

# *The Definitive Guide to*

# Windows 2000 and Exchange Migration

## **Chapter I**

Written by Archie Reed and Darren Mar-Elia  
Series Editor: Sean Daily

*Brought to you by:*

---



realtimepublishers.com<sup>™</sup>

# Introduction to Windows 2000 and Exchange 2000

Welcome to *The Definitive Guide to Windows 2000 and Exchange 2000 Migration*, the most concise and practical guide available on the topics of Windows 2000 (Win2K) and Exchange 2000 (E2K) migration. Because this is a guide to migration from existing platforms, I will assume that you have a reasonable level of knowledge around Windows NT 4.0 and Exchange 5.x throughout this book.

First, we need to define what we mean when we talk about the term “migration.” In some cases, people will be looking at upgrading existing systems and environments in-place. This will be using the same hardware, and running the install/upgrade option that Microsoft has built into the product. We will refer to this option in our discussion; however, most of this book is dedicated to reviewing your existing environment and deciding where to move. Through a true migration to Win2K and E2K, you will need to install new systems to assist in that move. Again, this does not preclude in-place upgrades, but there is a distinction. Another important aspect is that we will not really deal with migrations from other operating systems or other mail systems. Instead, this book will focus on how to move your existing NT 4.0 and Exchange 5.x installation to Win2K and E2K.

You should be aware that Microsoft has put a great deal of effort into providing documentation and case studies on Win2K and E2K migration. You can find an excellent set of guides at: <http://www.microsoft.com/windows2000/library/planning/default.asp>. The “Windows 2000 Deployment Planning Guide” is approximately 500 pages and the “Active Directory Branch Office Planning Guide” is approximately 250 pages. While Microsoft provides one perspective on the challenges of migration, I think you will find this book provides some unique and succinct views on the real-world issues you will face.

If your environment is anything more than a few machines in a single domain, it is likely you will need to make use of some third-party products to get around some of the more esoteric issues that Microsoft does not deal with specifically. Even internally, it is acknowledged by Microsoft that they had to use third-party tools to perform their own migration. Throughout this book, we will review your options in using the base tools, or making use of third-party solutions to get the job done, and the reasons for each choice.

This book is divided into two primary parts. Part I, Chapters 2 through 5, deals with Windows 2000 and covers the fundamentals you will need to know in order to have a successful migration from Windows NT 4.0. Part I is also essential reading to ensure a successful Exchange migration from 5.5 to 2000. Part II, Chapters 6 through 8, deals with the migration details from Exchange 5.5 environments to Exchange 2000.

Throughout this book we use a number of abbreviations to refer to various items, and as such our glossary, which is a separate document, will be important to you. Although we will refer to the full name or description at the first use of a term, the glossary, which appears at the end of the appendices, will grow over time. Take the time to reference the glossary if you see something you do not immediately recognize.

While maintaining a similar, but improved, look and feel of Windows NT, Microsoft has managed to hide an incredible amount of new technology under the covers of their 2000 product set. We will take quick look at these new technologies along with the changes to existing NT technologies that have been made. Let's meet the Windows 2000 product family.

## Meet the Windows 2000 Product Family

After more than six years in development using hundreds of engineers and significant customer involvement, Microsoft delivered four versions of the Windows 2000 product, designed to meet varying levels of functionality, scalability, resilience, and interoperability requirements.

Although the product line makes abundant use of common components, there are several key differences between each version.

While Win2K will work on many hardware platforms, there is the Hardware Compatibility List (HCL) which you should refer to in order to ensure Microsoft can fully support your installation. The HCL is available at <http://www.microsoft.com/hcl>. That said, new systems from major vendors do not immediately appear on the HCL due to the long testing process that is undertaken by Microsoft to certify hardware. The HCL is not the ultimate guide, but a good one.

Another important reference for your upgrade is the more general Hardware and Software Compatibility page at <http://www.microsoft.com/windows2000/upgrade/compat>

Microsoft also provides a set of base platform guidelines for upgrading or migrating to Win2K. You will be able to have an operational system with the minimal platforms. However, you should be aware that to achieve reasonable (usable) performance from the systems once you start running more than one application, you will want to enhance the base platform for your deployment. Items for consideration begin with memory, followed almost equally by the disk subsystem and the processor(s), depending on the application, and finally the graphics card(s). As such, we provide an update on the system requirements provided by Microsoft in the following introduction to the versions of Win2K.

Table 1 shows the various versions of Win2K you can use and an update to the base platform that Microsoft supplies.

Version	Description	Base Platform
Windows 2000 Professional	Windows 2000 Professional is intended to be installed on a desktop, workstation, or laptop of individual workers. Although it can operate independent of a complete Win2K or NT domain environment, it also provides a point platform for many functions that only become available when it is in such an environment. Examples are advanced security and remote installation. More importantly, Win2K Professional has greatly improved hardware support from NT 4.0, and Microsoft is claiming a 300-percent increase in the amount of supported hardware, as well as improved hibernation and plug-and-play support.	266 MHz or higher Pentium II compatible CPU. 128 MB RAM recommended minimum; more memory generally improves responsiveness (4 GB of RAM maximum) 2 GB hard disk with a minimum of 650 MB of free space. (Additional free hard disk space is required if you are installing

	hibernation and plug-and-play support.	over a network.) Windows 2000 Professional supports single and dual CPU systems.
Windows 2000 Server	As with all server components, Windows 2000 Server is designed to support the traditional file and print application services; however, it has also added a raft of new functionality. Along with Web services through Internet Information Server (IIS) 5.0, Win2K Server also introduces the widely touted Active Directory, which we will look at shortly. IIS is now a core part of the OS, as opposed to being part of the "NT 4.0 Option Pack." Microsoft has also increased symmetric multiprocessing (SMP) capabilities from 2 to 4-way SMP.	300 MHz or higher Pentium II compatible CPU. 256 MB of RAM recommended minimum. (128 MB minimum supported; 4 GB maximum.) 2 GB hard disk with a minimum of 1 GB of free space. (Additional free hard disk space is required if you are installing over a network.) Windows 2000 Server supports up to four CPUs on one machine.
Windows 2000 Advanced Server	Advanced Server doubles the SMP and memory capabilities of server to 8-way SMP and 8 GB of memory. Advanced Server adds a clustering capability including network load balancing and two-node clustering.	Same as for Server, plus Windows 2000 Advanced Server higher CPU counts and memory.
Windows 2000 Datacenter Server	Windows 2000 Datacenter Server is designed to support 32-way SMP and 64 GB of memory. Datacenter server also provides 4-way clustering. It is collaboration between selected hardware vendors and Microsoft, and is the most scalable OS Microsoft has to offer. Although we won't spend much time looking at Datacenter in this book, most of what we discuss is easily applicable to it if you choose to use it.	Datacenter server, as a highly tuned version of Win2K, and as a result of the agreements Microsoft has with specific hardware vendors, the actual minimum requirements for Datacenter are usually defined by the hardware manufacturer or OEM, as agreed with Microsoft.

**Table 1.1:Version of Windows 2000**

Microsoft is also releasing updates to the BackOffice and *Small Business Server (SBS)* BackOffice packages, which will include the standard set of applications such as Exchange 2000, SQL Server 2000, and Internet Security and Acceleration Server (ISA). This replaces Proxy Server, Host Integration Server (HIS) which replaces SNA Server, and Systems Management Server 2.0. Although we won't be dealing with these bundled packages that Microsoft provides, most of the discussions in this book will still apply.

## Benefits of Migrating to Windows 2000

Now that we have an idea about the versions of Win2K, what are the reasons to migrate to it? At a high level, the primary reasons are:

- Active Directory
- Stability
- Scalability
- Security Improvements
- Manageability
- Plug and Play Support
- Connectivity Benefits


### **Active Directory**

One of the most talked about additions to Windows 2000 is *Active Directory (AD)*.

Sitting at the center of almost everything Win2K, AD is perhaps the most significant change to the core of Windows technology since its inception. While AD replaces the NT 4.0 SAM database, thereby solving a number of problems with the NT 4.0 SAM, it also serves a much larger role in the management of Windows environments. Apart from finally having a worthy competitor to Novell's NDS, AD allows for:

- Improved Security
- Delegated Administration
- LDAP accessible network data
- Facilitation of Directory-Enabled Applications (such as E2K)
- Vastly increased scalability
- Better interoperability

The importance of AD is not so much to replace the SAM database, but moreover, to act as the central repository for all applications from the local machine to the wide area network environments. Perhaps the best way to think of AD (if you are not that familiar with directories) is as a super-charged registry, with a hierarchy, advanced security, and multiple data types that can be distributed and replicated across Win2K servers. The intent is that applications can use the directory for all sorts of configuration data storage instead of having to create their own configuration files, and deal with all the management liabilities that come with it. Take note that even given such a description, there are many forms of data that do not belong in a directory, and you should be aware of what a directory such as AD is used for before assuming that everything should go into it. If you are not familiar with directory services, related standards, and their purposes, you should make every effort to do so before planning your migration.

 It would be difficult in a book such as this to provide a detailed tutorial on directory services. We recommend that you also read ***Implementing Directory Services*** by **Archie Reed** (McGraw-Hill; ISBN: 007134408X). It provides a comprehensive overview of directory services, their role in system architecture, and details about how to deploy them. This is a key to understanding the significance of AD, and importantly, the technical details and standards behind it.

AD provides the introduction of *Microsoft's Active Directory Service Interfaces (ADSI)*. ADSI is an *Application Programming Interface (API)* for accessing various types of directory information, such as LDAP, NT 4.0, Novell NDS, and AD in particular. ADSI is exploitable from Windows Scripting Host as easily as it is from Visual Basic or C/C++. Because AD is at the core of Win2K management, this means that administrators can use scripting to create simple or advanced customized management tools as required. The corollary is that it will require administrators to review and update existing scripts and tools to support this new mechanism for managing Windows. Because ADSI allows you to get to the core of Win2K through AD, it requires very careful planning and use.

AD provides a hierarchical, flexible, and scalable data model for management of your network environment. AD changes the way you need to think about administration.

Before we begin, we need to define some terminology, some of which is AD specific. I'll be brief as there is certainly enough literature out there on these topics. Figure 1.1 shows a logical environment in which this terminology exists.

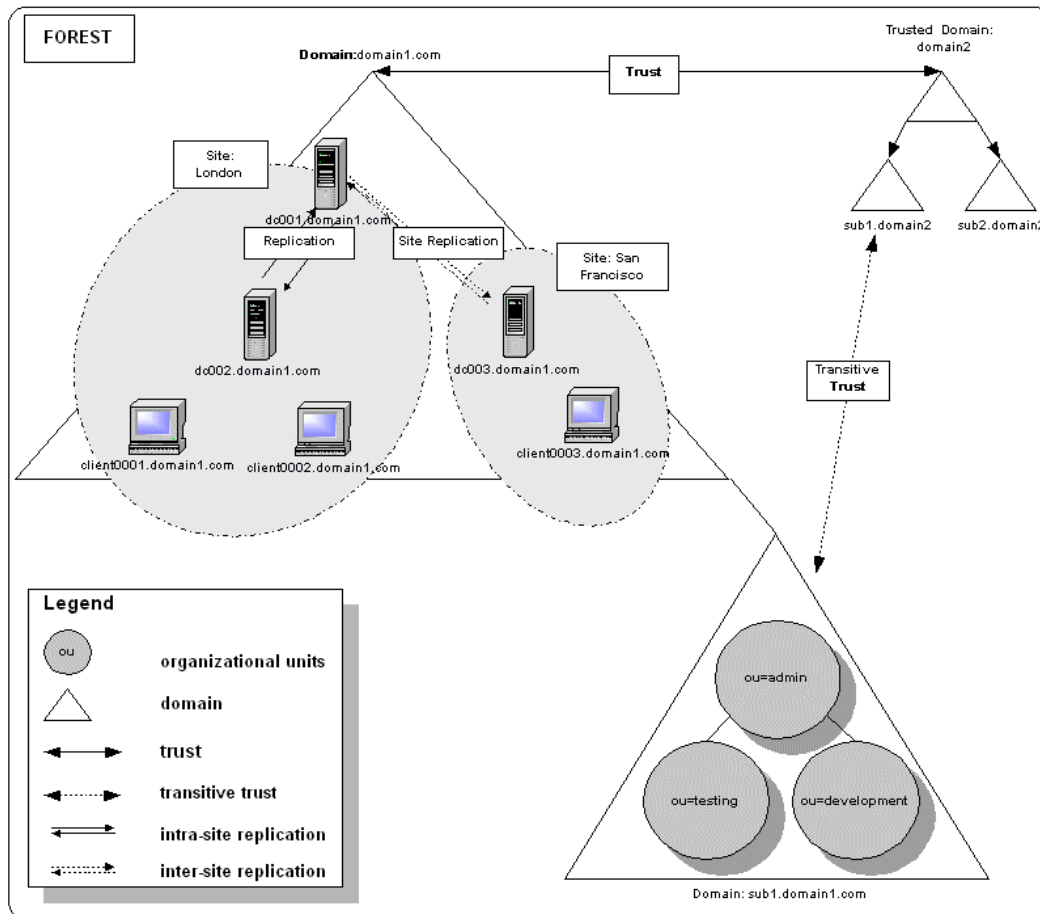


Figure 1.1: Logical AD environment

- Domains:** In AD, the term “domains” has two meanings that, while similar in concept, are distinct from the traditional NT definition of the word in the following ways. First is the traditional *Domain Name Server (DNS)* grouping of hosts. Win2K supports DNS (and *Dynamic DNS* which we will look at in Chapter 2), as well as using DNS for its namespace model. Second, *like object containers*, is the logical grouping of objects within the directory. In fact, within AD, a domain is also an object container. The importance of the two is that both hosts (machines) and accounts (users, groups) exist within a common boundary, allowing for ease of management.

- **Tree:** A tree is used to describe the hierarchal grouping of containers, very similar to a DOS file system. The bottom of the tree is called the *root*, and is commonly drawn with the root level at the top of the picture. The “branches” of the tree, known as *sub-containers*, spread out from the root until they hit a single object known as a “leaf node.” When applied to the domain namespace, we have a contiguous series of DNS names such as *company.com* and *northwest.company.com*.
- **Trusts:** A trust is an agreement between levels in a tree that is established to enable sharing of resources in a secure manner.
- **Forests:** A forest is a grouping of trees, each able to maintain its own schema and through the use of trusts at the root of each tree, are still able to share resources.
- **Objects:** An object resides within the AD tree. Objects can be built from multiple object classes that define the various attributes (name-value pairs). When added together, they describe the object itself. Objects must, at a minimum, be named, and the object’s *distinguished name* (DN) describes an object’s location exactly within the tree. Examples of objects are users, computers, groups, or even organizational units.
- **Container objects:** Container objects are important in a tree context, since they are parents to other objects (that is, they can contain other objects or container objects). The most common container within AD is the “*organizational unit*” (OU), which can be used to manage objects in a logical grouping. Because security policies are usually applied to an object container and can be inherited by sub-containers within the tree, the object hierarchy is just as important to your design as is your overall domain hierarchy.
- **Sites:** Sites within the Win2K context are used to define a relationship of hosts and domain controllers to areas of high bandwidth or connectivity. Domains can exist across more than one site at a time as there may be multiple sites per domain.

Perhaps contrary to logic, AD is a centrally managed, distributed data solution. As a result, careful consideration needs to be given to how you will manage your policies and whether you will need to create separate trees, forests, domains, or just object containers (or OUs) to suitably manage your environment. Domains are in place to allow you to define replication agreements and trusts. Sites allow you to define bridges, and ensure that they are managed in a known point-to-point environment so that large data transfers are not unnecessarily moved across networks with slower connectivity. Because of the complexity of AD and the presumptions made within

Microsoft's management tools, it is likely that you will want to check out other options to manage your environment, including the creation of your own tool through the use of ADSI.

AD's success is assured as a core part of Win2K, however, the real test will be how many Independent Software Vendors (ISVs) Microsoft manages to attract to their implementation. This was the premise of Novell with NDS, which has been available for many years now and has not produced the level of success Novell had hoped for in the ISV community. Because Win2K and AD will inevitably be the core of many organizations, you need to consider the ISVs you are working with today. For example, while looking at your migration strategy, you will need to consider any applications that rely on Windows NT 4.0 security and directory constructs, and find out whether or not updated versions that are Win2K- and AD-aware exist or are planned for the future. This applies equally to any custom management applications you may have installed. At this stage, most of the vendors of management solutions are working closely with Microsoft, and we will spend some time reviewing tools from companies such as NetIQ, FastLane, NetPro, and others that may help you in your migration.

### **Stability**

Perhaps the most compelling reason to migrate to Win2K is the reliability and stability of the product. There is both empirical and anecdotal evidence to support the improvements Microsoft has made with this product. Additional supporting evidence includes the ongoing references to the number of bugs that were still outstanding upon release which resulted in Service Pack 1, or the 30 million or so lines of code in the base product.

Apart from improvements to the base installation being able to deal with potentially ill-behaved applications, many features have been enhanced and new ones added. We will take a quick tour of these features in the following sections.

### **Driver Management**

In NT 4.0, ill-behaved device drivers were recognized as being the number one cause of failures, often resulting in the infamous blue screen of death (STOP error). With Win2K, the operating system (OS) has been modified to prohibit such ill-behaved device drivers from over-writing memory in use by the kernel and other devices.



An interesting tool has been created called the *Driver Verifier*, available in the Windows 2000 Device Driver Kit. The importance of this tool is that it monitors a driver's usage pattern, including buffer memory access, and can identify misbehaved drivers. This allows developers, and even system administrators, to quickly identify such drivers and deal with them as needed.

## Driver Signing

Driver signing is something that Microsoft has been trying to introduce for some time. There are two aspects to driver signing. Driver signing uses digital signatures to ensure the driver you are installing is the driver that has been released by the organization that signed it, and perhaps, more importantly, that it has not been changed in any way. This security aspect ensures that you are not installing malicious code into your system. The second aspect is that when Microsoft signs drivers, you can be assured they have been tested using Microsoft's testing services and validated to their satisfaction to work within the standard deployments of Win2K.

## File Protection

In an attempt to protect vital system files from being overwritten, Microsoft has created a few new tricks. Initially, system files are hidden from any user's view by a simple rule that stops them from being displayed in a Windows Explorer view. That said, it is very easy to remove the effect as an administrator of the system.

The next trick is the tracking of system files through a new service called *Windows File Protection (WFP)*. Essentially, WFP is a service that maintains a watch list of files (around 3,000) including system DLL's, drivers, fonts, and more. From that list, Windows will determine if changes have occurred, and will offer to restore an original copy of the changed file. There are several ways in which this can occur, either at startup, or invoked manually through the `sfc.exe` command line. The operator can then choose whether or not to reinstate the original file. To update the watch list requires this sort of manual intervention or the installation of signed files as previously described.

## Scalability

There are several means by which Win2K has increased scalability from NT:

- Hardware Support
- Active Directory Scalability
- Advanced Data and Storage Management

## Hardware Support

Microsoft has made a major effort to support more hardware devices than ever before, along with improvements on how it deals with new hardware being installed into the system.

Hardware clustering support is another of the major aspects of Win2K. One obvious advantage is in the support of larger hardware configurations. Server consolidation reduces raw *total cost of ownership (TCO)* in numerous ways, from lower hardware costs, backup efficiencies, staffing,

software, and licensing costs. This increased ability to support hardware scalability also reflects into other applications such as E2K, SQL Server 2000, and more, where you achieve these improvements through an increased number of seats per host.

The previously noted versions of Win2K include Datacenter server support of up to 32 CPU's and 64 GB of memory. It is important to note that Microsoft claims to have eliminated previously acknowledged limitations with SMP versions, such that scalability is more linear and predictable with all applications.

For a Windows NT 4 domain, Microsoft's recommendation is that the *Security Accounts Manager (SAM)* database only be allowed to grow to 40MB. In effect, this means that a single domain could only support around 30-40,000 objects. Remember, you should consider objects as much more than just user accounts, since objects represent groups and computer accounts as well. Microsoft claims Win2K domains can support millions of objects in AD, which can potentially grow to 17TB in size. Through the use of AD, Win2K can support potential interoperable domains of many millions of objects. The overall limitation is supposedly 15-20 million objects, however, despite the online example of queries against a large database, this has not been tested in the real world as yet. We will look at AD in more detail, and its *raison d'être*, shortly.

## Active Directory Scalability

As a result of AD services being in place, Win2K also has a model of the network topology within which it resides. The importance of this is that Win2K can review and dynamically update the topology, and intelligently route information between servers and domains on a much grander scale than NT 4.0. This is not an arbitrary improvement, as network traffic could easily increase as a result of the introduction of AD. A related view is that, as with all directory service solutions, the intent is to make sure that data is close to the applications that will make use of it.

## Advanced Data and Storage Management

The final aspect of scalability is support for storage sub-systems. Microsoft has improved many aspects of storage management. NTFS has made performance improvements, as well as the addition of Dynamic Disk management that allows for the expansion of disk volumes (as required) and quota management, long a wish of enterprise administrators.

To enable Win2K to support large-scale growth requirements, there is a new solution for hierarchical storage management known as *Remote Storage Service (RSS)*. RSS allows you to manage local storage systems such as NTFS volumes, and define rules as to how you want to off-load files to other secondary storage systems, such as tape or tape libraries. RSS manages the automatic movement of files between the various systems according to your rules, even recalling them (as available) if they are not directly accessible to a user when needed. Take note that Remote Storage also works with Microsoft's Backup utility, enhanced in the Win2K operating system to correctly handle data recovery from Remote Storage.

We will not be dealing with RSS in this book, however, if you are having storage problems, RSS might be an important discussion and decision point to support your migration.

Microsoft's *IntelliMirror* is a new set of technologies that allows you to support replication of a user's workstation applications, data, and settings to a server. More simply, IntelliMirror offers automatic software distribution and maintenance, centralized desktop configuration management, and remote operating system installation. This enables better support for traveling or roaming users, and allows for speedy recovery of user's settings in the event of a failure on their workstation or laptop. Furthermore, it allows for configuration changes to be applied to users based on location or situational requirements, enhancing the centralized control of distributed resources.

In relation to the security services, Microsoft has added *Encrypting File System (EFS)*. EFS offers enhanced protection for data, which can be especially important on a laptop. When in use, EFS runs in the background, and is not really seen by the end-user. The only time something different occurs is when the user must unlock the private key used to perform the encryption. We will not be dealing with EFS specifically in this book, however, it could be another important reason for you to migrate to Win2K.

Finally, Microsoft has added the *Distributed File System (Dfs)*, which can be installed with or without AD. When installed with AD, Dfs uses AD to locate file directory locations across systems. Although available in NT 4.0, including support for mirroring data, Dfs directories could not be shared because management of the Dfs root was by means of a single server. Through the use of AD, Win2K improves performance and does away with this limitation, including the single point of failure inherent in the single server dependence.

## **Manageability**

Microsoft has made many changes in the management of Windows in Win2K, both under the covers and through the user interface. One of the primary benefits of Win2K when it comes to manageability is AD, but there are others that we will look at now.

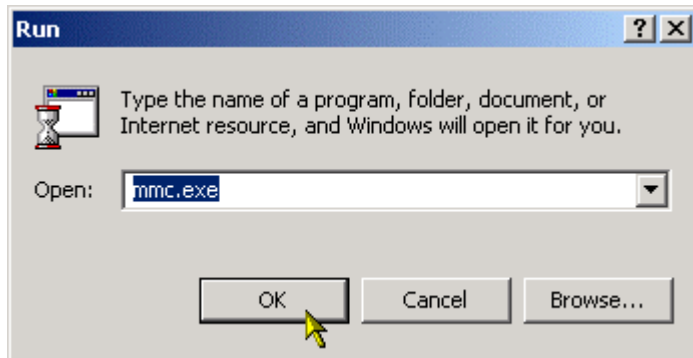
## **Microsoft Management Console**

The first thing most people will face with Win2K is the *Microsoft Management Console (MMC)*, which is common across all versions. It is basic and should be familiar in appearance and usage to anyone who has used Windows Explorer over the last few years, with tree structures appearing on the left, and data screens on the right. Right click menu options abound, as do context-sensitive operations and help. Although the MMC's integrated, customizable console represents a quantum leap over the inconsistent array of administration tools that existed in NT 4.0, it isn't perfect. For example, one complaint frequently raised by administrators is the MMC's lack of drag-and-drop functionality.

There are numerous predefined management consoles located in the "Start\Programs\Administrative Tools" menu, including "Computer Management,"

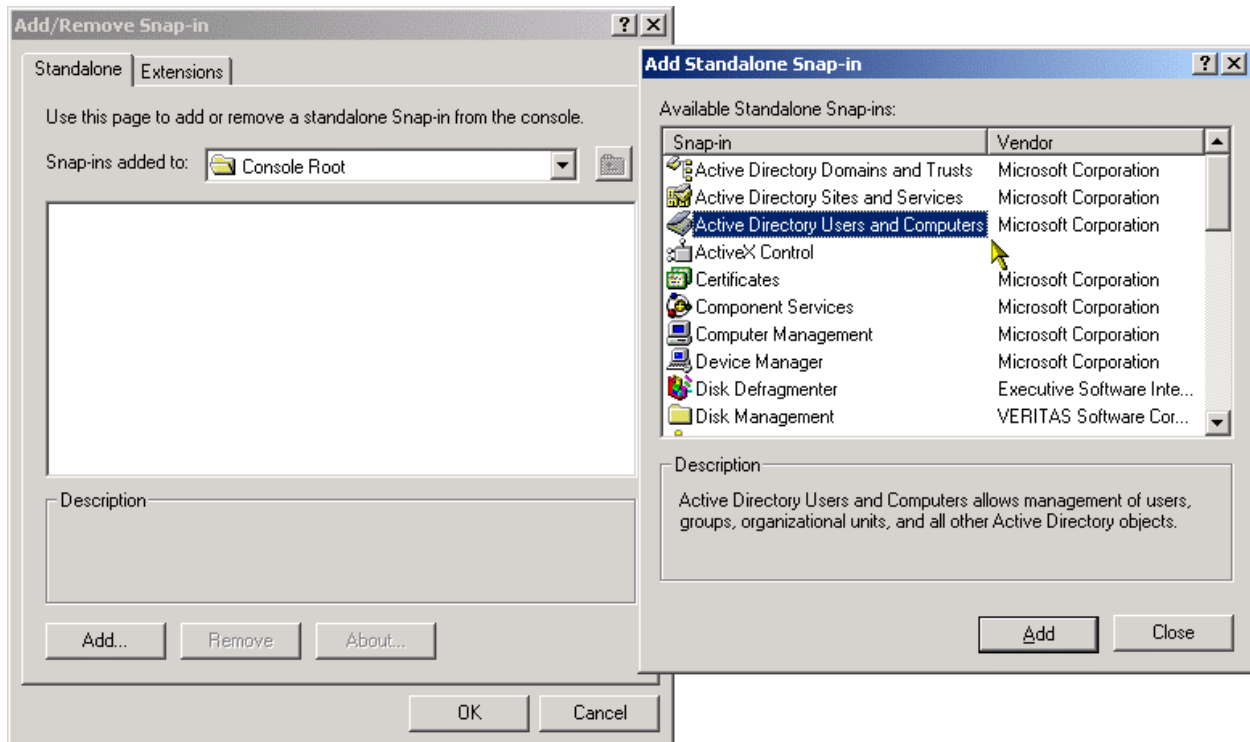
“Performance,” and “Internet Services Manager.” The MMC is essentially a shell within which consoles can be loaded and utilized. These consoles are called *snap-ins*, and many can be loaded into the same shell at the same time. I will not spend much time in this introduction on the MMC, other than to describe how to load extra snap-ins and create custom or task specific consoles.

To run the MMC separately, you can either create a shortcut somewhere, or simply use the “Start\Run” option, typing “MMC.exe” as shown in Figure 1.2.



**Figure 1.2. Running an empty MMC**

You will be shown an empty console, into which you can add existing snap-ins. To add snap-ins, select “Console\Add\Remove Snap-in,” or press Ctrl-M within the MMC. This takes you to the list of current snap-ins. If this is a new console, this list will be empty. Select “Add,” and you are presented with the screen shown in Figure 1.3.



**Figure 1.3. Adding a Snap-in to the MMC**

You are now shown a list of snap-ins currently installed in the console. There are two parts to the snap-in design. The snap-in itself can be loaded and used, and it may have a single function that it supplies. In some cases, however, the designers may choose to add extensions to the snap-in, which essentially means that increased or specific functionality can be by the vendor, or based on the current installation parameters. An example of this is the “Active Directory Users and Computers” snap-in, which allows you to decide whether to include specific functionality such as “Group Policy,” “RAS Dial-in,” and “Terminal Services.” This allows you to minimize the amount of extraneous options that appear in the console, and ensures that the options people do not need, will not appear.

Importantly, to make the system extensible, Microsoft allows you to embed several secondary snap-ins. These are an “ActiveX control,” “Folder,” and “Link to Web Address.” The importance of this capability is that you can use existing management or information screens that conform to the allowed types within the MMC framework. This, in turn, gives administrators the opportunity to easily migrate into the Win2K framework.

Although Microsoft provides numerous snap-ins, when applications are added to Win2K, they may register more with the system. For example, the installation of the various BackOffice components, including E2K, will add to the list of potential snap-ins you can use. Once you have defined the specific set of tasks you want within a console, you can now save the settings into a “Microsoft Management Console File” with the extension “.msc”. This is how the configurations


in the administrative tools are saved. Loading this .msc file will now also load the defined snap-ins.

You may choose to restrict access, in a pre-defined means, to specific functions by selecting “Console\Options,” and then selecting the console mode in which you would like to deploy the console. When you save the .msc file, this configuration goes with it so you can deploy it to other administrators. The options are:

- Author mode: Grants users full access to all MMC functionality.
- User mode – full access: Grants full access to all window management commands, however, restricts users from adding or removing snap-ins or changing console properties.
- User mode – limited access, multiple windows: Grants access to areas of the console that were visible when the console was saved. Users can open new windows, but cannot close existing windows.
- User mode – limited access, single window: Grants access to areas of the console that were visible when the console was saved. Users cannot open new windows.

You can also dictate the ability of the user to:

- Enable context sensitive menus on Taskpads
- Save the console settings
- Customize the views

 Using the “View\Customize” menu, you can also hide certain parts of the console such as the “Console Tree,” “Standard Menus (Action and View),” “Standard Toolbar,” “Taskpad navigation tabs,” and others. However, this is quite limited in its usefulness as a security solution, as it does not preclude using the mouse right-click menu to gain access to the same capabilities.

An interesting aspect of the MMC is the ability to create “Taskpads.” Taskpads allow you to provide a simplified interface to specific management tasks as defined in a specific MMC configuration. In the console, you select “Action\New Taskpad.” This will then launch the “Taskpad Creation Wizard” which takes you through the process of defining your simple management console.


AD improves manageability in the following ways:

- **Delegated Administration:** Because AD offers a hierarchical data model, it allows for administration to be assigned and distributed based on that hierarchy, as well as attributes within that hierarchy, such that administration can be targeted and simplified. Administrators can delegate rights to sites, departments, teams, individuals, and select groups of individuals. Rights can be defined at the object or attribute level. NT 4.0 offers only one level of administration and course security controls, which prohibits easy delegation of administration without the use of third-party tools.
- **Extensible Data Model (Schema):** Because the schema can be extended, other applications can make use of AD for their account and resource data, allowing easy use by internally-developed or third-party (ISV) applications.
- **Multi-master replication:** Domain controllers maintain full read/write replicas of the directory for their domain. This allows data to be available at any time, and located near the applications and services that need it, as well as ensuring that updates to data can be made even if one domain controller is offline. This also enhances overall performance of the environment, and is more resilient to potential network issues.

## Microsoft Software Installer

Along with improved driver support, signing, and file protection, several improvements have been made to general software installation. In a migration scenario, there will be new software deployed, so enhancements to that process can save a great deal of time.

Microsoft released a software packing and installation service known as *Microsoft Software Installer (MSI)* prior to Win2K. This has been carried into Win2K as core functionality. MSI consists of a service on the local machine called `msiexec.exe` and stored in `%systemroot%\system32`. When required, the service will process the installation packages known as a Microsoft Windows installer package. Given a file extension `.msi`, which is associated with the `msiexec.exe`, these files are storage files containing the instructions and data required to install an application.

 For more information on .MSI installation packages and the Windows Installer technology, see Chapter 3 of *The Definitive Guide to Windows 2000 Administration* by Sean Daily and Darren Mar-Elia (Realtimerepublishers.com), a free eBook that can be located at <http://www.realtimerepublishers.com>.

One of the common problems in a locked-down environment is the installation of software when the user trying to install it does not have administrator-level permissions on the machine. This causes permission issues when a package is installed. A new aspect of software installation is to choose whether to use the current permission levels, or the ability to temporarily raise the permission level of the installation package to the privileged LocalSystem account that the service itself uses to start.

At a later point in this text, we will examine the packaging and installation options in more detail as we review how you will install software into your environment.

## Remote Installation Services

Another useful piece of functionality in migrations (especially when new client desktops are deployed) is the *Remote Installation Services (RIS)*. RIS is a set of tools that allow you to install Win2K Professional images on to workstations across the network. The RIS host is a Win2K server that acts as a boot server for clients. Unlike traditional installation services, RIS does not necessarily require a boot-diskette or an existing installation on the workstation. In order to function, RIS uses a network card standard known as *Pre-boot eXecution Environment (PXE)* to boot from the network. This uses a combination of new technologies that allow the workstation to boot from the network, DHCP, DNS, AD, and more, to locate an installation point on the network from which to boot and install an image onto the local workstation.

Where the client does not support PXE, Microsoft offers a utility called the *Remote Boot Floppy Boot Generator (RBFGB)* that creates a boot disk that works with a specific list of PCI-based network cards. We will examine the remote installation options in more detail later.

## Security Improvements

Security is certainly one of the major benefits of migrating to Win2K. Microsoft has added a large number of security enhancements to Win2K, in what should be seen as an evolution from the NT security you know. Win2K Server offers the *Security Configuration Manager (SCM)*, which is a Microsoft Management Console snap-in. SCM is an attempt to simplify the common problem of misconfiguration of security settings in a complex, or even a simple, environment.

## Authentication

The ultimate goal most organizations dream of with their networked systems is that of *Single Sign On (SSO)*, whereby all systems recognize that an account is valid after the first time it is authenticated. In reality, the closest most come is *Similar Sign On* (my term), where all networked applications maintain their own version of a security principle and require users to perform separate authentication procedures.

There are several options for authentication: *NT LAN Manager* (NTLM and its various revisions); Kerberos; and X.509 smart cards. Kerberos authentication is a major benefit of Win2K. While Win2K still supports the NTLM authentication model allowing backward compatibility with Windows NT, 98, 95, and 3.11 clients, the move to Kerberos will only improve your situation once you have migrated to a native Win2K environment. This is because in mixed mode, Win2K still needs to support the NTLM model. Unfortunately, support for NTLM is still required Novell NetWare interoperability as well.

Support for Kerberos also allows transitive trusts to be formed between Windows domains as opposed to the NT 4.0's non-transitive trusts. We'll explore the true ramifications of this in later chapters, as we look at how to set up your Win2K domains.

#### Advanced Kerberos Tools

Many people deal with the issue of interpretability between Kerberos systems. Although claiming support for Kerberos V5 through the use of AD Service Accounts, there is only a subset of Kerberos functionality available. Microsoft has added a number of custom properties to their Kerberos tickets that are not supported by the various UNIX implementations available. As a result, third-party products are still required to support advanced interoperability, and you should look to third-party products in the interim to help you when facing this situation:

CyberSafe <http://www.cybersafe.com/>

Entegrity <http://www.entegrity.com/>

Unfortunately, there is only so much security you can add to a system without making it inaccessible or useless. Win2K is still susceptible to attacks from tools such as `pwdump2` that checks for weak user's passwords, and can be used as input to [l0phtcrack](#). They are even able to dump password hashes from AD when still using NTLM support. While I don't support their widespread use, they can be used as an auditing tool, and because other, more nefarious individuals will use them to attack your installation, you need to be aware of them.

#### Recommended Security Tools

To ensure your network is not susceptible to security breaches, you should check that you have the latest updates from Microsoft installed, as well as check your network internally using some of the tools that crackers use, such as:

`pwdump2` at <http://www.webspan.net/~tas/pwdump2/> is an application that dumps the password hashes (OWFs) from NT's SAM database, whether or not SYSKEY is enabled on the system. `pwdump2` produces output that can be used by `l0phtCrack`.

`l0phtCrack` at <http://www.securitysoftwaretech.com/l0phtcrack/> allows you to run dictionary-based and brute-force attacks against LANMan and NT hash codes.

## Group Policy Management

Active Directory introduces group policy management. *Group Policy Objects (GPOs)* reside in AD and maintain information on management policies for most other objects within the directory, from users and systems to applications and files. A GPO is actually an AD object that allows the security system to quickly calculate whether that policy applies to the object set it is dealing with, and a reference to files that contain the details of the policy.

A GPO is associated with group or container objects such as domain, site, or OU in AD, and can be assigned down through the tree through inheritance. This allows you, as an administrator, to enforce group-based policies to users and computers. Examples of the things you can enforce are:

- Login or logout restrictions
- Security settings for users, computers, and domains
- Registry settings on computers
- Software settings
- Network settings
- Configuration settings for local applications

We will spend some time in Chapter 4 looking over GPOs and the *Group Policy Editor* to ensure that your Win2K environment is secure and correctly deployed.

## Connectivity Benefits

Windows has long had support for TCP/IP; however, behind the scenes it was always looking for NetBIOS support, either natively or running over the top of TCP/IP. With the release of Win2K, you can now run a “pure” TCP/IP network. The caveat to that statement is that you must be running Win2K in native mode. This is because in mixed mode, where Win2K will work with NT 4.0 installations, NetBIOS is still required.

Beyond that, Win2K has either improved or added support for the following components:

- Dynamic Domain Name Service (DDNS – RFC 2136)
- Windows Internet Name Service (WINS)
- Dynamic Host Configuration Protocol (DHCP – RFC 2131, 2132 & 2141)

- Quality of Service (QoS)
- Protocols Supported: TCP/IP, DLC, AppleTalk, and NetBEUI

### ***Plug and Play***

It has taken some time, but Win2K finally provides an excellent and stable platform for use with Plug-and-Play (PnP). PnP also assists with power management through two services:

- The PnP Manager is responsible for control of PnP devices as they are added to and removed from the system. The PnP Manager will load and unload the appropriate drivers and INF files as required. If available, it will also assign the appropriate resources and report conflicts if they occur. Another part of the PnP Manager is called the *Arbiter*. The purpose of the Arbiter is to manage conflicts between devices. The Arbiter also allows the PnP Manager to reassign resource assignments on the fly, and make the drivers tweak device settings so that they can all work together.
- The Power Manager is an interesting PnP companion as well as a distinct kernel mode sub-system in itself. The Power Manager is responsible for managing battery consumption, and as such, works with the PnP Manager to power down devices when required.

To ensure that these services work appropriately, you need to use hardware that supports either the *Advanced Power Management (APM)* or the more recent *Advanced Configuration and Power Interface (ACPI)* standards.

The advantage of the PnP additions is the ability of Win2K to stop and start devices on the fly, including networking services. This allows users to have networking connections put to sleep, such as when you put a laptop to sleep or into standby mode, or easily disconnect from one network and move to another. When the machine is powered up again or reconnected to a network, the networking services are re-established.


### **Other Migration Considerations**

Any migration exercise will require that you experiment and perhaps, more importantly, train the teams who will perform the work.

Because migration will have an impact on more environments than the desktop and Windows NT servers, you may need to deal with other teams within the organization. This will require their cooperation, and your understanding of their environment. These include:

- DNS / DHCP administration
- Kerberos / Security Team

- Messaging Team
- Intranet Team
- Hosted Applications
- Training
- HR and Corporate Directory Services
- End users
- Network Services and Remote Access

 When we start to talk about your plan to migrate to Win2K, you will see that you can choose to install Win2K servers in what is known as mixed or native mode. Mixed mode is essentially running Windows 2000 in NT 4.0 compatibility mode. The caution is that unless, or until, you change to native mode, you won't gain all of the benefits that Win2K and AD provide. Refer to Chapter 3 to see the pros and cons of each mode.

There are many other costs to consider when migrating to Win2K. We will review them briefly to be sure that you are aware of them, before diving into the technical discussions in Chapter 2 onward.

- **New Hardware:** As mentioned earlier, the minimal specifications for running Win2K in any form are higher than that of NT 4.0. As such, there will likely be a requirement for a reasonable hardware refresh unless you have recently done so.
- **Training:** Training costs are likely to be high. Although a lot of information will be presented inside this migration guide, it is not a complete substitute for training from professionals.
- **Professional Services:** Despite the availability of training, you may need to consider professional services in your migration. Whether to gain a jump in planning or to gain resources, many Win2K deployments have been undertaken in the last year and there is valuable experience out there of which you should take advantage.
- **Tools:** Despite the availability of documentation and tools from Microsoft, you will likely find that they fall short in some area that is essential to your migration. As such, expect to use a number of tools from third-party vendors such as NetIQ, FastLane, NetPro, BindView, and others.

- **Software Updates:** Whatever maintenance agreements you have in place today, it is possible that some of the software you are using is not available on Win2K, or may never be. Wayward software vendors may even repackage their software for Win2K forcing you to buy a new package. Do not forget this in your planning.

## Meet Exchange Server 2000

Prior to the release of Exchange Server 2000 (E2K), Exchange 5.5 provided its own private directory service. In fact, AD is based on a similar version of the database technology originally used by Exchange known within Microsoft as Jet. Despite its explicit dependence on AD, E2K is now an excellent example of a directory-enabled application. E2K provides messaging and collaboration services for the enterprise, and to do so, it needs to “understand” the enterprise structure in terms of the people, relationships, and environment in which it is working. At one level, AD already provides this, and importantly AD is extensible enough to allow E2K to extend object class and attribute definitions such that E2K can ride on the back of AD.

Importantly, while AD does allow for delegated administration (which we’ll discuss in Chapters 3 and 4), the relationship between Win2K and E2K does increase the amount of interaction that will be required between the traditional network/OS and messaging administration teams. Organizational issues such as this will occur throughout the migration, and we will raise them in the summaries as well as when they occur throughout this book.

If we go down the previously referenced advantages of Win2K, we can see that Exchange actually builds on and inherits a large number of them. For example, the combination of AD and Scalability allowed Microsoft to consolidate their Exchange 5.5 installation of multitudinous servers down to eight servers running Win2K and E2K for the entire organization.

Win2K itself now uses SMTP for inter-site communications, as a protocol to talk between servers and Exchange replication or synchronization. When E2K is installed onto a Win2K server, it actually updates the SMTP service, such that both the core OS and Exchange use the same optimized solution.

Advances in the management of Win2K extend into E2K such as the simple hierarchical or tree model of the MMC, clustering, and Internet protocol services.

The reality is that if you want to have a successful deployment of E2K, you must intensely focus on your AD design and deployment. AD does not need to be fully deployed on every client and server before you begin to deploy E2K. However, if you plan to deploy E2K at all, you should ensure that this is taken into account in your AD design and deployment. There are tools available to help you in situations where AD is not fully deployed. You will need to consider the cost over time in terms of effort and potential frustrations. We will spend an appropriate amount of time throughout our explanation of AD doing exactly that as part of the migration discussion, as well as detailing how to move through your migration in the quickest practical route.

## Exchange Server 2000 Product Versions

E2K is delivered in three versions as defined in Table 1.2.

Version	Description	Notes
Exchange 2000 Server	Exchange 2000 Server is the basic version designed for Small to Medium Enterprises (SME's) and branch office deployments. Its primary distinction is that it preserves Exchange 5.5 Standard Edition's 16GB limit on data storage.	E2K Server and Enterprise Server allow customers to use the following:
Exchange 2000 Enterprise Server	Exchange 2000 Enterprise Server is designed for any size enterprise, and allows data storage to what is effectively unlimited size (16 TB) through a facility that allows it to create partitioned data stores as discrete database files.  Enterprise Server also enables deployment on up to a four-way cluster based on which version of Win2K you deploy.	Web Store architecture Outlook Web Access Instant messaging
Exchange 2000 Conferencing Server	Actually shipped as part of the E2K Enterprise Server, the Exchange 2000 Conferencing Server provides an organization with video and audio conferencing through H.323 or IP multicasting and data conferencing through the T.120 protocol.	

**Table 1.2: Versions of Exchange 2000**

### Why Upgrade?

There are numerous reasons to upgrade to E2K, and while some of these reasons iterated here may not apply to you directly, many of them will.

First, the tighter integration with Win2K makes this an essential upgrade if you plan to move to Win2K. If you run Exchange 5.5 (with SP3 or later) on Win2K, you will find that the advantages listed below are not there. This is also related to the discussion around mixed versus native mode for Win2K, whereby if you wish to maintain a 5.5 installation, you will need to maintain a mixed mode environment until you are prepared to change.

- Decreased administration costs can be achieved. Because of the integration with AD and the consolidation of services such as network routing, SMTP messaging, and management tools, the staff can more easily be cross-trained to manage the entire solution, despite its overall complexity.

- Scalability is inherent through the underlying reliance on Win2K server. The ability of Win2K servers to support SMP allows E2K to support more customers on a single host. The ability of AD to support widely distributed and colossal numbers of users ensures that E2K can grow to almost any organizational requirements.
- Reliability is also inherent through the reliance on Win2K server. Clustering support in Win2K is one way in which load can be spread across up to a four-way cluster.
- Consolidation: E2K allows for the creation of multiple message stores, all while increasing reliability and reducing restore time, and reducing management and maintenance costs.
- Outlook Web Access (OWA) is vastly improved in both appearance and performance. Enabling this outside the organization poses some security challenges, however, OWA is also usable within an organization whereby staff can be anywhere on the network and still have the ability to access their messaging solution. This even allows the deployment of kiosk or lobby terminals for staff to use as they move around or between buildings.
- Web Storage is another innovative solution available through E2K. Web Storage is an extension to Exchange that enhances the messaging store to allow users to store documents into folders over networks using a Hypertext Transfer Protocol–based (HTTP) protocol known as *Web Distributed Authoring and Versioning (WebDAV)*. Office 2000 supports WebDAV making it easy for Windows shops to utilize this technology. Finally, Web Storage is indexed and allows for custom attributes to be assigned to stored documents.
- Improved Routing: While still using Exchange 5.5, you will still be using 5.5 routing algorithms. E2K adds improved routing, and SMTP has been chosen as the default transport protocol for all message traffic, both within a site and between sites.
- Conferencing Technologies can help speed communications within the organization, and utilizes AD to help you collaborate with the right people when they are online.
- Installable File System: M: drive can be presented as file share.
- Streaming MIME Storage for Internet protocols

## Summary

In this chapter, we surveyed some of the most important new features included in Windows 2000 and Exchange 2000, and compared the different versions that exist within each product family. We also discussed some of the more important migration issues and challenges that exist with both products. In the following chapters, we'll dive into the specific techniques, tools, and information you'll need to employ to successfully migrate to these new platforms.

### Copyright statement

This site contains materials created, developed, or commissioned by Realtimepublishers.com, Inc. and is protected by international copyright and trademark laws. No material (including but not limited to the text, images, audio, and/or video) may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at [info@realtimepublishers.com](mailto:info@realtimepublishers.com)