what the prompt means. Standard users have done a great job of training themselves to auto-click anything that appears on-screen. Thus, the understanding, processing, and decision-making based on UAC's presence just isn't likely to happen very well, especially when those users are non-technical in the first place.

- *By default, non-administrators are prompted but that can be changed.* When a non-administrator attempts to accomplish a task that requires administrative access, UAC will by default present what is called an "over the shoulder" elevation prompt. This prompt allows the user to ask an administrator to approve the action by entering in their username and password. This is a great way to quickly solve problems that need administrative access without requiring the aforementioned log-out-and-log-back-in procedure. But it can also be a point of confusion with users. They're used to seeing "Access Denied." Using Group Policy, as we'll discuss in a minute, this behavior can be reverted to the old, and arguably more understood response.

- *Elevation prompts can be eliminated altogether.* Also using Group Policy, it is possible to automatically approve any elevation request. Doing so does not get rid of UAC. Rather, it configures UAC to dispense with the prompt. Any time a process or action requires elevation, that elevation will occur automatically and without prompting. Though this is better than shutting down UAC, it does eliminate some of its protections. Namely, when processes that shouldn't have administrative access do, they'll be automatically approved as well.

- *You can always just run as a standard user.* If you truly hate UAC, but you fear getting rid of it, you can always revert back to the old best practice—that being running your regular operations as a standard user and using elevation tools when you have the need. By doing this in combination with the Group Policy settings discussed in a moment, you can eliminate nearly all of UAC's prompting.

From the perspective of centralized management, there are nine Group Policy settings that can be used to configure the behavior of UAC within your domain. Each of these are available by opening the Group Policy Management Console (GPMC) from a Vista machine and navigating to *Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Security Options*. There, at the bottom of the list, are nine policy settings that all start with *User Account Control*. Let's talk about each of them, the configuration of which can help calm UAC's Attention Deficit Disorder and reduce the pain of managing your Vista workstations. For each, the setting in parenthesis is the default local setting for Vista:

- *Admin approval mode for the built-in administrator account (Disabled).* By default, the Administrator account has UAC turned off. Though this can be an alternative option for annoyed technicians, remember that uniquely identifying the activities of even a network's technicians is important for both security and compliance.

- *Behavior of the elevation prompt for administrators in Admin Approval Mode (Prompt for consent).* We talked about a way to quiet UAC. This setting can be configured to Elevate without prompting. This has the effect of automatically elevating when necessary and should be your first line of defense should you want to dial down UAC's chattiness.

- *Behavior of the elevation prompt for standard users (Prompt for credentials).* We also discussed how to revert normal users so that their attempts to accomplish a task resulted in the familiar "Access Denied" rather than an over-the-shoulder elevation. Do this by configuring this setting to Automatically deny elevation requests.

- *Detect application installations and prompt for elevation (Enabled).* You'll likely want to keep this setting as is. By keeping this at Enabled, an heuristic is applied to launched programs to determine whether they are application installations. This prevents an installation from attempting to start without needed administrative credentials.

- *Only elevate executables that are signed and validated (Disabled).* Another setting you may want to leave alone. By setting this to enabled, you'll be allowed to elevate only when executables have been signed using a certificate.

- *Only elevate UIAccess applications that are installed in secure locations (Enabled).* This setting validates that executables that require UIAccess privileges are launched from either the Program Files location or the Windows directory. These two locations are considered "secure" due to how Vista has changed their NTFS permissions model.

- *Run all administrators in Admin Approval Mode (Enabled).* This setting effectively disables UAC for all administrators. Use this as your last resort. Note that setting this will require a reboot.

- *Switch to the secure desktop when prompting for elevation (Enabled).* The grayed out screen that appears with the elevation prompt is called the "secure desktop." This method of operation is limited to receiving messages only from Windows processes. If you use the elevation prompt, keeping the secure desktop ensures the highest level of protection from malware.

- *Virtualize file and registry write failures to per-user locations (Enabled).* Another part of UAC we haven't discussed yet is the transparent movement of software files from locations considered "bad" by Vista to other locations considered acceptable. This is necessary to allow some poorly coded software to continue to function with Vista. Disabling this removes that transparency and can prevent some software from functioning.

The moral here is that UAC need not prevent you from moving to Vista. Though there are other published reasons why many are delaying the migration, UAC alone has the configuration capability to allow you to tailor it however you want. If you want to disable it entirely and return to a pre-Vista mode of operations, that capability is similarly available. But between all-the-way-on and completely-off, you can see that there are options that make UAC less cumbersome.

For more information about UAC, its uses, and the best ways to work with it, check out the TechNet article at http://technet2.microsoft.com/WindowsVista/en/library/00d04415-2b2f-422c-b70e-b18ff918c2811033.mspx?mfr=true.

Greg Shields, MCSE: Security, CCEA, is an independent author, speaker, and consultant, based in Denver, Colorado. With more than 10 years of experience in information technology, Greg has developed extensive experience in systems administration, engineering, and architecture. Greg is a contributing editor for both Redmond magazine and MCPmag.com, authoring two regular columns along with numerous feature articles, webcasts, and white papers. He is also the resident editor for Realtime Publishers' Windows Server Community at www.realtime-windowsserver.com. Greg is currently finishing his new book Windows 2008: What's New, What's Changed through SAPIEN Press.

Focal Point

Virtualization

by Don Jones

In this monthly column, I'll be exploring leading technologies that are sometimes overlooked or incompletely understood. This isn't an analysis piece, though; my goal is to help you more thoroughly understand these technologies at a deep level and determine if and how they might fit into your environment. Up this month is virtualization, a hot topic and one that's actually a lot broader than you might think.

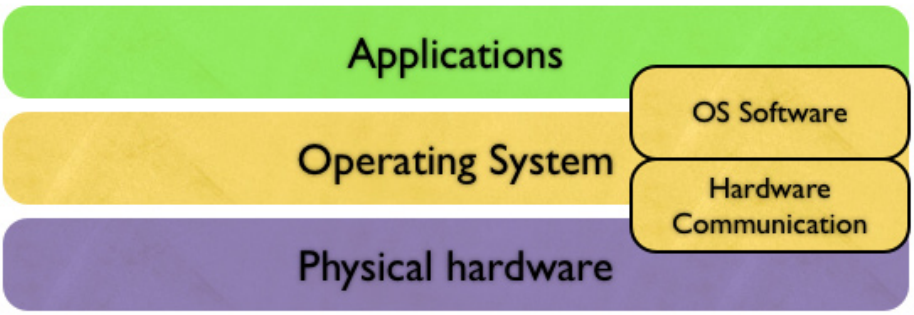


Figure 1

What's in a Name?

The term virtualization can be loosely defined as "faking it." You may be familiar with desktop virtualization software like that made by Microsoft (Virtual PC) or VMWare (Workstation); this software "fakes" PC hardware so that you can install complete operating systems (OSs) "inside" the virtual machine (VM). Many IT professionals and software developers use this kind of virtualization for software testing, and it's probably the oldest form of virtualization around.

However, virtualization has come to mean a lot more in our industry, and the many different types of virtualization that are now available each offer specific solutions for your environment. To kick things off, we need to take a moment and understand exactly how computers and OSs are built—or, at least, agree on some common terminology for referring to their various parts.

A Stack of Technology

Figure 1 shows a conceptual model of a computer's major components with regard to virtualization. At the bottom of the "stack" is the computer's physical hardware: memory, disk drives, processors, and other physical resources that you can actually lay hands on. On top of that is the OS, such as Windows or Linux, that you install on the hardware. Modern OSs tend to split themselves into two broad categories. The bottom one handles direct communication with hardware, while the upper one actually runs the OS code itself. That model is obviously a simplification because OSs differ so widely. In Windows, you can think of the bottom layer as Windows' Hardware Abstraction Layer (HAL), while the upper layer is the OS kernel. Above the OS are your applications. They're more or less unaware of the hardware they run on; instead, they simply run "on" the OS.

The purpose of virtualization is to wedge itself into this stack, somehow, and create a new stack. For example, VMWare Workstation runs on top of the OS as an application, and creates a new "virtual" stack that includes virtual hardware, an OS you install, and applications that run on that OS.

Hardware Virtualization

As I mentioned, the most common type of virtualization these days is hardware virtualization, perhaps best known from products such as VMWare Server, VMWare ESX

Server, VMWare Workstation, Microsoft Virtual PC, and Microsoft Virtual Server. As Figure 2 shows, these all run as applications, and virtualize—or more properly, emulate—PC hardware. They expose emulated hardware such as graphics cards and network adapters that are completely different from the actual hardware in the host machine but which communicate with the host hardware to display graphics and communicate with the network. The overhead of emulating all this hardware in software is pretty high, and as a result, you have to have a pretty beefy machine to run more than a couple of virtual machines. However, they offer some of the best flexibility, allowing you to run nearly any Intel-compatible OS within virtual machines. Add-on or bundled management products (such as VMWare VirtualCenter or Microsoft Virtual Machine Manager) allow virtual machines to be moved across host computers to help balance workloads, migrate physical computers into virtual machines, and other tasks. Perhaps the most common use for this type of virtualization is to consolidate dissimilar servers running older OS. A single well-equipped Windows Server 2003 host, for example, might run a dozen or more Windows NT 4.0 or Windows 2000 computers alongside Linux, UNIX, and other computers.

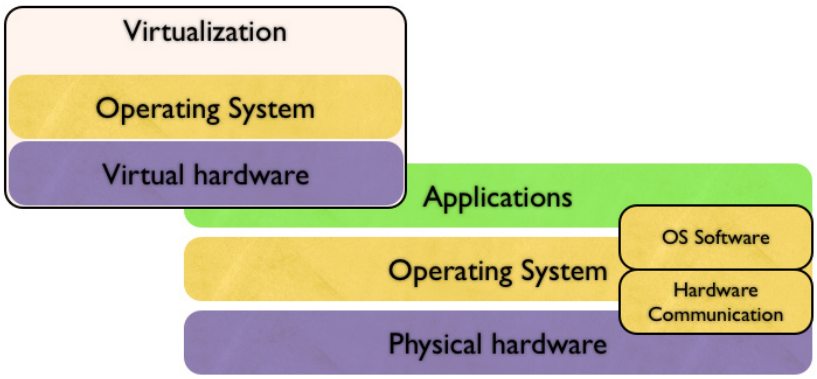


Figure 2

Another common use that I've already mentioned is software testing. These virtualization technologies generally support some kind of "snapshot" feature, allowing the current state of a virtual machine to be saved. After testing software and potentially damaging the virtual machine's OS or other software, the entire machine can be "rolled back" to the snapshot with a button click, instantly "resetting" everything back to the starting point. But hardware virtualization is often not the most efficient choice when you need to consolidate several computers running the same OS as the host computer.

OS Virtualization

Another choice, offered by products such as SWSoft's Virtuozzo is OS virtualization. The virtualization product doesn't emulate the hardware. Instead, each "virtual machine" starts off as a copy of whatever OS the host computer is running. From there, each virtual machine can diverge, changing OS configurations and installing software. This is a great solution when you want to consolidate several computers running the same OS, such as in a Web-hosting scenario. A Web host can successfully host dozens of customers on a single physical server, and each customer will think they're on a completely dedicated server. This is somewhat analogous to Windows Terminal Services environments, except that in Terminal Services, a computer-wide configuration affects all other users; under OS virtualization, a computer-wide configuration is limited to the "virtual machine" on which it was made. Another way of referring to this type of virtualization is partitioning, with each "virtual machine" acting as a single, isolated partition. But what if your goal is to have only one OS and one set of machine-wide OS configurations but still isolate applications from each other?

Application Virtualization

Applications such as Microsoft's SoftGrid "wedge" themselves in one step higher. Although they do serve a virtualization-like function, these solutions are less "virtualization" and more "redirection." Essentially, when an application runs, it "sees" the entire OS on the computer and can make changes such as writing files. The virtualization technology intercepts these changes and directs them to a file that is specific to the application being run. Whenever the application tries to access resources, such as files, the virtualization technology again intercepts the request; if the requested data is in the application's virtualization file, the request is fulfilled from there. If not, the data is read from the base OS. The idea is that an application can run without actually touching the underlying OS or affecting other applications—in essence, a form of partitioning not unlike that used by OS virtualization, although at a somewhat different level and for a somewhat different purpose.

Flavors of Virtualization

In the future, more organizations will use many forms of virtualization to meet their needs. New hardware-based technologies from processor manufacturers are making hardware virtualization easier and more efficient, and new techniques in virtualization are being dreamed up all the time to help solve specific business problems.

Don Jones is a nationally-recognized author, instructor, speaker, and consultant, with more than a decade of experience in the Information Technology industry. Don is the author of nearly two dozen published works on IT subjects, is a regular speaker at national conferences like Windows Connections, Microsoft TechEd, and TechMentor, and is a regular columnist for Microsoft TechNet Magazine. He is a multiple- year recipient of Microsoft's Most Valuable Professional award in recognition of his advocacy of scripting and automation, specifically for Windows PowerShell. Don currently serves as the Director of Projects and Services for SAPIEN Technologies, where he manages the company's Publishing, Training, and Community divisions. He is also the Series Editor and CTO for Realtimepublishers.com.

Practical PowerShell

Space Hogs

by Jeffery Hicks

The Problem: You have a file server running low on disk space. You would like to find the largest files and ideally who owns those files.

Using PowerShell on the file server can solve this problem with minimal effort. Technically, you could execute the PowerShell expressions in this article from your desktop, querying the file server over the network, but I think performance will be better if you can run a PowerShell session locally on the file server.

Let's start with a basic PowerShell expression. This is a one-line expression:

```
get-childitem -path "D:\Files" -recurse | sort-object length -descending | select-
object -first 50 FullName,Length,CreationTime,LastWritetime
```

This expression demonstrates the utility of the PowerShell pipeline. The first command uses the Get-ChildItem cmdlet to recursively get all files under the path D:\Files. As we work with this expression, I'll use cmdlet aliases and take advantage of positional parameters and parameter disambiguation.

The results of Get-ChildItem are piped to the Sort-Object cmdlet, which will sort all the files on their length property in descending order. The length property is the same as the file size. These results are then piped to the Select-Object cmdlet. This cmdlet has a parameter, -first, which allows us to return only the first specified number of objects. In our expression, the specified number is 50. Remember, the files have already been sorted in descending order by size. The last part of the Select-Object cmdlet instructs PowerShell to return only specific properties. These properties should be enough to identify the largest files as well as other pertinent information.

If you try this first expression, you'll see that it is pretty basic. But there are a few items missing. First, it is likely you'll want a report of some sort to show to management. Or perhaps you want to perform some other analysis on these files. The following example shows the previous expression with the output piped to the Export-Csv cmdlet which will create the specified CSV file:

```
gci D:\Files -rec | sort length -desc | select -first 50 fullname,Length,CreationTime,
LastWritetime | Export-CSV c:\spacehogs.txt -noType
```

I specified the –noType parameter to instruct Export-Csv not to include type information at the beginning of the file. I plan to open the file in Microsoft Excel; this setup makes it much neater. When I open the file in Excel, I can manipulate the data further and even create spiffy charts or reports. If you plan to import the data back into PowerShell, drop this parameter. But I'm still missing a piece of information.

I want to know the owner of each of these files. We'll forgo exporting for the time being so that you can see how this works:

```
gci d:\files -rec | sort length -desc | select -first 50 Fullname,Length,CreationTime,
LastWritetime,@{Name="Owner";Expression={(get-acl).owner}}
```

The only change I made to the expression was to add a calculated property to the Select-Object cmdlet:

```
@{Name="Owner";Expression={(get-acl).owner}}
```

This expression will create a new property called Owner. The value is returned by piping each file to the Get-Acl cmdlet and retrieving the Owner property. Now we're getting somewhere.

Still, the output could use some additional cleanup. Perhaps I'd like to change Length to Size to make it more meaningful. Also, the file size is listed in bytes. That information might look better displayed as megabytes. Let's tweak our expression:

```
gci d:\files -rec | sort length -desc | select -first 50 @{Name="File";Expression={$_.
fullname}},@{Name="Size (MB)";Expression={$_.Length/1MB}},@
{Name="Created";Expression={$_.CreationTime }},@{Name="Last Updated";Expression={$_.
LastWritetime}},@{Name="Owner";Expression={(get-acl).owner}}
```

Now I have more meaningful and shorter custom properties. Each one is calculated from each object in the pipeline, as represented by $_. The file size is returned by dividing by the length of the current file in the pipeline by the special 1MB variable. This is much easier than typing 1048576. If you prefer, you could also divide by 1GB to get a value in gigabytes.

We're getting closer, but I'm not satisfied. Here's a sample of the output:

```
File          : D:\Files\development\fundraising.mdb
Size (MB)     : 28.034215927124
Created       : 8/27/2005 3:07:30 PM
Last Updated  : 5/21/2006 9:34:10 AM
Owner         : MYCOMPANY\JHicks
```

It would be nicer if the file size was formatted, perhaps to two decimal points. Here's how this is done:

```
gci d:\files -recurse | sort length -desc | select -first 50 @
{Name="File";Expression={$_.fullname}},@{Name="Size (MB)";Expression={"{0:N2}" -f
($_.Length/1MB)}},@{Name="Created";Expression={$_.CreationTime}},@{Name="Last
Updated";Expression={$_.LastWritetime}},@{Name="Owner";Expression={(get-acl).owner}}
```

The only change is that I'm using the .NET format operator, -f, to handle the numeric formatting:

```
@{Name="Size (MB)";Expression={"{0:N2}" -f ($_.Length/1MB)}}
```

This operator applies a pattern, "{0:N2}" to the result of dividing $_.Length by 1MB. Now instead of 28.034215927124, I'll get 28.03.

Finally, I think I have a meaningful report. All that's left is to export the results to a CSV file. Here's the final expression:

```
gci d:\files -rec | sort length -desc | select -first 50 @{Name="File";Expression={$_.
fullname}},@{Name="Size(MB)";Expression={"{0:N2}"-f
($_.Length/1MB)}},@{Name="Created";Expression={$_.CreationTime }},@{Name="Last
Updated";Expression={$_.LastWritetime}},@{Name="Owner";Expression={(get-acl).owner}} |
export-csv c:\spacehogs.txt -noType
```

Yes, it is a lot to type, but you have to admit for a single line of code, it accomplishes a great deal. If you find yourself using this script block often, simply copy and paste into a .ps1 file and you have a PowerShell script. An even better approach is to turn this expression into a function like this:

```
Function Get-LargeFiles {
 Param([string]$Path=".",[int]$First=50)

Get-ChildItem $Path -recurse| Sort-Object length -desc |
Select-Object -first $First `
@{Name="File";Expression={$_.fullname}},
@{Name="Size (MB)";Expression={"{0:N2}" -f ($_.Length/1MB)}},
@{Name="Created";Expression={$_.CreationTime }},
@{Name="Last Updated";Expression={$_.LastWritetime}},
@{Name="Owner";Expression={(get-acl).owner}}

}
```

The function will default to the current directory and the first 50 files. With this function loaded into PowerShell, our expression now becomes much simpler:

```
Get-LargeFiles d:\files 50 | export-csv c:\spacehogs.txt -noType
```

Hopefully, you've been thinking about some of your own ideas for enhancing this code. PowerShell offers plenty of opportunities.

Jeffery Hicks, MCSE, MCSA, MCT, and Microsoft PowerShell MVP, is a Scripting Guru for SAPIEN Technologies. Jeff is a 16-year IT veteran. He has co-authored and authored several books, courseware, and training videos on administrative scripting and automation. His latest book is WSH and VBScript Core: TFM (SAPIEN Press 2007). You can contact him at jhicks@sapien.com.

Unified Messaging in Exchange 2007

Getting Microsoft's Vision of Unification Up and Running

by J. Peter Bruzzese

In the typical office, it's common to see email servers, fax services, voicemail systems with PBXs for private telephony, and a host of other systems. So when network admins hear the words 'Unified Messaging' their mouths begin to water at the promise of eliminating the disparity of services and access methods toward those services. Microsoft has been promoting new entries into the Unified Messaging (UM) sphere through Exchange 2007 and Communications Server 2007. Both are compelling products, worthy of our attention, and this article will discuss the features available in Exchange 2007 when deployed as the UM role.

Exchange 2007 offers UM by allowing your emails, incoming faxes, and voicemail to come through the Exchange Server and be accessible through one Inbox (see Figure 1). Outlook 2007, Outlook Mobile, and Outlook Web Access (OWA) already support the client side to UM. In addition, users have the ability to manage email, contacts, and calendar information from their telephone, desktop, or mobile device. But these are just the surface level features of UM with Exchange 2007. Let's go through a more comprehensive list.

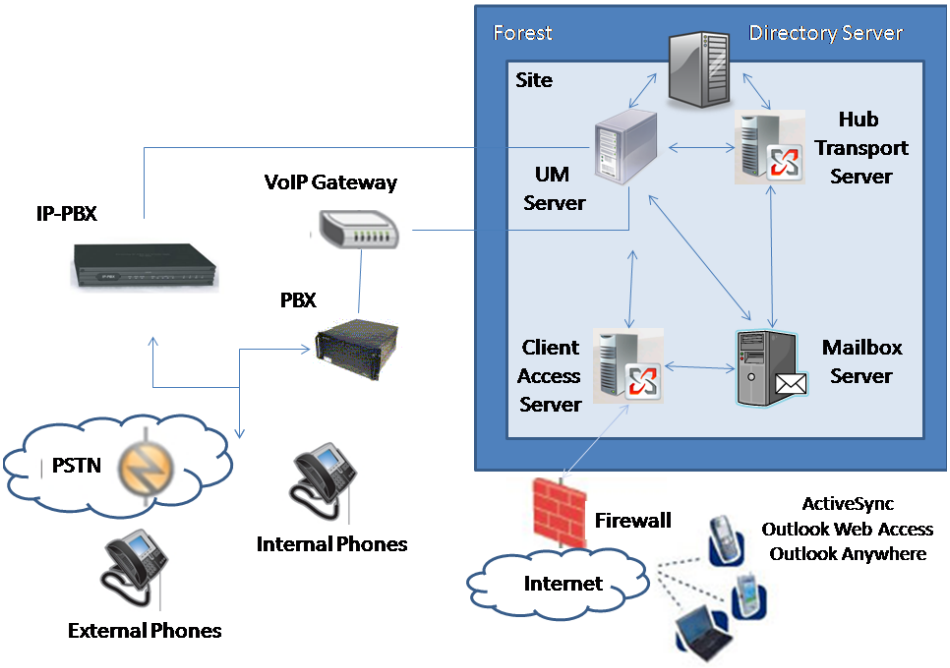


Figure 1: Implementing UM within your organization.

UM Features Explored

Microsoft refers to modern-day voicemail systems as "artifacts of the workplace of the past." Considering the capabilities of new applications combined with the backend server support of Communications Server 2007 or Exchange 2007, it is easy to see that they are correct. We want our systems to offer more integrated technology within a consolidated infrastructure. Simply put, we want more features that require less hardware and software. And we want it to be easy as pie to administer. Here is a breakdown of the primary features offered to us with UM in Exchange 2007:

Voice and Fax Messaging—Incoming voicemail or faxes are accepted by the UM Exchange Server and can be accessed through Outlook, OWA, Outlook Mobile, clients with an ActiveSync license, and Outlook Voice Access (OVA). Faxes come in as .tif files and are put in users' mailboxes.

One of the elements to supported gateways and IP-PBXs is that they have the capability to recognize an incoming fax message and send it to the UM Server. (However, outbound faxes will still require another delivery method).

- OVA—This feature allows users to access their mailboxes using a phone or through Office Communicator 2007 (or some other solution such as Skype, so long as your PBX/VoIP system allows call-in access). Using either voice-enabled menus or touchtone, you can listen to your email through the UM Server's text-to-speech capabilities. You can listen to your voicemail or call your personal contacts or those in the company directory.

- Play on Phone—When you check email and see you have a voicemail, you can route the voice messages to your phone rather than listen to them over your computer's speakers. Just supply the number, and the message will go to your cell, your desk phone, wherever.

- Calendar Management through Phone—Through OVA, you can manage calendar appointments by accepting/declining meetings, sending notices to persons letting them know you will be late, or making calendar changes such as cancelling appointments.

- One UM Server for Multiple Dial Plans—Allows a single UM Server to handle multiple dial plans, reducing the need for individual mail setup in each office.

- The Auto Attendant—Auto attendant can be configured to allow for directory lookups of people within your organization or to route calls by using menus such as "for technical support, please press 1." A caller can speak to the auto attendant or use touchtone menus if the attendant is having a difficult time understanding responses. A very cool feature is that the auto attendant can switch into the local accent depending on location.

- Multiple Languages—This aspect of UM is simply cool. You have menus and speech-to-text in many languages. Thus, if you receive messages in different languages, the system will detect the language and read it to you with the proper language. You can also configure different dial plans so that calls coming in to the same UM Server can be answered in different languages (making even the smallest of companies appear global).

- Administrative Features—UM is connected to Active Directory (AD), allowing you to quickly enable users already in the directory. You can easily work with UM through the Exchange Management Console or the Exchange Management Shell (making repetitious actions scriptable). There are support options built-in to the UM Server that allow users to accomplish common tasks such as reset voicemail PIN numbers, voicemail greetings, and out-of-office messages. This keeps users from calling YOU with these needs.

> For a full list and explanation of UM features, go to http://www.microsoft.com/exchange/evaluation/features/unifiedmessaging.mspx. And for a list of feature improvements/additions with SP1, see http://technet.microsoft.com/en-us/library/bb691398.aspx.

Hardware Concerns for Exchange UM

A standard server that meets the Exchange requirements will suffice as your UM Server, although the 'encouraged' settings include 4x Processor Cores and at least 2GB of RAM. You can install the UM role alone on a server or combine it with the Client Access Server, Hub Transport, or Mailbox roles. In fact, you can install all four roles onto one box if you like.

> The Edge Transport role is not combinable with any of the other roles; it is meant to exist on the perimeter of your organization on a standalone system.

Installing and configuring UM through the Exchange Management Console or Shell is possible even if you don't have the hardware configured just yet. However, nothing will function properly. First, you should contact a telephony expert (either your existing person/team or an outside consultant). Most Exchange administrators just do not know all the inner telephony concepts, so having the help will save you loads of time.

Exchange 2007 uses Session Initiation Protocol (SIP) and Realtime Transport Protocol (RTP) to function; however, not all PBXs are prepared to work with those protocols. Thus, you may need to procure new equipment; but don't start pulling out your credit card just yet. Your legacy PBX may work. The first thing you need to know is whether you already have a legacy PBX in place. If so, determine whether you can IP-enable the PBX. If not, determine whether your device can be combined with a VoIP gateway to provide the UM hardware support you need. The purpose of

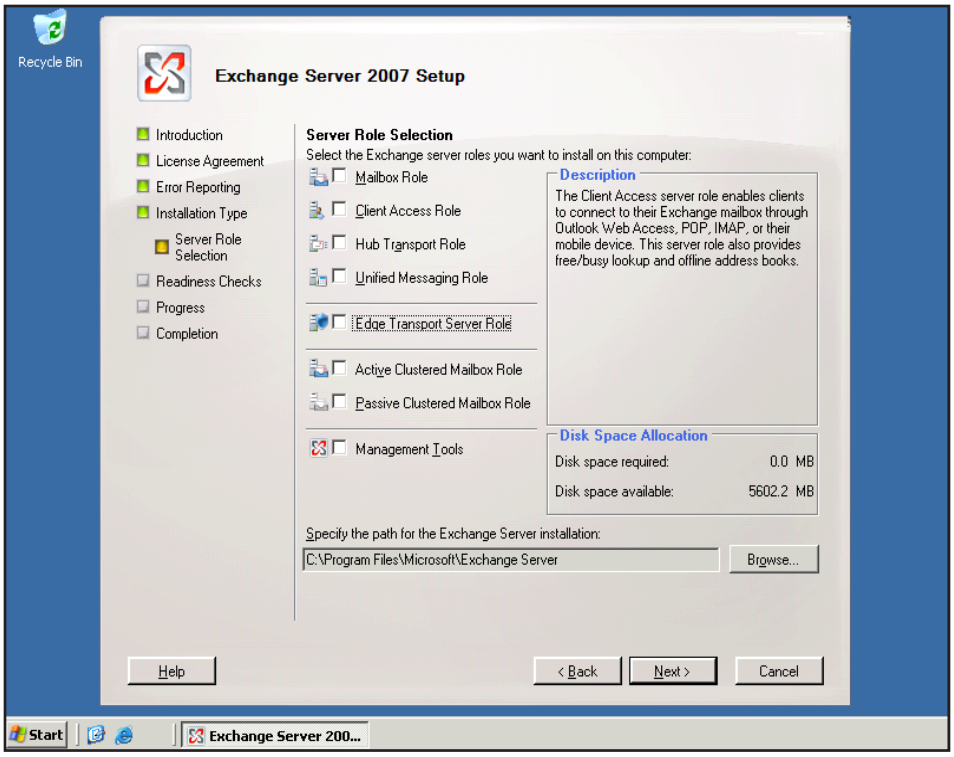


Figure 2: Installing the UM Role

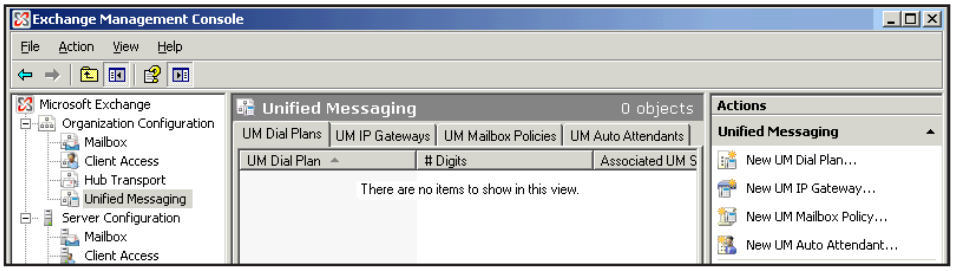


Figure 3: Configuration of the UM Role

the gateway is to allow your circuit-based network to work with your packet-based network. The VoIP gateway will perform the conversion. However, if you are starting your UM infrastructure from the ground up, you might be better off purchasing an IP-PBX, having the single device in place rather than two.

> For a list of Microsoft-supported VoIP gateways, PBXs, and IP-PBXs, consult the Telephony Advisor for Exchange Server 2007 site from TechNet at http://www.microsoft.com/technet/prodtechnol/exchange/telephony-advisor.mspx.

Install and Configure Your UM Server

You can install the UM Server role on a system running other roles or on a separate server. Simply select the Unified Messaging check box (see Figure 2). Keep in mind that you cannot install the UM role on a clustered Mailbox Server or on an Edge Transport Server.

Once the role is installed, you can configure your UM Server through the Exchange Management Console, as Figure 3 shows. Under both the Organization Configuration and Server Configuration headings, there is a Unified Messaging option that allows you to configure the settings on the server.

Beyond the role install, your first step is to create a dial plan. Without at least one dial plan, UM will not function. The purpose of the dial plan is to create a link between the telephone extension and a recipient. The link is established to an AD user with a UM-enabled mailbox. Thus, creating the plan creates an AD object that represents one or more PBXs with extension numbers. First you create the plan, then you associate a server with that plan. At the same time, a UM mailbox policy is created for you, although you will want to tweak it.

To get started, from the Actions menu, select the New UM Dial Plan option. A wizard will launch and walk you through the procedure. You will be asked basic information such as plan name and the number of digits in extension numbers (for example, if your number coming in is 555-6666 and the extensions would look something like 5-6666, then you want to indicate a five-digit extension number). Continue through the wizard to create the plan and then right-click the new plan from the UM Dial Plans tab and select Properties. Doing so provides you with six tabs you can work through in order to configure the plan:

- General—Provides an overview of the plan's basic information, such as the name of the plan and associated UM Servers and IP gateways. Check box options are available to *Send a non-delivery report if message delivery fails* or *Allow users to receive faxes (selected by default)*.

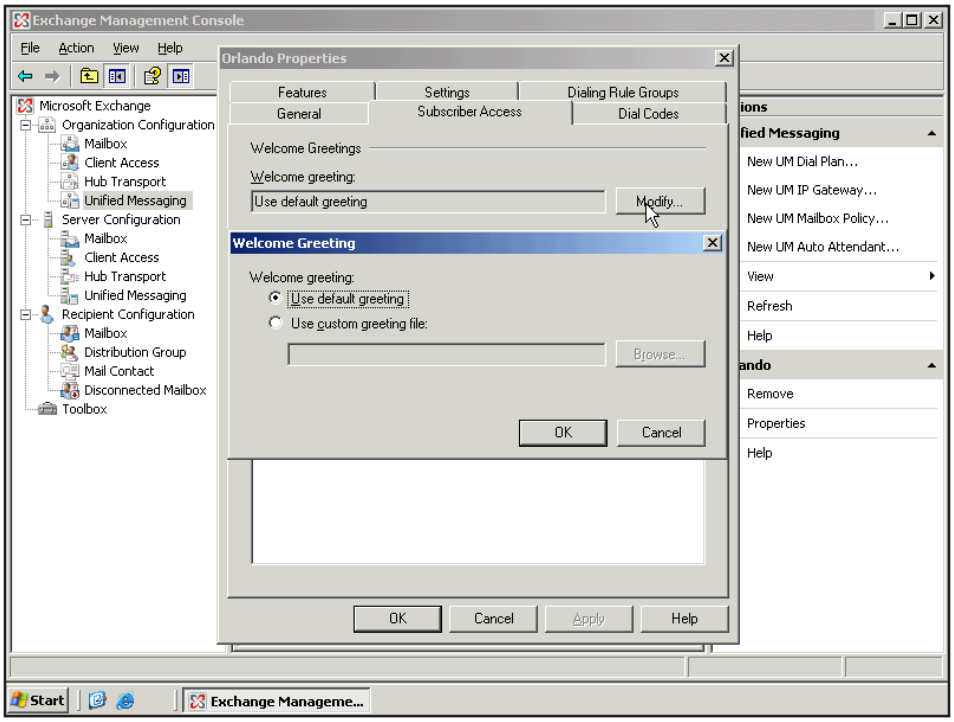


Figure 4: The Subscriber Access tab allows you to modify the greetings

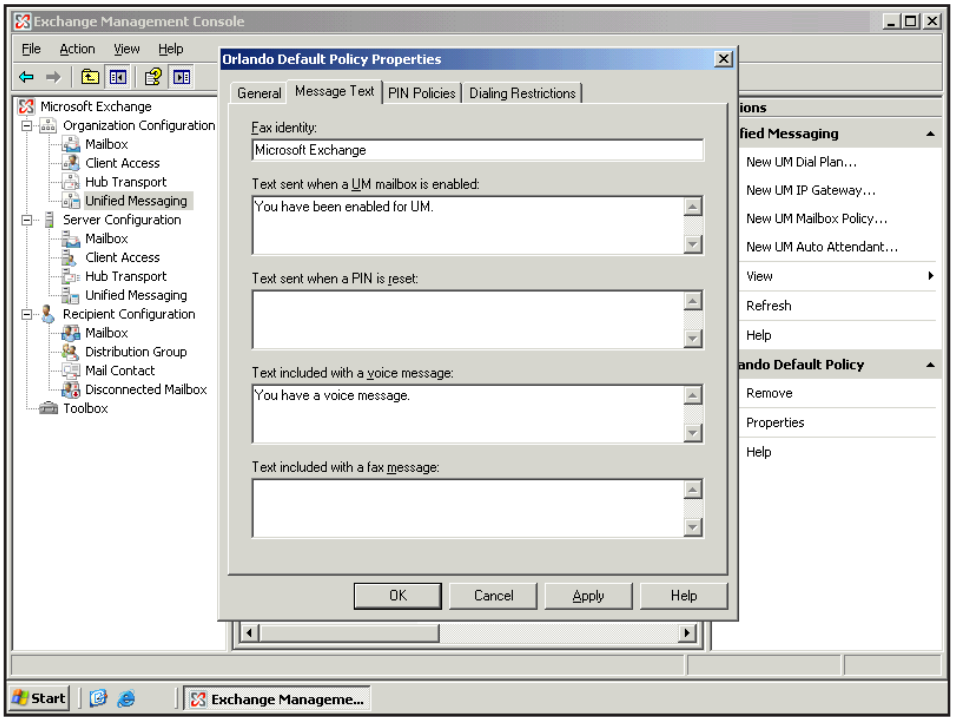


Figure 5: Establish text associated with the enabling of a UM mailbox, a PIN reset, a voicemail, and a fax.

- Subscriber Access—Allows you to customize the welcome greetings to use a personalized .wav file (see Figure 4). You can also change the associated subscriber access numbers on this tab.
- Dial Codes—This tab offers both outgoing and incoming configuration settings, such as *Outside line access code* (people may need to hit a 9 for an outside line) and *International access code* (people might have 011 for the United States or another code for a different country).
- Features—This tab has options like *Allow callers to transfer to users* and *Allow callers to send voice message*. You can also make changes to the *Callers can contact* section to limit the ability of callers to persons with the dial plan, persons in the global address list, persons with specific extensions, persons within a specific list, and so forth.
- Settings—Here you can select dial methods, timeouts and retries, and language settings.
- Dialing Rule Groups—Where you can add dialing rules and group them as needed. A dial rule group is a collection of one or more dialing rules. There are two kinds of dial rule groups: *In country or region and International*.

The next step is to configure settings on the UM IP Gateways tab. Select the *New UM IP Gateway* from the Actions menu to begin the wizard. The goal of this step is to create a connection between the server and the gateway. You will need to provide a name and an IP address or Fully Qualified Domain Name (FQDN) to associate the device with the dial plan. Select Browse and choose the plan you want (if you are just getting started, there is only one plan to choose). You will be informed of the creation of a hunt group. Select New, then Finish.

Now you will have a gateway and a hunt group. A hunt group is made up of line groupings so that callers can search for open lines from a group of extensions. If no lines are available, calls won't be able to get through unless you've configured the gateway with more than one hunt group so

that lines are available if they exist.

Next is the UM Mailbox Policies tab, which will already have a policy in place from when you created the dial plan. Right-click and go into Properties, and you will see four configuration tabs:

- General—Allows you to configure the *Maximum greeting duration (minutes)* with the default being 5, and allows you to turn on/off the *Allow missed call notifications*, which will notify a user with a message in their Inbox if they've missed a call.

- Message Text—Lets you configure text sent along with certain events (see Figure 5).

- PIN Policies—Allows you to configure simple PIN policy information such as the *Minimum PIN length* and the PIN lifetime (see Figure 6). You can prevent a history of PINs from being used and establish how many failed logons can be attempted before the PIN is reset and the mailbox locked out.

- Dialing Restrictions—This tab has two check boxes that are enabled by default: *Allow calls to users within the same dial plan and Allow calls to extensions*. You can also allow in-country/region rule groups and/or international rule groups from the dial plan.

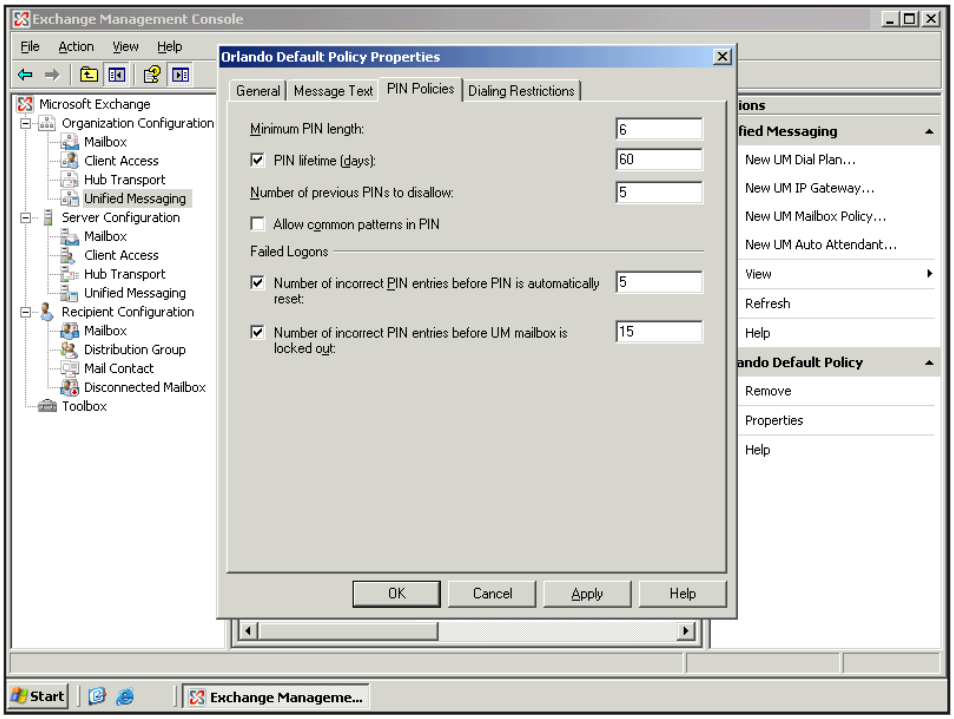


Figure 6: PIN policies, including failed logon attempt settings.

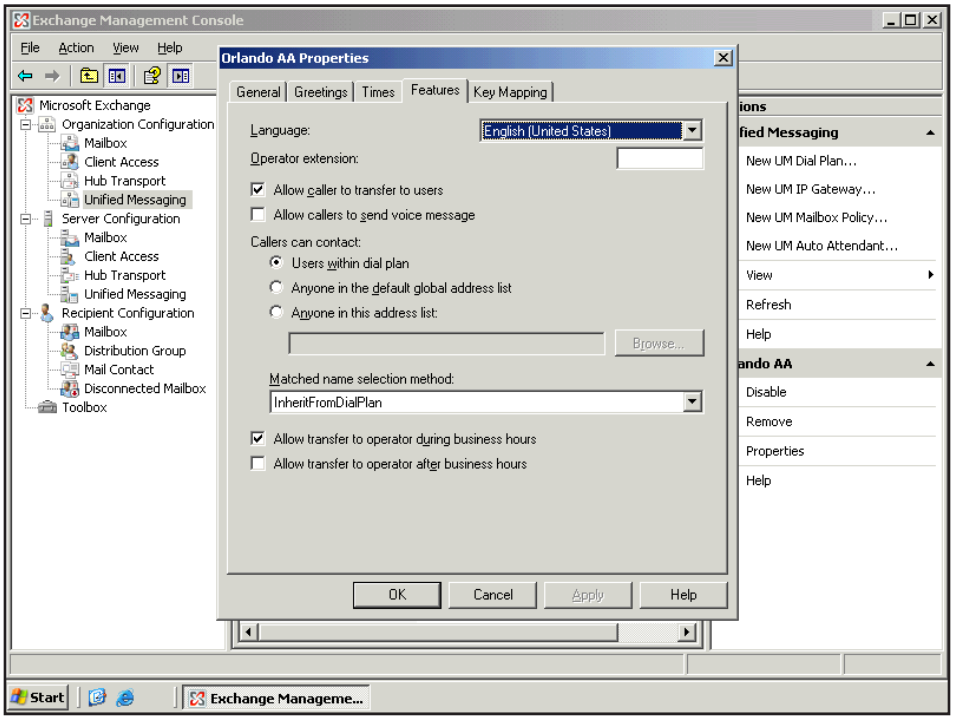


Figure 7: The Features tab lets you address operator extensions and caller contact permissions.

Our final step in the process is the UM Auto Attendant configuration. Start by selecting New Auto Attendant from the Actions pane. You will be asked to provide a name and dial plan for the attendant, and you can provide the extension numbers associated with the auto attendant. You also have two check boxes that are enabled by default: *Create auto attendant as enabled* and *Create auto attendant as speech-enabled*. Select New, then Finish. Next, right-click Auto Attendant and choose Properties. You will be greeted with five tabs:

- General—This tab offers most of the settings you provided during the creation of the auto attendant. One option that is unique is the Use this DTMF fallback auto attendant check box. Opt for this setting if you individuals who cannot use

speech are going to work with the attendant; they can work through a touch tone.

- Greetings—On this tab, configure greetings that you can alter with .wav files. There is a Business- and Non-Business-hour greeting, along with an Informational Announcement. There are also Business and Non-Business main menu prompts.

- Times—Here is where you can establish your company business/non-business hours. You can configure the time zone and add holidays into the schedule. You can even include a special greeting for callers on holidays.

- Features—This tab (see Figure 7) includes features we've addressed for users, but now we are discussing the ability the auto attendant has for allowing callers to transfer to users or send voice messages as well as who callers can contact, and so forth.

- Key Mapping—Here you can configure business- and non-business-specific connections between what a user presses on the phone or says over the phone and the response they get. They may receive a message or be transferred to another extension.

So far we have been discussing everything from the organizational level. On the server level, you can configure a little more, such as the number of concurrent connections, but there is not much more to do. You select the Unified Messaging option under Server Configuration, and go into the Properties of the server. On the UM Settings tab, select Add to register the dial plan. Then select the number of concurrent calls and fax calls you allow.

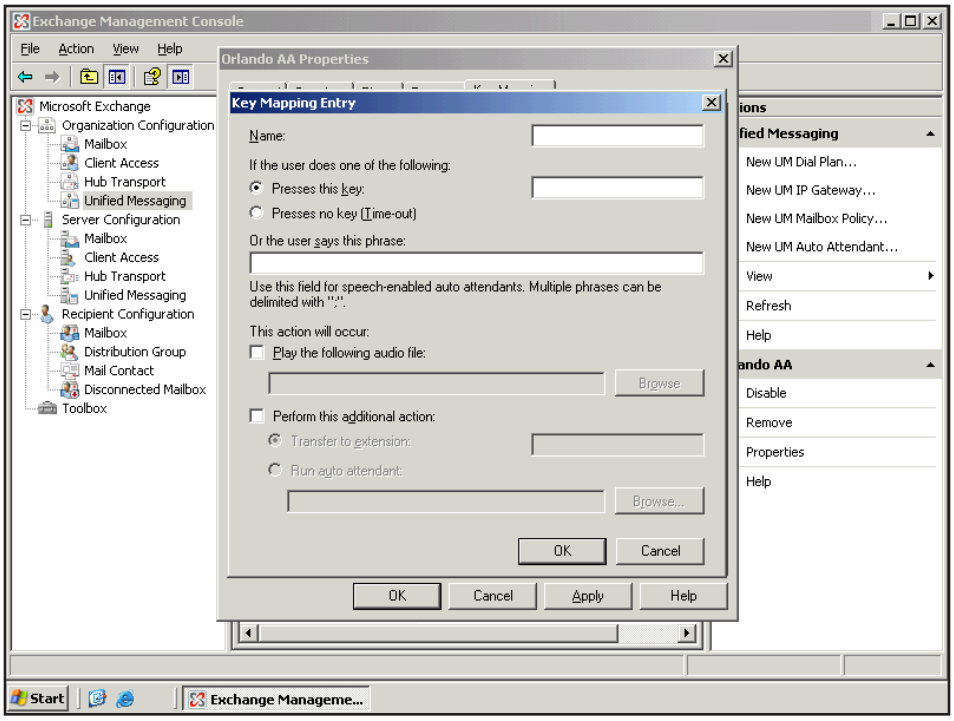


Figure 8: Configure automatic key selection or user voice activation entries.

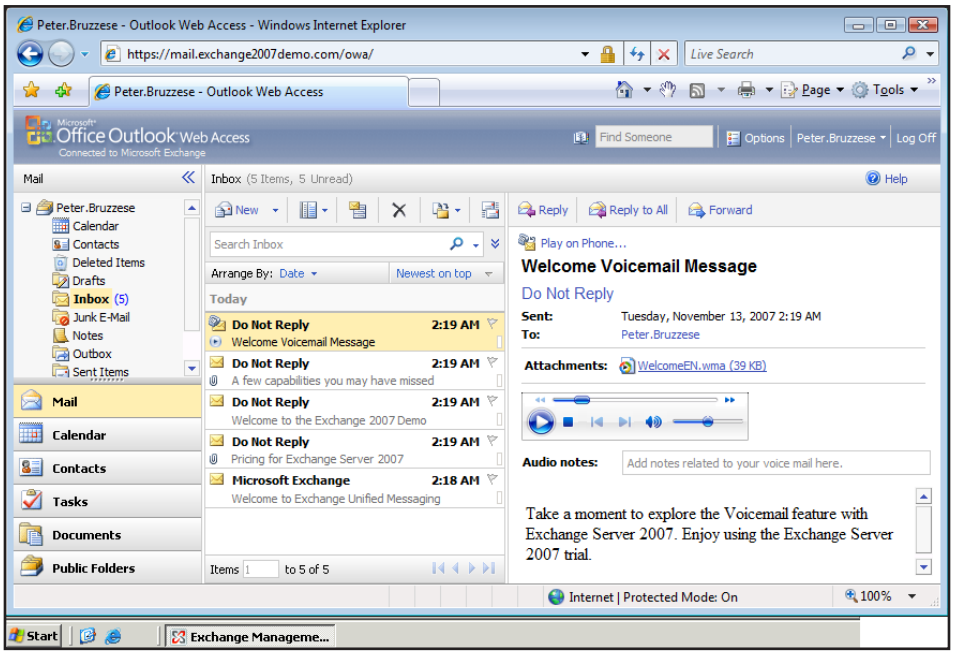


Figure 9: A voice message appearing in your Inbox through OWA.

Enabling UM for Recipients

With telephony equipment in place and UM Server role configured, you can enable UM on the recipients. Use PowerShell with a script or go to the

> To perform the task through PowerShell, and more appropriately, to perform the task through a script on a grouping of users all at once, use the following command: Enable-UMMailbox –Identity <email address here> –UMMailboxPolicy <policy name here>

Recipient Configuration section and right-click a user; you will be presented with the option to *Enable Unified Messaging*. You will then be asked to select the policy that applies to the user, and you need to automatically or manually have the extension put in place for the user. You will also be given user PIN options, such as *Automatically generate PIN to access Outlook Voice Access, Manually specify PIN*, and *Require user to reset PIN after first telephone logon*. Select Enable, then Finish.

> For a demo of how UM works within OWA, register for a free account with Microsoft and test the new features at https://signmeup.exchange2007demo.com/exchange2007demo/Register.aspx.

Once you have UM enabled, users will be able to appreciate all the benefits of UM through their Outlook or OWA clients (see Figure 9) or via any of the other methods that they have at their disposal for accessing email (phone, Communicator, and so forth).

Imagine

Certainly, for network admins, it has been our hope for some time to see a reasonable combination of services, and it looks like Exchange 2007's UM role is going to help move things in the right direction. Familiarity with the Exchange interface ensures that we are already comfortable with the Exchange side, we just need to solidify our UM understanding, pull in our telephony expert, confirm functioning hardware, configure our server, and enable the users. Whew! Are you ready to get started?!

J. Peter Bruzzese is an MCSE (NT,2K,2K3), and MCITP: Enterprise Messaging Administrator, and MCT. His expertise is in messaging through Exchange and Outlook. J.P.B. is the Series Instructor for Exchange 2007 for CBT Nuggets. His latest book is "Tricks of the Vista Masters". He is co-founder of ClipTraining.com, a provider of short, educational screencasts on Exchange, Windows Server, Vista and Office 2007. You can reach Peter at jpb@cliptraining.com.

Copyright Statement