

## *Microsoft Exchange Server 2010: Best Practices*

*Written by  
Missy Koslosky, Sr. Exchange Engineer and  
Ron Robbins, Sr. Product Manager Migration,  
Quest Software, Inc.*



White Paper

## © 2009 Quest Software, Inc. All rights reserved.

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

## WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

## TRADEMARKS

Quest, Quest Software, the Quest Software logo, AccessManager, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BusinessInsight, ChangeAuditor, DataFactory, DeployDirector, DirectoryAnalyzer, DirectoryTroubleshooter, DNS Analyzer, DSExpert, ERDisk, Foglight, GPOAdmin, iToken, I/Watch, Imceda, InLook, IntelliProfile, InTrust, Invirtus, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogADmin, MessageStats, Monosphere, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportADmin, RestoreADmin, SelfServiceADmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL LiteSpeed, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer Pro, vPackager, vRanger, vRanger Pro, vSpotlight, vStream, vToad, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, Vizioncore vTraffic, Vizioncore vWorkflow, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters  
5 Polaris Way  
Aliso Viejo, CA 92656  
[www.quest.com](http://www.quest.com)  
e-mail: [info@quest.com](mailto:info@quest.com)  
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

September, 2009

# CONTENTS

<b>INTRODUCTION</b> .....	<b>5</b>
<b>EXCHANGE SERVER 2010: WHAT'S NEW</b> .....	<b>6</b>
ANYWHERE ACCESS .....	6
<i>Outlook Web Access</i> .....	6
<i>Windows Mobile</i> .....	7
PROTECTION AND COMPLIANCE.....	7
<i>Personal Archive</i> .....	7
<i>Multi-Mailbox Search</i> .....	8
<i>Information Rights Management</i> .....	9
<i>MailTips</i> .....	9
<i>Message Transport Rules</i> .....	9
<i>Active Directory Rights Management Services</i> .....	10
FLEXIBILITY AND RELIABILITY .....	10
<i>Storage Options</i> .....	10
<i>Clustering with Database Availability Groups</i> .....	11
<i>Mailbox Moves</i> .....	12
<b>BEST PRACTICES: PLANNING AND PREPARING FOR YOUR MIGRATION</b> .....	<b>13</b>
UNDERSTANDING AND DOCUMENTING YOUR CURRENT ENVIRONMENT.....	13
<i>Network</i> .....	14
<i>Windows and Active Directory Infrastructure</i> .....	15
<i>Current Exchange Infrastructure</i> .....	18
<i>Other Messaging Systems</i> .....	21
<i>Third-Party Tools and Utilities</i> .....	22
ARCHIVING TO HELP SMOOTH MIGRATIONS.....	24
PUBLIC FOLDER CONSIDERATIONS.....	25
<b>PLANNING AND PREPARING FOR YOUR MIGRATION WITH QUEST TOOLS</b> .....	<b>26</b>
QUEST MESSAGESTATS.....	26
QUEST ARCHIVE MANAGER.....	26
QUEST PUBLIC FOLDER MIGRATOR FOR SHAREPOINT .....	27
<b>BEST PRACTICES FOR MIGRATING TO EXCHANGE SERVER 2010</b> .....	<b>29</b>
MIGRATING WITH NATIVE TOOLS .....	30
<b>MIGRATING WITH QUEST TOOLS</b> .....	<b>31</b>
<i>Migrating from Exchange 200x to Exchange 2010</i> .....	31
<i>Migrating from IBM Lotus Notes to Exchange 2010 or Exchange Online</i> .....	32
<i>Migrating from Novell GroupWise to Exchange 2010</i> .....	32
<i>Migrating from Exchange 5.5 to Exchange 2010</i> .....	32
<i>Tracking</i> .....	33
<b>BEST PRACTICES FOR MANAGING EXCHANGE SERVER 2010</b> .....	<b>34</b>
ADMINISTRATION AND PROVISIONING .....	34

PERFORMANCE AND AVAILABILITY.....34  
COMPLIANCE AND SECURITY .....35  
**CONCLUSION..... 37**  
**ABOUT THE AUTHOR..... 38**  
**ABOUT QUEST SOFTWARE, INC. .... 39**  
    *Contacting Quest Software.....39*  
    *Contacting Quest Support .....39*

# INTRODUCTION

With the release of Exchange Server 2010, Microsoft has expanded existing functionality and introduced new concepts. Exchange Server 2010 still provides organizations a robust messaging and collaboration platform while continuing to broaden their focus to enhance the feature set. Exchange Server 2010 provides three high-level benefits:

- Anywhere Access
- Protection and Compliance
- Flexibility and Reliability

These features were designed to meet the needs of today's mobile workforce, help organizations protect and retain information according to policy, as well as ensure that e-mail services are available at all times.

Organizations that consider adopting Exchange 2010 will need to weigh its benefits against the costs and complexities of managing it. This white paper describes the new features of Exchange Server 2010 and discusses best practices for migrating to and managing this unified communications foundation.

# EXCHANGE SERVER 2010: WHAT'S NEW

Exchange Server 2010 provides three high-level benefits:

- Anywhere access
- Protection and compliance
- Flexibility and reliability

## **Anywhere Access**

Today, e-mail needs to be accessible from any location as end users are no longer tied to a single desktop computer that is used only during the work day. Microsoft considered this when designing Exchange 2010, and has made accessing and manipulating messaging data easier than ever.

## **Outlook Web Access**

Internet-based e-mail access has been common for many years; in Exchange Server 2010, Outlook Web Access (OWA) has evolved. It now looks and feels like the standard Outlook client. The much-improved conversation view in OWA provides a quick way to browse through a thread of messages without having to change the focus to each individual message. This is a significant improvement over the threading capabilities in Microsoft Office Outlook 2007 that is on par with the conversation view in Microsoft Office Outlook 2010. Messages in a single conversation are included in the consolidated conversation view even if the message is held in another Outlook folder; messages that a user has sent to a thread are automatically displayed in the conversation view, even though the message itself resides in the Sent Items folder.

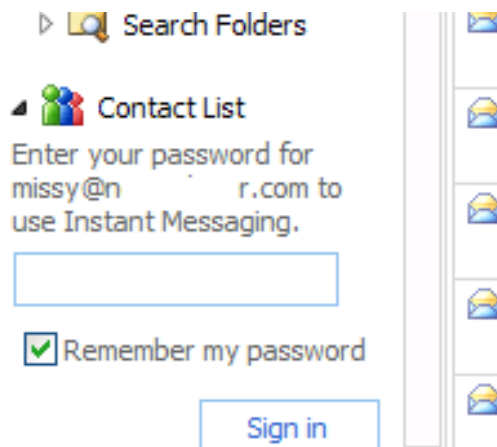
Although many organizations use Internet Explorer as the standard Web browser, some users may have a preference for a different one or use a computer that does not have Internet Explorer installed. Microsoft designed the latest version of OWA to operate with Firefox v3 and higher and Safari v3 and higher equally as well as it does with Internet Explorer 7 and higher. This allows users to have a consistent browsing experience across all major browsers.

The newest version of OWA includes many other useful features. The nickname cache provides users with a familiar drop-down listing of possible name matches as they type a name or e-mail address into the To, Cc, or Bcc fields of a message. Searches have more flexibility, and users can filter searches quickly by typing qualifiers directly into the search field using an easy-to-understand format. For example, to search for messages with the word "operations" in the Subject field, you simply type subject:operations in the search box.

In addition, one limitation of earlier versions of OWA is now removed: previously, you could view only a limited number of messages in a folder before having to click to view the next page of message. OWA 2010 presents

all messages in one view, enabling users to scroll through all of the messages in a folder without paging.

OWA 2010 also offers new integration points with other technologies. Short message service (SMS) text messages can now be sent directly through OWA. Incoming text messages can appear in a user's mobile device as well as the user's Exchange Inbox. Microsoft Office Communications Server (OCS) can be integrated with OWA, as shown in Figure 1, to enable instant messaging conversations and indicate presence information from the OWA client without the need for the Microsoft Office Communicator client to be installed on the computer.



**Figure 1: OCS Integration with OWA 2010**

## Windows Mobile

Anywhere access is also enhanced by functionality that allows mobile device users, including those with Windows Mobile 6.1, to access messaging data; Outlook Mobile is being updated to include the features available in Windows Mobile 6.5. The conversation view available in Outlook 2010 and OWA 2010 is also available in the latest version of Outlook Mobile, making it easier to triage message threads. Free/busy calendaring information for users within an organization can be obtained through Outlook Mobile, simplifying the process of scheduling meetings from mobile devices.

## Protection and Compliance

The protection and compliance features of Exchange 2010 help organizations achieve regulatory compliance and ensure that end users use and send messaging data according to policies.

## Personal Archive

Organizations are more concerned with regulatory compliance, and Microsoft has responded by introducing a personal archive with Exchange Server 2010. This new capability is useful for organizations that are comfortable allowing their users to manually classify, retain, and manage their messaging data for longer-term retention. However, the archive does not capture all of the information necessary to meet many regulations. Many organizations will

need a more robust archive; there are many third-party products that provide additional functionality for archiving and discovery.

There are several points to remember when deploying the personal archive in Exchange 2010. The archive is easily accessible, since it appears as an additional top-level hierarchy in a user's messaging client (much like a PST file). But it cannot be synchronized as an OST file, and is inaccessible without Internet access. The personal archive must be stored in the same mailbox database as the user's primary mailbox; this means that data cannot be stored on the less expensive storage media that is used for a traditional mailbox database.

The personal archive can be used as a repository for historical data that was previously stored in PST files, which are inherently insecure and can be unreliable. Users can drag and drop data from PST files into the personal archive, but there is no way to automate this process or ensure that all data within PST files has been moved into the archive. Once users have moved their PST data into the personal archive, there is no way to save disk space by deleting the original PST files. Also, no reporting is available to track how much or what data was captured from each PST file. Therefore, during regulatory compliance or legal motions, administrators or compliance officers might have to search the online databases, as well as manually track down users' PST files, open each file, and perform keyword searches against each individual file – a time-consuming and frustrating process.

Exchange administrators can define retention policies for entire archive mailboxes, as well as specific archive mailbox folders, and items within the personal archive. Once the retention period has passed, messages are automatically deleted from the archive. Administrators can also create policies that automatically move messages from users' primary mailboxes into their archive mailboxes. Messages that are subject to retention policies will display an additional header that explains the policy's settings and the message's scheduled deletion date. Users are able to apply a new expiration date to the items that are set for deletion; however, this could be a problem if messages need to be retained longer than the organization has defined. Legal hold is available to ensure that pertinent messages are not deleted during an active investigation.

## **Multi-Mailbox Search**

One of the most useful features of Exchange Server 2010 is the multi-mailbox search, which allows users with appropriate permissions to search the entire organization for messages containing specific keywords or characteristics. For example, an administrator could easily search for all messages from a particular user to the CEO. This capability is designed to simplify e-discovery. However, it can also be helpful in other situations, such as when confidential information has been leaked from an organization or a new virus is spreading; administrators or other named parties can easily search for information and extract the results to a mailbox for inspection. Unfortunately, search results cannot be exported directly to a PST file; administrators or compliance officers need to manually export the search results to a PST file when they need to provide search results to others.

## Information Rights Management

Preventing information leaks has become a concern for many organizations. In Exchange Server 2010, Microsoft has improved some of the mechanisms in Exchange Server 2007 and introduced new ways of protecting messaging data.

Information Rights Management (IRM), which restricts access and makes data accessible only to specifically named parties, has been expanded to work with Outlook Web Access (OWA) in addition to the Outlook client. This enables users to create and access messages that have been protected using IRM, even when they are not at their workstations. The rich OWA client, including IRM support, works not only in Microsoft Internet Explorer, but also in Apple Safari and Mozilla Firefox browsers.

Many organizations are attracted to the idea of encrypting specific data using IRM but are concerned about the long-term ramifications, since encrypted messages cannot be read easily by anyone other than the sender and the intended recipients. Accordingly, Microsoft enabled the Exchange 2010 transport agents to decrypt messages for inspection by anti-spam and anti-virus programs when they are being bifurcated and sent to the message journaling mailbox.

## MailTips

MailTips is sure to be a popular new feature especially with end users who have made the mistake of sending a message to a large distribution group instead of a few recipients. MailTips is based on a simple idea: giving users hints about what they are about to do before a message is actually sent. MailTips includes preconfigured options and can also be tailored by the user; for example, the user can change the number of recipients in a distribution list that will result in the presentation of a MailTips hint. One of the most useful features of MailTips is that it indicates when intended recipients of a message have their Out of Office (OOO) message set; a preview of the OOO is even displayed in the draft message to enable the sender to re-address the message more appropriately.

While MailTips is not natively supported by Outlook 2007, a plug-in is available to extend MailTips to this legacy client. Both the Outlook 2010 client and OWA 2010 include native support for MailTips.

## Message Transport Rules

Microsoft keeps making huge strides in message transport rules; these rules continue to become more flexible and meet more diverse criteria. The standard transport rules have been expanded to cover additional message characteristics, such as information from a user's Active Directory account. For example, rules can be created to block, IRM-protect, or force moderation of messages from a group of users (such as the Marketing department) to a specific domain or e-mail address. They can also scan messages (including those with any Microsoft Office-based attachments) for certain keywords or phrases and then take specific action against those messages, such as sending the message to a supervisor for moderation. When moderation is

chosen, the moderator can approve a message for delivery or block the message from being delivered to its original recipient and optionally provide an explanation about the blocking to the author of the message.

## **Active Directory Rights Management Services**

With Windows Server 2008, Active Directory Rights Management Services (AD RMS) become much simpler to deploy and manage, and AD RMS is well integrated into Exchange 2010. The new transport protection rules can apply AD RMS templates to messages (and attachments) without the need for end users to get involved in the decision-making process. Just a few AD RMS templates are included with Exchange 2010, and the "Do Not Forward" template will likely prove to be the most popular. When the "Do Not Forward" template is applied to a message, the recipient can perform only limited actions on the message. For example, recipients can be prevented from printing or copying message data; this provides an additional measure of protection for organizations that are concerned about information leaks.

### **Flexibility and Reliability**

In addition to enhanced anywhere access and protection and compliance, Exchange Server 2010 also offers improved flexibility and reliability. Keeping messaging data available at all times has become a necessity for most organizations, and it is a big focus for Microsoft in Exchange 2010. The new clustering functionality in Exchange 2010 is a giant leap forward from the continuous clustering options available with Exchange 2007, and light years away from the single copy clustering available in Exchange 2003 and earlier versions.

## **Storage Options**

With 32-bit versions of Microsoft Exchange Server (i.e., Exchange Server 2003 and earlier versions), using a storage area network (SAN) for data storage was often the optimal solution. When Exchange Server 2007 was introduced, the expanded application access to memory provided by the 64-bit platform reduced disk I/O by up to 70 percent,<sup>1</sup> so the disk subsystem was no longer a bottleneck in Exchange environments. With Exchange 2010, disk I/O is further reduced. Microsoft put a lot of effort into reconfiguring the database structure, and the result is impressive: disk I/O is reduced by up to 50 percent of Exchange 2007 levels, which is a reduction of up to 85 percent from Exchange 2003 levels. Microsoft began recommending the use of direct attached storage (DAS) for Exchange data with the introduction of Exchange 2007 and continues to do so with Exchange 2010.

With Exchange 2010, there is no need to use an expensive SAN to hold messaging data. Exchange 2010 was designed to work well with desktop-class disks, such as serial advanced technology attachment (SATA) disks. Disk writes do not come in bursts with Exchange 2010, which enables SATA disks to easily support the messaging infrastructure's storage needs.

---

<sup>1</sup> <http://technet.microsoft.com/en-us/library/bb738147.asp>

Although using a SAN for Exchange-related storage is not prohibited, it seems like overkill, since Exchange 2010 can perform consistently and reliably on less expensive storage.

Microsoft has long recommended specific RAID configurations for Exchange Server implementations: RAID 10 (mirroring plus striping) or RAID 5 (striped with parity) for the mailbox databases, and RAID 1 (mirroring) for the transaction logs. But with Exchange Server 2010, RAID configuration is no longer necessary because database availability groups (DAGs) (a new type of continuous clustering introduced in Exchange 2010) provide enough redundancy that disks become disposable. If a disk fails, the mailbox database can switch over to another DAG instance, and administrators can simply pull the disk, replace it, and rebuild the database instance. Therefore, Exchange 2010 can use just a bunch of disks (JBOD) for storage, eliminating the need for RAID configurations.

## **Clustering with Database Availability Groups**

Clustering Exchange 2003 and prior versions was a complicated process that didn't offer a lot of protection against serious failures in the environment. It has long been believed that the administrative complexity of early Exchange clusters led to at least as many data outages from human error as organizations would have experienced without clustering. Continuous replication clustering technologies were introduced in Exchange 2007, removing much of the complexity of managing clustered Exchange servers. The legacy method of clustering, single copy clustering (SCC) did not provide a second copy of the mailbox databases; continuous clustering created additional copies of each storage group and kept the copies up to date by using log shipping.

With the introduction of the DAG, Exchange 2010 has gone beyond the initial promise of continuous clustering and finally offers a solid clustering solution that provides a level of assurance that has too long been absent from Exchange Server. A DAG is a set of up to 16 Exchange 2010 servers assigned the Mailbox role, where each server that is a member of the DAG can contain a copy of the mailbox databases assigned to that DAG. Initial database instance seeding is done through ESE (the database technology behind the Exchange database itself) streaming, and each database instance is kept up to date through log file shipping using TCP raw sockets. Interestingly, databases are no longer designated as belonging to a specific Exchange server instance; instead, each database is managed on the organizational level as an independent object.

Microsoft also eliminated storage groups in Exchange 2010. One reason was because of the aggregation of transaction log files for a storage group in a single folder hierarchy. With the DAG, storage groups and their associated combined transaction logs could have complicated database failover, so Microsoft chose to simplify the architecture to allow quick recovery and return to operations.

All clustering in Exchange 2007 uses the DAG architecture, which replaces all of the clustering types available in Exchange Server 2007, including cluster continuous replication (CCR), local continuous replication (LCR), standby

continuous replication (SCR), and SCC. Some organizations have expressed dismay that SCC has been discontinued; they are often using SAN replication technology to replicate the single database copy used by SCC to a remote location for disaster recovery purposes. Although the DAG technology provides better, more reliable service, there seems to be a general feeling that if they were to use the native Exchange clustering available in 2010 they would lose the significant investment they made in the SAN and associated replication technology. In reality, if the DAG is implemented with DAS or JBOD, the SAN can be repurposed to serve applications that do not natively provide high availability configurations, and Exchange 2010 can be deployed using much less expensive storage technologies.

One of the most impressive characteristics of the DAG architecture is that DAGs can be created on the fly; there is no need to commit to DAG membership during the installation process. If there is more than one Exchange 2010 mailbox server running with live mailboxes, a DAG can be created with ease and the existing mailbox databases can be assigned to it. DAGs can easily span sites to provide geographic clustering without any special configuration, eliminating the tedious configuration process required with earlier releases of Exchange clustering.

A few additional items of note: the client access server (CAS) and hub transport server (HUB) roles can be co-located on servers that joined to a DAG, and public folder replication is incompatible with the replication technology used by the DAG. Public folders being replicated from servers that are members of a DAG should be isolated.

Some people support the idea of going without backups, since DAGs can be configured to lag log file replay and can provide point-in-time restores. While the DAG architecture provides more mailbox database protection than was previously available, making regular, quick volume shadow copy service (VSS) snapshots of the databases should still be considered a best practice.

## **Mailbox Moves**

Moving users from one Exchange Server to another has always involved disconnecting them from their mailboxes for the duration of the moves; for this reason, mailbox moves have traditionally been done during maintenance windows or carefully coordinated with all users whose mailboxes are being moved. Exchange 2010 introduces online mailbox moves: users can remain connected to and active within their mailboxes throughout the mailbox moves. Online mailbox moves are possible only when moving users from one Exchange 2010 server to another; users with mailboxes being moved to or from Exchange 2007 or Exchange 2003 will still be disconnected during the mailbox move process (note that Exchange 2003 must co-exist with Exchange 2007 servers for co-existence with Exchange 2010). Online mailbox moves are called through the New-MoveRequest PowerShell cmdlet, while standard mailbox moves continue to use the Move-Mailbox PowerShell cmdlet.

# BEST PRACTICES: PLANNING AND PREPARING FOR YOUR MIGRATION

Organizations move to Exchange 2010 for a variety of reasons: to take advantage of the new features described above, to consolidate and reduce the number of servers in your organization, to replace a version of Exchange Server that is no longer supported, to replace a different messaging system (such as Lotus Notes or Novell GroupWise), or to move to an Exchange Online solution. But regardless of the reasons for your migration, careful planning and preparation are crucial to the success of your project.

If you have Exchange Server 2007 deployed today and are happy with your current environment, your planning process may be as simple as determining which hardware to purchase for your servers and storage. Once you've decided on the appropriate hardware, you simply deploy the hardware, and then move mailboxes and replicate public folders between the servers.

If you are unhappy with your current Exchange 2007 deployment, or have an Exchange 2003 (or earlier version, or a non-Exchange based) environment, the planning process is more complex. For pre-Exchange 2007 environments, special care needs to be given to the routing environment; Exchange 2010, like Exchange 2007, relies upon the Active Directory Sites and Subnets configuration for routing, instead of the routing groups used by Exchange 2000 and Exchange 2003.

In general, the following steps are critical to the pre-migration process:

- Conduct a thorough discovery and analysis of your current environment
- Archive older, rarely accessed data from active mailbox databases to a secure, reliable messaging archive before the migration
- Carefully analyze public folders to determine which data is an appropriate fit for Microsoft Office SharePoint Server (MOSS)

The following sections provide recommended best practices for each of these steps.

## **Understanding and Documenting Your Current Environment**

While some organizations are meticulous about documenting their environments over time, many more neglect documentation. Sometimes it is because they are busy putting out fires or they feel documentation is unnecessary or too tedious to bother with. But accurate documentation is critical to good migration planning, and ensures that knowledge about the environment (such as how things are configured and why certain design and configuration decisions were made) is not lost when due to staff turnover.

Best practices for documenting your environment include careful examination of the following:

- Network

- Windows and Active Directory infrastructure
- Exchange infrastructure
- Other messaging systems
- Third-party tools and utilities

## Network

Even little things about the underlying network can have a big impact on Exchange Server. For example, a network interface card (NIC) set to auto detect the network speed instead of to a static value can prevent Outlook clients from connecting to the Exchange server consistently. While cached mode in later versions of Outlook has reduced the impact of this type of configuration, tracking down this type of issue can be time-consuming and unintuitive. Therefore, carefully documenting your network is an important part of pre-migration planning.

Table 1 provides a sample network questionnaire that can be used to document the network configuration for your environment.

<b>Question</b>	<b>Answer</b>
How many primary data centers are in use within the organization?	
Where, physically, is each primary data center located?	
How are the primary data centers connected? (For example, what speed pipe is available between the data centers?)	
What subnets are in use at each primary data center?	
How many secondary data centers are in use within your organization?	
Where, physically, is each secondary data center located?	
How are the secondary data centers connected? (For example, what speed pipe is available between the data centers?)	
What subnets are in use at each secondary data center?	
Is there an accurate network diagram available?	
Which data center(s) will host	

Exchange servers?	
Do all data centers that will host Exchange servers currently host Global Catalog servers?	
How many physical locations are there where users are located?	
What subnets are in use by user populations?	
How is DNS currently set up (e.g., split brain, Active Directory integrated, BIND)?	
What are the internal and external DNS zones in use?	
What is the current MX? Are multiple MX records in place? If so, have all been verified as accurate?	
What is the current forwarder?	
Are DNS zone transfers being done? If so, to whom?	
What is the underlying speed (e.g., 100MB/s, GbE) of each LAN?	
Are all network cards on Exchange Servers and Active Directory cards using a static value?	
Is WINS in use?	
Are non-routable IP addresses (e.g., 10/8, 192.168/16, 172.16/12) used for internal systems?	

**Table 1: Network Questionnaire**

If you have a good understanding of your network infrastructure, the entire planning process for moving to Exchange 2010 will be easier. While Exchange 2010 provides more native functionality across data centers than ever before, it is still important to ensure that you can pick out any possible bottlenecks or problem points prior to deployment.

## Windows and Active Directory Infrastructure

Without Windows and Active Directory present in the environment, Exchange cannot be installed. Ensuring that your domain controllers (DCs) are running at the necessary functional level and that adequate numbers of Global

Catalog (GC) servers exist can help make your Exchange 2010 deployment go more smoothly.

While the formal recommendation from Microsoft is one GC CPU per four Exchange CPUs, many organizations now make every DC a GC within their environment. Unless your organization has legitimate, unchangeable reasons for not making this change, it's best to follow that example and make all DCs GCs.

Other points to document about your current Windows and Active Directory infrastructure are outlined in Table 2.

Question	Answer
What versions of Windows are currently in use as standard within your organization?	
Are language packs in use? Which languages?	
Is Active Directory currently deployed?	
How many Active Directory forests are in use?	
How many Active Directory domains are in use?	
Do you use a master domain model? A multi-master domain model?	
How many child domains exist?	
How many levels of domains exist within the organization?	
What versions of Windows are currently used to host Active Directory?	
What forest functional level is Active Directory currently running?	
What versions of Windows are being used to host newly created servers?	
What is the current routing configuration for Active Directory?	
What is the current site and subnet configuration for Active Directory?	
Is Exchange Server currently in use within the organization?	

Which domains currently host Exchange Server computers?	
Is a resource domain or resource forest being used to host Exchange Servers?	
If multiple forests are in use, what is the current trust model being used?	
How many Global Catalog servers currently exist within the infrastructure?	
Which domains currently host Global Catalog servers?	
Do Global Catalog servers exist within every domain that hosts Exchange Servers today?	
Are there any instances where Exchange co-exists with a domain controller or Global Catalog server in the environment?	
Are there any instances where Exchange Server exists in a physical location yet there are no local Global Catalog servers at that location?	
Where are mailbox-enabled accounts located within the Active Directory structure (within a dedicated organizational unit (OU), or within the default users OU)?	
Where are mail-enabled accounts located within the Active Directory structure?	
Where are distribution groups located within the Active Directory structure?	

**Table 2: Windows and Active Directory Infrastructure Questionnaire**

In the early days of Windows 2000 and Active Directory, many organizations invested hundreds of thousands of dollars to develop an Active Directory design. Unfortunately, many of the resulting designs were based upon the erroneous idea that an Active Directory domain was a security boundary. Today, we know that the Active Directory forest is the only true security boundary, and you should revisit overly complex domain configurations and simplify the architecture whenever possible.

## Current Exchange Infrastructure

Even though you have already decided to move to Exchange 2010, it is still wise to document your current Exchange infrastructure to understand any limitations you face and help you determine the best path forward. Table 3 provides a questionnaire you can use to help document the current environment.

Question	Answer
What versions of Exchange Server are currently deployed?	
Is the current Exchange organization running in mixed or native mode?	
Is there a single Exchange organization in use, do multiple Exchange organizations need to be consolidated?	
What is the organizational name of each Exchange organization currently in use?	
Are the organizational names currently in use the original organizational names, or was either the CN or the Display Name ever changed?	
What is the current routing infrastructure for Exchange Server? (Note that Exchange 2007 relies upon the Active Directory site and subnet routing configuration, while Exchange 2000 and 2003 had their routine defined separately.)	
If pre-Exchange Server 2007 versions are in use, how many routing groups are present?	
If pre-Exchange Server 2007 versions are in use, what are the names of the routing groups?	
If pre-Exchange Server 2007 versions are in use, which routing group is each server assigned to?	
If pre-Exchange Server 2007 versions are in use, is the current Active Directory routing appropriate for	

Exchange Server 2010?	
How many Exchange Servers currently exist?	
What role is assigned to each Exchange Server that is currently deployed? (Pre-Exchange 2007, this would be Front End or Back End. For Exchange Server 2007, this would be Edge, Hub, Mailbox, Client Access Server (CAS), or Unified Messaging (UM).)	
What is the name of each deployed Exchange Server?	
What version of Exchange (including service pack level and hot fixes) is running on each Exchange Server?	
Are foreign connectors (PROFS, X.400, GroupWise, Notes, etc.) in use?	
Are language packs in use? Which languages?	
Is ActiveSync in use? If so, how many active mobile devices exist?	
What was the first Exchange Server 5.5 computer in each site (if applicable)? Was it properly removed from the organization?	
Has the Exchange Best Practices Analyzer been run in the organization?	
Is clustering currently used?	
If clustering is in use, which type of clustering is running (single copy clustering, cluster continuous replication, standby continuous replication, or local continuous replication)?	
How many storage groups are in use on each specific mailbox server?	
How many mailbox databases are in use within each storage group?	

How many mailboxes are in use within each mailbox database?	
What is the average mailbox size for each mailbox database?	
What is the maximum mailbox size within each mailbox database?	
Have mailbox size limits been defined within the organization? If so, what are the guidelines?	
Are special rules in place for message transport?	
Are there portions of the user population that may not communicate with one another by email?	
Are message size limits in place?	
Is message archiving currently underway?	
Is message journaling currently being done?	
Are delegates named for other users?	
How many public folders are currently used?	
Is there a policy defining how long messages can be retained?	
Are PST files allowed?	
Where are PST files stored?	
How many messages are received by the Exchange infrastructure each day?	
How many messages are received on average per user per day?	
How many messages are sent within the Exchange environment each day?	
How many internal messages are sent on average by each user per day?	
How many messages are sent to external users on average per day?	

How many messages are sent on average by each user per day?	
Are there different user usage profiles (light, medium, heavy) in the environment? If so, approximately how many users fall into each category?	

**Table 3: Current Exchange Infrastructure Questionnaire**

While this questionnaire is fairly comprehensive, be sure to examine your current infrastructure for any other information that may be important to your migration project.

## Other Messaging Systems

Not every organization is migrating from an existing Exchange organization to Exchange Server 2010. Migrations to Exchange from other messaging systems, such as Lotus Notes and GroupWise, and even simple SMTP-based systems, happen every day. Table 4 includes points of consideration for organizations migrating from foreign systems to Exchange 2010 or Exchange Online solution.

Question	Answer
What messaging system is currently in use? What versions?	
How many mailboxes are assigned to each server?	
What is the average mailbox size for each mailbox database?	
What is the maximum mailbox size within each mailbox database?	
Have mailbox size limits been defined within the organization? If so, what are the guidelines?	
Are special rules in place for message transport?	
Are there portions of the user population that may not communicate with one another by e-mail?	
Are message size limits in place?	
Is there a policy defining how long messages can be retained?	
How many messages are received by	

the messaging infrastructure each day?	
How many messages are received on average per user per day?	
How many messages are sent within the messaging environment each day?	
How many internal messages are sent on average by each user per day?	
How many messages are sent to external users on average per day?	
How many messages are sent on average by each user per day?	
Are there different user usage profiles (light, medium, heavy) in the environment? If so, approximately how many users fall into each category?	
Are there tools available to connect the current infrastructure with an Exchange 2010 infrastructure for coexistence and migration?	
What directory service is currently in use? Has this been mapped to Active Directory?	
Are there other tools, such as workflows, that would need to be migrated to a Microsoft-centric environment?	

**Table 4: Other Current Messaging System Infrastructure**

Each specific foreign messaging system has its own quirks and fine points. For example, Notes uses NSF files and replicates data in very different ways than Exchange does. Understanding your current system, how it will change when you move to Exchange 2010, and your organization's motivation for the move can help ease the coexistence and migration process.

### **Third-Party Tools and Utilities**

One thing that many organizations love about Exchange Server is the rich third-party toolsets that are available to help support and enhance Exchange. While third-party tools are heavily used in many organizations, they can be overlooked during a migration. Ensure that you have inventoried each third-party tool in use and determined its ability to function with Exchange Server

2010 prior to beginning any migration process. Table 5 provides some points to clarify before finalizing any migration plans.

<b>Question</b>	<b>Answer</b>
What anti-virus is in place? Is this an on-premises or hosted solution?	
Is information store scanning being done, or is scanning taking place at the gateway (or both, or neither)?	
Is file system anti-virus software in place? Are exclusions included in the configuration to avoid contention with the appropriate Exchange files?	
What anti-spam system is in use? Is this an on-premises or hosted solution?	
Is e-mail archiving being done? How is the archive fed (journaling, mailbox contents, or transaction logs, or a combination thereof)?	
Are message encryption tools (PGP, PKI, etc.) being used?	
Is non-Exchange-based unified messaging (Cisco Unity, Avaya, etc.) in use?	
What mobile device services (Blackberry, Good, etc.) are in use?	
Are workflow tools in use? If so, which ones?	
Has a CRM system been integrated into Exchange? If so, which one, and how?	
Are document management tools being used? If so, which one?	
Does Exchange receive inbound or send faxes?	
What backup software is currently in use? Are streaming backups or VSS backups being done? How often?	
What type of monitoring is in use?	

Are performance management tools in use?	
What type of reporting tool is in use?	
Is instant messaging in use? What tool is being used? Does it integrate with Exchange?	
Is a desktop search tool deployed as a corporate standard? If so, which one?	
Are e-discovery tools in use? If so, which one?	
Is a message recovery tool in use? If so, which one?	
Are any other third-party products in use?	

**Table 5: Third Party Tools Questionnaire**

Third-party tools seem like part of the family, and often get overlooked during migration planning. It is important to consider each tool's validity in the current and planned environment, to find replacement tools if necessary, and to ensure that your organization has the ability to upgrade existing tools to a version that will support Exchange Server 2010.

### **Archiving to Help Smooth Migrations**

One change in Exchange Server 2010 compounds the problem of the growth of messaging data. All prior versions of Exchange use single instance storage (SIS) to save disk space, but in Exchange Server 2010, the database tables are restructured and SIS is no longer retained across mailboxes or mailbox databases. For example, with SIS, a message sent to 25 different recipients resulted in only one instance of that message being saved on disk, with each recipient's mailbox retaining a pointer to the specific message. SIS was maintained on a per-store basis, so if 25 users spanned two mailbox databases, only two instances of the message would have been stored. The effect of the architectural change in Exchange 2010 is that organizations with a high SIS ratio (viewable through Performance Monitor) will see an increase in database sizes when moving to Exchange 2010.

Even without the loss of SIS in Exchange 2010, Exchange administrators need to be aware of the growth of messaging data. As time has passed, message size limits have increased greatly – when a 5 MB message size limit was common several years ago, today's message size limits tend to be between 25 and 30 MB. Today, users are much more carefree about sending large attachments and rarely consider the ramifications of sending a large file through e-mail before hitting the send button.

A best practice for mitigating the growth in storage needs is to archive older, rarely accessed messaging data before migrating to Exchange 2010. This will

enable you to retain important older data for legal, regulatory, or intellectual property reasons, but keep it in an efficient archive instead of an active Exchange mailbox database. Also, archiving data before migration speeds up the migration process.

### **Public Folder Considerations**

In many organizations, public folders have been neglected instead of managed, and administrators would prefer to ignore their existence. While this approach may work in the short term, there are often users who rely upon the public folder infrastructure and value its data. Public folders will be supported by Microsoft until at least 2020, ten years after the release of Exchange 2010, so there is no need to rush to move data from the public folder hierarchy.

If your organization is migrating to Exchange 2010 from an earlier version of Exchange, it is simple to move data to the new Exchange 2010 servers: simply add replicas of the public folders you want to replicate to the new servers, and then wait for the folders to contain the same data. To synchronize data across organizations, you can use the [Microsoft Inter-Organization Replication Tool](#), or third-party tools such as [Quest Migration Manager for Exchange](#) and [Quest Exchange Migration Wizard](#).

But before you move any public folder data, take time to determine which public folders in your organization are ever actually used. If you're lucky enough to work in an organization with few public folders, it is easy to touch base with each folder owner and determine the long-term prognosis for the data within the folder. In larger organizations, or even smaller organizations where public folders have been heavily used throughout the years, determining the path for each public folder can be a difficult task.

Before the release of Exchange 2007, there were rumors that Microsoft was considering discontinuing public folders altogether. At that time Microsoft Office SharePoint Server (MOSS) was not widely seen as a viable replacement for public folders, since it was a relatively new product with many limitations. Over the past several years, however, Microsoft has improved MOSS significantly, and it is now flexible enough to be a repository for much of the content in public folders. MOSS still lacks some public folders features, such as the ability to provide multiple replicas of data (which is especially handy in widely dispersed organizations). However, in many cases, MOSS is a more appropriate tool for data than public folders ever were.

Public folders are not going away soon, and they are still a viable endpoint for a lot of data. However, MOSS is a now more mature platform; there in some cases may be a more accessible, flexible solution for data storage. Determining whether the data in your public folders is an appropriate fit for MOSS can be a very important, but can be a time-consuming task.

# PLANNING AND PREPARING FOR YOUR MIGRATION WITH QUEST TOOLS

As shown in the previous section, there are a large number of questions that need to be answered during an Exchange assessment. You need to do a one-time and ongoing gathering of information to determine trends and traffic patterns. Given the busy workload of most Exchange administrators, these tasks will seem daunting, but Quest provides a wide range of solutions to help save time and reduce expenses when you prepare and plan for your migration

## Quest MessageStats

[Quest MessageStats](#) can assess usage, availability, capacity, and inventory before, during and after a migration. Pre-migration, MessageStats delivers detailed reports on what needs to be migrated, what stale and unused objects can be left behind, and how the current environment is functioning in terms of storage and traffic so that the target environment can be appropriately planned. During a migration, MessageStats can prove whether or not the target environment is functioning as desired. Post-migration, MessageStats can measure e-mail traffic, report policy compliance, defend SLAs and ensure sufficient capacity. MessageStats offers graphics, metrics, interactivity, drill-down capabilities and powerful customization for both high-level, business-focused reports and deep insight into usage at the user and object level.

MessageStats can also give you a running start on public folder usage and statistics, relieving much of the manual burden on administrators. MessageStats includes reports on public folder sizes, replication, permissions and owners, and public folder usage that provide the basis for a comprehensive plan to migrate content to SharePoint or a newer version of Exchange.

## Quest Archive Manager

[Quest Archive Manager](#) can help organizations move older, rarely accessed data from active mailbox databases to a secure, reliable messaging archive. Archive Manager supports archiving not only from Exchange Server, but also from Novell GroupWise and many other SMTP-compliant messaging systems. While Archive Manager does not natively archive from Lotus Notes, if you are using [Quest Notes Migrator for Exchange](#), data can be exported from Notes into PST files, which can then be imported into Archive Manager to backfill the archive with historical data.

The administrative console in Archive Manager offers a lot of flexibility in determining which data to archive; you can choose to archive messages over a certain age, over a certain size, or a combination of both. Message attachments can be simply stripped from messages, with a link to the attachment left in the original message, or those with large attachments can be archived as a whole. The flexibility of the Archive Manager rule set allows

you to pick and choose the archiving options that fit your organization's needs.

Unlike many other archiving products, Archive Manager was designed to handle attachments optimally, and store them separately from their associated messages. Each attachment is stored in a file system and identified by a unique hash, enabling SIS for attachments within the archive store. Each message is stored within SQL, with pointers to its attachments. This is a very efficient way to handle messaging data, as SQL is optimized to handle expected content (such as messages and their attributes), while the file system can flexibly handle a variety of attachments.

Archive Manager is an ideal choice for pre-migration archiving because it is easy to implement and configure. And once pre-migration archiving has been completed, you can choose to continue to archive messages based upon specific criteria, or to simply archive all data, new and old.

Some administrators debate whether to stub archived messages. Message "stubs" are remnants of, or placeholders for, an original message; a URL points to the message that has been archived. Microsoft often recommends against stubbing messages, in part because Outlook has limitations on the number of items it can display within a folder. Archive Manager gives you the choice of whether to stub archived messages. Because end users can get confused if stubs are not left for messages, it is often wise to stub archived messages until users are familiar with Archive Manager, and then age out the stubs as time passes. Archive Manager is flexible; you can modify its settings multiple times until you find the correct balance between stubbing and cleaning out old items from mailboxes.

A benefit of archiving before migrating is that you can help protect your organization from regulatory or legal issues later. Because Archive Manager can be configured to capture all messaging data, whether stubs are being left or not, users can be taken out of the retention process, which means that you will have a clear record of all data from the day the archive is enabled. While messages that were previously deleted cannot be automatically moved into the archive (unless old backup tapes are recovered—an arduous and expensive process), the archive will have a good historical record, especially in organizations where users tend to be e-mail pack rats.

### **[Quest Public Folder Migrator for SharePoint](#)**

Public Folder Migrator for SharePoint eases the migration path from public folders to SharePoint, and also includes a six-month trial license for MessageStats. Public Folder Migrator for SharePoint does not remove content from the public folder hierarchy; the data is replicated into MOSS. As shown in **Error! Reference source not found.**, administrators can redirect Outlook users to the MOSS site URL with the replicated content, either as soon as the content was replicated or at a scheduled time. Permissions can be revoked from the source folders and reset so that users may read, but not add new content to the public folder.

### Outlook Redirection

Redirect migrated public folders in Microsoft Outlook to SharePoint. Users will see the target SharePoint site, list or document library when they select a migrated public folder.

Enable Outlook redirection

### Permission Revocation

You may need to restrict access to migrated public folders by limiting permissions to the selected access level. You can also designate a user as a folder owner to retain administrative access to the migrated content after the switch.

Revoke permissions from source folders

Reset permissions for folder users to:

Read-only

Set this user as a folder owner:

Peter Holmes

Browse...

### Schedule Redirect

If not scheduled, redirection starts automatically when synchronization is completed.

Start redirecting on:

Thursday , November 08, 2007

Help

< Back

Next >

Cancel

**Figure 2: Public Folder Migrator for SharePoint Access Options**

# BEST PRACTICES FOR MIGRATING TO EXCHANGE SERVER 2010

Whether you are migrating from an earlier version of Exchange Server or from a legacy platform such as Lotus Notes or Novell GroupWise, the migration process involves a number of steps:

- Deploying the new Exchange Server 2010 infrastructure
- Deploying Outlook 2010 (or Outlook 2007) client software
- Establishing co-existence with the existing infrastructure
  - Directory synchronization
  - Public folder replication
  - Free/Busy synchronization for calendar data
- Mailbox migration (including calendars, tasks, personal address books, archives, etc.)
- Outlook profile updates
- Decommissioning original servers

Some of the steps involved in a migration are straightforward, while others involve a lot of planning and testing prior to making any changes to the existing environment.

## **Migrating with Native Tools**

Moving from one version of Exchange to a newer version can be very simple or very complicated. If you have an existing Exchange Server 2007 infrastructure that works well, moving to Exchange Server 2010 can be as simple as installing the new servers into the existing Exchange organization, configuring the new CAS servers, moving mailboxes to the new Exchange 2010 servers, replicating the public folder hierarchy to the new servers, and ensuring the Exchange 2010 HUB servers are configured to perform the tasks previously handled by Exchange 2007. This process is commonly referred to as a transition instead of a migration, and can be completed using native Microsoft tools. (Upgrades, where a later version of Exchange Server is installed over an existing older version of Exchange Server, are not possible when moving to Exchange 2010.)

Unfortunately, most migrations are not straightforward. Many organizations are still running Exchange 2003, and others are migrating from Lotus Notes/Domino or Novell GroupWise to a brand-new Exchange infrastructure. The few organizations that are still running Exchange 5.5 need to undertake not one, but two migrations—first to Exchange 2003, and then to Exchange 2010. Migrations are more complex than transitions and usually cannot be performed with the tools that Microsoft offers.

In addition, some organizations are using Exchange 2007, but want to re-architect their Exchange deployment based on new capabilities provided by Exchange 2010 or because of a merger or acquisition. These situations require an inter-forest migration. Since Exchange Server organizations cannot span Active Directory forests, organizations need to migrate Exchange when starting fresh with a new Active Directory forest.

Microsoft does provide some tools to help organizations migrate between different Exchange organizations and Active Directory forests; cross-forest mailbox moves were first enabled with the release of Exchange Server 2007, enabling users' mailboxes to be moved between forests, often with minimal disruption. But the native migration process is often convoluted, and Microsoft does not provide tools to track mailbox moves or to ensure that mailbox delegates are moved alongside the associated mailboxes.

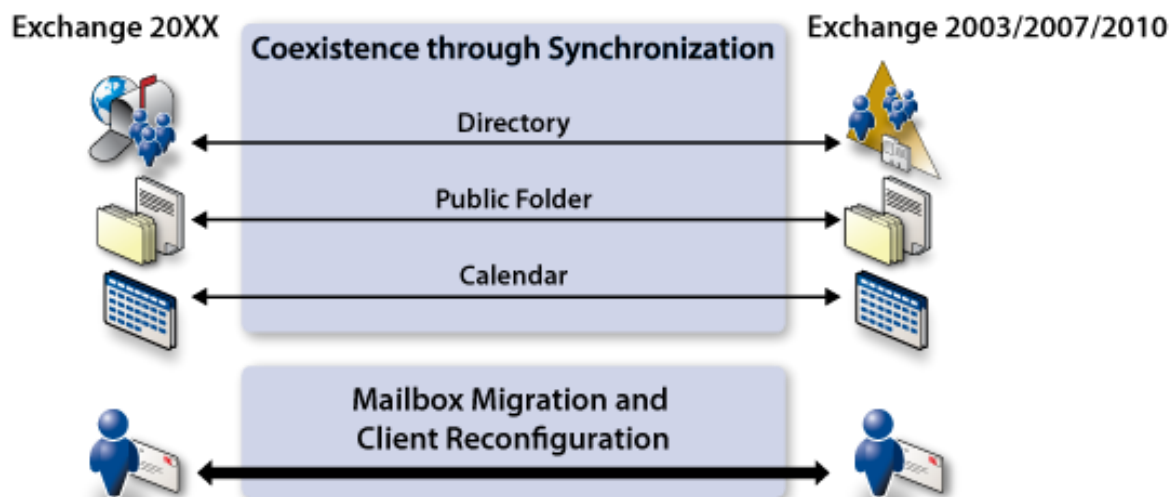
# MIGRATING WITH QUEST TOOLS

Quest migration tools are widely respected and recommended within the Exchange Server community. Quest has helped organizations migrate more than 20 million mailboxes to Exchange Server, including more than five million Lotus Notes and Novell GroupWise users. Quest can also provide experienced, consultants who are intimately familiar with the processes, procedures, and tools necessary to ensure a successful migration project.

## Migrating from Exchange 200x to Exchange 2010

[Quest Migration Manager for Exchange](#) allows organizations to migrate from Exchange Server 200X to Exchange Server 2010, and guides organizations through the process of inter-organizational migration. When you need to restructure your existing Exchange infrastructure, Quest Migration Manager for Exchange is a proven, reliable tool that ensures all data is moved without disruption to your users.

Migration Manager for Exchange transfers data from both Active Directory and Exchange Server, and synchronizes all pertinent data from the legacy environment to the new infrastructure, allowing coexistence between the organizations and ensuring continuity of service during the migration. Migration Manager also synchronizes calendar data (including free/busy data) and public folders (including permissions), as illustrated in Figure 3.



**Figure 3: Quest Migration Manager for Exchange Capabilities**

Migration Manager for Exchange has features lacking in native tools, including the ability to filter disabled accounts from the migration console. When you use Migration Manager for Exchange in conjunction with [Quest Reporter](#), you can also filter inactive accounts and unused accounts from the console. This allows you to migrate only data that is still pertinent to your organization and avoid bringing stale data and accounts into the new environment.

## **Migrating from IBM Lotus Notes to Exchange 2010 or Exchange Online**

For migrations from Lotus Notes/Domino to Exchange Server 2007, Microsoft offered the Transporter Suite, which included tools for directory synchronization and migration, calendar interoperability, and messaging data migration. Transporter Suite has been discontinued, and all native Notes/Domino connectors have been deprecated from Exchange Server 2007. Organizations will need to use a different toolset in order to migrate from Lotus Notes to Exchange Server 2010, Exchange Online, or to a hybrid of both.

[Quest Notes Migrator for Exchange](#) offers all of the needed functionality for migrating Notes directory data, calendar information, personal address books, and messages to a new Exchange Server 2010 environment. Notes Migrator for Exchange includes an intuitive management console that offers reporting and project management capabilities. With migration scheduling included in the console, Notes Migrator allows administrators to configure migration processes to run when users are not connected to the system, thus reducing the impact of the migration. Multiple users can be migrated simultaneously on multiple migration machines, accelerating project timelines and reducing costs.

Notes Migrator for Exchange also provides fast, efficient migration to Exchange Online, including a direct migration of Notes e-mail, calendars, tasks, and personal address books. Organizations can also use Notes Migrator to implement a hybrid approach, where some mailboxes are managed onsite while others reside online.

## **Migrating from Novell GroupWise to Exchange 2010**

Microsoft has deprecated all third-party connectors, including the Novell GroupWise connector, which was designed to allow GroupWise and Exchange Server to coexist. Because the last version of the GroupWise connector was released with Exchange Server 2003 (which has passed the end of mainstream support), there is no native method to have GroupWise and Exchange Server coexist or migrate from GroupWise to Exchange.

[GroupWise Migrator for Exchange](#) enables organizations to migrate users' calendars, personal address books, frequently used contacts, and other messaging data from GroupWise to Exchange Server 2010. The management console automates much of the migration process, simplifying administrative tasks. Multiple mailbox migrations may be run concurrently, reducing the overall timeframe of the migration project. Like Notes Migrator, GroupWise Migrator for Exchange also provides migration to Exchange Online or to a hybrid environment.

## **Migrating from Exchange 5.5 to Exchange 2010**

[Exchange Migration Wizard](#) enables organizations that have yet to take the leap to an Exchange Server 200x version to move their user base from Exchange Server 5.5 to an Exchange Server 2010 infrastructure.



## Tracking

One simple way to track how the migration process is going is to use [Quest Spotlight on Messaging](#) to keep an eye on the environment. Spotlight on Messaging can help you quickly find any issues with performance bottlenecks or other problems quickly, and it provides guidance to help you quickly resolve any issues.

# BEST PRACTICES FOR MANAGING EXCHANGE SERVER 2010

Once your new Exchange 2010 infrastructure is in place, you may need management functionality beyond what Microsoft natively offers. While day-to-day administrative tasks are covered well by the native toolset, organizations that need to collect data for long-term analysis, use real-time diagnostics to solve problems, track or audit administrator actions, or find, recover, and produce data that has been sent or received will find that additional tools are necessary.

## Administration and Provisioning

Administrative tools for Exchange were initially sparse; the first three releases of Exchange used the Exchange Admin program. With Exchange 2000 Server, Microsoft first introduced the Exchange Management Console (EMC), a snap-in for the Microsoft Management Console (MMC). EMC has become more usable with each subsequent major release, and the addition of a third pane for action items in Exchange 2007's EMC made navigation less painful. Microsoft has made additional improvements in EMC for Exchange 2010, reducing the number of levels that must be clicked through in order to perform management tasks.

With the release of Exchange Server 2007, Microsoft added the Exchange Management Shell (EMS), based upon Microsoft PowerShell, a non-GUI based administrative tool, enabling organizations to have a more flexible management experience. While EMS does provide flexibility that is not available in EMC, many organizations have found the learning curve for EMS to be steep, at best. In order to help organizations use PowerShell more effectively Quest created the [PowerGUI](#) tool and [PowerPacks for Exchange](#), both of which are available for use at no cost.

[Quest ActiveRoles Server](#) enables administrators to easily provision, manage, and deprovision user accounts and their associated mailboxes, as well as provides role-based security and automated group management based upon the profile of a user. More organizations are focused on compliance and security initiatives and controlling user access. ActiveRoles Server not only controls access to Active Directory (and Active Directory Lightweight Directory Services (AD LDS), formerly known as ADAM), but also provides a change-approval path to provide a second layer of protection against errors and inconsistencies.

## Performance and Availability

While most administrative tasks are fairly straightforward in Exchange Server 2010, Microsoft doesn't natively provide much insight into how the system is being used. [Quest MessageStats](#) continuously collects data from Exchange and provides reporting on hundreds of messaging statistics, including the number of messages sent and received per day, the top domain names with which messages were exchanged, the volume of messaging traffic traversing your network, and messages containing specific subject keywords.

MessageStats also includes graphical representations of many reports, and specific reports can be collated into a printable format that can be presented to management on a regular basis.

While MessageStats was initially focused solely on Exchange-based reporting, today Quest offers numerous Report Packs that may be added to MessageStats to provide reporting on other system components, including Blackberry Enterprise Server, SendMail/Postfix, Quest Archive Manager for Exchange, and Office Communications Server.

Quest also provides [Spotlight on Messaging](#). Spotlight on Messaging is not a traditional monitoring tool—it enables organizations to track system performance during a migration, and provides a quick graphical view of performance and possible system problems during day-to-day operations. Like MessageStats, Spotlight also can monitor other system components such as Blackberry Enterprise Server and Office Communications Server, providing a holistic view of the health of your messaging environment.


### **Compliance and Security**

One of the major challenges of managing a huge messaging infrastructure is dealing with the sheer amount of data in the system. Finding the data you need—for regulatory queries, legal investigations, or internal informational purposes—is a huge challenge if your current data is in Exchange mailbox databases and historical data resides on backup tapes. [Quest Archive Manager](#) captures and indexes new and historical messaging data transparently to end users, and offers powerful search capabilities that enable authorized users to quickly locate and retrieve the data to satisfy legal or internal requests.

However, all is not lost if you haven't deployed an archive—Quest has tools that can help you find and retrieve data from mailbox databases and backup tapes without the need to restore each individual tape to a recovery server.

[Quest Recovery Manager for Exchange](#) has saved many administrators who were in tight situations. Recovery Manager can recover entire mailboxes, or searches can be run using keywords and message attributes to find only the specific data that matches those criteria. Recovery Manager is a flexible tool that allows items to be retrieved from a wide range of sources, including backup media created using products from the majority of backup vendors (both traditional streaming backups and VSS are recoverable), unmounted Exchange database (.edb) files, users' personal messaging files (PSTs), and even Lotus Domino database (.nsf) files. Recovery Manager can not only recover mailbox data without the need for an additional server, it can also recover public folder content and hierarchy.

One of Exchange's main challenges has been the difficulty of determining who changed what within the system, and when the change was made. Exchange includes no auditing functionality. In today's world, organizations must meet a host of regulatory requirements and there is a real need to be able to track changes to critical systems. [Quest ChangeAuditor for Exchange](#), one of Quest's newest Exchange products, effectively fills the gap in Exchange's native capabilities.



ChangeAuditor provides in-depth information on who changed what, when they did it, and where the change was made. It allows administrators to add details to the log about why they made the change. Companies that struggle to meet regulations such as Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA) will find that ChangeAuditor does a great job of helping them track changes within the Exchange environment.

One of the best features of ChangeAuditor is the built-in Compliance Library. Most IT personnel have little interest in delving into the intricacies of each regulation their organizations must follow. The Compliance Library turns the audited information into in-depth reports that align with specific regulations. These reports can be presented to regulatory bodies when required, and Exchange administrators are relieved from the burden of compiling them.

Managing Exchange permissions using native tools is also very cumbersome. Quest [Security Explorer for Exchange](#) is a powerful, graphical solution for real-time management of Exchange permissions. You can manage permissions on mailbox folders (such as Calendar, Contacts and Inbox folders) without having to access the Outlook client, and search for permissions on a very granular level. Security Explorer for Exchange also consolidates the backup and recovery of all Exchange objects for simpler restoration of permissions for an individual object or multiple object.

## CONCLUSION

Exchange Server 2010 offers a lot of new features that will please end users and administrators alike. Microsoft has done a great job addressing many of the shortcomings of Exchange. This premier software supplier continues to move forward with compelling new features for Exchange while solidifying the underlying structure and improving performance.

Where Microsoft has left gaps, Quest offers tools and resources to help organizations migrate to Exchange 2010, and to better manage, monitor, and maintain the messaging infrastructure once it is in place.

## ABOUT THE AUTHORS

**Missy Koslosky** is a former nine-time Exchange MVP. Missy has managed Exchange server organizations for the federal government, designed Exchange architectures, and worked as a consultant, helping organizations architect and deploy Exchange. She is a co-author of *The Exchange Server Cookbook* (O'Reilly, 2005), and has edited various books on Exchange for Microsoft Press, O'Reilly, Digital Press, and Sybex. She has researched and written numerous Microsoft white papers including the Solution Accelerator for Exchange Migration and Consolidation.

**Ron Robbins**, MCSE, has provided Exchange migration assistance to Quest's customers and strategic partners as they moved from Exchange 5.5 to Exchange 2003 and 2007. He has over a decade of experience in the areas of help desk management, systems administration and consulting. Robbins has provided Exchange consulting services to many organizations, including one Fortune 500 company, and has co-authored with Microsoft an article on Exchange migration considerations. As product manager, Robbins guides the product direction of Quest Software's solutions for migration to Exchange 200X from environments including Exchange 200X, Novell GroupWise and Lotus Notes. Robbins earned a bachelors degree from Mount Vernon Nazarene University.

# ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. For applications, we deliver, manage and control complex application environments from end-user to database. For databases, we improve performance, availability and manageability from design through production. For Windows, we simplify, automate secure and extend your infrastructure. And for virtual environments, we help you automate and control virtual desktop and server environments to reduce costs and simplify ongoing management. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and [www.quest.com](http://www.quest.com).

## Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)

Email: [info@quest.com](mailto:info@quest.com)

Mail: Quest Software, Inc.  
World Headquarters  
5 Polaris Way  
Aliso Viejo, CA 92656  
USA

Web site: [www.quest.com](http://www.quest.com)

Please refer to our Web site for regional and international office information.

## Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at <http://support.quest.com>

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the **Global Support Guide** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: [http://support.quest.com/pdfs/Global Support Guide.pdf](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf)