QUEST SOFTWARE®

Exchange 2010 and Your Audit Strategy

Authors

Valentine Boiarkine
Software Architect, Blade

Contributors

Jamie Manuel
Product Marketing Manager, Quest Software

Keith Bick
Editor, Blade

WHITE PAPER

Quest Software, Inc.
Attn: Legal Department
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
E-mail: **legal@quest.com**

Trademarks

Contents

Abstract

This white paper reviews the audit strategy guidance provided in the white paper "Creating and Implementing an Audit Strategy for Exchange," in the light of the release of Exchange 2010 and its new features. Now, more than ever, auditing is a key tool for advancing security and compliance. Today's environment is increasingly competitive and you must vigorously protect your intellectual assets, as well as comply with corporate and regulatory guidelines.

Security and accountability are critical in attaining and maintaining leadership positions in today's competitive environment. There is pressure on IT staff to protect the organization against incidents involving sensitive information loss, computer forensics and litigation. Unfortunately, as the number of these incidents grows, our e-mail systems are becoming more distributed and the amount of information they store is growing exponentially.

Because of this, auditing any access to individual pieces of information becomes more difficult, if not impossible. In this white paper we will re-examine the recommended approach to auditing in light of new tools available.

Introduction

Exchange Server 2010 introduces many new features for enhanced security, compliance and discovery. These features were introduced to provide a core toolset for carrying out tasks that were impossible in earlier versions of Exchange Server. In this white paper, we will examine how auditing and security differs between Exchange 2010 and Exchange 2007.

No matter which software your organization uses for its e-mail system, it's very important to have a sound audit strategy. As discussed in detail in the white paper, "Creating and Implementing an Audit Strategy for Exchange", a successful audit strategy will provide visibility into your systems and user behavior and ensure that no unauthorized activities go unnoticed. A formal audit strategy will go a long way towards preventing, investigating and prosecuting malicious activities. Although this white paper focuses on Microsoft Exchange 2010, an audit strategy is vital no matter what e-mail system you use.

The following activities should be considered priority auditing candidates:

- Changes to administrative security groups – This includes the addition and changes in rights of system administrators
- Exchange Server configuration changes
- Access to "Key Mailboxes" – Certain mailboxes, for example those belonging to HR representatives, sales staff and senior executives, contain sensitive and proprietary information and are priority candidates for auditing.
- Changes to membership of "Key Distribution Lists" – These lists may be used to distribute important and sensitive e-mail. Organizations want to prevent unauthorized persons from appearing on these lists, either maliciously or by accident. For example, the "Senior Leadership Team" distribution list members will receive highly privileged e-mail containing company strategies – the kind of information you don't want in any other hands.

In both Exchange 2007 and Exchange 2010, it is somewhat possible to audit these activities. Unquestionably, Exchange 2010 has improved usability with an enhanced toolset for configuring auditing, as well as viewing audit information.

But even with these advances, you may find that auditing using built-in tools is difficult and effort intensive. You will still be swamped with vast amounts of auditing information, most of which depicts legitimate activity. This makes suspicious events very difficult to identify.

Because all medium to large organizations are required by law and corporate policy to have a formal audit strategy, Quest ChangeAuditor for Exchange is the solution that will best meet their needs. Quest ChangeAuditor for Exchange is also the most comprehensive solution for auditing complex messaging environments that are running multiple versions of Exchange Server.

What's New in Exchange 2010 Objects and Security?

Exchange 2010 with Service Pack 1 extends the compliance and discovery theme of Exchange 2007. Exchange 2010 enhances many features introduced in Exchange 2007 and introduces entirely new features in the compliance and security space.

Let's briefly examine the new auditing, security and compliance features in Exchange 2010. A key innovation is its clever use of mailboxes as storage for system information. For example, audited events and discovered messages are stored in a hidden part of a user's mailbox or dedicated discovery mailbox. The reliance on mailbox for storage of sensitive information further accentuates the need to control mailbox access and maintain an audit log of mailbox activity.

Discovery Mailboxes

The discovery mailbox is a new type of mailbox in Exchange 2010. It is created by default when the first Exchange 2010 server is installed. You can create as many discovery mailboxes as you choose, and give access to users that are authorized to perform discovery.

The purpose of a discovery mailbox is to hold data obtained in a discovery search. When a discovery manager performs a discovery search, the messages located by the search can be exported to a discovery mailbox. The messages will be stored there and will be protected against deletion and messaging records management cleanup. Messages stored in the discovery mailbox can be accessed at any time by the discovery manager. Note that the discovery mailbox does not have an e-mail address, and cannot receive e-mail – it is used for discovery activities only.

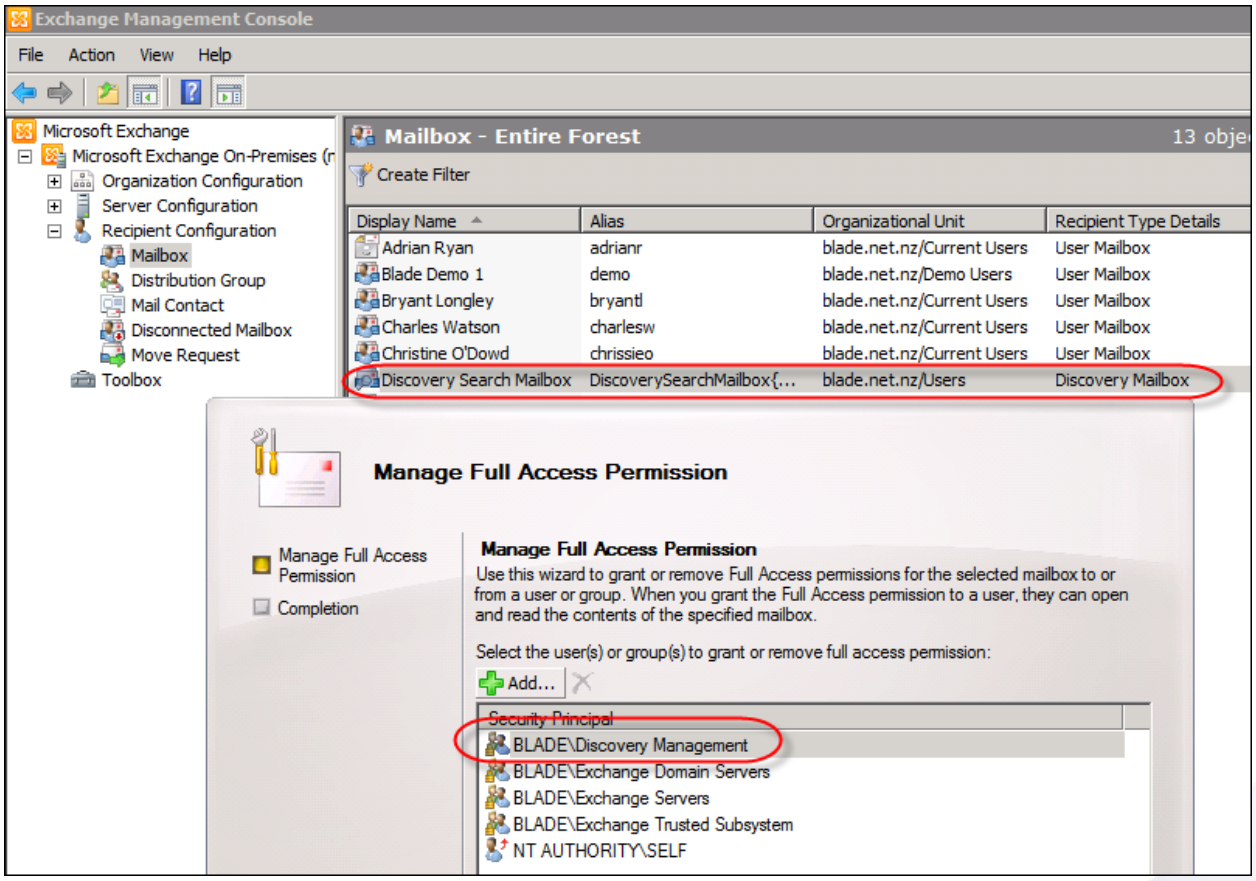

Figure 1 The Default Discovery Search Mailbox and Permissions

You can create a discovery mailbox in the Exchange Management Shell by using the following command.

```
New-Mailbox DiscoveryMailbox1 -Discovery -UserPrincipalName
DiscoveryMailbox1@contoso.com
```

While you have to use the Exchange Management Shell to create Discovery Mailboxes, you can manage it and remove it just like a standard mailbox using either the Exchange Management Console or the Exchange Management Shell.

Exchange Control Panel

The Exchange Control Panel (ECP) is an extension of Outlook Web Access. The ECP can be accessed by administrators with adequate permissions. These permissions will be discussed in "Exchange 2010 Administrative Model" of this white paper. The following activities can be performed from the ECP:

- Configuring Exchange integration with text messaging and voice messaging providers
- Configuring additional e-mail addresses for mailboxes
- Moderating the membership of a distribution list
- Performing a discovery search across multiple mailboxes

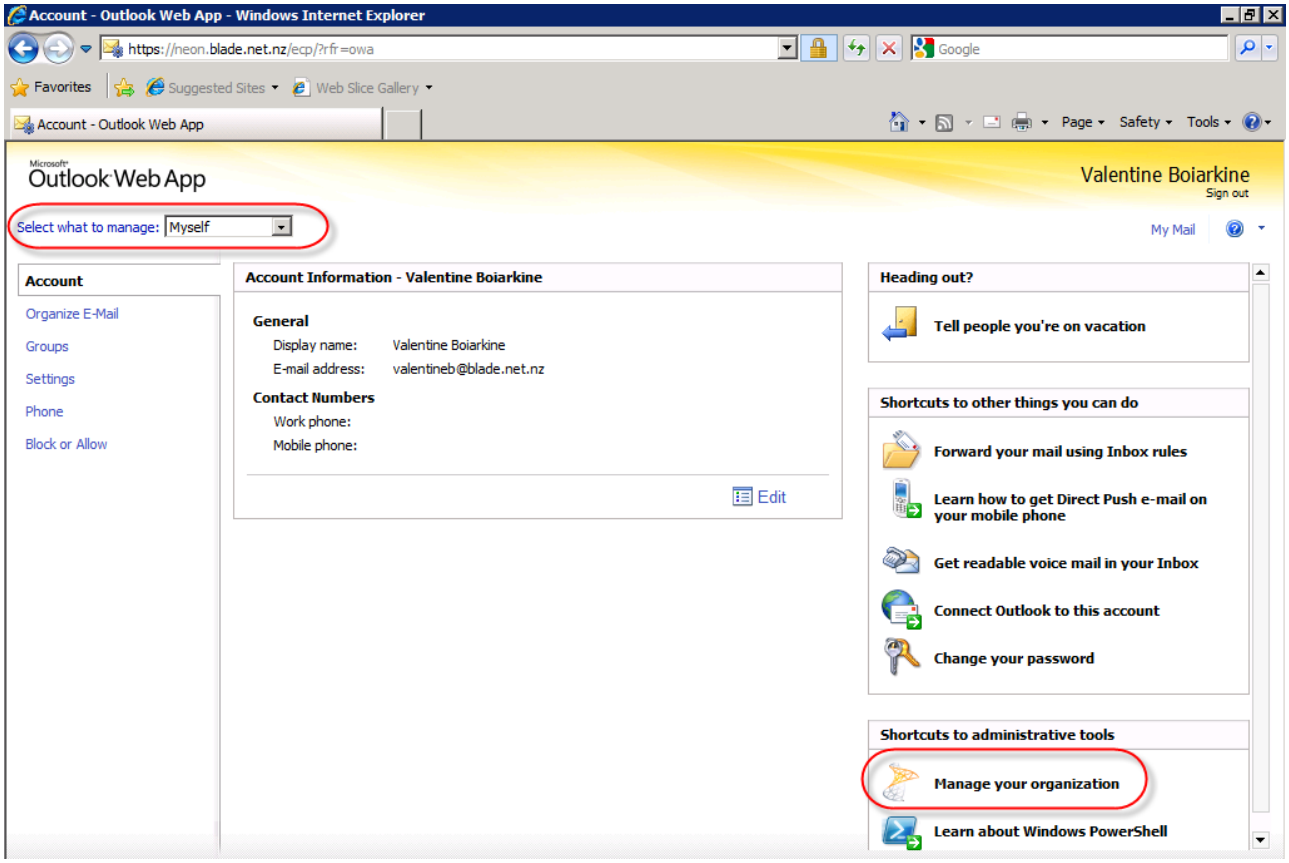

Figure 2 Exchange Control Panel (ECP) Accessible in OWA

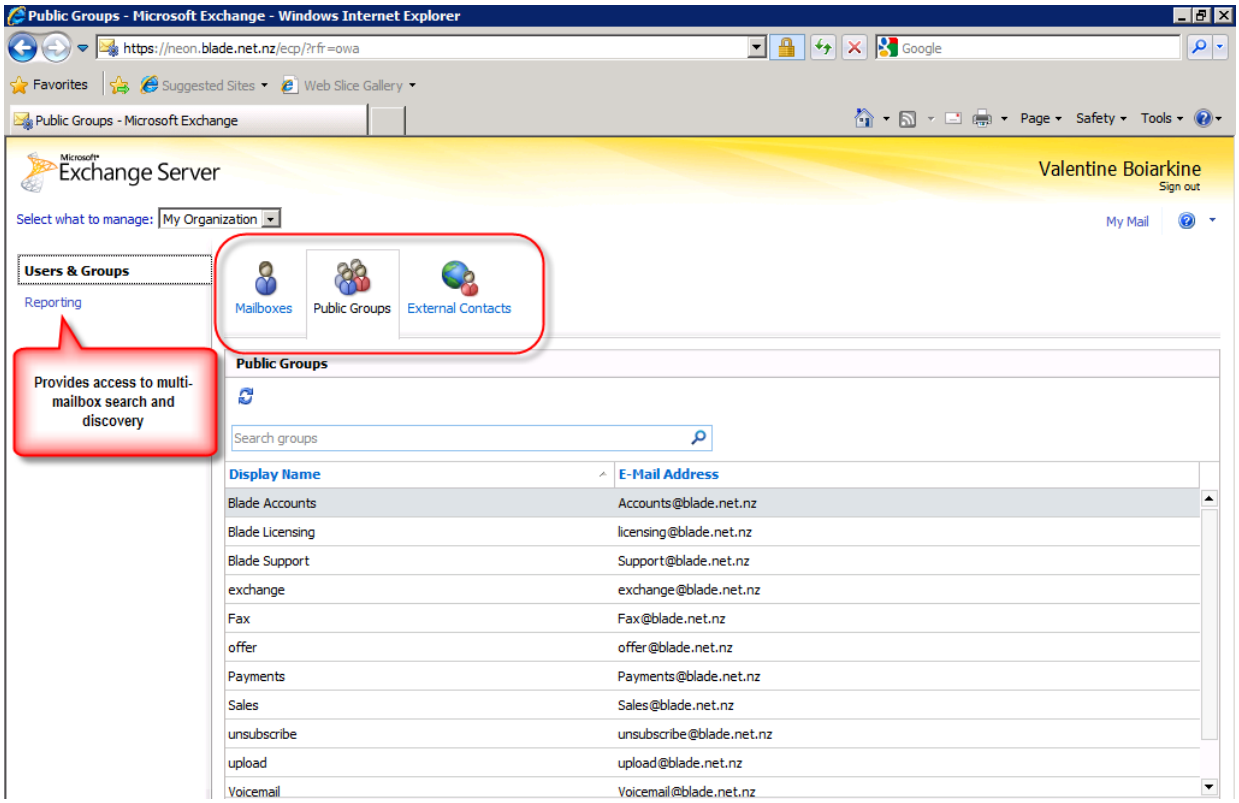

Figure 3 Exchange Control Panel Features

You must have appropriate role membership in the system before the ECP is displayed in the menu of your Outlook Web Access. These rights are discussed in “Exchange 2010 Administrative Model”.

Multi-Mailbox Search

Exchange 2010 allows people who are members of the discovery management role to search the content of all mailboxes held on Exchange 2010 servers. This feature assists with e-mail discovery; discovery is performed using the Exchange Management Shell, or the Exchange Control Panel (ECP) – a new extension to Outlook Web Access introduced in Exchange 2010.

The multi-mailbox search feature relies on the catalogs created by the Exchange Search Service. Mailbox data no longer has to be scanned, significantly improving the performance of the search. These scans are inefficient when applied to mailboxes several gigabytes in size.

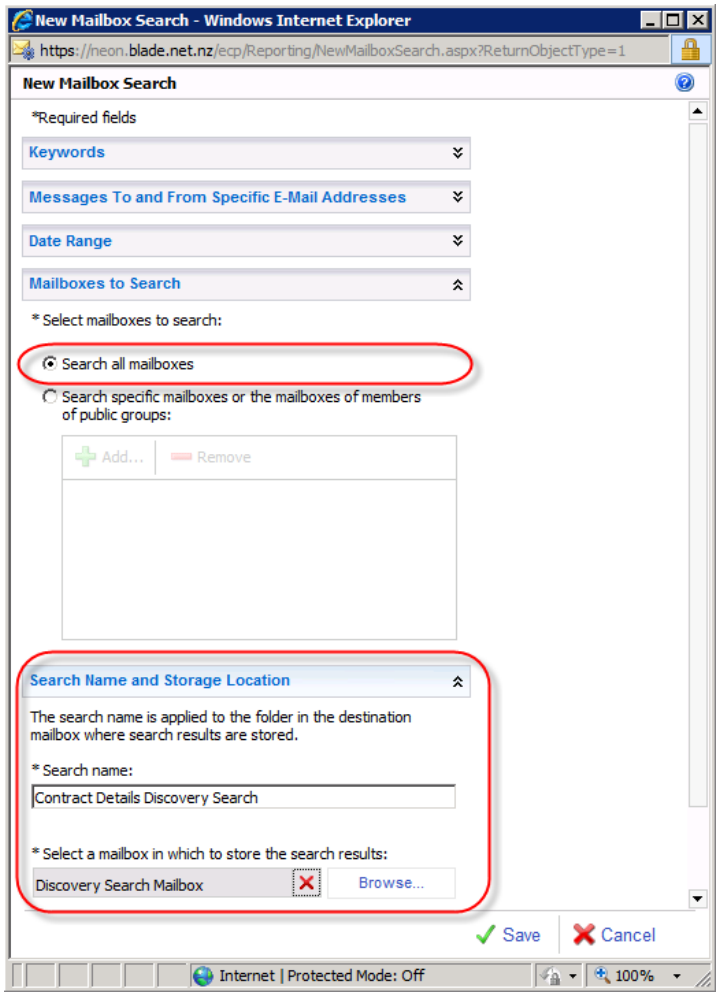

Figure 4 Discovery Search Criteria

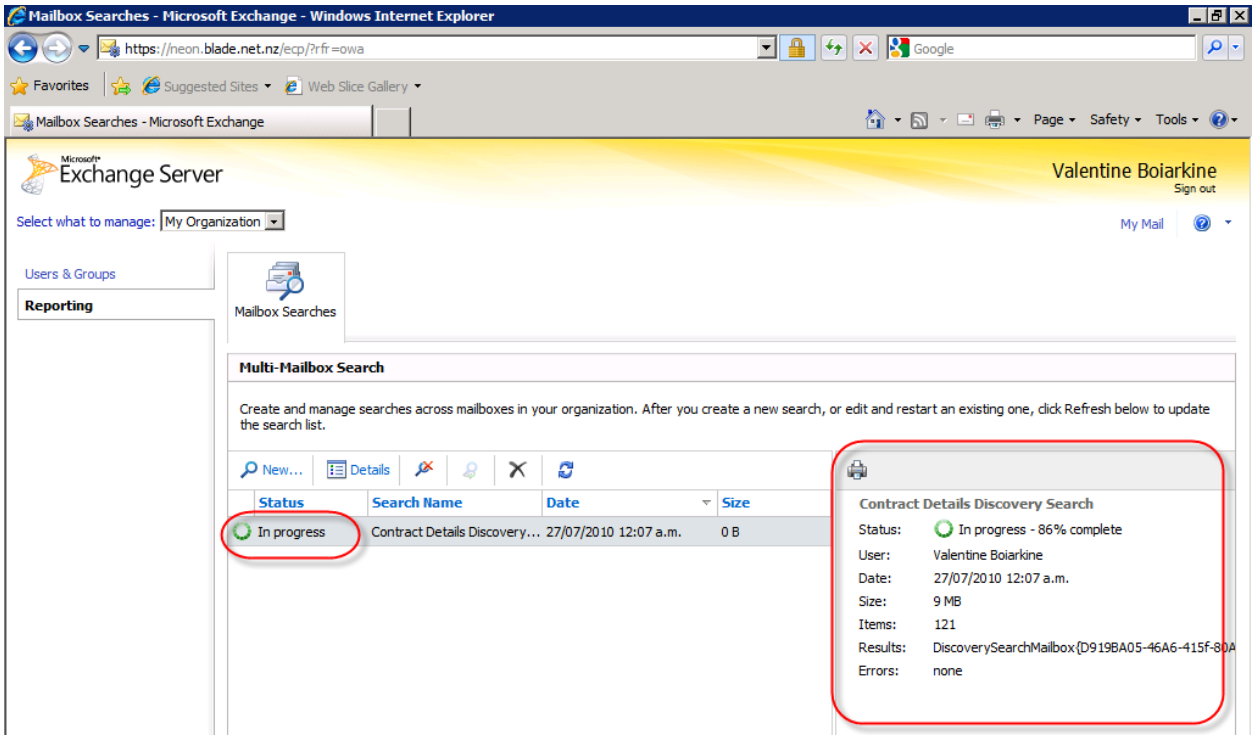

Figure 5 Multi-Mailbox Search - Saved Search

Multi-mailbox search is a powerful feature, allowing users with special rights access to mailbox data. Be sure these activities are audited, as they may cause damage.

The results of the search can be accessed by opening the Discovery Search Mailbox in OWA. In Exchange 2010 Service Pack 1, you can add an annotation to each discovered message, as well as obtain a search preview estimating the count of discovered items before they are copied to the discovery search mailbox. Exchange 2010 Service Pack 1 also adds a data de-duplication feature to remove duplicate items discovered by the multi-mailbox search.

Litigation Hold

You can also place a litigation hold on a mailbox to store it in an unaltered state. During an investigation, the mailbox becomes evidence and must not be touched.

When a mailbox is put on litigation hold, the following occurs:

- All mailbox content that is deleted or changed is preserved in its unaltered state in a special “Recoverable Items” folder. This folder is searchable by the multi-mailbox search.
- All messages deleted or moved using messaging records management (MRM) are preserved in the “Recoverable Items” folder
- An optional retention comment may be displayed to the mailbox owner

In Exchange 2010 RTM, the only way to put a mailbox on retention hold is by using the set-mailbox cmdlet as shown below.

```
Get-Mailbox “Joe Smith” | Set-Mailbox
-LitigationHoldEnabled:$true -RetentionComment:”Litigation in
progress”
```

In Exchange 2010 Service Pack 1 users with the discovery management role can use the Exchange Management Console and the Exchange Control Panel to place mailboxes on litigation hold.

Other Notable Features

Other features to be considered when reviewing your auditing strategy and procedures are:

- *Moderated distribution lists.* It is possible in Exchange 2010 to assign a user to manage distribution list membership. If changes to distribution lists are not covered by your audit policy, you may wish to add these activities to prevent privilege misuse. Key distribution lists likely to receive sensitive information are primary candidates for auditing.
- *New cmdlets for folder-level permissions management.* Get-MailboxFolderPermission, Set-MailboxFolderPermission and Remove-MailboxFolderPermission cmdlets allow administrators to manage folder-level permissions in recipient mailboxes. This new management capability requires auditing if you are concerned about administrative privilege misuse.
- *Sharing Policies*. In Exchange 2010, it is possible to create sharing policies that control sharing of calendars with external users and affiliated organizations. These policies are linked to user mailboxes. Because it is now possible to mass-share calendars using policies, you may wish to audit calendar access for unauthorized attempts.

Administrator Audit Logging

In Exchange 2007, you could audit administrative activities and configuration changes by changing the System Access Control List (SACL) audit entry on the Active Directory object you wish to monitor. Exchange 2010 introduces a new way of auditing administrative changes.

To make a change to Exchange system objects, you must execute Exchange Management Shell cmdlets. Operations performed in the Exchange Management Console and Exchange Control Panel (ECP) also call the cmdlets behind the scenes. Execution of all cmdlets that change the state of the system i.e. New-, Set-, Remove- etc can be logged as part of administrator audit logging.

The logging is performed by a component called Admin Audit Log agent. This component is an addition to the Exchange Management Shell. When a cmdlet is executed in the shell, the Admin Audit Log agent matches the cmdlet to a list of logging activities. If the cmdlet matches the list, the Admin Audit Log agent logs the details of the activity in a hidden arbitration mailbox.

The arbitration mailbox stores audit log entries. In Exchange 2010 SP1 personnel with appropriate role membership can use the ECP, or –AdminAuditLogSearch cmdlets to access and view the audit log entries. In Exchange 2010 RTM, administrators must open the arbitration mailbox directly using OWA or Outlook.

It is important to note that only changes made using Exchange 2010 management tools are logged as part of administrator audit logging. Changes made using Exchange 2007 tools, or by using ADSIEdit, VBScript or other tools are not logged. Therefore, for complex and mixed environments it is recommended that you use a purpose-built auditing solution such as Quest ChangeAuditor for Exchange. Quest ChangeAuditor for Exchange will audit all administrative changes, regardless of the tool used to make the change.

Configuring Administrator Access Auditing

Administrator access auditing is configured using the Set-AdminAuditLogConfig cmdlet. The cmdlet allows you to configure the following options:

- Admin Audit Log Enabled. This true / false option allows you to control whether or not Administrator Access Auditing is enabled for the organization.
- Admin Audit Log Cmdlets. This allows you to specify the specific cmdlets you are interested in auditing, for example “New-Mailbox” or “Set-ReceiveConnector.” You can also use wildcards, for example “*Mailbox*”.
- Admin Audit Log Parameters. This allows you to restrict auditing further by specifying only certain parameters that are selected for audit. For example, you can audit Set-ReceiveConnector cmdlet with –RemoteIPRanges parameter only, to ensure you audit unauthorized access to the connector.
- Admin Audit Log Age Limit. This parameter specifies how long the audit log entries are stored in the arbitration mailbox. The default is 90 days.

The following example configures administrator access auditing for all mailbox-related activity:

```
Set-AdminAuditLogConfig -AdminAuditLogAgeLimit:"120.00:00:00"
-AdminAuditLogEnabled:$true -AdminAuditLogCmdlets:"*mailbox*"
-AdminAuditLogMailbox:"x-valentineb@blade.net.nz"
```

Note that the mailbox specified by the AdminAuditLog parameter is only configurable in Exchange 2010 RTM. In Exchange 2010 SP1 the dedicated arbitration mailbox is used and cannot be configured.

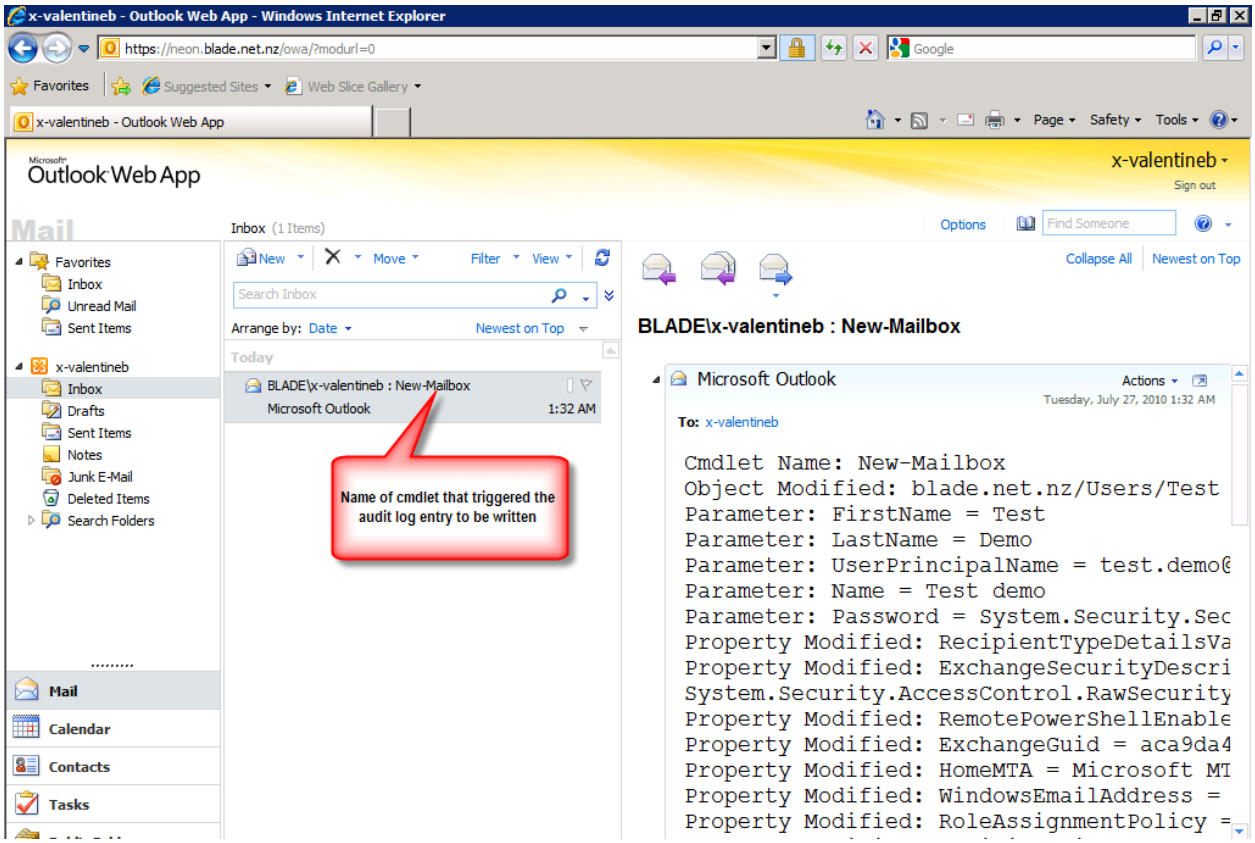

Figure 6 Audit Entry in Arbitration Mailbox

Information Logged

The following important information is logged as part of the audit entry:

- Cmdlet Name. The cmdlet that triggered the audit entry to be written.
- Object Modified. The Exchange object, such as the mailbox or connector affected by the operation. The object is presented in the format of its Active Directory path e.g. “blade.net.nz/Users/Test Demo”
- Parameters. One line is created per parameter of the cmdlet that triggered the audit entry to be written.
- Properties Modified. Lists the properties of the object that were affected by the cmdlet.
- Caller. The user name of the user who called the cmdlet.
- Succeeded. Displays if the cmdlet executed successfully.
- Error. Any error information output by the cmdlet during execution.
- Run Date. Server date and time when the activity took place.

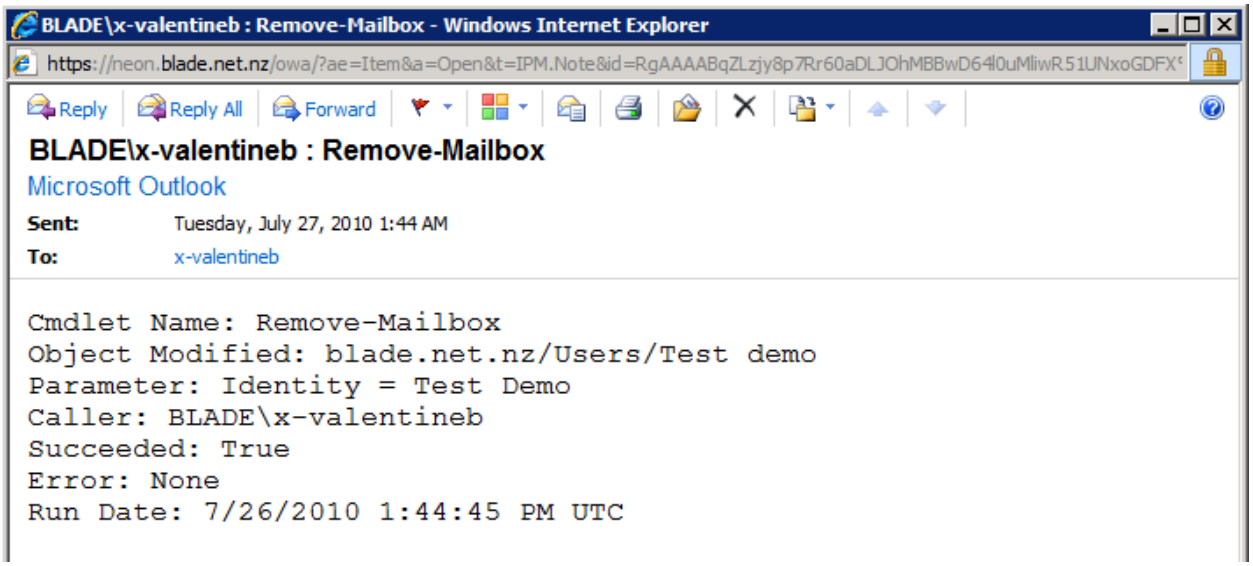

Figure 7 Administrator Access Auditing Entry Message

Mailbox Audit Logging

Mailbox audit logging is a new feature, introduced in Exchange 2010 Service Pack 1. Similar to administrator access audit logging, mailbox audit logging stores the log entries in a mailbox. However, unlike administrator access audit logging, audit entries are stored in the mailbox of the user being audited. The audit entries are stored in a hidden table, inaccessible to end users using Outlook and OWA.

To enable mailbox audit logging for one or more mailboxes, use the Set-Mailbox cmdlet. The following example configures auditing on all mailboxes located on server NEON with owner access and delegated access i.e. someone with permission other than the mailbox owner.

```
Get-Mailbox –Server:”NEON” | Set-Mailbox –AuditEnabled:$true –
AuditOwner: Update, Move, MoveToDeletedItems, SoftDelete –
AuditDelegate: Update, MoveToDeletedItems, SoftDelete,
HardDelete, FolderBind, SendAs, SendOnBehalf
```

Configuring Mailbox Audit Logging

Let’s examine the mailbox events, or activities, that can be audited in Exchange 2010 SP1. The following table summarizes the principals that can be audited and the events (mailbox or folder activities) that can be audited for the principal.

Administrator access occurs when a member of one of the Exchange administrator roles exercises their administrative rights and successfully accesses data in the mailbox.

Delegated access occurs when a user with delegated permissions to a mailbox or to a folder within the mailbox, for example, a calendar, successfully accesses the designated mailbox or folder.

Owner access occurs when a user accesses their own mailbox.

	Administrator	Delegate	Owner
Update	X (Default)	X (Default)	X
Copy	X	X	-
Move	X (Default)	X	X
MoveToDeletedItems	X (Default)	X	X
SoftDelete	X (Default)	X (Default)	X
HardDelete	X (Default)	X (Default)	X
FolderBind	X (Default)		-
SendAs	X (Default)	X (Default)	-
SendOnBehalf	X (Default)	X	-
MessageBind	X	X	-

Table 1 Mailbox Audit Logging Principals and Events

Auditing is not enabled by default - you must use the Set-Mailbox cmdlet with an AuditEnabled parameter to enable default logging on a mailbox. Note that owner access is not audited by default.

The AuditLogAgeLimit parameter can be used to control the period of time the audit log entries are retained within the user’s mailbox. The default retention period is 90 days.

Microsoft advises that you must seriously consider the implications of turning on mailbox access auditing for one or more mailboxes. Mailbox access auditing is likely to generate thousands of events for each

mailbox. You must have a clear strategy regarding how you will sift through these events to find ones that are relevant. It is not feasible to do a prophylactic review, i.e. acting to defend against these events, due to the sheer volume of information.

Accessing Mailbox Audit Logs

Users with organization management or records management roles can search through events created by mailbox audit logs using the Exchange Management Shell or ECP.

The Search-MailboxAuditLog cmdlet can access a single mailbox for audit entries and output them into the Exchange Management Shell window. The New-MailboxAuditLogSearch cmdlet can perform a search and e-mail the results to a specified e-mail address.

The new auditing tab in ECP can be used to search and export mailbox audit entries, and also provides access to a predefined “Non-owner mailbox access” report.

While Exchange 2010’s built-in mailbox audit logging is extremely useful for ad-hoc auditing, enterprises with more complex compliance and auditing requirements should consider an auditing solution such as Quest ChangeAuditor for Exchange. This solution offers easy GUI configuration and consolidated reports, as well as proactive functionality such as alerting.

Exchange 2010 Administrative Model

Exchange 2010 steps away from the access control lists (ACLs) that were used to control permissions and system rights in Exchange 2007. Customer experience has shown that the ACL infrastructure can be complex, confusing and lead to unexpected problems if they are used in a non-standard way. In Exchange 2007, administrative roles of “Organization Administrator”, “Server Administrator”, “View Only Administrator” and “Recipient Administrator” bridged the gap between ACLs and true role-based security. However, these administrative roles controlled only system rights, i.e. the ability to manage, not use, the messaging system.

Exchange 2010 takes role-based security further, by introducing role based access control (RBAC). RBAC places administrators and users into pre-defined roles with rights to perform administrative or end-user tasks. RBAC is implemented using the following methods:

1. *Management role.* A management role groups together the access rights required to perform a function within the system. A role contains one or more role entries – usually cmdlets required to perform a task. For example, the “Monitoring” management role contains cmdlets like Test-OWAConnectivity and Export-ActiveSyncLog, while the “MyProfileInformation” role allows you to run the Set-User cmdlet with parameters like FirstName, LastName, DisplayName. You can create your own management roles and define which cmdlets and granular parameters are associated with the role.
2. *Management role group.* This object represents a universal security group with users and mailboxes as members. Members of the management role groups can exercise rights associated with all of the roles linked within their groups. Some examples of management role groups are “UM Management”, “Organization Management” and “Help Desk”.
3. *Management role assignment.* This object links the management role group object with the management role object.
4. *Management role scope.* The Management role scope specifies which objects or containers are affected by the role. The scope can be restricted to a certain server, an OU, or even a custom recipient filter. For example, the “MyProfileInformation” role is scoped to “Self”.

The RBAC User Editor is a tool accessible from the toolbox in the Exchange Management Console. Similar to other ECP tools, this tool is launched in a web browser and can be accessed from anywhere. This tool allows some administration of management roles and association of users with management roles. Further administration can be performed by using Exchange Management Shell cmdlets such as: New-RoleGroup; Add-RoleGroupMember; New-RoleAssignmentPolicy and New-ManagementRole.

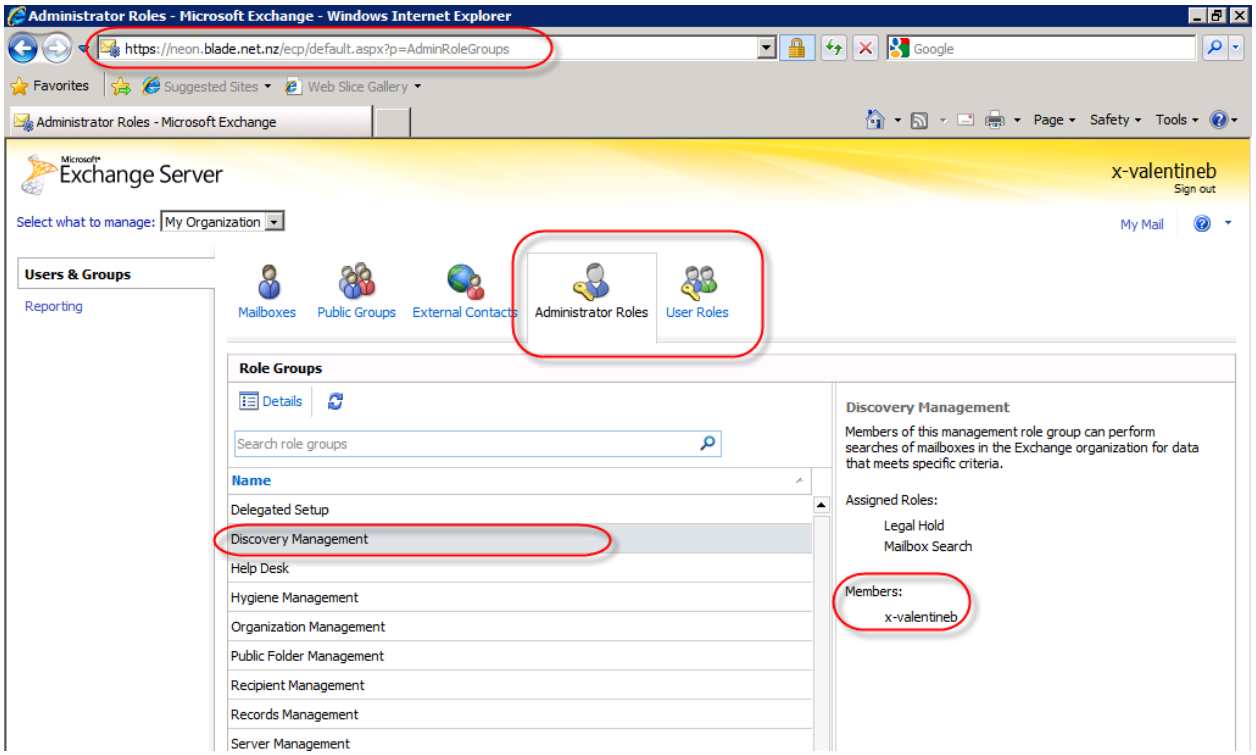

Figure 8 RBAC User Editor Tool - Managing Administrator Roles

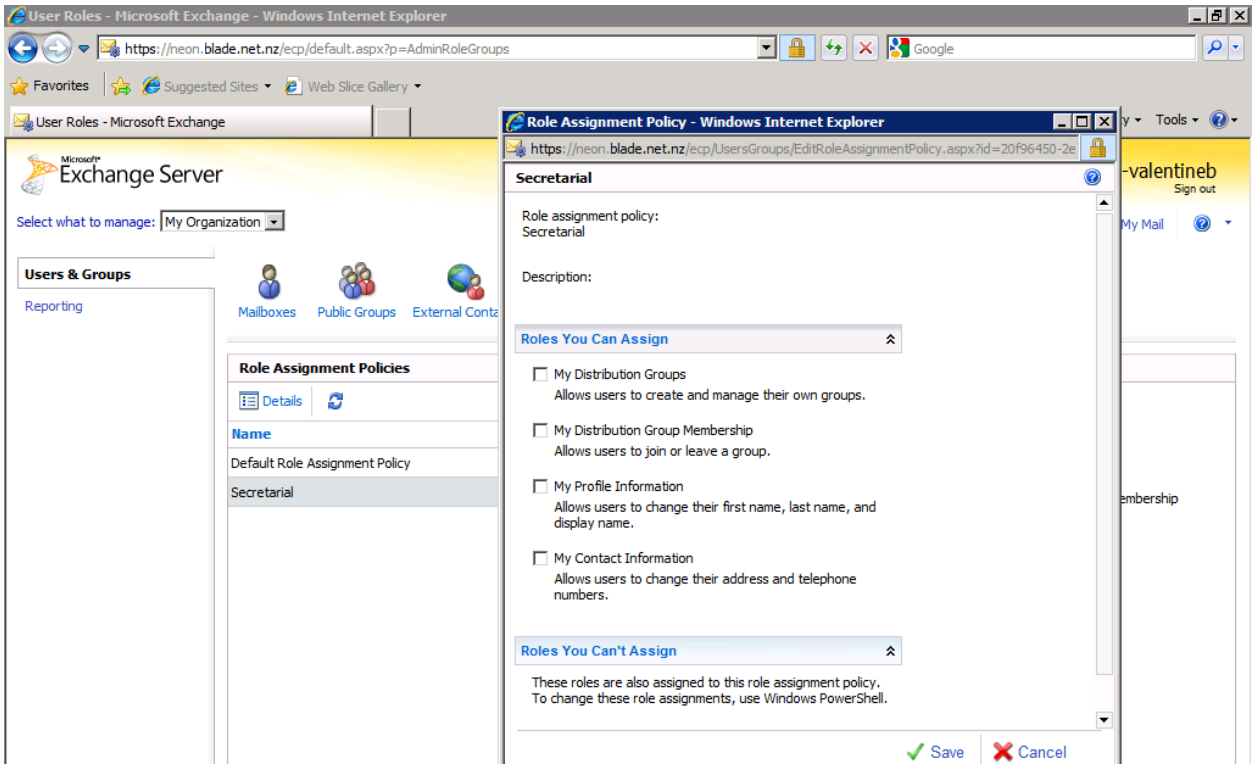

Figure 9 RBAC User Editor Tool - Managing Role Assignment Policies

Role based security allows organizations to apply fine-grained control to administrators, users and special accounts. It is possible, however, to accidentally add a wrong user to a role, and the possibility for malicious role exploitation still exists. An audit strategy that includes auditing management role changes will assist in mitigating these risks and identifying incidents.

Auditing Exchange 2010 with Quest ChangeAuditor for Exchange

Quest ChangeAuditor v 5.1 allows organizations to audit changes and access to key systems, including Microsoft Exchange 2010.

Administrator access auditing and mailbox audit logging are very powerful features available out-of-the-box; they are well suited to ad-hoc auditing. Some organizations will consider administrator access auditing and mailbox audit logging adequate for their auditing needs. However, if you need a formal audit strategy that includes scheduled audit reviews, as well as storing and viewing consolidated auditing data, you will find the built-in tools inadequate. While most activities of interest are logged by built-in auditing, it is difficult to present and search the information in a consolidated, structured format using built-in tools. It is possible to create custom Exchange Management Shell scripts to export, cleanse and consolidate the raw audit data from mailbox storage, however, reliance on these “home-grown” systems is often more expensive than implementing a purpose-built solution.

Before relying solely on administrator access auditing for auditing system changes, consider the following:

- Mixed topology and toolset. If your topology includes Exchange 2007 as well as Exchange 2010, and your administrators use Exchange 2007 tools and/or ADSIEdit, changes made using these tools will not be audited by administrator access auditing alone.
- Number of log entries. The number of messages written daily to the arbitration mailbox depends on the number of system changes performed. In an enterprise environment, this could be thousands. It may be prohibitively laborious to search for specific activities using the built-in tools alone. Additionally, it will be impossible to perform “routine audit log reviews,” since no one is able to read through and analyze several thousand log entries.
- Reporting requirements. If you require special reports or charts, built-in administrator access auditing tools will not be adequate for you.
- Proactive notifications. You may require a proactive notification when a certain event occurs.
- Data storage. Corporate or regulatory policies may require you to store audit logs for far longer than the default 90 days, perhaps as long as seven years. Storing this amount of auditing information for this long is not feasible, as you will probably upgrade your Exchange Server during this time, and the arbitration mailbox will grow to an unmanageable size.

Consider the factors above when choosing to rely solely on administrator access auditing’s built-in features. If you have a large number of daily changes and a complex messaging topology, a dedicated solution like Quest ChangeAuditor for Exchange may meet the requirements better than the built-in tools.

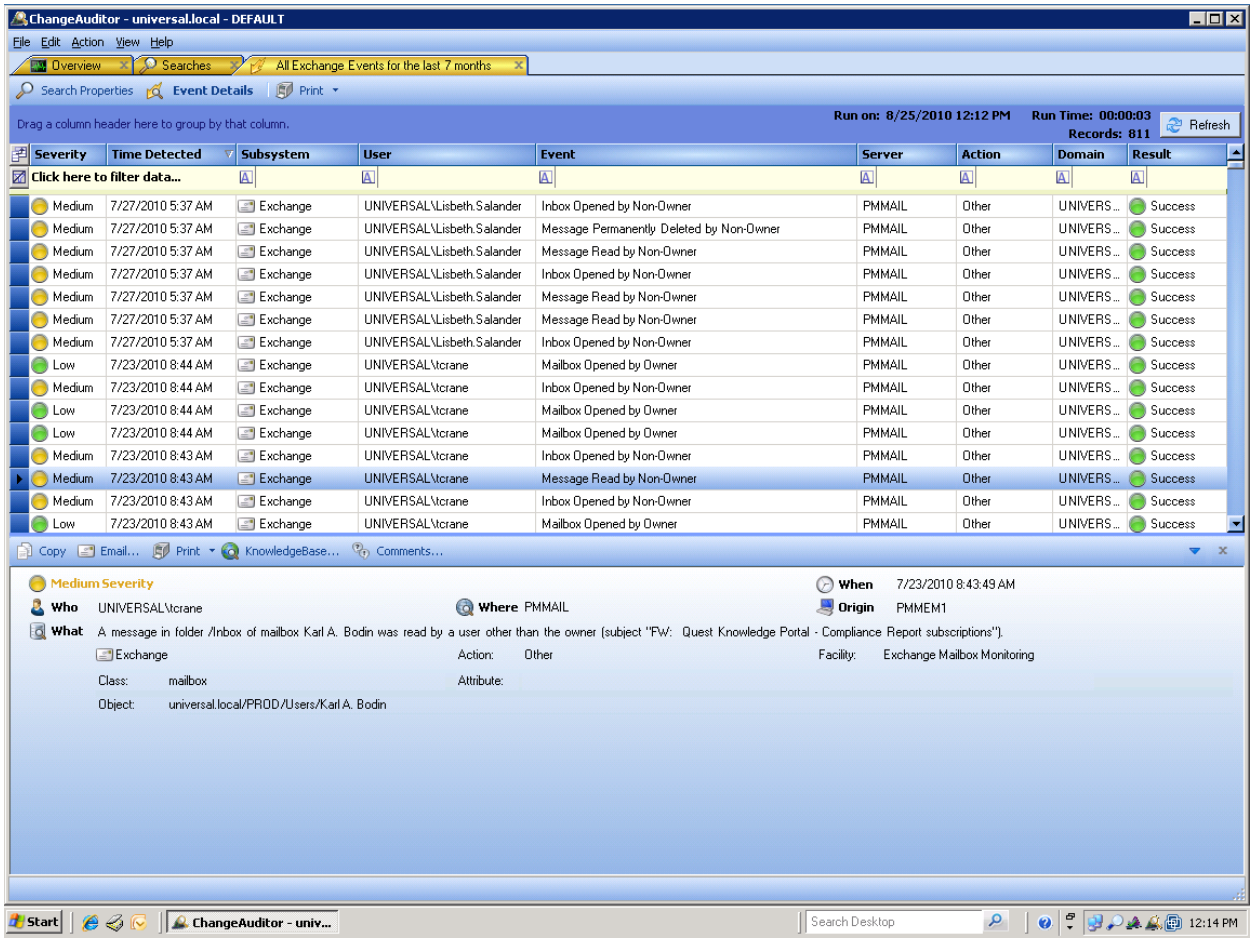

Figure 10 Quest ChangeAuditor Agent Configuration

Quest ChangeAuditor and Regulatory Compliance

Organizations that are required to comply with regulatory standards such as SOX, HIPAA and ISO will find Quest ChangeAuditor of special interest. Quest ChangeAuditor includes out-of-the-box reports that can be used to assess and monitor your compliance.

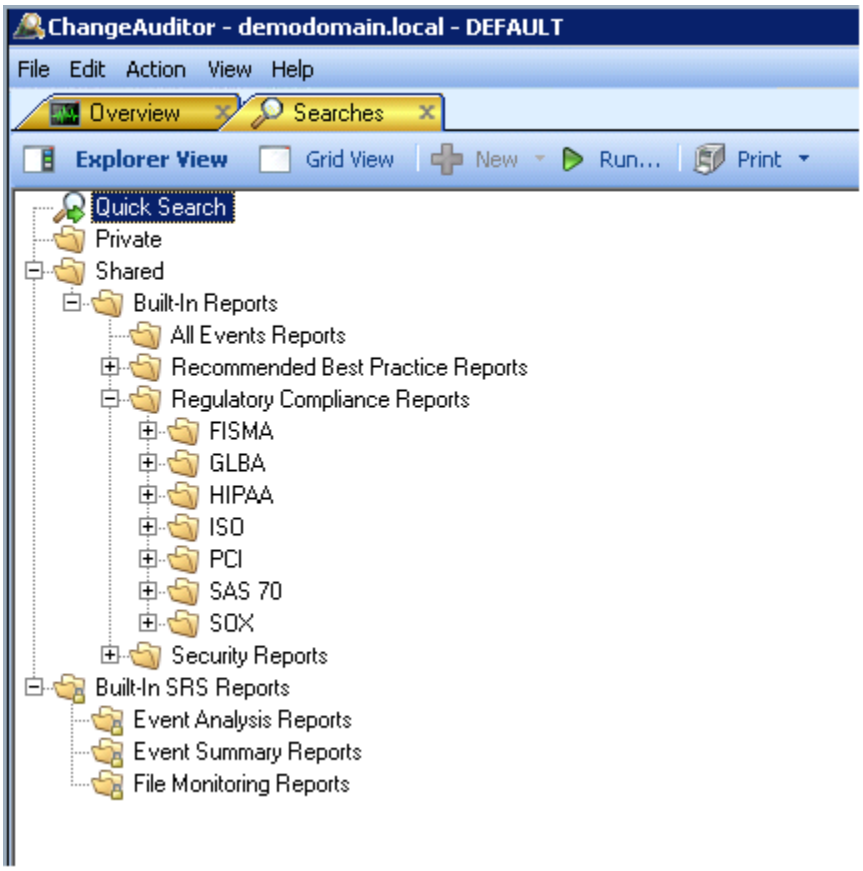

Figure 11 ChangeAuditor for Exchange Regulatory Compliance Reports

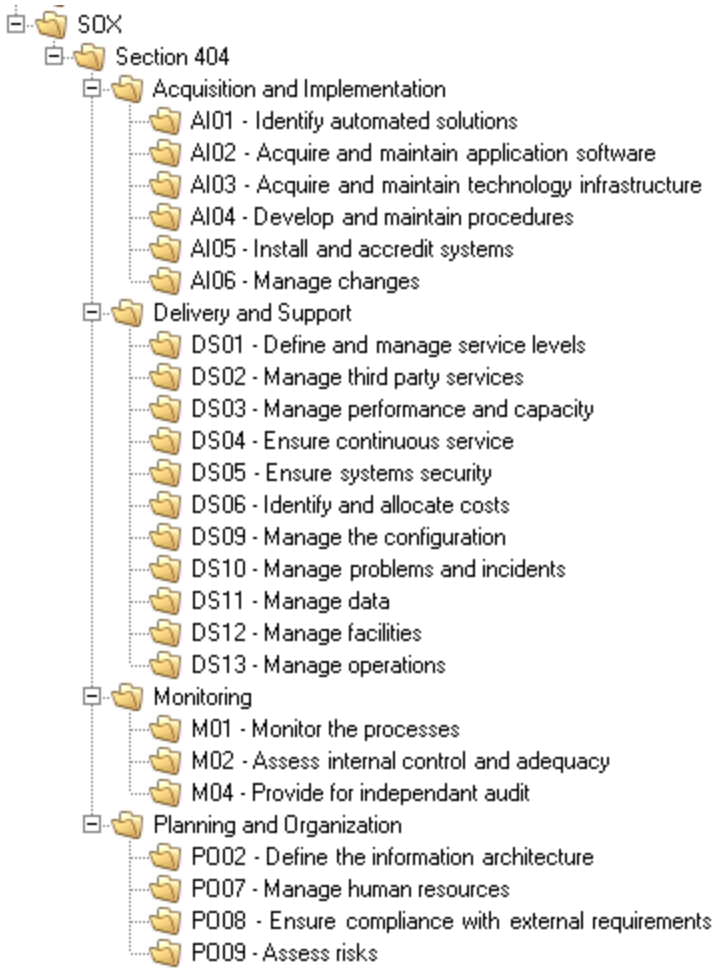

Figure 12 Quest ChangeAuditor SOX Reports

Conclusion

Exchange 2010 has introduced many new compliance, security and auditing features. A key development is the move towards role-based security with role-based access control (RBAC). RBAC places users into management role groups that are associated with management roles with one or more role entry tasks. Another key development is the introduction of self-service tasks, such as allowing users to manage their own Active Directory attributes. Many administrative tasks can now be performed from the web-based Exchange Control Panel, accessible to authorized users from anywhere connected to the Internet. These features provide new capabilities to your users and administrators, but also expand the need for auditing, accountability and control.

Exchange 2010 has redefined the way activities of interest can be logged. Unlike Exchange 2007, which uses the Windows SACL entries for configuring auditing and the security event log for viewing audit events, Exchange 2010 uses mailboxes to store audit entries.

Administrator access auditing examines cmdlets of interest as they are executed against Exchange 2010, and stores audit entries as messages in a special arbitration mailbox. Administrator access auditing can be configured using Exchange Management Shell cmdlets, and can be accessed using Exchange Management Shell cmdlets or the Exchange Control Panel.

Mailbox audit logging is a feature introduced in Exchange 2010 SP1. Mailbox audit logging can be configured for individual Exchange 2010 mailboxes using Exchange Management Shell cmdlets. Each audit log entry is stored as an e-mail message in a hidden area of the user's mailbox. It is possible to search through the audit log entries using the Exchange Control Panel or the Exchange Management Shell.

While these auditing improvements are excellent for ad-hoc auditing, larger organizations with more ongoing auditing requirements will find that audit configuration, data consolidation and reporting require custom scripts. The alternative of viewing individual audit log entries may prove unfeasible to organizations with a large amount of audit data collected.

If your organization has a complex messaging environment consisting of more than Exchange 2010, or if your audit strategy calls for ongoing auditing, summary reports and proactive notifications, you should consider a mature auditing solution like Quest ChangeAuditor for Exchange.

About Quest Software, Inc.

Quest simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest go to **www.quest.com**.

Contacting Quest Software

PHONE 800.306.9329 (United States and Canada)
If you are located outside North America, you can find your local office information on our Web site.

E-MAIL **sales@quest.com**

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

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 **https://support.quest.com**.

SupportLink gives users of Quest Software products the ability to:

- Search Quest's online Knowledgebase
- Download the latest releases, documentation, and patches for Quest products
- Log support cases
- Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policies and procedures.

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com
If you are located outside North America, you can find local office information on our Web site.