

Microsoft®  
**Exchange** 2000  
**Server**

**The Role of Groups and Access Control  
Lists in Microsoft Exchange 2000 Server  
Deployment**

Published: August 2000

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Outlook, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Table of Contents

Introduction.....	4
Overview of Groups .....	4
Exchange 5.5 Distribution Lists .....	5
Windows NT Groups .....	5
Exchange 2000 Groups .....	5
Windows 2000 Groups .....	5
Overview of Changes in Group Design.....	7
Migration Considerations.....	8
Windows Domain Considerations (Mixed Mode vs. Native Mode) .....	8
How the Active Directory Connector Works .....	9
Deploying Groups in Exchange 2000 Environments .....	9
Using Global Groups Instead of Universal Groups.....	10
How Token Augmentation Works .....	12
Best Practices .....	12
Limiting Membership in Universal Groups .....	12
Universal Security Groups with Mixed-Mode Membership .....	12
Trouble Spots .....	13
Sample Migration Scenarios and Topologies.....	13
Exchange Scenarios .....	13
Migration Topologies.....	15

# The Role of Groups and Access Control Lists in Microsoft Exchange 2000 Server Deployment

Published: August 2000

For the latest information, see <http://www.microsoft.com/exchange/>

---

## Introduction

Microsoft® Exchange 2000 Server is the only messaging system that is fully integrated with the Microsoft Windows® 2000 Server security model. This is the major difference between Exchange 2000 and earlier versions of Exchange. Exchange 2000 relies on Windows 2000 groups and the Active Directory™ directory service for access control and distribution tasks that, on servers running Microsoft Windows NT® version 4.0 and previous versions of Exchange, are separated from the operating system.

Because of this significant change, you should familiarize yourself with the differences between Windows 2000 groups, distribution lists in Exchange Server 5.5 and earlier, and Windows NT groups. With careful planning, you can migrate your existing Exchange distribution lists to the corresponding Windows 2000 groups. Familiarity with the various Windows 2000 groups enables you to convert Exchange distribution lists and retain their original functionality.

**Note** If you deploy in a single domain or if you deploy all Exchange servers in your company in the same domain with a multiple-domain environment, differences between the Windows 2000 groups are irrelevant. Group scopes and membership constraints across multiple domains are not concerns in a single domain environment.

## Overview of Groups

In most Exchange 5.5 environments, three groups exist: the distribution list and two Windows NT groups—domain local group and domain global group. Exchange 5.5 makes very little use of the Windows NT groups and relies heavily on the functionality of Exchange distribution lists for distribution and access control lists (ACLs).

Windows 2000 introduces an additional group—universal. It extends the capabilities of groups to include mail distribution in addition to their security functions. Exchange 2000 relies on these Windows groups for distribution and permission functions. A successful deployment involves converting Exchange 5.5

distribution lists to the appropriate Windows 2000 group without losing functionality.

## **Exchange 5.5 Distribution Lists**

Exchange 5.5 servers use distribution lists for two purposes:

- To distribute mail to a group of recipients
- To assign ACLs to public folders

Exchange 5.5 distribution lists can have mailboxes or other nested distribution lists as members.

## **Windows NT Groups**

Although Exchange 5.5 doesn't rely much on Windows NT groups, Windows NT nevertheless supports two types of groups—domain local and domain global. Both groups are security-related, and neither has e-mail functionality. These groups also exist in Windows 2000 with added mail functionality; they can associate an e-mail address with, that is, mail-enable, a group.

### **Domain Local**

Domain local groups permit membership from any trusted domain, but the scope is restricted to only the local domain. You can use a domain local group to assign permissions to a resource that exists in the same domain as the group. A group member from a trusted domain (outside the local domain) can then access the resource. For example, a resource exists in domain A and domain B is a trusted domain. You can use a domain local group to grant users from domain A and domain B access to this resource. However, you cannot use a domain local group in domain A to assign permissions to a resource in domain B, because domain local group scopes are valid only in the local domain, domain A.

### **Domain Global**

Domain global groups are limited to members in the local domain, but their scope is global. You can use a domain global group to grant local domain members access to resources on any domain. For example, the group exists in domain A; you can use a domain global group to grant access to users in domain A for a resource in domain B. However, you cannot grant users in domain B access to this resource, because domain global groups only grant membership to users in the local domain, domain A.

## **Exchange 2000 Groups**

Exchange 2000 relies entirely on Windows 2000 for both security and mail distribution groups. Exchange distribution lists no longer exist.

## **Windows 2000 Groups**

### **Group Types**

Windows 2000 supports both types of Windows NT groups and adds e-mail functionality to these groups. A major change in Windows 2000 group design is that groups can function as either security groups (as they do in Windows NT) or distribution groups (groups that are mail-enabled). All Windows 2000 groups can function as one or both of these types, but for a group to assign users permissions to access resources, it must be a security group.

### **Domain Local**

Domain local groups in Windows 2000 function the same as they do in Windows NT, except that in Windows 2000 you can have distribution groups as well as security groups. Groups with domain local scope have the following attributes:

- In a native-mode domain, groups can contain user accounts, global groups, and universal groups from any domain in the forest, as well as domain local groups from the same domain.
- In a mixed-mode domain, groups can contain user accounts and global groups from any domain.
- You can grant permissions to domain local groups only for objects in the domain in which the domain local group exists. You cannot grant permissions to network resources and public folders in other domains.
- You can convert a group to a universal group when it exists in a native-mode domain, provided there is not another domain local group nested inside.
- The group object is listed in the global catalog, but the group membership is not.
- Microsoft Outlook® users in other domains cannot view the full membership.
- Group membership must be retrieved on demand if expansion takes place in a remote domain.

### **Domain Global**

Domain global groups limit membership to the local domain in which the group resides, but they have global scope. Global groups can be referenced in ACLs on resources in any domain. Global groups permit one level of nesting. This means you can have global groups as members of a parent global group, but only if the member global groups do not have any global groups as members. Global groups have the following attributes:

- Global groups in native-mode domains can contain user accounts from the same domain and global groups from the same domain.
- Global groups in mixed-mode domains can contain user accounts from the same domain.
- You can grant permissions to global groups for all domains in the forest, regardless of the location of the global group.
- A global group in a native-mode domain can be converted to a universal group, if it is not a member of any other global group.
- Global groups can contain only recipient objects from the same domain.
- The group object is listed in the global catalog, but the group membership is not.
- Outlook users in other domains cannot view the full membership.
- Group membership must be retrieved on demand if expansion takes place in a remote domain.

## Universal Groups

Windows 2000 introduces a third group: the universal group. Universal groups behave most like Exchange 5.5 distribution lists. They have the following attributes:

- Universal groups in a native-mode domain can contain user accounts from any domain, global groups from any domain, and universal groups from any domain in the forest.
- Universal groups of the security type, called universal security groups (USGs), can be used only in native-mode domains; universal groups of the distribution type, called universal distribution groups (UDGs), can be used in mixed-mode and native-mode domains.
- You can grant permissions to universal groups for all domains in the forest, regardless of the location of the universal group.
- Universal groups cannot be converted to any other group scope.
- Outlook users in any domain can view full membership.
- Membership never needs to be retrieved from remote domain controllers.
- Membership modifications incur replication to the global catalog servers.

**Note** In a single domain environment or a deployment of all Exchange servers in the same domain, you do not need to use universal groups. This is because scope and membership across domains, which universal groups provide, is not necessary in a single domain environment.

### Uses for Universal Distribution Groups

Use UDGs in the same instances in which you used Exchange distribution lists in an Exchange 5.5 environment. UDGs can be used for e-mail distribution and are available on all domains and visible to all Outlook users. However, if your Exchange distribution list functioned as an ACL to a public folder, this group type is not appropriate. Only security groups can grant permissions to public folders, so you should use a security group.

### Uses for Universal Security Groups

USGs are the most like existing Exchange 5.5 distribution lists that are used as ACLs for public folders. Use a USG to assign permissions to a public folder and retain membership and scope throughout the organization. Although you can create a USG only in a native-mode domain, you can use a mixed-mode membership. A USG allows members from mixed-mode domains, so you do not have to upgrade your entire environment to use USGs.

## Overview of Changes in Group Design

The following table compares the groups used in Exchange 5.5 and Windows NT 4.0 to groups used in Exchange 2000 and Windows 2000. It shows the Exchange 5.5 or Windows NT group type, how it functions in Exchange 5.5 or Windows NT, and the type of membership it permits. The Windows 2000 analog shows the comparable Windows 2000 group and its functionality.

**Table 1 Comparison of Group Functions**

<b>Exchange 5.5 or Windows NT 4.0 group type</b>	<b>Function in Exchange 5.5 or Windows NT 4.0</b>	<b>Membership</b>	<b>Windows 2000 analog</b>
Exchange 5.5 distribution list	(1) E-mail distribution lists. (2) Used in ACLs on public folders.	A distribution list can have a mailbox from any site in the organization and it can also have another distribution list as a member. Nesting of distribution lists is not limited.	(1) UDG (for distribution lists). (1 and 2) USG (used as both distribution lists and as ACLs on public folders).
Domain local	Used in ACLs for resources that exist in the same domain as the group itself.	Domain local groups permit membership from any trusted domain. The scope of the group is restricted to the local domain. Domain local groups cannot be nested.	Domain local security group.
Domain global	Used in ACLs for resources on any domain.	Domain global groups permit membership from only the local domain, but they have a global scope. Global groups can have one level of nesting.	Global security group.

## Migration Considerations

### Windows Domain Considerations (Mixed Mode vs. Native Mode)

#### Groups in a Mixed-Mode Environment

Exchange 2000 requires at least one domain in native mode to support a mixed-mode organization. This is because, in mixed mode, the domain might contain Windows NT 4.0 domain controllers, and the domain is therefore restricted to supporting only the group types that Windows NT 4.0 supports—domain local and domain global. Specifically, this means that mixed-mode domains cannot support USGs. To implement universal groups, you need a domain in native mode, and you need to target that domain when you use Active Directory Connector (ADC) to export distribution lists from Exchange 5.5.

#### Groups in a Native-Mode Environment

In a native-mode environment, all group types are supported. If your organization has more than one domain, it is recommended that you use universal groups. As stated earlier, this group type most closely matches your Exchange 5.5 distribution list functionality. In a single domain, the differences

between the groups are moot. All users and all resources are contained in a single domain, so membership and scope outside of the domain are not an issue. You don't need to use universal groups in a single domain environment.

## How the Active Directory Connector Works

As stated earlier, universal groups play a special role for Exchange 2000. The ADC replicates all Exchange 5.5 distribution lists to Active Directory as UDGs in a native-mode domain. This group type was selected because the majority of distribution lists in Exchange 5.5 are only used as distribution lists, not in ACLs. This means that immediately after ADC replicates the Exchange 5.5 distribution lists to Active Directory, they can be used as e-mail distribution groups, but not to assign permissions in ACLs.

In general, this works well; however, public folders require special consideration.

### Groups and Public Folders

Exchange 5.5 public folders have ACLs, which should support membership from any domain. When public folders are replicated or upgraded to Exchange 2000, the corresponding ACL must be represented as a USG.

Not all Exchange distribution lists are used for setting permissions on public folders; only a subset of distribution lists is used. If all distribution lists were converted to USGs, replication traffic would increase unnecessarily. Therefore, Exchange 2000 is selective about converting UDGs to USGs and converts only those that are being used to grant permissions to public folders.

The conversion process occurs at three points:

- During upgrade from Exchange 5.5
- During public folder replication with Exchange 5.5
- Whenever a user defines permissions on an Exchange 2000 public folder and specifies a distribution group

**Note** If you are replicating from Exchange 5.5 to a mixed-mode domain, the ADC converts Exchange 5.5 global groups and you lose the ability to have membership outside the domain. To avoid this problem, use a group management domain in native mode (for more information on using a group management domain, see "Universal Security Groups with Mixed-Mode Membership" later in this article).

## Deploying Groups in Exchange 2000 Environments

The type and scope of the group that you use for Exchange 2000 depends on your business and user requirements. For full flexibility, implement USGs. Although a USG has a security group definition, you can make it mail-enabled by adding a Simple Mail Transfer Protocol (SMTP) address and you can view it in the global address list (GAL). You can create USGs only in native-mode domains, so you must designate at least one native-mode domain to use universal groups. You can change from mixed-mode to native-mode domains by upgrading the domain controllers to Windows 2000. Changing to native-mode domains eases the upgrade and deployment process for Exchange 2000 and provides additional directory scalability, but it is not a requirement for Exchange 2000 deployment.

**Note** If you are deploying in a single domain or if you place all Exchange servers on the same domain, you do not need to use universal groups. In a single domain, universal groups are not necessary because membership and scope across domains, which universal groups provide, are not needed.

When deploying universal groups, you should consider that their membership is listed in the global catalog servers, so any membership change causes replication traffic. Although Active Directory supports replication at the property level, the membership for a group is held in a multi-valued property on the group object. Since groups are in the global catalog, member changes cause replication traffic. One way to reduce replication traffic is to place user objects in other groups and nest these in umbrella universal groups. When the membership changes for a user in the group, the large universal group object—the umbrella group—is not changed and no replication traffic is created. Because universal groups have been used in this scenario, Outlook users can still view full membership of both the umbrella group and its subgroups. You can use global groups instead of universal groups. However, global groups do not have their membership listed in the global catalog servers, and this might affect the ability of an Outlook client to view membership at the recipient level.

When a message is sent to a group, the SMTP service must expand the membership of the group object. If it is a domain local or domain global group defined in the local domain, the membership list can be retrieved from any local domain controller. Additionally, if it is a universal group and users appear directly on the list, the membership can be obtained from any local global catalog server.

If a message is sent to a domain local or domain global group that has been created in another domain, or if a universal group contains global groups that are in other domains, there are two choices for expansion:

- Forward the message to the remote domain and let it expand there.
- Expand the message locally, but make direct Lightweight Directory Access Protocol (LDAP) calls to a domain controller in the remote domain to retrieve the membership. This implies that there is direct IP connectivity between the expanding server and the remote domain controller.

The disadvantage of the second method is that, depending on the speed of the network, remote retrieval might slow message delivery. If an Exchange server exists in the remote domain, it might be more efficient to set the expansion to that server instead of remotely retrieving the membership.

**Important** For a full discussion of expansion servers, read the article “Expansion Servers on Exchange 2000” elsewhere on this Web site.

## Using Global Groups Instead of Universal Groups

Exchange 2000 architecture is designed and tested to work best with universal groups. If you want to use global groups instead of universal groups, you must invest in additional planning, careful configuration of your environment, and potential policing of group usage.

**Note** Because ADC creates universal groups only in native mode, you need to create any global groups on Windows 2000 and replicate them back to Exchange 5.5 by using a two-way connection agreement.

### **Object Visibility vs. Membership Visibility**

Although the names of global group objects are replicated to every domain in a forest, the membership of global groups is visible only from domain controllers or global catalogs in the same domain as the group. This membership is not replicated to global catalogs outside of the home domain.

For example, if you create a global group in domain A, the group object and its membership are replicated in domain A, but only the group object (not the membership) is replicated to domain B.

### **Using a Global Group for Mail Distribution**

Routing and transport use a global catalog to resolve the addresses of users and groups. However, unless a global group resides on the same domain as the global catalog, the global catalog has no membership and is not able to resolve addresses.

For example, Exchange server 1 is using a global catalog from domain A. A user on server 1 sends mail to the global group on domain A. The transport mechanism on Exchange server 1 is able to read the membership of the group and successfully deliver the mail. Exchange server 2, however, is using a global catalog from domain B. If a user on server 2 sends mail to the same group (whose object name is replicated to domain B), the transport mechanism cannot read the membership of the group and deliver the mail.

### **Solution: Using an Expansion Server**

The problem of membership not being visible outside the home domain of a global group can be addressed by specifying an expansion server. If the specified expansion server uses a global catalog from the home domain of the group, the mail is delivered.

For example, the group in domain A is modified to specify server 1 as the expansion server. A user on server 2 sends mail to the group. The transport mechanism on server 2 is able to read the expansion server attribute and sends the message to server 1. Server 1 receives the mail being forwarded from server 2 for expansion. The transport mechanism reads the membership of the group and successfully delivers the mail.

For this process to work, you need to ensure that the Exchange server specified as the expansion server is using a global catalog that exists in the home domain of the global group.

### **Solution: Controlling Global Catalog Selection**

You can control global catalog selection by either of the following techniques:

- Ensure that your Exchange server is in the same Windows 2000 domain as the global group you want to use for mail distribution and that the Windows 2000 site does not contain global catalogs from any other domain.
- Use DSAccess registry keys to limit the list of global catalogs from which Exchange 2000 server selects.

## **Public Folders**

You can use global security groups to assign permissions to public folders in Exchange, but you must be careful. If you assign permissions to an Exchange 2000 folder by using a global group and replicate that folder outside the domain, when a user accesses that instance of the public folder, the permissions given to that group are not evaluated. The permissions are valid only in the domain of the global group.

## **How Token Augmentation Works**

When a user logs on to Windows NT or Windows 2000, the logon process creates a token. This token is used in access checks. In native mode, a user token contains all the security identifiers (SIDs) of the USGs to which the user belongs. In mixed mode, the token does not contain the USG SIDs. However, to support the interoperation of Exchange 5.5 and Exchange 2000, Windows 2000 has a mechanism to extend the token of the mixed-mode Windows 2000 user to include the USG SIDs. Distributed Authoring and Versioning (DAV), OLE DB, MAPI, and installable file system (IFS) augment the user token to include these SIDs. They also take into account whether the user is in a native-mode or mixed-mode Windows 2000 domain and whether a disabled user object is involved. Refer to "Trouble Spots" later in this article for more information about disabled user accounts.

## **Best Practices**

Best practices for deploying Exchange 2000 include:

- Designating a group management domain for mixed-mode deployment so you can use universal distribution and security groups instead of Exchange 5.5 distribution lists
- Using smaller groups when possible, either universal or global as members of universal groups

## **Limiting Membership in Universal Groups**

When you limit the membership of large universal groups to smaller universal groups—as opposed to individual user accounts—you can adjust the user accounts that are members of the larger universal group by adjusting the membership of the smaller groups that are part of the umbrella universal group. Because this does not directly affect the membership of the larger universal group, replication traffic is minimized. If you use global groups as members, no replication traffic is generated when membership changes. The disadvantage of using global groups is that their membership is not listed in the global catalog, so Outlook clients cannot view it.

## **Universal Security Groups with Mixed-Mode Membership**

A primary design goal of Exchange 2000 was to enable customers to proceed with Exchange 2000 deployment in advance of full conversion to Windows 2000 native mode across their domains. One way to mitigate the limitations of deploying in mixed-mode environment is to use a group management domain. You deploy one native-mode domain in your environment and then specify this domain in ADC connection agreements with Exchange 5.5 sites that use distribution lists.

As stated earlier, ADC converts Exchange 5.5 distribution lists to universal groups in native mode. Windows 2000 supports a USG that has member objects in mixed-mode domains (the USG itself must be in a native-mode domain). When a user logs on to a mixed-mode Windows 2000 domain, a token is constructed that contains the user object's SID and the SIDs of any global groups of which the user is a member. USG membership is evaluated only at logon and included in the token when the user object exists in a native-mode Windows 2000 domain.

When you use a group management domain, you make use of the functionality of native-mode Windows 2000 groups without affecting user authentication domains. When you upgrade the remaining Windows NT user domains to native mode, the universal groups created in the group management domain can be moved into that domain, and the group management domain can be removed from the topology.

## Trouble Spots

### Disabled User Accounts

If you deploy Exchange 2000 by using trusted domains, some instances occur in which the Exchange 2000 mailbox is actually a disabled user object and mailbox rights are assigned to a user object (or Windows NT 4.0 account) in a trusted domain. This complicates the token augmentation logic because the logic now needs to verify the presence of the Exchange Master Account SID attribute and acquire the corresponding disabled user object. This disabled user object becomes a member of USGs, not the trusted account. Thus, after the object is acquired, the augmentation logic can continue, adding to the token the SIDs of the USGs of which this disabled user is a member. In addition, when disabled users are used and the mailbox rights are assigned to a user in a native-mode domain, the *msExchAddGroupsToToken* attribute must be set to invoke the token augmentation logic.

## Sample Migration Scenarios and Topologies

The following sections contain examples of the appropriate uses for each group type based on a given set of criteria.

### Exchange Scenarios

**Requirement** Members of the sales team need to send e-mail to each other with lead information. All users are in the same domain.

**Solution** Create a group with type distribution and with global scope.

**Reasoning** Because all these members are in the same domain, you can use a global group. The purpose of the group is to enable members to send e-mail to each other, so access to network resources is not a consideration. It might be appropriate to create a security group now, so that the team can be given access to network resources and printers. This prevents having two groups with the same membership if requirements change in the future. The list is used only by members of the team in the same domain, so membership does not need to be retrieved from remote domain controllers.

**Requirement** The marketing employees in all corporate domains need access to an intranet Web site that contains upcoming sales events in the Toronto domain.

**Solution** Create a group with type security and domain local scope.

**Reasoning** Domain groups permit members from any domain. The permissions assigned to the upcoming sales event folder are valid only in the Toronto domain. This does not cause a problem because users can access only the Web site on this domain.

**Requirement** The global marketing unit wants to create a list so that anyone in the company can e-mail their team. Users do not need to know who is on the mailing list.

**Solution** Create a group with type distribution and with domain local scope.

**Reasoning** You cannot use global groups because the members of the group are in numerous domains. Because you do not need network access and you will not be publishing to the membership, you do not need to create a universal group. The marketing unit also experiences frequent changes to their group; therefore, it is not appropriate to create a universal group. However, to prevent membership from being remotely retrieved when a user in a remote domain sends a message to the group, the list is set to expand on a server in the domain in which the group is defined.

**Requirement** You must create a small, mail-based discussion forum for a new company product and give the team access to all Web sites and network shares that contain information about the product.

**Solution** Create a group with type security and with universal scope.

**Reasoning** Members of the discussion forum can be located anywhere in the world. Because there is a strong possibility that members are in different domains, it is necessary to use universal scope for the group. The team is quite small and membership is not expected to change frequently. Thus, it is appropriate to put the user membership directly in the universal group. This increases usability because members can see who is on the list before they send sensitive or confidential information. The group created is of the security type because network resource access is also a requirement. Note that the domain in which the universal group is created must be in native mode.

**Requirement** The corporate security team needs a bulk mailing list to send security announcements and important information to the entire company.

**Solution** Create a group with type distribution and with global scope in every user domain, and then nest these global groups in a universal group.

**Reasoning** Access to network resources is usually controlled per team or through the default access control entry, which grants permissions for users who have not been explicitly defined on the ACL. As a result, it is extremely unlikely that you need to grant permissions on network resources for these groups. Membership for this group changes rather frequently, making it inappropriate to populate full membership into a single universal group. When a membership change takes place, only the domain controllers in that domain

need to be updated with the modification. Global catalog servers do not have to replicate any data. It is extremely unlikely that a user will want to see the membership of this group. The global groups are nested in the universal group, so it is very easy for users to send e-mail to the entire company (if permissions allow) by using a single address instead of selecting each individual team or region. Another advantage of this method is that users can send e-mail to an individual group very easily.

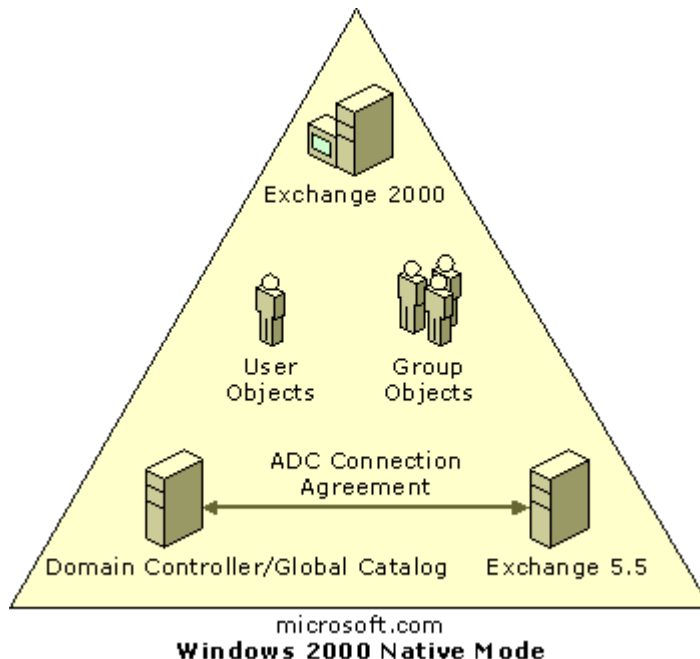
**Note** Domain local groups cannot be used in this scenario because they cannot be placed in universal groups.

## Migration Topologies

Five example topologies with brief explanations of their different components are shown in the following diagrams. These examples depict simple environments without multiple Windows 2000 sites, domain controllers, global catalogs, and so forth. The size and complexity of your current organization, coupled with business and functional requirements, should dictate the topology you choose as a model.

### Single Native-Mode Domain

An environment consisting of a single native-mode domain is the simplest topology to upgrade. With all user and group objects in a native-mode domain, Exchange is able to convert the UDGs into USGs. The token augmentation logic is not necessary (because the user's token already includes the USGs). A forest of multiple native-mode domains is a variation on this topology. In a single native-mode domain, a single ADC connection agreement exists between the Exchange 5.5 server and the domain controller/global catalog.

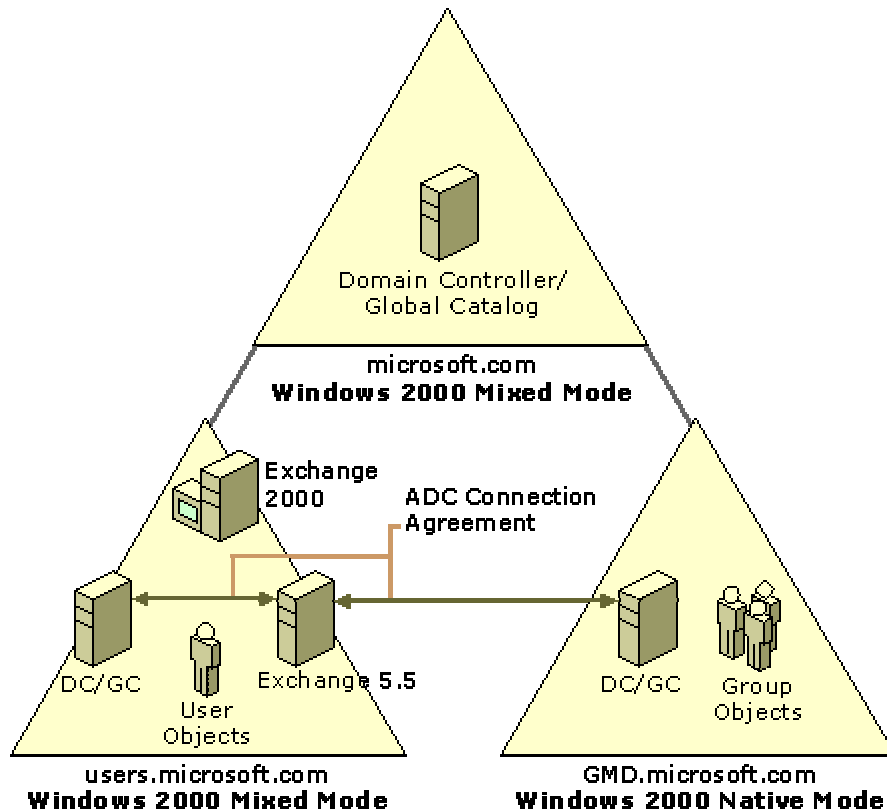


**Figure 1 Single Native-Mode Domain Topology**

### Group Management Domain

If your environment contains multiple domains, consider using a group management domain for your Exchange 2000 deployment. This topology provides

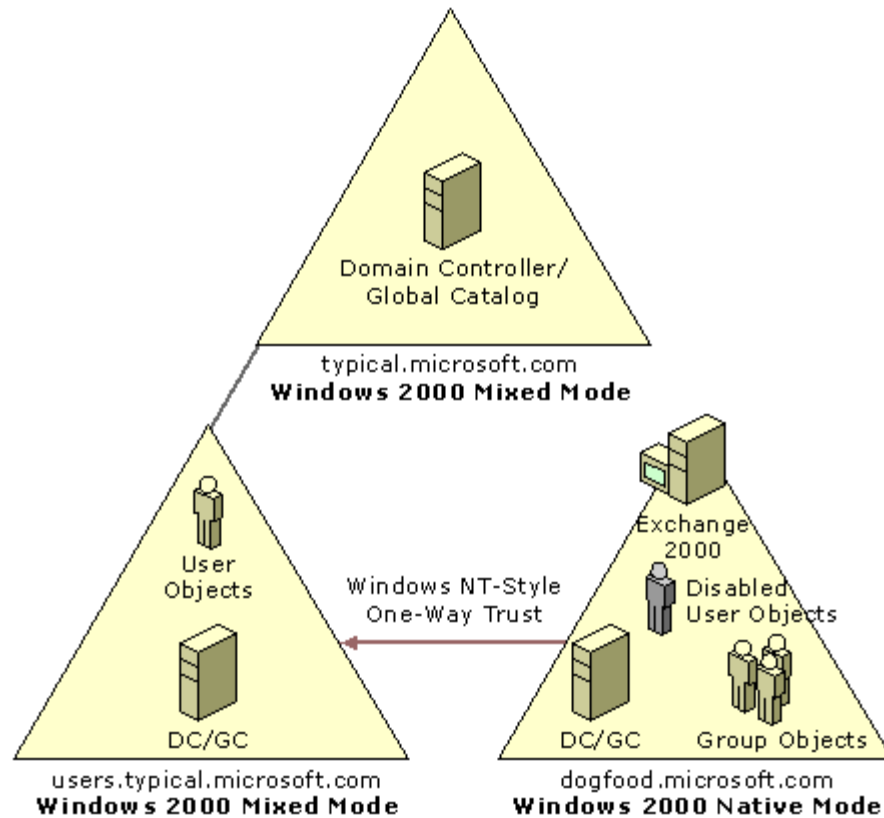
you with a path to Exchange 2000 that does not require that you wait until you have fully deployed Windows 2000 and enabled native mode on all your domains. The user objects and the Exchange servers can exist in mixed-mode Windows 2000 domains. As stated earlier, in order to have USGs, you must have at least one native-mode group management domain in the topology that is used to host groups. The token augmentation logic adds the SIDs of the USGs of which the user object is a member to the token prior to evaluation.



**Figure 2 Group Management Domain Topology**

### Trusts Spanning Forests

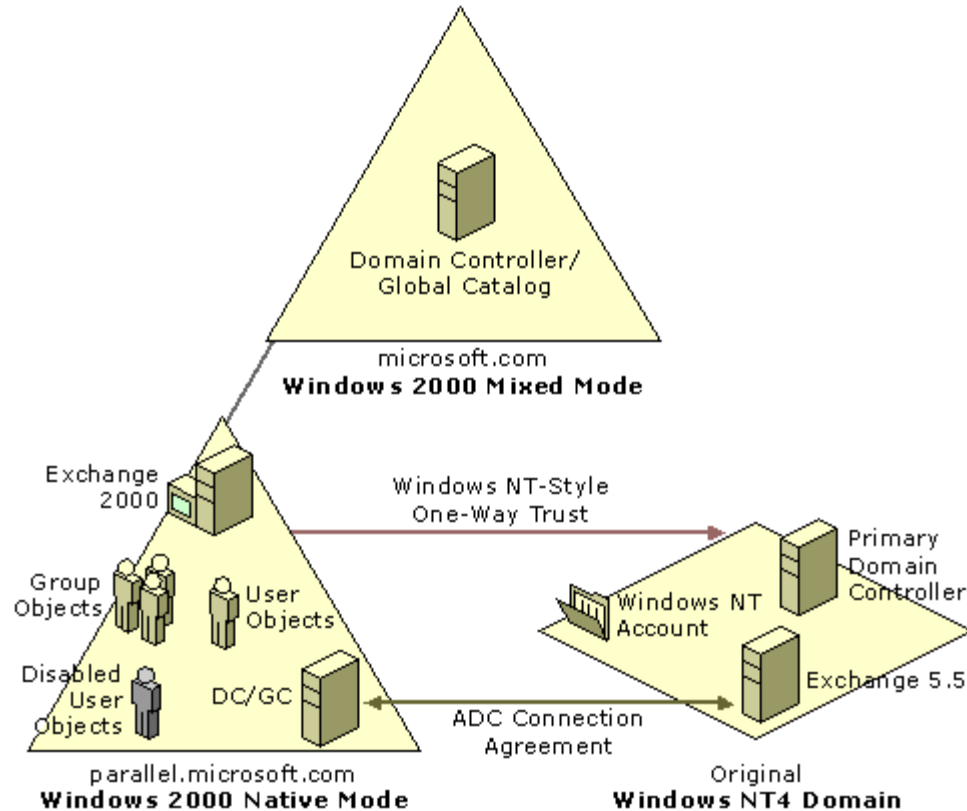
In a topology with trusts that span forests, you must consider the user who logs on with credentials from an explicitly trusted domain and accesses an Exchange 2000 server in a different forest. The result is an Exchange 2000 disabled user object that has mailbox rights assigned to an enabled user object in the trusted authentication domain. You use the Exchange Master Account SID attribute to handle this added level of complexity. The token augmentation code determines this situation, finds the corresponding disabled user object, and augments the token with the SIDs of the USGs of which that object is a member.



**Figure 3 Topology with Trusts Spanning Forests**

### **Windows 2000 Domains Trusting Windows NT 4.0 Domains**

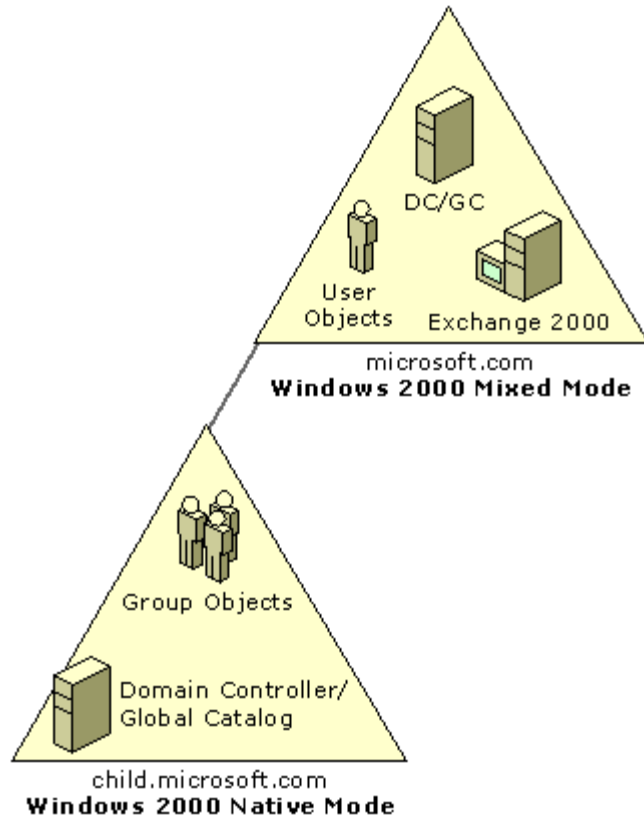
If your Windows NT 4.0 domain architecture is poorly designed, you should consider not upgrading it and instead deploying a pristine Windows 2000 environment parallel to your current environment, which trusts the original Windows NT 4.0 domains. This results in a situation in which a disabled user object in the domain with Exchange has mailbox rights assigned to a Windows NT 4.0 account in the trusted authentication domain. As in the preceding section, "Trusts Spanning Forests," you use the Exchange Master Account SID attribute to handle the added level of complexity, and the augmentation logic accounts for this.



**Figure 4 Parallel Windows 2000 Environment Trusting Windows NT 4.0 Domains**

### Testing Basic Token Augmentation Validation

To test basic token augmentation validation, remove all other variables involved with the previous scenarios from the topology, such as group conversions, different versions of Exchange, and public folder replication. In the test topology, deploy Exchange 2000 and user objects in a mixed-mode domain and create a child native-mode domain. Create a USG in the child domain and add a user from the mixed-mode domain as a member. Create a public folder in Exchange 2000 and assign permissions to the USG. Access the public folder from the user that you created. Successful test results show that token augmentation has added the SID of the USG to the user's token, thus enabling successful access. This eliminates the issues of Exchange interoperation, public folder replication, and group conversion, so you can test token augmentation without other factors interfering.



**Figure 5 Environment Trusting Windows NT 4.0 Domains**

