realtimepublishers.com™

The Definitive Guide™ To

Windows Desktop Administration

SCRIPTLOGIC

Bob Kelly

Introduction

By Sean Daily, Series Editor

Welcome to *The Definitive Guide to Windows Desktop Administration*!

The book you are about to read represents an entirely new modality of book publishing and a major first in the publishing industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical IT topics—at no cost to the reader. Although this may sound like a somewhat impossible feat to achieve, it is made possible through the vision and generosity of corporate sponsors such as ScriptLogic, who agree to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these books does not in any way diminish their quality. Without reservation, I can tell you that this book is the equivalent of any similar printed book you might find at your local bookstore (with the notable exception that it won't cost you $30 to $80). In addition to the free nature of the books, this publishing model provides other significant benefits. For example, the electronic nature of this eBook makes events such as chapter updates and additions, or the release of a new edition of the book possible to achieve in a far shorter timeframe than is possible with printed books. Because we publish our titles in "real-time"—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that although it is true that the sponsor's Web site is the exclusive online location of the book, this book is by no means a paid advertisement. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100% editorial control over the content of our titles. However, by hosting this information, ScriptLogic has set itself apart from its competitors by providing real value to its customers and transforming its site into a true technical resource library—not just a place to learn about its company and products. It is my opinion that this system of content delivery is not only of immeasurable value to readers, but represents the future of book publishing.

As series editor, it is my raison d'être to locate and work only with the industry's leading authors and editors, and publish books that help IT personnel, IT managers, and users to do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to feedback@realtimepublishers.com, leaving feedback on our Web site at www.realtimepublishers.com, or calling us at (707) 539-5280.

Thanks for reading, and enjoy!

Sean Daily

Series Editor

Copyright Statement

Chapter 1: Desktop Administration Overview

The latest computers, the fastest network, and the best-rated software can quickly turn from a good investment into a money pit without proper planning and implementation of desktop administration practices. So what is desktop administration? As you'll discover in this book, desktop administration is the methods and technologies used to deploy, configure, maintain, and track client workstations. It encompasses system deployment, user settings and data management, application management, security, support, and asset management. How you handle these critical facets determines the success of your workstation support. From a small office of 10 machines to a worldwide network consisting of tens of thousands of systems, the desktop administrator must address the same issues.

GartnerGroup studies have found that 82 percent of implemented management systems fail to meet user expectations. The reason is that the expectations of the solutions on the market are often simply unrealistic. There are no point-and-click solutions to deploying new systems or applications. There is no way of automatically backing up and managing user settings and data. Access to reports showing just the asset management, software inventory, or usage metrics you want to see isn't going to be displayed on your screen. You won't meet any of these mission critical needs *unless* time is taken to identify, plan, evaluate, test, and implement the right desktop administration solutions for your organization. As if meeting these mission-critical needs isn't motivation enough, let's delve into additional benefits of desktop administration.

✎ Keep in mind that implementing desktop administration solutions don't necessarily require new software purchases. You can take advantage of a number of solutions built-in to Windows and the resource kits. Although, commercially available solutions are often easier to work with and provide more robust feature sets, if your needs are basic, built-in tools and scripts might result in the right solution for you.

The Benefits of Desktop Administration

The potential rewards for implementing sound desktop administration practices can be great. Although we will cover the details of several critical areas of desktop administration throughout this book, the following benefits are common to all of these desktop administration components: a lower total cost of ownership (TCO), increased user productivity, and rapid and accurate system recovery.

Lower Cost of Ownership

The most significant benefit of desktop administration is the potential for reduced TCO. As the following list illustrates, there are many ways to measure the costs that may be saved by following desktop administration best practices.

- Increase support staff efficiency—For example, suppose that a hard drive in accounting just crashed. A user can no longer log on to the system after installing a new screen saver. It could be a very long day for the administrator who must address these kinds of problems—even a long week. However, with the help of an automated deployment solution, a machine could be rebuilt in minutes. In addition, policy and security restrictions could have prevented the user from breaking the workstation in the first place. With the right tools and skills, a support staff may solve (and hopefully prevent) far more problems than they could without them. A quickly solved, or prevented, support issue benefits both the support staff (who can move onto something else) and the end user (who can get back to work).
- Reduce Help desk costs—The ability to visually demonstrate a solution to a user can save the time it takes for you to explain how to perform a task over the phone, or worse, to take a trip to a remote office. A remote control solution provides this ability and is among the most common desktop administration tools implemented. For example, many organizations have implemented Microsoft's Systems Management Server (SMS), which Figure 1.1 shows, as a Help desk tool to make use of its remote control abilities.

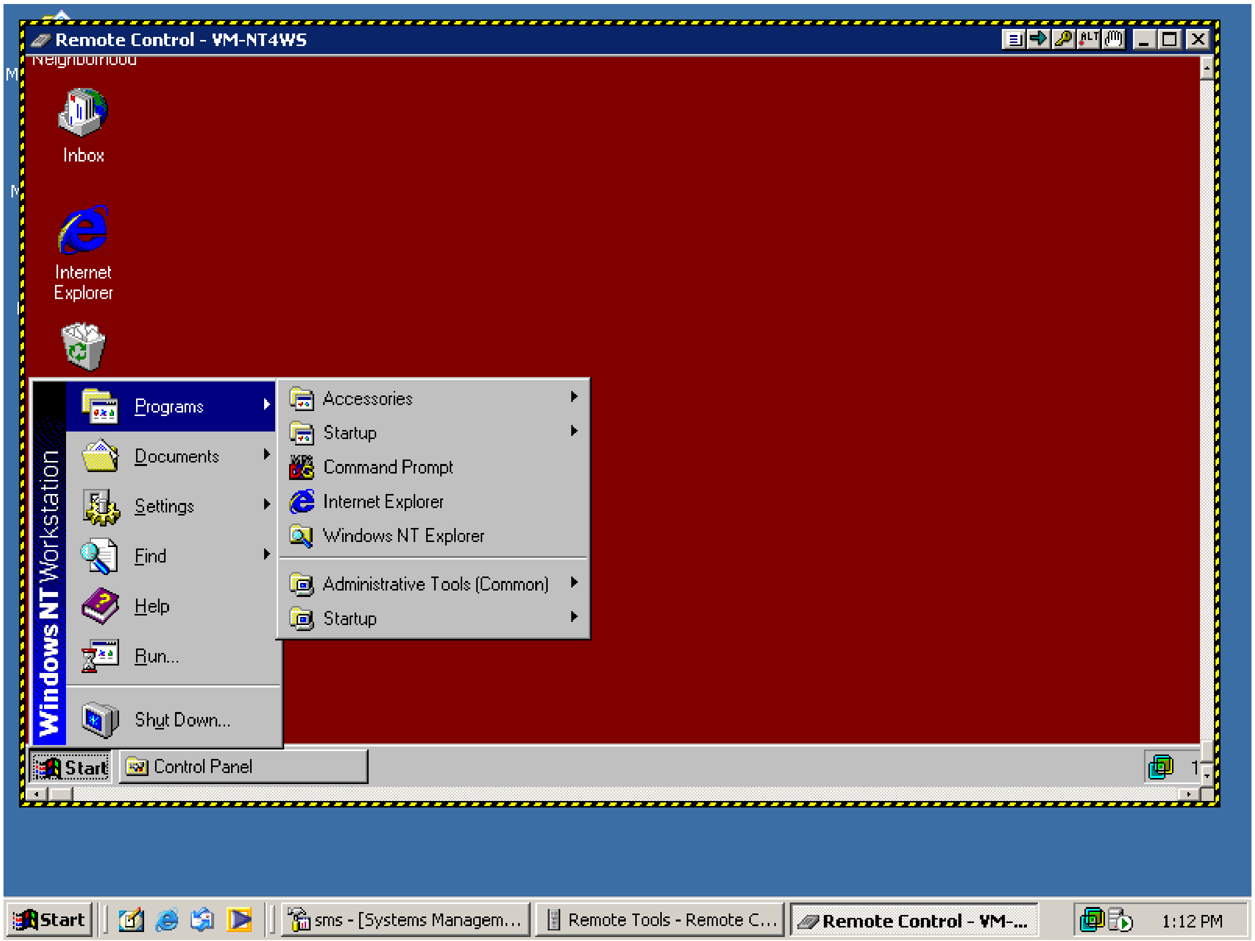


Figure 1.1 SMS Remote Control Session View

- Increase support staff productivity—As you probably know, installing Windows, applications, and software updates across a large base of systems is tedious work. The time taken to visit each system and deal with user inquiries can greatly reduce the amount of work a support staff will be able to accomplish. By implementing desktop administration practices, tools or scripts may be utilized to greatly increase support staff productivity.
- Optimize software license requirements—Many inventory and metering software products provide a means of collecting statistics on application usage. This provides the ability to purchase only the updates that are needed, and to move licenses from those not utilizing them to those that need them rather than simply purchasing more licenses.
- Automate inventory to prevent failed deployments—Which systems fall below your standard configuration? Which systems do not meet the requirements for a software or operating system (OS) upgrade? A detailed hardware inventory can save you from doomed software and OS deployments that result from mistakenly targeting systems that do not meet the minimum requirements.

Increased User Productivity

Whether attempting to handle an issue themselves or waiting while you do it for them, users that aren't doing their work as a result of an IT concern cost the company. Although seemingly insignificant on an individual basis, the following scenarios occur often enough that they can affect a companies' bottom line. Solid desktop administration practices can prevent such situations, thus increasing user productivity.

Having users stand aside while updates and fixes are applied can be a frustrating inconvenience for those users and, more important, cost the company money. Without fail, an unexpected situation occurs and the half hour the user was going to have to wait quickly doubles. Automation of update and fix installations as well as proper testing of the automated installations significantly reduces the likelihood of unexpected problems and ensures that users return to productivity quickly.

In addition, solid desktop administration practices eliminate situations in which users handle installations on their machines. Such situations can result in problems because users don't correctly perform the installation. Rather than taking time away from their "real" work by messing with their systems, users can benefit from desktop administration that efficiently handles IT administrative tasks such as installing updates and fixes.

> Having users handle installations puts an undue demand on them and can have unpredictable results due to the varying degrees of technical aptitude users will possess. This situation will be frustrating to the end user as well as to management because of the inconsistent results and higher support costs.

Unfortunately, users who encounter a problem or are unable to perform a task are very likely to ask the people around them for help before calling the Help desk. Involving the users around them in solving system problems causes even more productivity to be lost. Enforcement of configuration management through a consistent Windows installation (that is, installation of tested software installation packages) and limiting a users' ability to cause problems will reduce the number of problems a user experiences and thus increase productivity.

As a technical individual, you might find it ridiculous that a user would want to hold onto an older, slower system. When faced with the option to replace their system, many users would rather stick with what they have than spend hours or days getting everything back to how they like it. Items such as wallpaper, color selections, and screen savers will be of great concern to many who will spend as much time as it takes—time that could be spent productively—to get their new system to look just like their old system. Thus, a script or tool to backup and migrate user data and settings can save the average user hours.

Finally, you can ensure that business computers perform only business functions through proper configuration and security management. The installation of unauthorized software and use of the games installed with Windows can be controlled through security restrictions and attention to Windows configuration options.

Rapid and Accurate System Recovery

Another benefit of desktop administration, automated and controlled system restores for systems or user data can save lost work and greatly reduce down time when repairing or replacing a computer. This desktop administration practice can be having an automated deployment process in place, having a method for restoring the applications that were there previously, or a combination of the two. The more automated the process, the faster and the less prone to inconsistencies it will be.

A system failure can mean extended down time and loss of data and settings in many environments. However, it does not need to be that way. Regular backups of user data and settings coupled with the speed of drive imaging software can mean that users are back up and running in minutes instead of hours or days. This process may be further engineered to automate the application of a drive image from a network management console. Taking this concept even further, you may hide a copy of the drive image on a local hard drive partition. In this way, the image may be instantly available without need for a lengthy network download.

When a system crashes and needs to be reloaded or replaced, even with days to perform the recovery manually, it might be impossible to get the recovery just right. Although many applications are common to most workstations, without an accurate software inventory, you might be forced to rely on the user to remember what other software existed on the system. With solid desktop management recovery and inventory practices in place, such doesn't have to be the case.

> ☞ Have you spent hours or days fixing a problem that is limited to a single machine? It happens, but if you have an automated system recovery process in place, you shouldn't spend more time on the problem than it would take to reload the system. Especially when an imaging and automated software deployment process has been implemented; in such a case, starting over can prove to be the most effective solution to many hard-to-solve computer problems.

When to Automate

As I stated in the introduction, small offices and worldwide corporations alike will face the same desktop administration issues. However, automation of desktop administration tasks might more clearly benefit larger networks. But what is a large network? When does spending the time and money to engineer an automated process outweigh the time and money spent to handle the task manually? Before we jump into a discussion of the scope of desktop administration, take into account the following considerations to determine whether automation will benefit your desktop administration practices:

- Regularity of administration tasks—If your organization reloads, migrates, or sets up a new computer more than a couple of times per week, the need to automate such a process becomes clearly visible.
- Speed of deployment—When taking into account additional application installation and administrative configurations, the time to install Windows might take as long as 6 hours. Imaging solutions can perform this process easily in less than an hour, with the possibility of reducing the operation to mere minutes.
- Configuration consistency—Even if Windows installations or upgrades occur just a couple of times a month, the benefit of consistency gained through implementation of an automated process has great value. Support issues may be more easily addressed if all systems start with a consistent installation of Windows.
- Lack of on-site technical staff—When there is little support staff available, having a system and application deployment process in place can help those less technical individuals reestablish a known good configuration. With an automated system deployment process is in place, people do not even need to know how to install Windows to get a system back up and running.

> I provided support for a daycare center where children would play learning games on computers. The kids would do all kinds of damage to the computers, mostly by turning them off while they were running. After fixing the computers for about 2 weeks, it became clear that I needed to provide a way for the non-technical people that worked there to fix the systems themselves. With a bootable CD-ROM that could apply an image of the hard drive, they were able to restore any problem systems themselves in just a few minutes. Of course, the kids still went through mice like candy, but troubleshooting Windows and the installed software took up no more of my time. This is just one example of how a desktop administration practice can not only save time and money, but also provide a permanent solution to a real-world problem.

Deployment Automation

Automating the deployment of systems and applications is critical to realizing both speed and consistency. Although speed is the most obvious and sought after benefit, the value of consistency should not be overlooked. You can thoroughly test and document the automated solution, providing invaluable data when addressing problems down the road. When all machines are not set up in the same manner, it is the inconsistencies (however small) that will make any issues that arise both hard to identify and to reproduce. If you cannot reproduce a problem, it becomes increasingly difficult, if not impossible, to identify. An automated deployment method ensures consistency.

Backup Automation

Particularly in situations in which user data and settings are stored locally, an automated backup implementation can save users the frustrations and delays that go with recovering them manually. Even when roaming profiles are in use, corruption of such profiles is not uncommon. An automated backup and recovery mechanism for maintaining a separate copy of the user profile can go a long way in the recovery process.

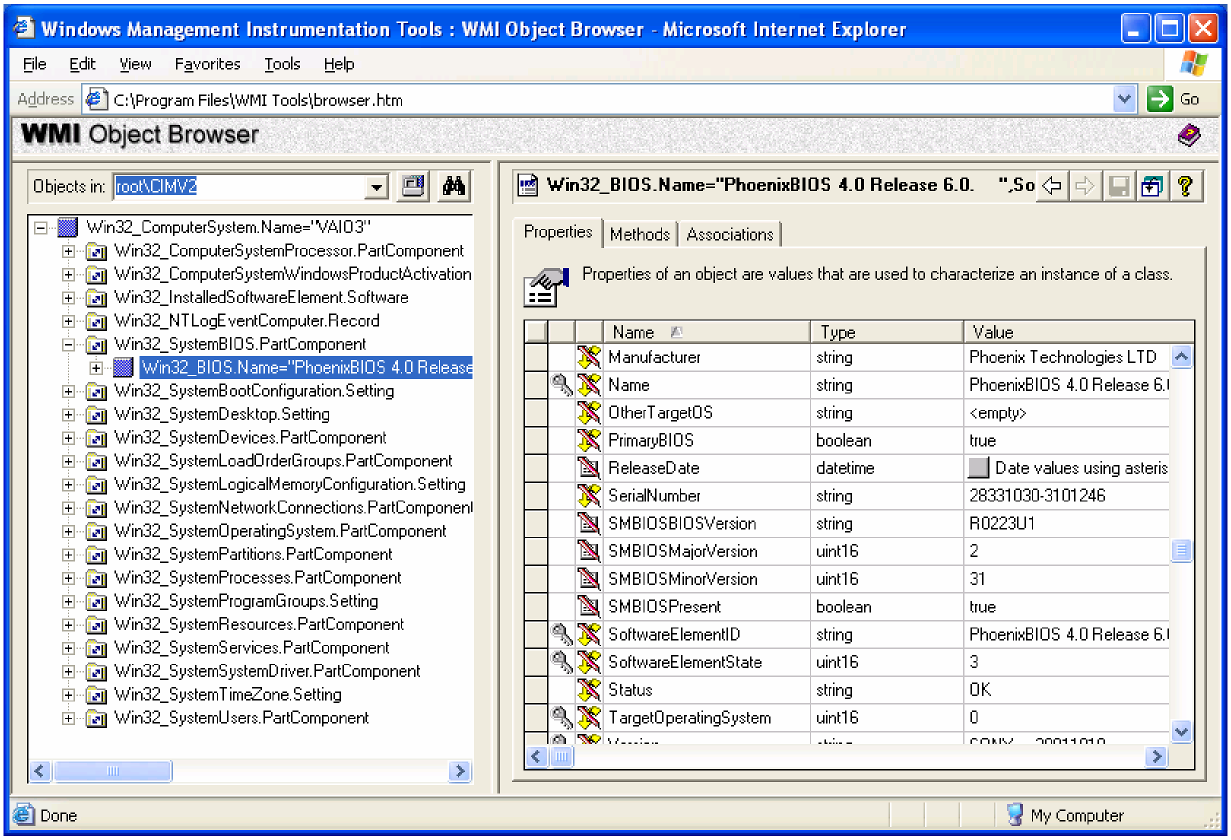
Inventory Automation

The decision to automate inventory tasks is greatly dependant upon how often, how accurate, and how detailed you need such reports. Even for a network of 30 machines, having an accurate picture of what is on the network can be invaluable, yet hard to obtain manually. Managing license requirements, deciding how many upgrades you need to purchase, and being able to report where software is installed are all difficult tasks to accomplish without the right tools. Software and hardware inventory can be detailed, up to date, and readily available with fairly little investment. Knowing what it is you have (hardware and software) is one of the first and most critical steps in performing large-scale updates and deployments.

Windows Management Instrumentation

When it comes to inventory, one of the most helpful new technologies is Windows Management Instrumentation (WMI). Microsoft has included more and more manageability with each release of WMI. Among other things, WMI provides a means of collecting an extensive amount of information about a system.

The WMI Object Browser, which Figure 1.2 shows, is one of the tools available in the WMI Administrative Tools. The WMI Object Browser lets you see all the WMI information available along with the associated values for the specified system (the local system is specified by default). Taking a look around in this tool lets you see just how much information is available to you.



Address: C:\Program Files\WMI Tools\browser.htm

Objects in: root\CIMV2

Win32_ComputerSystem.Name="VAIO3"
- Win32_ComputerSystemProcessor.PartComponent
- Win32_ComputerSystemWindowsProductActivation
- Win32_InstalledSoftwareElement.Software
- Win32_NTLogEventComputer.Record
- Win32_SystemBIOS.PartComponent
  - Win32_BIOS.Name="PhoenixBIOS 4.0 Release
- Win32_SystemBootConfiguration.Setting
- Win32_SystemDesktop.Setting
- Win32_SystemDevices.PartComponent
- Win32_SystemLoadOrderGroups.PartComponent
- Win32_SystemLogicalMemoryConfiguration.Setting
- Win32_SystemNetworkConnections.PartComponent
- Win32_SystemOperatingSystem.PartComponent
- Win32_SystemPartitions.PartComponent
- Win32_SystemProcesses.PartComponent
- Win32_SystemProgramGroups.Setting
- Win32_SystemResources.PartComponent
- Win32_SystemServices.PartComponent
- Win32_SystemSystemDriver.PartComponent
- Win32_SystemTimeZone.Setting
- Win32_SystemUsers.PartComponent

Win32_BIOS.Name="PhoenixBIOS 4.0 Release 6.0. ",So

Properties of an object are values that are used to characterize an instance of a class.

Name	Type	Value
Manufacturer	string	Phoenix Technologies LTD
Name	string	PhoenixBIOS 4.0 Release 6.
OtherTargetOS	string	<empty>
PrimaryBIOS	boolean	true
ReleaseDate	datetime	☐ Date values using asteris
SerialNumber	string	28331030-3101246
SMBIOSBIOSVersion	string	R0223U1
SMBIOSMajorVersion	uint16	2
SMBIOSMinorVersion	uint16	31
SMBIOSPresent	boolean	true
SoftwareElementID	string	PhoenixBIOS 4.0 Release 6.
SoftwareElementState	uint16	3
Status	string	OK
TargetOperatingSystem	uint16	0

Figure 1.2: The WMI Object Browser.

The WMI Administrative Tools are available at http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6430F853-1120-48DB-8CC5-F2ABDC3ED314.

The Scope of Desktop Administration

As you're probably beginning to realize, desktop administration covers just about everything except servers and the network infrastructure. In this book, we will focus on the areas of deployment, management, and control of computers and users. In the following sections, I'll briefly introduce you to the areas of desktop administration that we'll discuss throughout this book as well as reference the chapters in which each topic will be covered in more detail.

System Deployment

The deployment of systems is the first step in desktop administration. A properly configured and well-tested Windows rollout is critical to the health of a system. Any problems with this initial system will need to be identified and corrected for all systems to which the deployment process is applied. Any issues not identified early might be compounded further with the addition of software and other configuration processes.

When deciding whether to perform manual installations, script automated installations (unattended installations), apply drive images, or make use of duplicated hard drives, there are several factors to consider. There are benefits and drawbacks to each of these methods.

- Manual installations—The benefit of manual installation is the ability to deviate from an established process when necessary. In contrast, inadvertently deviating from an established process is one of the primary reasons for automating installations. Manual installation is more costly in terms of time—it takes the administrator's time to perform the installation and takes time away from users' work while they wait.
- Unattended installations—Installation consistency and a reduction of time for the installation are benefits of unattended installations over a manual installation; however, unattended installations can still take more time than the other options. Microsoft provides a method for supporting unattended installations of Windows. There are also third-party tools available to assist in this process.
- Drive imaging—There are a handful of hard drive imaging products on the market that provide a means of distributing an exact copy of a hard drive across many systems. Many implementations provide support for both locally and remotely applying these images to a hard drive. Speed is certainly the primary reason for implementing such a tool on your network. (However, if you have multiple hardware configurations on your network, you might need multiple images.) The ability to include additional software applications in an image is also a key benefit to drive imaging, but taking advantage of this capability can further increase your need for multiple images. The drawbacks to this method include the fact that hardware incompatibilities can also make using a single image for all machines very difficult or even impossible. The more images you have to work with, the more difficult it will be to keep them all up to date and easily accessible. Additionally, in situations in which a network installation is to be performed, bandwidth restrictions may cause significant delays in applying something as large as a drive image. For this reason, it might not be possible to image more than a couple of machines at a time.
- Drive duplication—Hardware solutions exist that provide a means for cloning disks from one to another or from one to many drives at the same time. Speed is the primary benefit of this method. The negative aspects of drive duplication are the same as that of software imaging. In addition, the time spent removing and installing hard drives from systems must also be taken into consideration.

In Chapter 2, we will explore these options as well as the tools available in more detail.

User Profile and Data Management

As I previously mentioned, user profile and data management is another aspect of desktop administration. You can manage user settings and data in many ways. Proper configuration of the default user profile and enforcement of settings via Group Policies can provide great control over a user's experience with applications and the OS. In addition, custom scripts and third-party tools such as ScriptLogic provide an ability to manage user profiles and data without some of the restrictions that exist in Group Policy. The following points highlight the user profile and data management practices that we'll explore:

- Default user profile—Creating and continuing to manage the default user profile can provide users with a customized default base of application and Windows settings.
- Implementing roaming profile size limitations—You can set a quota on the size of a roaming profile to avoid situations in which users create or drag large files into their profiles. Having too large a profile can result in extended logon and logoff events. In addition, this situation increases the likelihood of corruption.
- Folder redirection—Redirecting folders using the new capabilities offered by Windows 2000 (Win2K) and Windows XP can go a long way to keep the size of roaming profiles down. Even if you have not implemented roaming profiles, redirecting folders to a server location can still be very valuable in your efforts to have users store data on the server where it can be backed up.
- Troubleshooting—Simply delete the user's profile—that ought to fix it! We will discuss a more methodical approach than this to troubleshooting, including how to determine whether the profile is the problem and ways to identify where in the profile the problem might exist.

📖 We will discuss these options and related topics in Chapter 3.

Application Management

Suppose you've completed your initial deployment of all systems just as they should be—with all the tools needed by everyone, before long a new version or update would rear its ugly head, which brings us to the next facet of desktop administration—application management. There a number of tools and methods available to avoid the need to visit each machine to perform updates and installations. As the following list points out, you can implement desktop administration practices to meet many of your application management needs:

- New software deployments—In a simplistic view, it is the software that allows many businesses to operate. The timely deployment of a mission-critical application can often be measured in dollars. There will always be newer and better software released, and a streamlined process for implementing these deployments must be carefully considered.
- Deployment of Windows application updates—Microsoft releases new hotfixes, security patches, and service packs every day. Although they might not all address the needs of your network, a great many of them will. The need to quickly implement patches, especially where security is involved, can be critical.
- Metering and usage metrics—Application metering provides the ability to monitor license usage, and in some implementations, even halt the execution of an application when a specified number of concurrent licenses are in use. This capability also produces a means of measuring the usage of applications. In many cases, you can extend this functionality to define restrictions and collect access times for specified Web sites or Web-based applications.
- Keep applications running—Help desk calls may be minimized and user productivity is maximized when the applications supporting their work run reliably. You can take advantage of the self-healing nature of Windows Installer (MSI) installations to avoid failure as a result of file corruption, deletion, or versioning discrepancies.

- Virus management—The presence of a damaging virus on one of your systems can quickly become the presence of a damaging virus on all of your systems. Ensuring that systems are up to date with the latest scan engines and the latest virus definitions can save your network from disaster.

> 🕮 These application management topics will be discussed in Chapter 4.

Desktop Security

In addition to system deployment, user settings management, and application management, desktop administration encompasses desktop security. Effectively managing desktop security can keep users from causing problems through improper configuration or installation of software. Solid desktop administration security practices include taking advantage of third-party logon solutions, file and registry access control, the restriction of user rights, and limited peripheral device access.

- Third-party logon alternatives—Policies and system restrictions that enforce complex passwords might not be enough in your environment. Access cards and biometric devices (for example, fingerprint, speech, and face recognition devices) are available to provide added security to control desktop access.
- File and registry access control—If you want all data stored on a server for ease of backup and recovery, simply directing users to put their data on that server might not be enough. Either intentionally or through ignorance, users might continue to store data on their local systems (despite your direction) unless their ability to do so is hindered through proper security configuration. Further benefits of file and registry access control include the ability to restrict software installation and the prevention of the proliferation of viruses.
- Restriction of user rights—Windows provides two distinct controls when it comes to security: permissions (to access and change the file system and registry) and rights. Rights dictate what a user is allowed (and not allowed) to do on the system. For example, a commonly restricted right is the right to change the system time. Although this limitation might seem an inconvenience to some, the effectiveness of security logs and audit logs can be greatly diminished by allowing users to perform such a change to the system.
- Peripheral device access—One way to take a step toward limiting exposure to viruses and stopping users from installing software is to limit the use of peripheral devices. One often overlooked way around device access restrictions is the potential for new devices to be easily attached to the system. A USB storage device might be automatically recognized by the system, bypassing your efforts to restrict peripheral device access.

> ✎ Enforcement of security restrictions, particularly in the way of limiting or preventing the ability to customize or change a system, can cause some users to become quite upset. Remember (and perhaps remind users in a tactful way) that these are business computers and not personal computers.

📖 I'll discuss desktop security in more detail in Chapter 5.

Desktop Support

Remote control products are one of the most commonly used desktop administration tools. Saving the time it takes to walk, drive, or fly to remote workstations has many obvious benefits. Through use of a remote control product, you may "take over" a user's desktop remotely and correct a problem or demonstrate how to perform an action without having to leave your chair.

The ability to remotely take over the desktop of a remote system is known as remote control. A call on the phone to report a problem can often lead to a manual visit, even if the user is able to articulate his or her problem well. For functions such as software installation and settings management, there are solutions that we will discuss that provide far more efficient and targeted solutions. However, when you need to perform a "one off" action with administrative privileges because you need to show them something (rather than try to explain it), or you simply need to see something with your own eyes, there is no tool more valuable than a remote control utility.

In addition, a remote execution service or tool, even the built-in Windows Task Scheduler, can be a very powerful solution. The ability to remotely execute a command could mean implementing a fix across thousands of machines without a need to visit them. Even when you only need to work with a couple of computers, this capability can save you from multiple trips of varying distances.

Another desktop administration support option is the ability to shut down and turn on computers over the network through Wake on LAN (WoL) support. By taking advantage of this capability, you can save power at night by shutting down all systems on the network and still perform those nightly maintenance tasks by turning on the necessary systems.

Finally, you can avoid problems by using proactive alerts for critical conditions and advise administrators of problems before the calls start coming in. Event notification and alert software can help you head off and even prevent problems.

📖 We'll discuss these and related desktop support topics in Chapter 6.

Scripting Custom Solutions

Windows has provided increasing support for the automation of desktop administration tasks from the command line. Aside from those built-in to Windows, the Windows resource kits are loaded with even more helpful utilities. The Windows Script Host (WSH) provides Windows with support to run Visual Basic Scripting Edition (VBScript) and JScript. This support has resulted in an increased use of these languages by administrators. The simpler yet powerful KiXtart scripting language provided in the Windows resource kit provides easy-to-learn syntax for automating most administrative actions. In addition, you can implement customized scripted solutions, such as those highlighted in the following list, with little to no scripting knowledge by using tools such as ScriptLogic or WinBatch.

- Logon and logoff scripts—When you want to automate a task for a user, logon and logoff scripts are available to trigger such actions. The system executes the logon script automatically during the logon process, and this script can be used to perform user-centric actions mapping network resources such as drives and printers. Want to clear the Recycle Bin or perform a file backup of user profile data? The logoff script provides an excellent opportunity to perform such actions.
- Startup and shutdown scripts—When you want to automate a task for a system, the startup and shutdown scripts are available to trigger such actions. The system executes the startup script automatically during the startup process before the user is presented with the option to log on to the computer. The shutdown script performs its actions during the shutdown of the system. Both perform actions in the security context of the local system account, which allows for the triggering of actions users might not have the permissions to perform (for example, software installations or system level changes).

✎ Though support for logoff, startup, and shutdown scripts has only recently been introduced as a standard feature of Windows (NT and earlier do not provide native support), there are third-party tools that offer similar functionality, including ScriptLogic and ShutdownPlus from WM Software.

- Automation scripts—Migrating user data, creating accounts, checking for files, and most other repetitive tasks provide an excellent opportunity for automation via a custom script.

📖 I'll cover scripting custom solutions in more detail in Chapter 7.

Asset Management

Do you have enough licenses? Do you have too many licenses? You have four copies of a program—where are those copies installed? Are they being used? Keeping a tight grip on asset management can provide you with quick answers to these questions, helping to save money and avoid potentially steep fines for violating license agreements (which are far more than the cost of implementing an asset management solution).

Often, you review software inventory and licensing reports to make sure that enough licenses have been purchased. However, just as costly and sometimes less apparent, is that you have purchased too many licenses. If software is not being used, why pay for it? You could save a substantial amount of money by taking licenses from those who do not need them instead of just continuing to buy more. When it comes time to purchase an upgrade or new version, you can use solid asset management processes to determine how many you need to purchase.

📖 In Chapter 8, we'll explore asset management.

The Politics of Desktop Administration

An oft-overlooked aspect of desktop administration is politics. It can be frustrating to be in a situation in which you cannot make a change you feel is necessary as a result of the political setup in your company. Determining who has ownership and control of the network and its resources can cause problems in some organizations, particularly in situations in which there are remote sites that employ their own administrators. In this section, I'll explain how establishing responsibilities and providing appropriate access can go a long way in minimizing problems between business groups. In addition, you will be better able to implement strong desktop administration practices if you consider how decisions will affect users, how control is delegated, and how you plan to work with users to ensure success.

Making Decisions that Affect Users

Someone or some group of people must have the final say in what can be done on a network. If the ability of users to install software on their systems is causing problems, can you simply take that ability away? If you want to take control of a workstation, do you have to ask first? It is these types of issues that must be identified and documented by each organization.

For example, any limitations imposed on users are very likely to cause complaints. In such situations, it is not normally the role of the administrator to make the decision to implement limitations, but simply to recommend and then enforce those decisions. Having this type of delegation ensures that users have an outlet other than the Help desk to voice non-IT complaints.

If users want administrative control over their workstations, they might come to you, the administrator, for that access. Without an established process in place, it might be difficult to point the user elsewhere for permission to make such a change. This situation has been the downfall of many networks. Without a reason to say no to users' request for administrative control, over time, there can easily become too many individuals with administrative control and configuration management is lost. You can avoid such a situation by establishing how decisions are made that affect users' systems.

☞ Particularly in environments in which users have had unrestricted control of their systems, change in the way of implementing restrictions can mean loud complaints. Be sure to have management completely onboard before implementing this type of change to avoid becoming very unpopular very quickly.

Delegation of Control

As a desktop administrator, what you control and how much control you have will vary greatly depending on your organization. Do remote sites have their own administrators? If yes, what roles are performed onsite? Responsibilities must be agreed upon and then laid out on paper to avoid problems down the road.

Ideally, the same way users are given enough access to their systems to perform their jobs and no more, administrators should have access to perform only the tasks they must. Everyone that requires permission to back up a file, access a certain share, or join a computer to the domain does not necessarily need to be granted membership to the Domain Administrators group. Creating groups for administration roles and providing only what is required to those groups is an effective method for the delegation of administrative controls.

Depending upon the versions of Windows deployed in your organization and the presence of Active Directory (AD), there are several options available for you to define administrative roles. The following sections detail three options: via Windows NT domains, using AD, and through third-party solutions.

NT Domains

Domains represent administrative boundaries at which security policies and settings (such as administrative rights, security policies, and access control lists—ACLs) can be administered separately for each domain. Administrators of a domain have rights to set policies only within their domain (by default). Therefore, different domains in your organization can each be managed independently.

NT 4.0 has a limit to the number of user accounts that a directory can store. Therefore, in large computing environments, it is often necessary to create and manage several domains, each with its own directory of user accounts. Domains are typically organized into two types: master domains (used to store user and group accounts) and resource domains (used to store files, printers, application services, and so on). This multiple-domain computing environment is known as a multi-master domain model, which Figure 1.3 shows. A multi-master domain model means that resource domains need multiple trust relationships with all master domains. These trust relationships allow users in master domains to access resources in resource domains.

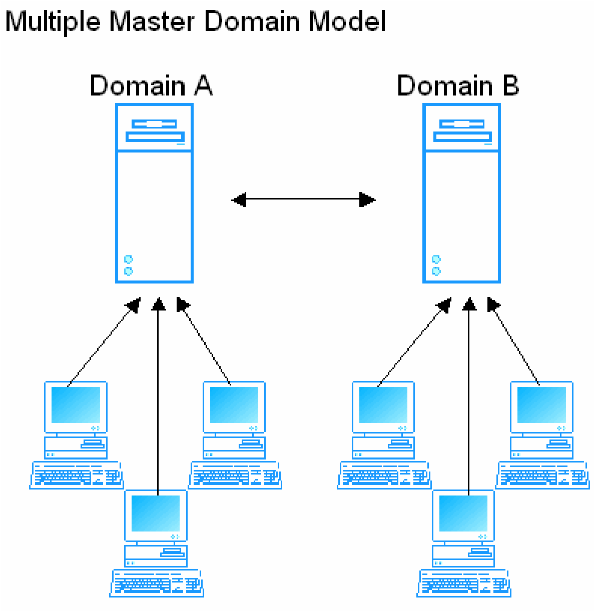


Figure 1.3: Multiple master domain model (trusted domains)

AD

AD replaces the need for multiple domains by providing the ability to store a large capacity of user, group, and computer accounts. With AD, administrators can consolidate all accounts (which formerly had to be stored on master domains) and all resources (which formerly had to be stored on resource domains) across domains into a single domain. To further maintain logical groupings of objects for administrative purposes, you might group computers and users into organizational units (OUs) within the domain.

Third-Party Solutions

Without the benefits of AD, assigning rights to administer some users means assigning rights to administer all users. However, there are tools available, such as Aelita Software's Enterprise Delegation Manager, that provide a more granular structure for defining administrative roles. Though Win2K addressed many of the limitations inherent in delegation of control within an NT environment, the available third-party solutions enable the creation of a Win2K-like directory in an NT network.

📖 For more information about Win2K and AD administration, check out *The Tips and Tricks Guide to Windows 2000 and Active Directory Administration* and *The Definitive Guide to Windows 2000 Administration* (Realtimepublishers.com), links to which can be found at http://www.realtimepublishers.com.

Working with Users

When things go wrong, there is a tendency for users to point to the unknown as the cause. The magic you perform with your desktop administration tools may be seen as the malefactor behind errors, latency, and just about anything else that is difficult for a user to explain. Simple practices such as keeping users informed and providing explanations will go a long way to ensuring successful desktop administration as well as office harmony.

✎ Perhaps it goes without saying, but even more important than education is that you perform the planning and testing necessary to minimize the potential for causing problems for users. A single failure can brand the desktop administration team with a bad reputation that might be difficult to recover from.

When a deployment is planned, notify users beforehand, then advise them of your success or any problems you encountered that might affect them. It is a common mistake to keep users out of the loop. Doing so ultimately means that they end up hearing about the occasional failure and not the successes of your work. Some administrators worry that problems will be blamed on management tools and remote updates if the users are informed of such installations. However, it is very likely problems will be blamed on desktop administrators even when operations are not being performed. Build a positive reputation by educating users and taking credit for your successes.

☞ A weekly or monthly newsletter may be overkill; however, normal announcements about what is happening as it happens can open communication with users. Consider setting up a simple Web page that users can visit to discover what's going on and what is scheduled for the near future.

In particular, a capability such as remote control can be very intimidating to users. Does this mean that someone is watching everything I do? Decide what to tell users about your tools, but avoid saying nothing at all. Put some thought into this process—for example, you might want to prevent paranoia by explaining tools but ensure that you don't eliminate the slight fear of software usage reporting (metering)! It might be a good thing that users worry about being discovered playing Solitaire for half of the day.

Factors in Effective Desktop Administration

Company politics aside, your ability to implement effective desktop administration practices might be limited for several reasons. You can address some factors, such as standardization, but others, such as geographic dispersion, are simply something you must learn to work with. In the following section, we'll explore the possible challenges you face as a desktop administrator.

Standardization

Whether your organization lacks standardization is the number one factor when measuring the complexity involved in desktop administration. Such is particularly true when dealing with the deployment of applications and updates. Varying OSs and hardware can multiply the effort required to engineer a deployment.

☞ Almost without exception, the more you buy the less it will cost. Choosing one software package that satisfies your users will be far less costly than making several smaller purchases from different vendors.

The more versions of Windows on your network, the more difficult certain desktop administration tasks will become. Particularly in the area of application deployment, you will need to develop, test, and manage the distribution of packages separately for each OS on the network. Measuring the minimum requirements of software will also require much more attention in environments in which multiple OS versions and service pack levels must be considered.

Chances are that most every workstation in an organization requires largely the same applications and utilities on each. By establishing a common baseline from which to start all workstations, you can more easily realize an increase in the consistency between systems. Whether through documentation, unattended installation, or imaging, start all users out with an identical common workstation load and then install additional software on an "as needed" basis.

☞ With a common software baseline established, Help desk personnel and users alike may become proficient with the same tools. Users are better able to assist one another and training programs may be instituted that benefit the largest possible number of users.

Determining the minimum requirements for versions of Windows and its applications may not be too large of an issue for many organizations. However, if a drive cloning (hardware- or software-based) method of system deployment is in place, consistency in the hardware on the network can greatly reduce testing requirements and the number of images required. With NT and earlier systems, even a different model network card could mean the creation of a new image. The plug-and-play (PnP) capabilities of newer versions of Windows provide less of an issue with inconsistent hardware, but the problem has not gone away. Even when creating an image with Windows XP, the reference and destination computers must have compatible Hardware Abstraction Layers (HALs).

🕮 We'll discuss standardization in more detail in Chapter 2.

☞ When purchasing hardware, ask vendors about their update cycles. In some cases, the same model of a computer is shipped with slightly different hardware configurations. Even a slight change has the potential to cause you considerable troubles with imaging or accounting for available device drivers. Some vendors address this potential problem by offering computers aimed toward businesses. For example Dell offers the OptiPlex series for business and Dimension series for home use. Hewlett-Packard (which acquired Compaq) offers an Evo series for business use and a Presario series for home use. Each vendor provides documented assurances that hardware configurations will remain consistent in a given shipment of systems or for a specified number of months.

Geographic Dispersion

The ability to walk down the hall and put your hands on a system is easily taken for granted unless you must account for a single remote site (often with decreased bandwidth and stability). Remote sites can be the cause of much consideration and engineering. Often separate desktop administration policies and procedures are put in place to handle these environments, sometimes resulting in a reduction or loss of configuration management as well as an increase in the time spent planning and supporting these remote systems.

In Figure 1.4, we see a few desktop administration problems to overcome. First the wide area network (WAN) connection (the remote Tampa site) might be slow or costly to utilize, and second, the remote site does not have a local server. This scenario is not unusual for sites with few workstations and little to no onsite desktop administrative support. Virtually all network-intensive services may be subject to reduced network speeds. Windows installation, software deployment, profile management, and other desktop administrative tasks will often need to be altered for such remote sites.

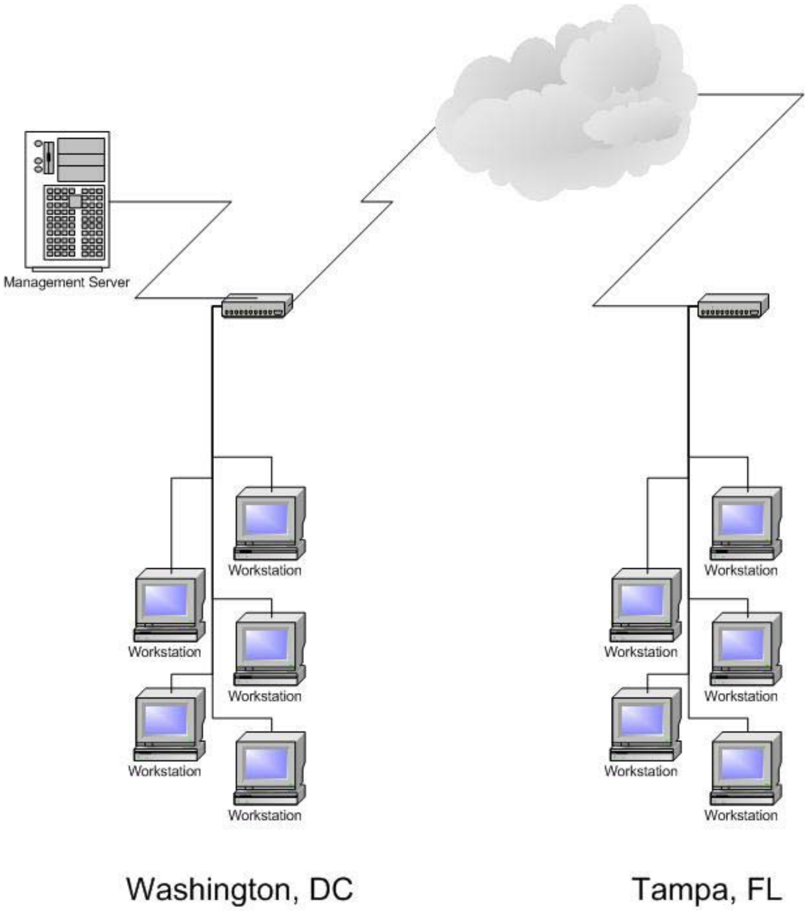


Figure 1.4: Geographic dispersion and connectivity considerations are elements that can add significant levels of complexity to desktop administration.

Dedicated Staffing

The larger the network, the more likely a dedicated desktop administration staff is present. A staff able to focus and build proficiencies will clearly have an increased opportunity to succeed. In situations in which desktop administration is one of many tasks you must perform, desktop administration operations might take longer to perform and risk the possibility of being forgotten completely.

Budget

The first limitation to come to mind for management, and thus for the desktop administrator, is usually budget. One way to ensure that your desktop administration tool purchase request is approved is by drafting a business case for the request (in contrast to an IT case—usually that such tools will make your life much easier). If you can demonstrate that the $5000 management software package that you want to implement will save many times that amount in just the first year, it is far less likely your request will be denied. If your purchase request for administration tools is considered too great a cost to spend and you are left to spend weeks or months developing the same capability with free tools and scripts, consider the situation a windfall—many careers have been built on the development of customized solutions to desktop administration issues.

Connectivity

As I mentioned in the geographic dispersion discussion, remote and disconnected clients significantly increase complexity when it comes to desktop administration. Deploying new and updated software and enforcing software-metering policies are a challenge when working with notebook computers that dial up only a couple of times a week. Rest assured, there are products that tackle these and most every problem you will encounter—including the pesky problem of connectivity.

Process

On one hand, if your organization doesn't have a process for implementing changes, problems such as undocumented and untested software is installed or approved and needed software isn't implemented. On the other hand, having too detailed and lengthy a process can slow (sometimes indefinitely) the ability to effect change on a network. This need for a balanced process management plan is sometimes overlooked as a factor in effective desktop administration. You need a process, such as the one that Figure 1.5 illustrates, that ensures that ad hoc changes as well as months of meetings, boards, and reviews are avoided.

Obviously, this situation is yet another in which the size of a network takes a significant role in a sensible approach. If a change affects very critical systems or a very large number of systems, a more detailed and rigorous process for test and review becomes a necessity.

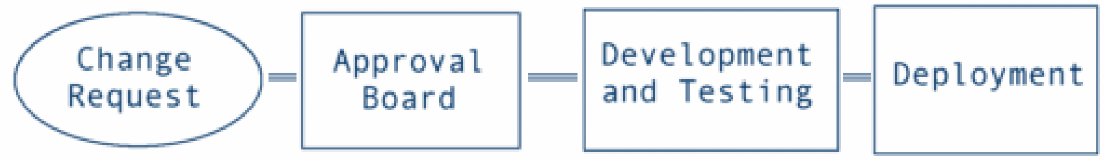


Figure 1.5: Example of a simplified change and deployment process.

Security

Security is also a factor in how effectively you can implement desktop administration practices. Some organizations lock down their desktops so that users can do no more than run their required software. Others provide everyone with local administrative access to the system to avoid errors or warnings when even the most basic, built-in security restrictions are violated. What a logon script can accomplish is an indicator of how security can affect your ability to administer the network. With default security implemented, a logon script can do very little outside automating user settings and environment. Changes to the machine must usually be handled via an administrative service account or the local system account. In this book, we will later discuss many of the utilities and third-party solutions available (such as SMS and ScriptLogic) to address the security limitations inherent of the logon script, which run under the security context of the local user.

For those that work in a secure environment, it might be hard to imagine that there are networks in which users have full control of their systems. However, it is not uncommon for users to be granted administrative access to their systems so that they may handle administrative functions themselves. Obviously, there is a significant potential for damage to the system, both by users who do not know what they are doing and users who *think* they know what they are doing. However, despite the potential for problems, users who *do* know what they are doing can reduce Help desk calls and prevent time wasted waiting for support staff to make a change on the user's behalf.

In contrast, some networks are locked down beyond the default settings to protect users from themselves and to maintain control of system configuration and content to the greatest degree possible. Keeping users from being able to modify certain settings can account for a direct decrease in support costs. Although this security method might sound favorable, there is a definite downside to this approach. Significant testing must be performed on new applications and updates to ensure that they are able to operate in the locked down environment. Deployment capabilities may also be hindered and will result in an increased complexity in many areas of desktop administration.

Desktop Administration in Action

Although these factors are very real, perhaps a few examples of how you'll actually use desktop administration would be helpful. The following situations provide a more situational overview of problems you might face and how desktop administration tools and practices will help you overcome them.

Help Desk Calls

One of the most often-employed desktop administration solutions is the Help desk. Whether you are implementing tools to help engineer solutions for a Help desk or you are the Help desk, the problems you face can be broken down into just a couple of categories.

Probably the most common Help desk call is for help with a specific application. Not necessarily because there is a problem, but because the user simply does not know how to perform the action he or she requires. The frequency of this type of problem will vary depending on the level of technical knowledge of your user base, but rest assured that every administrator has at least a handful of individuals that just like to ask questions. For such individuals, a remote control tool can save you considerable time. Show the user how to accomplish the required task while talking them through it on the phone to avoid the trip to the user's desk and the inevitable other distractions that come with that trip.

Requests for software installations and upgrades are yet another common type of Help desk call. The ability to remotely satisfy this request using a documented and tested installation package is invaluable. With such a solution in place, the support call can be reduced from a half hour or longer to just a couple of minutes.

Handling New Systems

As your organization expands and grows, you will encounter a constant need for the deployment of new systems. Whether you have a staging area in which such systems are configured beforehand or the new computer is already at the user's desk, new system rollouts can be a lengthy endeavor.

Requests to add a new machine or move an existing one can be among the most time-consuming desktop administration tasks if your organization lacks an automated process. Having a new employee wait while a fresh machine is built from the ground up would be the worst way to handle such a situation. Here, the new employee gets a bad impression of the way things work and the administrator spends hours or even a full day away from his or her other tasks. An automated process for setting up a machine and applying required software goes a very long way to reducing the impact of this demanding administrative chore.

Outsourcing Desktop Administration

There are a growing number of management service providers (MSPs) that provide desktop administration services as a monthly service. With the capabilities of remotely managing and supporting systems, it is easy to see how such operations could be handled as an off-site service. The more complex the operation, the more cost-efficient it becomes to outsource such an operation.

There are positive and negative aspects of this approach. Regardless of whether you outsource or internally handle desktop administration, it is important to understand the best practices and methods available so that you can be sure that your organization's desktop administration practices (even if they're outsourced) make sense for your company.

The Benefits of Outsourcing

The following points highlight the considerations for outsourcing desktop administration.

- Reduce implementation risks—There is risk in taking on the implementation of remote and automated solutions. Many such systems take a very long time to plan and implement, others might fail to perform the implementation altogether. An MSP focuses on such deployments on a regular basis, which translates into an ability to perform implementations of these systems with a much higher degree of success.
- Gain access to subject matter experts—A company that focuses on desktop administration issues and performs such tasks for multiple networks will have a proficiency in this area that would be difficult to develop in-house.
- Known costs—Desktop administration is an afterthought for some organizations that, in turn, apply little resources to its success. This shortcoming often leads to failures, which increase the costs associated with desktop administration. With a service approach, the costs and services are laid out and are therefore easier to plan a budget around.
- Process integration speed—Planning, implementing, and administering desktop administration tools can be challenging and time-consuming. A company that does so for multiple clients, such as an MSP, will be considerably faster implementing desktop administration tools and processes than a group of individuals who are doing so for the first time.
- Focus on core competencies—In the IT field, a certain specialization of skills can be a necessity. With technology changing on a constant basis, it is easier for many companies to outsource some part of their IT operation to a firm with expertise, particularly in an area as challenging as remote management.

The Drawbacks of Outsourcing

If the benefits listed sound too good to be true, that might very well be the case. Like every other decision, you must consider the drawbacks of outsourcing.

- Level of control—By out sourcing desktop administration operations, you inevitably loose some control of the network. To meet certain service level agreements (SLAs), policies may be required that restrict your ability to perform these tasks.
- Security—Though you would never take on such a service without reasonable assurances regarding security, there is still a controlled security hole being opened when you outsource administration. Desktop administration services may involve remote control, imaging, and application deployment—all of which are very damaging in the hands of the wrong people.
- Staffing conflicts—If you are reading this book, there is a good chance that your job could be threatened by outsourcing desktop administrative tasks. It will be critical that the existing IT staff be either moved on to more advanced work or that the outsourcing service work with the existing IT staff as a secondary authority. Placing powerful day-to-day operations in the hands of an external company might cause friction between internal and external IT staff if not handled in a very delicate manner.

☞ For a directory of companies that provides these services visit http://www.msplocator.com.

Summary

In this chapter, we covered some of the basic concepts behind desktop administration. We discussed the many benefits of implementing sound desktop administration practices including a reduced TCO, an increase in user productivity and the ability to realize rapid and accurate system recovery. In addition, we touched on whether the size of your company justifies automating desktop administration practices. As we explored, desktop administration encompasses a large scope of tools, tasks, and practices, and I let you know which topics will be covered in future chapters. I provided information about the need to establish a process to determine how decisions are made that affect users' systems, how control is delegated, and how users will be informed and educated about desktop administration activities. Finally, we considered the factors in effective desktop administration and whether avoiding these potential pitfalls through outsourcing makes sense for your organization.

In the chapters that follow, we'll delve deeper into the detailed aspects of desktop administration, and discuss the technologies and tools available to meet these mission-critical needs. Specifically, in Chapter 2, we'll discover system deployment considerations, options, and tools.