

Exchange 2000 pre-migration planning guide

Upgrading from Exchange 5.5 to Exchange 2000 is not a typical migration project. Issues such as Active Directory preparation, instant messaging, and front-end server topology introduce unprecedented complexities to the process. But by carefully planning and allowing sufficient lead time, you can make an Exchange 2000 migration a manageable undertaking. This collection of task-focused articles by TechRepublic contributor Carol Bailey will help you develop an effective—and relatively painless—upgrade strategy and ensure that you cover all the bases.

Table of Contents

Plan now or pay later	2
Active Directory and IM preparation.....	4
Internal Exchange preparation	9
Server placement and topology	12
Front-end servers, clustering, and ports	14
Configuration design preparation	17

Plan now or pay later

As suspected, Microsoft is dropping support for its most successful mail server product: Exchange Server 5.5. We knew it was inevitable because of Microsoft's push to get all customers on the latest versions of its products.

Of course, many of us were relieved to hear that we have a little time. Microsoft has [announced](#) that regular support for Exchange Server 5.5 ends in December 2003. But still we have less than a year to make preparations for upgrading to Exchange 2000—and make no mistake: Exchange 2000 requires some serious preparation.

Baby steps to Exchange 2000

Upgrading from Exchange 5.5 to Exchange 2000 is slightly different from other Microsoft upgrades we've faced to date. For starters, Exchange 5.5 runs quite happily on both Windows NT Server 4.0 and Windows 2000 Server. The only major consideration is that if you run Exchange Server 5.5 on Windows 2000 domain controllers, you have to change the LDAP port number in the Exchange Administrator so there isn't a clash when Active Directory uses the same port for LDAP calls (see [Q224447](#)).

The ability to run Exchange Server 5.5 on Windows 2000 meant that we got all the benefits of upgrading the operating system and migrating to Active Directory without having to make any changes to our working Exchange 5.5 infrastructure. So, for a number of reasons, many administrators opted to stay with Exchange 5.5 rather than upgrade to Exchange 2000. As we all prepare to migrate to Exchange 2000 in the next 12 months, it's important to keep those reasons in mind:

- **Active Directory**—Exchange 2000 requires Windows 2000 *and* Active Directory. Many companies are still in the process of upgrading their servers and domains to Active Directory, even after deploying Win2K. With support for NT 4.0 servers declining, upgrades to Windows 2000 have taken precedence over Active Directory deployments.
- **Hardware**—Exchange 2000 requires more memory and more processing, so a hardware upgrade or a server migration is often required. That means additional cost and/or downtime.
- **Security**—Exchange 2000 has higher security implications. One example is that it must run in conjunction with IIS (and we all know how many security problems there have been with IIS).
- **Training**—Exchange 2000 requires significant retraining to understand the new product set, including how and whether to use Instant Messenger, working with multiple storage groups and data stores, managing routing groups, and setting up policies.
- **Migration**—Careful planning is needed for integration with existing Exchange 5.5 servers during the migration period to Exchange 2000.
- **Configuration**—Some Exchange 5.5 configuration options cannot be directly upgraded.

The last point in this list is worth further explanation. Upgrading Exchange 5.5 is more complicated than upgrading an NT 4.0 domain to Windows 2000 domain, which was a conversion of one database to another. Upgrading Exchange 5.5 to Exchange 2000 is actually an amalgamation of two databases into one, and the two do not have a like-for-like structure. This means that some preparation work has to be done on the existing Exchange 5.5 database so it can be smoothly upgraded.

A clear example of this can be seen immediately in the relationship between user and mailbox. Exchange 5.5 has its own independent database for mailboxes, which it links to a Windows domain (either NT 4.0 or Windows 2000 Active Directory). Consequently, one user can have multiple mailboxes, or you can have a mailbox without a user. Exchange 2000 has only one database (Windows 2000 Active Directory), which contains user accounts. Mailboxes become an attribute of those accounts. This means that now each user can have only one mailbox, and each mailbox must belong to a user. If you upgrade your existing Exchange 5.5 database without preparing for this, you risk having inaccessible mailboxes.

Upgrading to Exchange 2000 has also been postponed on many production networks for another, highly compelling reason: It's rightly perceived to be a risky upgrade. Mail exchange, both internal and

external, has become a core IT service and is critical to almost every organization's functioning. E-mail, together with Exchange's public folder system (and calendaring system, task tracking, etc.), has become a common method of communication and an efficient method of transferring and disseminating data.

E-mail and groupware functionality have become services that everybody takes for granted—until they fail. This failure not only could impede business but also could become a career-limiting move if that failure is associated with your actions—or lack of Exchange 2000 migration planning. Understandably, nobody welcomes the risk of being responsible for breaking a working e-mail system, even if it is perceived as a necessary risk within a sanctioned upgrade project.

For all these reasons (and more), upgrading to Exchange 2000 has often been last on the list when it comes to upgrade projects on busy, production networks.

Get a head start

I recommend that companies use the grace period to their advantage and plan a gradual preparation for Exchange 2000 that can be completed over the next few months. If you take the appropriate steps to lay the groundwork, you'll find the upgrade process much more manageable. You'll also avoid a mad rush with bad decisions at the end of next year, and you'll have more time to think through design issues that could stall your migration planning at several points.

Preparing for Exchange 2000 is more than simply upgrading hardware, upgrading servers and domains to Windows 2000 and Active Directory, and retraining staff—although all those issues need to be addressed. You'll need to check, modify, and prepare for a number of key technological stumbling blocks so that the upgrade process will go smoothly and you won't have any nasty surprises with unplanned downtime (and irate users).

So much reference material is available on installing, upgrading, and running Exchange 2000 that it can be a little overwhelming. You might want to start with this collection of [Exchange 2000 deployment white papers](#). And, of course, it's tempting to jump in and try out all the new features. By all means, try Exchange 2000 on an isolated network on a test machine, but don't underestimate the risks involved in upgrading a production system. This is particularly relevant if you're planning on an in-place upgrade, as many administrators are, instead of installing new servers and moving resources over.

Summary

To help you develop a viable upgrade strategy and avoid the missteps that have brought some Exchange 2000 migrations to a screeching halt, I'm going to cover, step-by-step, the migration planning issues you need to consider.

Active Directory and IM preparation

Migrating from Exchange 5.5 to Exchange 2000 requires a lot of preparation work to merge the two databases—Exchange 5.5 and Windows 2000 Active Directory (which is what Exchange 2000 uses). Let's look at the Active Directory elements that you must understand and modify as part of an Exchange 2000 upgrade. I will provide some valuable tips for those preparing to roll out corporate instant messaging services as part of their Exchange 2000 deployment.

DNS

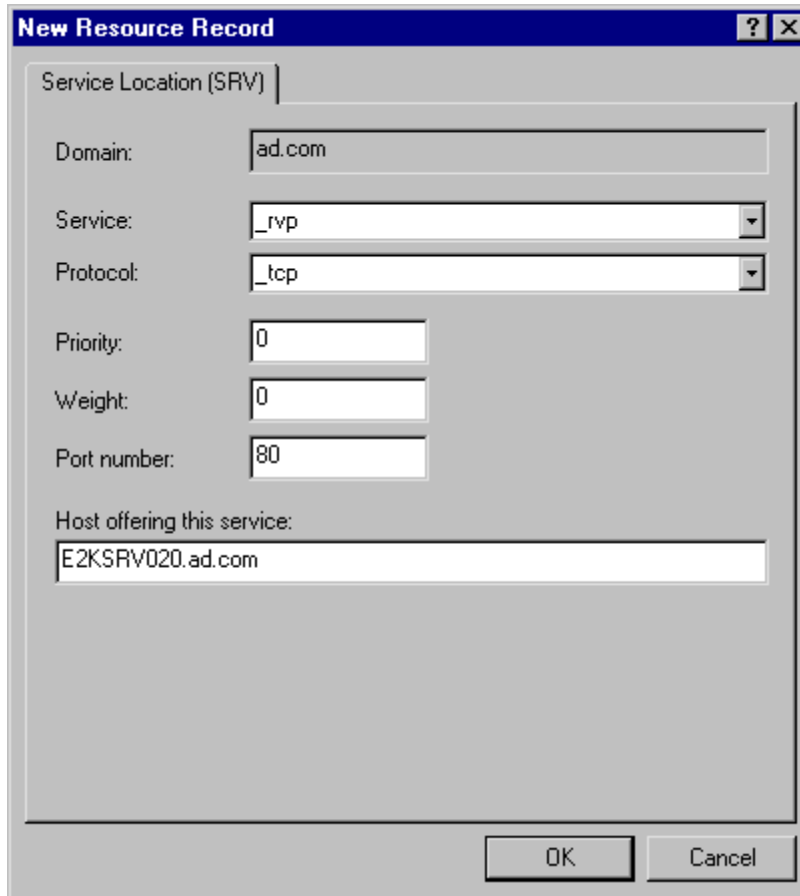
DNS is a critical part of Active Directory, so you need to ensure that DNS is working properly long before you begin the Exchange 2000 installation process. You can do this using the tools [DCDiag](#) and [NetDiag](#) on the Windows 2000 servers that will run Exchange 2000. Also, since Exchange 2000 will probably be the first program you'll install in your Win2K Active Directory domain that requires dynamic DNS service records, it's important to verify that your DNS servers are supporting that feature without a hitch. You'll want to check this in a deployment on a test network.

You'll also need to get your internal DNS system integrated with the external (Internet) DNS, verifying that all Exchange servers register with your internal DNS servers. External DNS servers (for example, your ISP's Internet DNS servers) should be configured only as forwarders on your internal DNS servers. See [Q300202](#) for an explanation of how this can be achieved simply (although for security reasons, many networks will incorporate a caching-only forwarding DNS server on the DMZ).

You'll need to prepare for Instant Messenger if you're going to take advantage of this new feature in Exchange 2000. This requires an `_RVP` Service record for Instant Messenger if you plan to have a unified namespace (with users having the same logon as their e-mail account). In addition, you must specify the fully qualified domain name (FQDN) of the IM router or IM home server.

The easiest way to create this record is to use the DNS console in Win2K. From the DNS console, right-click on your forward lookup zone and select Other New Records. From the drop-down list, select Service Location. Then, in the Service Location (SRV) dialog box, enter `_rvp` for the Service (it's not available via the drop-down list) and change the Port Number to 80. Under Host Offering This Service, enter the FQDN of the IM router or IM home server. Make sure that you have an A record for that router/server. **Figure A** shows an example of an `_RVP` record.

Figure A



New Resource Record [?] [X]

Service Location (SRV)

Domain:

Service:

Protocol:

Priority:

Weight:

Port number:

Host offering this service:

OK Cancel

Once you've created the `_RVP` record, you should be able to see it under the `_tcp` folder in the DNS console, listed beside records for other services, such as Global Catalog servers, Kerberos servers, and LDAP servers. To verify that your clients can find this record, use the `nslookup` utility in interactive mode, set the query type to any (*set q=any*), and then type `_rvp._tcp.<domain name>`. For example:

```
C: />nslookup
>set q=any
>_rvp._tcp.ad.com
```

You should see a response similar to the following:

```
Server: W2KSRV010.ad.com
Address: 10.10.0.2
_rvp._tcp.ad.com SRV service location:
    priority      = 0
    weight        = 0
    port          = 80
    svr hostname  = e2ksrv002.ad.com
```

You must specify these additional records on external DNS servers if you're going to offer Instant Messenger services to your users over the Internet. You need this on internal DNS servers if you're planning to offer Instant Messenger services to internal users (and/or VPN users).

Keep in mind that if you don't plan to use a unified namespace with Instant Messenger, you don't have to create an `_RVP` record. In that case, it's optional; although if users are complaining of long logon times when using Instant Messenger, you should add one. If you are not using an `_RVP` record, you'll have to

make sure that the host name (A record or CNAME) of the IM server you are going to use is entered into your DNS. Microsoft recommends using the host name "im" as a suggested standard if you decide to use a nonunified namespace. This makes it easier for users to guess which name to use. An example Instant Messenger logon using a nonunified namespace for the ad.com domain would be user1@im.ad.com.

After installing Exchange 2000, you'll need to enable users for Instant Messenger before they can connect to it (using Active Directory Users And Computers). Also, check the Instant Messaging Settings, Firewall Topology tab in Exchange System Manager if users connect over the Internet. For more on setting up instant messaging in Exchange 2000, see [this article](#).

When preparing for Exchange 2000, many administrators get confused about configuring DNS correctly, or they neglect it. Don't make that mistake.

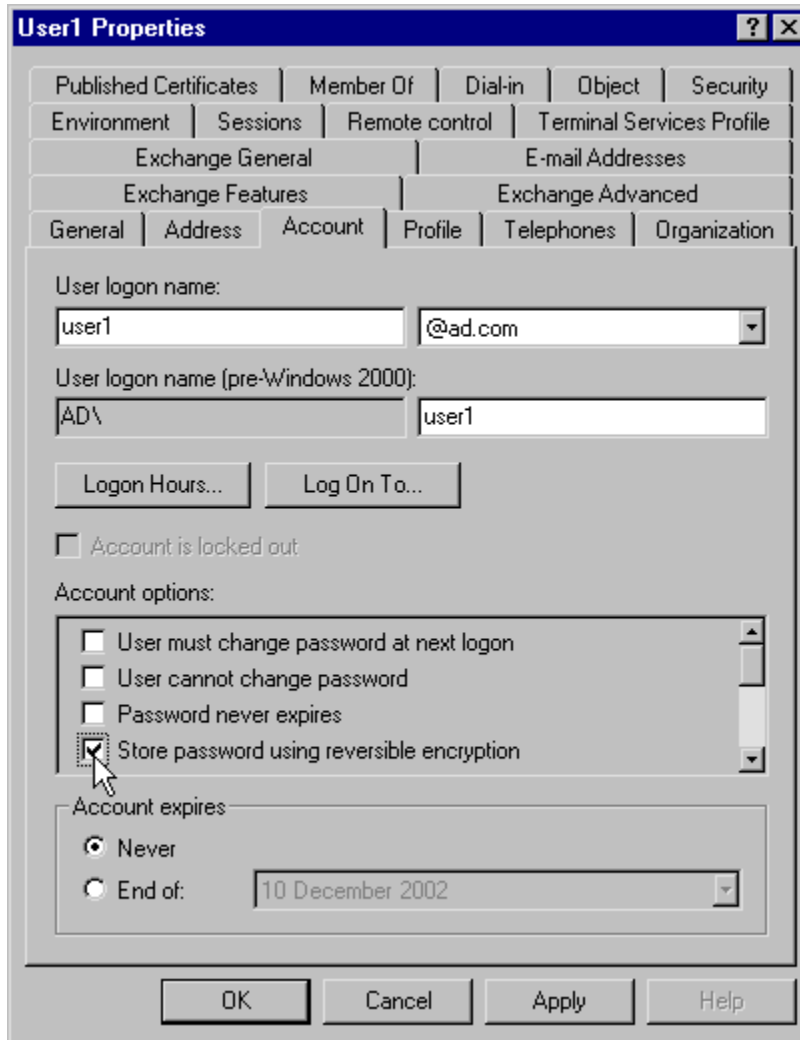
Changing network authentication

Here's something else to keep in mind if you roll out Instant Messenger: You will need to change the authentication method if users log on to Instant Messenger over the Internet using a proxy server, such as ISA Server. Instant Messenger uses IIS, and the default IIS authentication of Integrated Windows will not work with proxy servers. You'll need to configure the Instant Messenger virtual server to use Digest authentication after installing Exchange 2000. Getting this to work requires a change on either the domain policy or the user account to store passwords using reversible encryption.

Once this change has been made, the user must reset his or her password, and the new password will be stored in the new format. It's not until the new password is in effect that this will work, which is why it's a good idea to change this setting well in advance.

Microsoft's standard advice is to change this setting for reversible encryption as a domain Group Policy Object (Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy). However, it's better from a security point of view if you can identify the users who will need this setting and configure it at the account level (see **Figure B**).

Figure B



When you configure Instant Messenger later, remember to select Digest Authentication For Windows Domain Servers on the InstMsg virtual directory in IIS. You'll also use this setting if you have remote non-Windows users logging on via RRAS, which requires CHAP authentication rather than MS-CHAP.

Global Catalog servers

Global Catalog servers play a key part in Exchange 2000, so you need to check their placement, quantity, and server resources. Unfortunately, this is not an exact science but more a matter of trial and error. You should have at least one Global Catalog server in the same site as your Exchange 2000 server; otherwise, Global Address List (GAL) lookups may go over WAN links, which is obviously less than ideal from the point of view of speed and bandwidth.

As well as performing GAL lookups, Global Catalog servers locate which server hosts the user mailboxes. Although you may want to factor in redundancy and scalability (some documentation recommend a minimum of two per site), don't make the mistake of having too many Global Catalog servers. That will increase Active Directory replication traffic. An Exchange 2000 server will look to use a Global Catalog in its own Active Directory site first. If it doesn't find one, it will look in its own domain, and if it doesn't find one there, it will look in any site or domain.

Update domain controllers with service packs

Windows 2000 SP3 has been released for some time now and is considered stable by most administrators. Because of various fixes and the security patches that service packs contain, it's a good idea to keep domain controllers up to date with them. However, it's easy to forget some servers, especially if they're on remote sites and are not considered to be a high security risk.

It's well known that Exchange 2000 requires at least Windows 2000 Service Pack 1 and will fail to install on just the base version of the operating system. But it's probably less well known that all domain controllers in your Active Directory forest should be on a minimum of Service Pack 1 to accommodate the new schema. If you haven't already done so, do an inventory of the Win2K versions for your domain controllers and make sure that they are running at least Service Pack 1 without any problems before you install Exchange 2000.

Active Directory Native Mode

Microsoft suggests that you make the switch to Windows 2000 Native Mode as soon as possible to take advantage of some of the new features, such as universal groups, nested groups, and unlimited objects in a domain. However, especially for smaller networks, these benefits seem small in comparison with the risks and limitations of a one-way switch and being unable to integrate with Windows NT 4.0 Backup Domain Controllers.

Upgrading to Exchange 2000 may be the very incentive you need to switch to Native Mode. You risk losing access to public folders when you use the Exchange Active Directory Connector as part of the upgrade process (which you must do if you're not in Native Mode) because this converts Exchange 5.5 Distribution Lists into universal groups.

Summary

I have provided a number of tips and suggestions that can help you get things in order with Active Directory and DNS in preparation for upgrading to Exchange 2000. I've also shown you some things you need to do to prepare to roll out instant messaging services, one of the exciting new features of Exchange 2000.

Internal Exchange preparation

Your Exchange 5.5 servers will require significant preparation before you upgrade them to Exchange 2000. To help you cover all the bases, we'll look at the following:

- Loading service packs
- Installing IIS
- Mailbox preparation
- Database consistency
- Expansion servers
- Running ForestPrep and DomainPrep
- Installing and configuring the Active Directory Connector

This discussion assumes you're running Exchange 5.5 on Windows 2000 servers in an Active Directory forest.

Loading service packs

Make sure that all your Exchange 5.5 servers are running at least Service Pack 3 (SP4 is the latest). Strictly speaking, this service pack requirement is necessary only on those servers that will be upgraded to Exchange 2000 or that will be used with the Active Directory Connector. But it's easier and safer to ensure the same service pack level across the network. Don't forget that all Windows 2000 domain controllers should be running a minimum of SP1.

Installing IIS

Before installing or upgrading to Exchange 2000 on a server, make sure that the server has IIS installed with SMTP and NNTP (note that NNTP doesn't install by default). Then, as with any server running IIS, patch it with any necessary security hot fixes and harden the server appropriately.

If your server has IIS installed with SMTP domains configured, these will be deleted when you install Exchange 2000, and you'll have to manually re-create them, so be sure that they are well documented.

Mailbox preparation

Unlike Exchange 5.5, Exchange 2000 has a one-to-one relationship between user and mailbox. Because there isn't a straight conversion between the Exchange 5.5 directory and Active Directory (which is used for Exchange 2000), you will need to do some work to ensure that if you are merging the two, all of the mailboxes are still accessible.

This means that you need to make sure that each user has only one mailbox associated with his or her username. Previous versions of Exchange allowed users to have more than one mailbox and allowed "resource mailboxes," which were mailboxes without an associated user. This configuration is not supported with Exchange 2000 because mailboxes become a property of an Active Directory user account, and it's not possible to have more than one mailbox per user. In Active Directory, you cannot have a property (mailbox) without the original object (user account).

If you don't have a direct one-to-one relationship between mailbox and user, and you leave it like this, Exchange 2000 will attempt a best effort to create a new suitable configuration. As a result, resource mailboxes without an associated user account will have a user account created but disabled. Users with more than one mailbox will have one mailbox associated with their account (based on the mailbox that most closely matches the username), and any additional mailboxes will be associated with new, disabled accounts.

If users have more than one mailbox associated with their account and cannot access their primary mailbox after the upgrade to Exchange 2000, it's possible that the account has been associated with the wrong mailbox. You can rectify this by deleting the mailboxes in Active Users And Computers and then

connecting the user to the right account with the Exchange System Administrator, but it's best to prevent this from happening in the first place.

For proactive rather than reactive measures, either go through all of the mailboxes manually and configure a one-to-one relationship of usernames and mailboxes or have the [NTDSNoMATCH](#) utility identify resource mailboxes in advance by using the mailbox's custom attribute 10. This utility with documentation can be found in the latest Exchange 2000 service pack (SP2) under `\Support\Utils\i386\Ntdsatrb`.

Once you have created your one-to-one relationships, you'll need to keep the same functionality as before. You can enable the new user account with what used to be the resource mailbox and log on as that user to view or forward e-mails. But the recommended way is to give the original user Full Mailbox Access permission on the user account. Use the Advanced view with Active Directory Users And Computers and the Mailbox Rights button in the Exchange Advanced tab of the user Properties. The user can then access this mailbox from his or her own e-mail client.

You can also use the Active Directory Cleanup Wizard (which installs with Exchange 2000) to help identify and merge multiple mail accounts in Active Directory that refer to the same user, which is particularly useful if you are migrating users across multiple domains.

Database consistency

It's a good idea to run the Exchange 5.5 DS/IS Consistency Adjustment on the databases (public folders and mailbox stores) to remove any "zombie" Access Control Entries. This refers to a user who has deleted mailboxes. These zombie accounts can prevent access after upgrading to Exchange 2000, although this was fixed in Exchange 2000 SP1. Make sure that you tidy this up before migrating the database.

You'll find the Consistency Adjuster in the Exchange 5.5 administrator utility under File | Properties | Advanced tab. Click on Consistency Adjuster and then click Remove Unknown User Accounts From Public Folder Permissions and Remove Unknown User Accounts From Mailbox Permissions. Clear all other check boxes and then select All Inconsistencies.

Invalid characters

Check for characters in your Exchange 5.5 organization name or site names that will be invalid in Exchange 2000. Valid characters are alpha/numeric and a hyphen. Common examples of invalid characters are the period and underscore. The names also cannot exceed 64 characters. If you have any invalid characters, you will not be able to successfully extend the schema for Exchange 2000 (installing Exchange with the ForestPrep switch). If you find invalid characters, change the display name with the Exchange 5.5 Administrator.

Expansion servers

Make sure that all distribution lists are configured for Any Server In Site before an in-place upgrade. Expansion servers contact Global Catalog servers to retrieve membership information, and then the Global Catalog server looks up the users' home servers, so good connectivity to Global Catalog servers is necessary.

Running ForestPrep and DomainPrep

The Active Directory schema needs extending to accommodate Exchange 2000, and to do this, you'll need to run the Exchange 2000 Setup with the /ForestPrep switch:

```
F: \Setup\i386\SETUP.EXE /ForestPrep
```

The account you use must have membership in the Schema Admin and Enterprise Admin groups. You'll also need access to the Exchange 5.5 Service account and password, plus local Administrator rights on the server where you're running the command. To upgrade your existing Exchange 5.5

Organization, select Join An Existing Exchange 5.5 Organization and follow the prompts. Note that you'll need to enter the 25-digit Product Identification number at this point, so make sure that you have it handy.

As part of running ForestPrep, you'll be prompted to supply the Exchange 2000 Administrator Account, which will be the user who will install Exchange 2000 later. This user will be granted Full Exchange Administrator rights and will be able to delegate Exchange permissions throughout the forest to other administrators.

Because ForestPrep modifies the schema as well as the configuration partition of Active Directory, it's recommended that you run it on a Windows 2000 domain controller that is also a Global Catalog server and at a time when the network has a lull in activity. Be prepared for replication latency if you have multiple domains. You should run it when you have time on your side—for example, last thing on a Friday.

Once ForestPrep has run successfully, you'll need to run the DomainPrep command (the Exchange 2000 setup command with the \DomainPrep switch) in all your domains to modify the Active Directory domain partition. You need to do this even in the domains that don't have Exchange servers. The account you run this command with should be a member of that domain's Domain Admins group and should have local administrator rights on the machine.

This installation switch creates two additional groups (a domain local group called Exchange Enterprise Servers and a global group called Exchange Domain Servers), plus a user account called Euser_exstoreevent (for the script host event).

For more information on ForestPrep and DomainPrep, see the relevant sections on these in Microsoft's Knowledge Base article ["XADM: How to Set Up Exchange 2000."](#)

Install ADC

To merge your Exchange 5.5 and Active Directory databases, you'll need to install the Exchange 2000 Active Directory Connector (ADC). You install this from the latest Exchange service pack. Once ADC is installed, configure it with Connection Agreements (CAs). CAs are responsible for replicating recipient and folder configuration information between Exchange 5.5 and Active Directory.

When it comes to replicating users between the two databases, you can have either one-way replication, which will be sufficient if you're simply upgrading one server from Exchange 5.5 to Exchange 2000, or two-way, which you'll need if you're going to continue to run Exchange 5.5 servers. For more information on how to configure the ADC, see the Knowledge Base article ["XADM: Understanding Connection Agreements in Exchange 2000 Server."](#)

If you're running Exchange 5.5 on a Windows 2000 domain controller, remember to check with the Exchange 5.5 Administrator to see which alternative port number you're using for LDAP (it won't be the default of 389), because you'll also need to specify this number in the Active Directory Connector.

Summary

That takes care of the tasks needed to prepare your existing Exchange 5.5 servers for an upgrade to Exchange 2000. These are important factors to prepare for and can easily be overlooked as part of the upgrade process.

Server placement and topology

Another important aspect of pre-migration Exchange 2000 planning involves taking a look at how Exchange servers fit into the topology of your enterprise network. You need to consider their placement and roles prior to upgrading from Exchange 5.5. During this planning phase, you should:

- Consider collapsing existing 5.5 sites before the upgrade.
- Verify connector support and assess placement of bridgehead servers.
- Determine which Routing Groups to place servers in.
- Decide whether to use Outlook Web Access (OWA).

Consider collapsing existing 5.5 sites before the upgrade

Exchange 5.5 (and earlier) "sites" are replaced with Administrative Groups and Routing Groups in Exchange 2000, which means you can effectively split the server configuration from the connector configuration. This gives you a certain amount of added flexibility because when all your servers are upgraded to Exchange 2000, you can switch to Exchange 2000 Native mode and then drag and drop all Routing Groups into a new Administrative Group. Typically, you'd do this to delegate control of this new Administrative Group to specific users who specialize in configuring connectors only.

This flexibility of moving Routing Groups is great once you're in Native Mode. However, you still can't move the Servers containers (unless you uninstall the servers and reinstall them into a new Administrative Group). This means that an in-place upgrade from Exchange 5.5 to Exchange 2000 will involve a direct one-to-one relationship—a 5.5 site will become an Exchange 2000 Administrative Group.

If you want to move your servers between Administrative Groups or collapse them, it's a good idea to do it before the upgrade, because the Exchange 5.5 Move Server Wizard can help you. You can get the Move Server Wizard from the Microsoft site or from the Exchange Service Pack (see [How to Obtain Move Server Wizard](#)).

Connectors and bridgehead servers

You want to verify that your existing connectors are supported in Exchange 2000 (for example, mainframe connectors, such as SNADS and PROFS, are not). Document their configuration, because after an in-place upgrade, some reconfiguration may be required.

Familiarize yourself with Exchange 2000 connectors and their configuration abilities and suitability. In Exchange 2000, the Site Connector is replaced with the Routing Group Connector, which is the most common and easiest of the Exchange 2000 connectors to work with. It simply requires a reliable, permanent network connection, and available bandwidth is less an issue than it was with Exchange 5.5 Site Connectors. However, an SMTP Connector may be a better choice if you need messages to be encrypted with SSL or you need to queue messages until the other end requests them. This offers better bandwidth usage and control.

You should also assess bridgehead server placement. Bridgehead servers in Exchange 2000 are designated to route traffic rather than house data stores. If you're looking to migrate to new, more powerful servers to run Exchange 2000, you might consider converting your less powerful machines into bridgehead servers.

Server placement in Routing Groups

An Exchange 2000 Routing Group is the equivalent of an Exchange 5.5 site, with peer-to-peer communication. But you need to consider whether your servers should be in the same Routing Group. Put them into the same Routing Group if communication between them will enable a permanent and reliable connection and:

- Scheduling with other servers is not needed.
- Restrictions on messages are not needed.

- You have no requirement for Public Folder customization (preventing referrals).
- There is good communication with the server designated the Routing Group Master to receive the latest link state information.

Put servers into different Routing Groups if you want to:

- Control message flow (using bridgehead servers and costs).
- Control public folder access (disable Public Folder referrals).
- Schedule communication between servers.
- Set user permissions at different times.
- Send large attachments at various times.

With the factors listed above, note that WAN speeds are a lesser issue, but reliability is very important.

Decide whether to use Outlook Web Access

Outlook Web Access (OWA) offers a Web-based interface to Exchange so that users can access their e-mail remotely without having to install the full "fat client," Microsoft Outlook. One of the nice things about OWA is that it is also suitable for non-Windows clients.

Many administrators have been offering OWA with Exchange 5.5 after installing it from the NT4 Option Pack and IIS v4. However, OWA didn't ship with the base version of Exchange 5.5, and some administrators were not prepared to have outside HTTP access into their Exchange databases.

Now is the time to reassess whether you could benefit from OWA. It's much improved in Exchange 2000 and comes as part of the base product. Also, IIS is a required part of Exchange 2000.

However, you should be aware that OWA lacks the following features your users may be used to with the full Outlook client:

- Tasks
- Journaling
- Rules
- Offline folders
- Copying items between Public Folders and personal mailboxes
- Printing templates
- Spell checking
- Some delivery options
- Calendar reminders

For additional security with OWA, consider:

- Disabling client-side Web caching (this can make OWA seem slower for users).
- Disabling the Save Password feature if using IE5 or above.
- Educating users to log off or close the Web browser when they have finished checking their mail.

Microsoft recommends always using SSL with OWA, so make sure that your Web server has a secure server certificate to support this. If you're using your own internal Certificate Authority (CA), be sure that it's in place and that users have installed the root certificate so they know to trust the server certificate source.

Summary

We've covered several important topology, design, and network planning issues involved in Exchange 2000 migration prep. Next, we'll look at some availability and security issues.

Front-end servers, clustering, and ports

As part of your topology planning for an Exchange 2000 migration, you need to consider:

- The deployment of front-end servers.
- The utilization of clustering for high availability.
- The reconfiguration of ports on routers and firewalls.

Deploying front-end servers

Front-end servers are new in Exchange 2000 and typically exist on the DMZ to simply route traffic and decrypt data. They do not have mailboxes or public folder stores—these belong on the back-end servers, which usually exist on your private network.

You need to decide whether your topology needs front-end servers as part of your Exchange 2000 deployment. Front-end servers provide a number of security, availability, and scalability benefits. Of course, you will have to be able to justify the additional hardware and licensing costs.

Front-end servers are easy to configure. You simply activate a check box and then delete or move any data stores from that server. Their purpose is to focus on security, load balancing, and scalability (using DNS RR or NLB; for differences between the two, see [this article](#)). Front-end servers also allow you to give users a simplified and unified namespace so that everyone can be set up to access the same server name, even when their mailboxes are hosted on different servers.

Note that Integrated Windows authentication cannot be used with front-end servers, so you will need to use SSL with the appropriate protocol to ensure that usernames and passwords are kept secure. It's also important to remember that front-end servers cannot be used with MAPI clients (e.g., Outlook) but can be used with clients that use IMAP4, POP3, NNTP (e.g., Outlook Express), or Outlook Web Access. See [this article](#) for more information on front-end servers.

Clustering for high availability

Microsoft typically talks about clustering Exchange 2000 with back-end servers in the front-end/back-end server deployment. But of course you can enjoy the benefits of clustering without having front-end servers.

Consider clustering the back-end data stores to help ensure availability at the resource level (but remember clustering does not protect data). Exchange 2000 is fully cluster-aware and supports Active/Active clustering—meaning that you can simultaneously run multiple instances of Exchange within the cluster by creating a cluster group that acts as a stand-alone server (referred to as an Exchange Virtual Server, or EVS).

Each EVS can host multiple storage groups, but the maximum number of storage groups per node is four. So, for example, you can have two storage groups on each active node to ensure full redundancy if either one of the servers fails. However, if you had three storage groups on each active node, neither server could support full redundancy in the event of a failure, so plan your clusters and storage groups carefully.

There are two main differences in Exchange 2000 operation when running on a cluster:

- Cluster Service makes IsAlive calls to resources to ensure that they are responding.
- Since each EVS acts as a stand-alone server, messages between separate EVSs are transported by SMTP.

In a planned failover (e.g., for maintenance downtime), the information store removes the storage groups and stops the virtual Exchange servers. The resources are failed over, and the information store on the new node assumes the storage groups and starts the protocols needed. In an unplanned failover, typically the resources will be restarted in an attempt to bring them back online. If a restart fails, the

resources are failed over and the new node will read the transaction logs in an effort to synchronize the databases.

Interestingly, RAM requirements for Exchange 2000 will be smaller than on a nonclustered server because RAM on a cluster is dynamically allocated or released to each cluster node as needed. The amount of physical storage required for virtual memory will also be less.

Although Exchange 2000 resources support clustering, the level of support varies, so it's important to be aware of exactly which resources support high availability and in what configuration. Here is a brief rundown:

- **System Attendant:** Active/Active
- **Information Store:** Active/Active
- **Message Tracking Agent:** Active/Passive
- **POP3/IMAP4/SMTP/HTTP:** Active/Active
- **NNTP:** Not supported
- **Key Management Service:** Not supported
- **Full Text Indexing:** Active/Active
- **Instant Messaging:** Not Supported
- **Chat:** Active/Passive
- **Conferencing Services:** Not supported

Reconfiguration of router and firewall ports

When you've decided what Exchange 2000 components you are going to use and determined your server placement, you'll need to check whether intervening routers and firewalls need reconfiguration to support additional traffic between servers and/or from clients to servers. **Table A** lists the possible ports used with Exchange 2000.

Table A

Function	Port
Link State Protocol within a Routing Group	TCP port 691
Link State Protocol between Routing Groups	TCP port 25
RVP for Instant Messenger (note that HTTPS is not supported with IM, so consider using IPSec or VPNs for additional security)	TCP port 80
Domain Controller lookups LDAP	TCP port 389
Global Catalog lookups LDAP	TCP port 3268
NetBIOS	TCP 135, 139, 1024+
DNS	TCP and UDP port 53
Remote Procedure Calls	TCP ports 111, 135, 1024+
Netlogon	UDP port 445
Kerberos	TCP and UDP port 88
SRS (Site Replication Service for E5.5 sites)	TCP port 379 by default on ADC CA
Outlook Web Access (OWA)	TCP port 80 for HTTP, TCP port 443 for HTTPS
IMAP4	TCP port 143, TCP port 993 if using with SSL
POP3	TCP port 110, TCP port 995 if using with SSL
SMTP	TCP port 25

Summary

The three issues covered here will help take care of some important security and availability concerns in your pre-migration Exchange 2000 planning.

Configuration design preparation

One of the final preparation steps for an Exchange 2000 migration involves examining some design implications of various parameter configurations. These settings include:

- Data stores and storage groups
- Indexing
- Hard disk storage
- Policies
- Delegating control
- Recipient Update Service (RUS) for multiple domains
- Additional public folder trees

Data stores and storage groups

The ability to have multiple data stores and multiple storage groups is new in Exchange 2000's Enterprise version, so you need to evaluate whether you can use these features to your advantage. For example, Exchange 2000 allows you to have up to four storage groups, with up to five mailboxes of public folder data stores.

So should you use multiple data stores? Good reasons to do so include:

- Quicker restores.
- Specific policies for individual groups, such as different mailbox limits for different departments.
- Indexing for fast searches on one data store (e.g., public folders) but not on others (e.g., newsgroups).
- Different logging requirements on different data stores—for example, circular logging for newsgroups and full logging for mailboxes.

When you have identified the need for a new data store, should it be in the same storage group or a new one? Good reasons to create a new storage group are:

- Ability to have more than five data stores overall.
- Better security (data is more segregated).
- Simplified backup and restore. (NTBackup supports backup at the storage group level and supports simultaneous restores on storage groups.)
- Simplified management.
- Staggered or different backup routines and different policies on how long backups should be kept.

However, multiple storage groups do have some drawbacks. They require 50 MB minimum of disk space, plus a minimum of 10 MB RAM for each data store; this amount increases as the size of the data store increases. Because you should place associated transaction logs on different physical disks for other storage groups, this results in requirements for additional storage and disk protection.

Indexing

If you want to use indexing on any of your stores to speed up searches—public folder stores are a popular choice for full text indexing—make sure that you have sufficient disk space to accommodate the index. Microsoft says that an index typically requires 20 percent of the disk space occupied by the files to index. Remember, this space requirement will grow as the store grows.

Since indexes must be rebuilt to reclaim disk space previously occupied by deleted items, you'll need to schedule this routine maintenance task during quiet periods. Carefully plan when you want to rebuild and repopulate indexes. This process is CPU-intensive, so find a maintenance window when the server is needed less, perhaps overnight when you're not backing up or performing normal database defragmentation.

Note that you do not have to include provisions for indexing binary files and image files because these file types are not supported with indexing. There's conflicting advice on whether you should back up indexes. Many admins say this is a waste of time and resources, since a lost index can easily be rebuilt.

Hard disk storage

When it comes to protecting your servers' hard disk storage, the usual advice is to mirror the operating system and also to mirror disks that have transaction logs, keeping transaction logs separate from data stores. Use either RAID 1 or RAID 10 (mirror with stripe set) for better performance, and use a separate mirrored disk if possible for each transaction log. Use RAID 5 for the actual data stores. Again, employ one separate physical RAID array per store.

This is fairly standard stuff, but because the Enterprise version of Exchange 2000 supports multiple data stores and multiple storage groups (you can have up to 20 mailbox stores on one server instead of just one), you may need to increase your servers' hard disk capacity to accommodate the new configuration and keep the same level of redundancy and performance. Fortunately, hard disks are relatively cheap these days, but your servers' ability to physically accommodate them is another matter, so check this in advance when planning for multiple data stores or storage groups.

The general recommendation is to keep 50 percent of your available disk space free. If the disk space gets to less than 10 MB, Exchange 2000 will stop to ensure database integrity.

Policies

Decide in advance what system and recipient policies you want to put in place. Policies in Exchange 2000 are similar in concept to Active Directory Group Policies in that they let you specify a single configuration and apply it to multiple objects. For example, policies can be applied to multiple servers, public stores, and mailbox stores.

When you later change a configuration option within a policy, changes are automatically applied to child objects beneath the policy through natural inheritance. For example, you may define a mailbox store policy that gives all users a certain storage limit. You later add more hardware that will allow you to increase storage limits. You would have to define the option only once, and the configuration could take effect on all (or some, if preferred) of your servers.

Other commonly used policy options include maintenance settings for both public and mailbox stores, replication intervals for public stores, and message tracking for servers.

Delegating control

Decide in advance which of the three Exchange roles you want administrators to have:

- **Exchange Full Administrator** offers full control at the Organization level, including the ability to delegate control to others.
- **Exchange Administrator** offers the ability to fully administer Exchange at the given level but can't modify permissions or delegate control.
- **Exchange View Only Administrator** can view all configurations but is unable to modify anything. However, users with this permission can create a new mailbox-enabled user, a mail-enabled user, and a contact, if they can create a user in Active Directory—for example, if they are an Account Operator or are delegated access to a specific OU.

You typically would delegate control to Exchange administrators at the Administrative Group level. Note that Exchange Administrators can't create new users or give users Exchange mailboxes unless they also have the equivalent of Account Operator permission. Similarly, Account Operators can't create mailboxes or mail-enable users without also having the minimum of Exchange View Only Administrator permissions.

Once you have decided on the administration strategy you want to use, it's relatively simple to use the Delegation of Control Wizard in Exchange's System Manager; the process is similar to the Active

Directory Delegation of Control Wizard. The difficult part, as with Active Directory delegation, is in deciding which permissions to grant to your administrators.

Recipient Update Service (RUS) for multiple domains

RUS is used to update the Global Address List (GAL), new mailboxes, new address lists, and recipient policies. You must have one instance of the RUS configured for every domain that has recipients, even in domains that have no Exchange servers in them.

When you upgrade your first Exchange server to Exchange 2000, the process creates two default RUS services—one for your enterprise and another for the domain. To create another instance of RUS for additional domains, you'll need to first run the DomainPrep switch on a Windows 2000 server in the additional domain and then create a new RUS instance for each domain, specifying the Exchange server to run the service and a domain controller in that domain to use for recipient information.

Additional public folder trees

Although not accessible to MAPI clients, such as Outlook, this new feature in Exchange 2000 offers more flexibility in how publicly stored data is accessed, replicated, and viewed. For example, you could create a public folder tree that is visible only to a specific group or department to help ensure confidentiality and minimize confusion.

Additional public folder trees support deep searches through the entire tree and use Windows 2000 security permissions. They are also visible with Exchange 2000 Installable File System (IFS), NNTP clients, and through common Microsoft applications, such as Word. MAPI clients can access additional public folder trees if they view them as a Web page.

Ready to roll out

Of course, there's much more to configuring Exchange 2000 than I've covered here, but I've mentioned some of the key configuration issues you should consider when designing your upgrade strategy. These checklists should form the basis of a successful design plan to upgrade from Exchange 5.5 to Exchange 2000.