

The White Papers

Advanced Security and Directory Administration for Exchange 2000

by

**Dung Hoang Khac, Principal Consultant
Hewlett-Packard**

**Dave Champine, Group Product Manager
Microsoft Solutions, Quest Software**

**David Sengupta, Product Manager
Microsoft Solutions, Quest Software**

October 2002

Contents

<i>Abstract</i>	3
<i>Introduction</i>	4
Policy-based Management of Exchange Servers.....	4
Distribution of Configuration Policies	4
Resultant Set of Policies.....	5
<i>Managing Access Control</i>	6
Securing access	6
Delegating Administration	7
<i>Distributed Administration with Centralized Enforcement</i>	7
ActiveRoles Business Views.....	7
<i>Self-service Distribution Group Administration</i>	8
Self-service Attribute Management.....	9
<i>Conclusion: The Value of Directory-enabled Applications</i>	10
<i>About the Authors</i>	11
<i>About HP</i>	12
<i>About Quest Software</i>	12

Abstract

Companies running Microsoft® Exchange have very specific requirements for an optimized underlying directory. Both Exchange 5.5 and Exchange 2000 rely heavily on directory services for configuration, routing, addressing and security information – with Exchange 5.5 utilizing its own directory and Exchange 2000 using Windows® 2000/Active Directory®. This whitepaper discusses best practices for advanced security and directory administration for Exchange 2000. Its intended audience is both companies who have already adopted Exchange 2000 and those companies planning to migrate to Exchange 2000.

With a good understanding of corporate needs and with the right management and diagnostic tools, messaging managers can enhance security, reduce administrative effort and increase end-user productivity.

In most cases, additional hardware is not required and improvements take effect immediately. Companies using Exchange 5.5 can roll these best practices into their migration plan, while those already using Exchange 2000 can increase efficiencies and realize the value inherent in using directory-enabled applications such as Microsoft Exchange.

Advanced Security and Directory Administration for Exchange 2000

Dung Hoang Khac, Dave Champine, David Sengupta

Introduction

Policy-based Management of Exchange Servers

In order to facilitate consistent configuration management of distributed Exchange servers, Microsoft provides Active Directory Group Policy Objects (GPOs) that can apply to each server depending on its role in the infrastructure. At this point we should differentiate between GPOs and the new Exchange Policies such as the Mailbox and Server policies that were introduced in Exchange 2000. This article will only focus on GPOs.

In order to function properly, an Exchange 2000 environment relies on numerous correctly configured services. Administrators can secure their Exchange 2000 environment by minimizing the active services and protocols and restricting access to these to a minimum. Front-end Exchange 2000 servers are generally isolated in a De-Militarized Zone (DMZ) or at the perimeter of a secure network, while back-end mailbox and public folder servers generally reside within segmented private networks. Reducing the potential attack surface for those servers exposed to the Internet is core to achieving a secure messaging infrastructure. Maintaining consistent configuration of the servers throughout the corporate environment is essential in order to achieve operational efficiencies.

While policy objects provide an effective way to secure and administer Exchange 2000, managing all the policies associated with the variety of roles and functions in a given company can be a daunting management challenge. It is important to understand how and when policies are applied and how these policies interact. Creating and maintaining accurate documentation of policies is also critical, and documentation should be included in established corporate change control processes such as adding or moving servers or changing the features or role of a given server.

Distribution of Configuration Policies

As indicated in Figure 1 below, baseline policies for servers and domain controllers should be set at the domain level of the directory. Application servers (IIS, SQL, Exchange, etc.) should have policies: for example, “Disable Active Desktop” alongside file and print servers and other infrastructure servers. The group responsible for delivery of a particular service can then specifically manage the incremental policies for each application. Exchange servers should have policies defined for every different role (OWA Front-end server, Exchange Back-end server, public folder server, etc.). The creation of these policies can be an intensive exercise initially, but will provide the necessary discipline and systematic enforcement for the greatest possible security and operational efficiency.

Companies with multiple domains face an even greater challenge, as policies must be applied consistently across each domain. This ensures security and functionality throughout the Exchange infrastructure and across different administrative boundaries. Quest Software’s FastLane® ActiveRoles product provides an easy way to create policy templates that can be applied at any level of the directory and across multiple domains. This strategy provides an additional level of security, since creation of these policy templates can be restricted to a high-

efficient processing and security, the mailbox servers should not run services or expose communication protocols such as http, which are required on front-end servers.

Adding a new Exchange server in a policy-enabled environment requires testing to ensure security and service availability. Moving a server from one OU to another or from one domain to another could create a change in the resultant set of policies (RSOP). Changing the role of a server (IM, MIS, Conferencing, etc) can be facilitated with changes to policy templates, but the resulting role must be tested to ensure that the resultant set of policies matches the required functionality. In order to test the effects of these changes, ActiveRoles provides ActiveRSOP to predict the behavior of the proposed change before deploying it in production. Additionally, it provides the ability to roll back changes to a previous set of baseline policies.

Managing Access Control

A major advantage of Exchange 2000 over Exchange 5.5 is the ability to fine-tune very specific roles for system administrators, thus limiting access to extremely sensitive corporate information. The challenge for Exchange managers is that in many companies, a separate group maintains configuration and administration of Active Directory. It is critical that messaging staff receive proper access to maintain operational control of Exchange. Additionally, those directory entries common to both Exchange 2000 and Windows 2000 (users and groups) must be maintained in such a way that neither impacts the functionality of Exchange nor jeopardizes the security of the Windows infrastructure.

Securing access

Microsoft has outlined very specific permissions to be granted in Active Directory to effectively manage Exchange.² Given the distributed nature of Exchange 2000 and the high degree of integration with Active Directory, managing permissions can be very complex. Native tools for Active Directory management don't provide the ease of use and flexibility required by most companies. Virtually every configurable item in Exchange 2000 is described and accessed via Active Directory. Navigating through hundreds of objects and applying dozens of Access Control Entries (ACEs) for each administrator can take a significant effort. Human error or other failure to consistently apply these security settings leaves companies vulnerable to attacks or critical outages.³

To ensure consistent and efficient access control, it is necessary to use a tool such as ActiveRoles, which easily identifies critical objects and uses pre-defined or custom Roles to define rights using native AD Security. A *Role* represents a set of ACEs that can be applied to an Active Directory resource and then assigned to a specific user or group. ActiveRoles provides pre-defined Roles for every level of access defined in Microsoft's permissions whitepapers.

Additionally, ActiveRoles enables an administrator to create different collections of users, groups and computers regardless of their group membership or directory placement. These ActiveRoles *Business Views* – which essentially can contain many objects from across domains

² Microsoft's recommendations on Exchange 2000 permissions are available at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/deploy/depovg/exchperm.asp>.

³ More information on advanced security management in Active Directory can be found in the "Advanced Security Management of Active Directory in Windows 2000" white paper written by Quest Software and Hewlett Packard, available at <http://www.quest.com/requests/?RequestDefID=806>.

–enable the creation of new collections spanning multiple OUs. Since Business Views are native objects within Active Directory, they can then be used as a basis for delegated administration. This greatly simplifies delegation and solves the ‘one object, one location’ problem.⁴ Administrative tasks can then readily be delegated to departmental administrators or end-users – something previously restricted to Exchange administrators.

Delegating Administration

Exchange 2000 introduces the concept of administrative and routing groups. Whereas routing groups replace Exchange 5.5 sites, administrative groups are new and allow companies to isolate administrative and routing functions. This permits administrators to limit administrative access to certain servers or functions. While Exchange 5.5 effectively treated routing and administration as one function, Exchange 2000 administrative groups enable powerful delegation capabilities. In some cases, for example, it may be necessary to separate the Windows 2000 and Exchange 2000 administrative functions due to corporate structure or internal politics.

Additional delegation of some services can only be achieved by delegating specific permissions to other departments. For instance, a specific role could be assigned to helpdesk administrators which gives them permission to administer only mailboxes in a specific department – without permitting access to any of the sensitive Exchange configurations or even requiring an understanding of Exchange administration.

By maintaining mailbox information in Active Directory, helpdesk staff can manage a major subset of Exchange administrative tasks when given basic permissions to add, modify and delete user and contact objects (a contact is a directory entry which is mail-enabled but has no security credentials, similar to a custom recipient in Exchange 5.5). Exchange managers and administrators should, of course, be cautious when delegating even this simple task. Well-intentioned helpdesk staff may inadvertently modify SMTP aliases or other attributes critical to mail delivery. Many of these issues can be addressed by applying appropriate access control through specific roles, or through delegating administration at the attribute level. Ongoing controls are required to ensure compliance with corporate policies.

Distributed Administration with Centralized Enforcement ActiveRoles Business Views

Automating or delegating administration can be beneficial for Exchange administrators and end-users if done in a controlled and easy-to-understand manner. Ongoing distribution group administration, for example, can consume valuable administrative resources that could be better utilized elsewhere. Most users and companies are highly dynamic, so modeling all the possible scenarios could prove unwieldy. The fact that Active Directory only allows an object to be represented in a single OU also means that, by design, the Active Directory hierarchy cannot be used to model an individual with multiple responsibilities.

Let’s look at a simple example – a sales department that for some reason has to be distributed across many OUs and domains throughout the forest. Using ActiveRoles, the Role of a *sales administrator* could be applied once to a Business View containing user objects from each of these OUs and domains. Members of this Business View could then be delegated administration rights to manage the entire sales division.

⁴ Ibid., <http://www.quest.com/requests/?RequestDefID=806>.

Self-service Distribution Group Administration

Another way to increase the efficiency of administration in an Exchange 2000 infrastructure involves self-service distribution group administration. Essentially, “self-service” (or “subscription”) administration of distribution groups allows certain end-users to add or remove themselves from certain distribution groups. ActiveRoles provides a simple Web interface where subscribers can easily add or remove themselves from *subscribed* groups. This means that Exchange administrators or their delegates need only manage the remaining *assigned* distribution groups.

ActiveRoles provides several features that enable a self-service model similar to the one in our example. ActiveRoles allows administrators to assign each distribution group an ACE that identifies it as an *assigned* or as a *subscribed* distribution group. These are illustrated in the Table 1.

Type of group	Purpose	Examples
Assigned	Allows administrators to group users for security or other administrative reasons.	“Miami Office Users”, “First Floor Printer Users”
Subscribed	Allows administrators to create self-service groups to which users can subscribe at will.	“West Coast Sales Discussion”, “Chicago Sales”

Table 1: ActiveRoles® Assigned and Subscribed Distribution Groups

For example, let us say a sales person has recently been moved from Chicago to Los Angeles. In a self-service administrative model, the sales person could easily add him or herself to the “West Coast Sales Discussion” distribution group and remove him or herself from the “Chicago Sales” distribution group. Table 2 illustrates ACEs that would support such a self-service model.

Distribution Group Name	Access	Modified by
Chicago Sales	Subscribed	Sales
West Coast Sales Discussion	Subscribed	Sales
Softball Team	Subscribed	Everyone
Salary Review	Assigned	HR Admin
Companywide	Assigned	Exchange Admin

Table 2: Access Control Entries (ACEs) for Distribution Groups

This sales person, then, could end up with the following assignments and subscriptions:

Distribution Group Name	Effective Access
Chicago Sales	Not Subscribed
West Coast Sales Discussion	Subscribed
Softball Team	Not Subscribed
Salary Review	Not Assigned
Companywide	Assigned

Table 3: Example of Sales Person's Effective Access

In our example, the sales person is enabled to serve him or herself without any impact to the helpdesk or Exchange administrator. The company, in turn, achieves a cost savings from reduced administrative overhead and equips its sales force to adjust rapidly to changes in the marketplace.

ActiveRoles, then, provides flexible distribution group management, permitting both mandatory, *assigned* groups for administrative control and security and optional, *subscribed* groups for self-service administration. Companies employing a self-service distribution group management model benefit from the increased agility and reduced cost of this approach.

Self-service Attribute Management

End-users or departmental administrators can also be empowered to maintain individual attributes displayed in Address Lists (ALs) and the Global Address List (GAL). For example, if the “home phone number” and “address” attributes are populated in a company’s Active Directory, it makes sense for individual end users to manage these and keep them up-to-date. The telecom department, however, might want to manage the “business phone” and “cell phone attributes. Neither the end users nor the telecom department need to be given access to edit the entire Active Directory user object. It isn’t even necessary for them to have access to the Active Directory Users and Groups MMC snap-in. The ActiveRoles Web interface supports creation of roles for each group, permitting ongoing management that’s tailored to the needs of the particular division.

Each attribute in Active Directory can have an associated ACE identifying it as *assigned* or *modified*. End-users are assigned the role of attribute assignee (no attribute modification privilege) or attribute modifier (ability to modify an attribute) as explained in Table 4.

Type of Attribute	Purpose	Examples
Assigned	Attribute is fixed and cannot be changed by end users who have been designated an ‘attribute modifier’.	Display Name would likely be an <i>Assigned</i> attribute to ensure consistency throughout the company.
Modified	End users with ‘attribute modifier’ role can change the value of this attribute.	Home Phone Number would be a good example of a <i>Modified</i> attribute.

Table 4: ActiveRoles® Assigned and Modified Attributes

End users with the attribute modifier role can use the simple ActiveRoles Web interface to modify attributes identified as “modified.” The ActiveRoles Web interface is shown below.

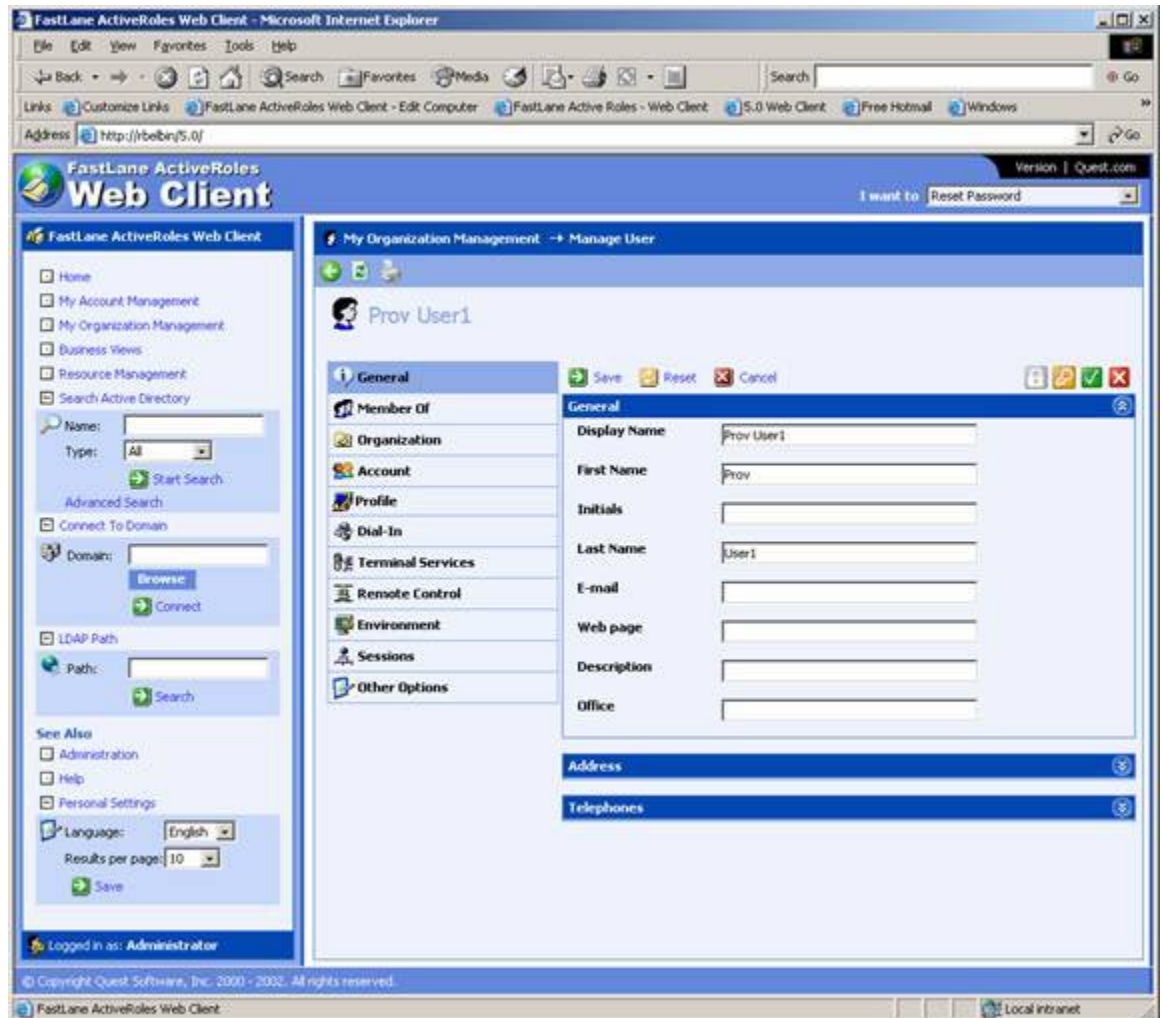


Figure 2: ActiveRoles® Web Client

Needless to say, the value of self-service attribute management is similar to that of self-service distribution group management. End users are empowered to respond rapidly to change and administrative overhead is reduced, resulting in greater agility, reduced cost and overall value to the company.

Conclusion: The Value of Directory-enabled Applications

Exchange 2000 provides significant opportunities for the creation of collaborative applications and for workflow automation. As third party and proprietary applications for Exchange 2000 continue to emerge throughout the marketplace, managing Active Directory security and administration is becoming mission-critical. In many companies, Active Directory is the central repository of critical attributes. Applications built around Exchange 2000 generally make very

heavy use of Active Directory and can only function properly if required attributes are fully populated, regularly updated and otherwise available.

Microsoft's Active Directory and Exchange 2000 provide the infrastructure for your company to easily create sophisticated applications and do business more effectively. The best practices discussed in this whitepaper illustrate just some of the reasons why security and directory management are critical to most companies using Exchange 2000 today. This whitepaper has demonstrated how messaging managers with a good understanding of corporate needs and the right needs can enhance security, reduce administrative effort and increase end-user productivity. Quest Software's FastLane ActiveRoles provides the tools you need to efficiently manage these critical components of your infrastructure and, as a result, the directory-enabled applications which rely on them.

About the Authors

Dung Hoang Khac works as a Principal Consultant in HP Consulting and Integration. Dung mostly deals with large customer Windows 2000 deployments and enjoys designing and implementing Windows 2000 infrastructure. Dung has been living and breathing Active Directory since 1999 and has wide experience in designing and deploying Active Directory in global enterprise environments. In addition to this whitepaper, Dung has co-authored various Windows 2000 migrations publications, is a contributor to the Exchange Administrator newsletter and regularly presents at Windows 2000 industry events. Dung recently moved from Europe to North America and is now based in Seattle, Washington.

Dave Champine is the Group Product Manager for Quest Software's Exchange solutions. Dave has more than 10 years experience as an IT director. Prior to Quest Software, Dave managed messaging and directory services at Citibank and Charles Schwab. He has participated in Microsoft's Joint Development Programs for Windows 2000 and Exchange 2000 and was an advisory board member for DEN (Directory Enabled Networks), co-sponsored by Cisco and Microsoft. Dave has been a featured speaker at Microsoft deployment conferences, Network/InterOp, messaging trade shows and has published and edited articles for Windows & .Net Magazine. Dave has a Bachelor of Arts Degree from Michigan State University.

David Sengupta is a Product Manager for Quest Software's Microsoft Infrastructure Management solutions. David focuses on products including Quest's Spotlight[®] on Exchange, MessageStats[™] and Quest Central[™] for Exchange. Prior to Quest Software, David was a senior architect/consultant with Qunara Inc. and previously held positions as Vice President of Information Services and Director of Knowledge Management at Zivex Technology Solutions.

David has worked with Microsoft Exchange since the Exchange 4.0 beta and has worked on various Joint Development Partner initiatives and partner advisory committees with the Exchange product group at Microsoft. David was granted the "Most Valuable Professional" award in the Exchange Server category for significant technical contributions to the international Exchange community from 1999 to 2002. He has contributed to various Exchange 2000 and Windows 2000 books, publications and white papers from Addison Wesley, Digital Press, Fawcette Publications, Microsoft and others. David frequently represents Microsoft, on staff, at "Ask-the-Experts," the "Microsoft Experts Area" and "Peer Talk" at conferences such as MEC and TechEd. In addition, Microsoft recently invited David to lead the development of a national training lab on Windows .NET Server 2003 and XML Web services for Microsoft and Intel. David holds a B.Sc. from the University of Ottawa, Canada and an M.T.S. from Tyndale Seminary, Canada.

About HP

HP is a leading technology solutions provider for consumers and businesses with market leadership in fault-tolerant servers, UNIX[®] servers, Linux servers, Windows[®] servers, storage solutions, management software, imaging and printing and PCs. Furthermore, 65,000 professionals worldwide lead our IT services team. Our \$4 billion annual R&D investment fuels the invention of products, solutions and new technologies, so that we can better serve customers and enter new markets. We invent, engineer and deliver technology solutions that drive business value, create social value and improve the lives of our customers. For more information on HP, visit www.hp.com.

HP ActiveAnswers: <http://activeanswers.compaq.com>

About Quest Software

Quest Software, Inc. (NASDAQ: QSFT) is a leading provider of application management solutions. Quest provides customers with Application Confidencesm by delivering reliable software products to develop, deploy, manage and maintain enterprise applications without expensive downtime or business interruption. Targeting high availability, monitoring, database management and Microsoft infrastructure management, Quest products increase the performance and uptime of business-critical applications and enable IT professionals to achieve more with fewer resources. Headquartered in Irvine, Calif., Quest Software has offices around the globe and more than 18,000 global customers, including 75% of the Fortune 500. For more information on Quest Software, visit www.quest.com.

Download a free trial of FastLane ActiveRoles: <http://www.quest.com/fastlane/activeroles>

Download **Advanced Security Management of Active Directory in Windows 2000**:
<http://www.quest.com/requests/?RequestDefID=806>



Quest Software, Inc.
8001 Irvine Center Drive
Irvine, CA 92618
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000



Hewlett-Packard
3000 Hanover Street
Palo Alto, CA 94304-1185
www.hp.com
(650) 857-1501

All content Copyright© 2002, Quest Software, Inc. and Hewlett-Packard Corporation. The information in this publication is furnished for information use only and is subject to change without notice. Neither Quest Software, Inc. nor Hewlett Packard Corporation assume any responsibility or liability for any errors or inaccuracies that may appear in this publication. FastLane and Spotlight are registered trademarks of Quest Software, Inc. FastLane ActiveRoles, FastLane Reporter and MessageStats are trademarks of Quest Software, Inc. Microsoft, Windows and Active Directory are registered trademarks of Microsoft Corporation. Other product or company names mentioned herein may be the trademarks of their respective owners.