

Single Mailbox Recovery 6.0

Administrative Server User Guide

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089 U.S.A.
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>

Part number: 215-04998_A0
January 2010

Copyright and trademark information

Copyright information

Copyright © 1994-2010 NetApp, Inc. All rights reserved. Printed in the U.S.A.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Ontrack® PowerControls™ is a software application that has been developed, copyrighted, and licensed by Kroll Ontrack, Inc. Use of the software is governed by the terms and conditions of the end user license agreement contained within the software.

This manual should not be construed as any representation or warranty with respect to the software named herein. Occasionally, changes or variations exist in the software that are not reflected in the manual. Generally, if such changes or variations are known to exist and affect the product significantly, a release note or Read Me file will accompany the User Guide, or will be available on the Kroll Ontrack Web site. In that event, please read the release note or Read Me file before using the product.

Copyright © 2005 Kroll Ontrack Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into a language or computer language, in any form by any means, electronic, mechanical, optical, chemical, manual or otherwise, without the express written consent of Kroll Ontrack Inc.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Notice to Users

Ontrack® PowerControls™ Single Mailbox Recovery is a software application that has been developed, copyrighted, and licensed by Kroll Ontrack Inc. Use of the software is governed by the terms and conditions of the end user license agreement contained within the software.

This manual should not be construed as any representation or warranty with respect to the software named herein. Occasionally, changes or variations exist in the software that are not reflected in the manual.

Generally, if such changes or variations are known to exist and affect the product significantly, a release note or Read Me file will accompany the User Guide, or will be available on the Ontrack PowerControls NetApp web site. In that event, please read the release notes or Read Me file before using the product.

Trademark information

NetApp, the Network Appliance logo, the bolt design, NetApp—the Network Appliance Company, Cryptainer, Cryptoshred, DataFabric, DataFort, Data ONTAP, Decru, FAServer, FilerView, FlexClone, FlexVol, Manage ONTAP, MultiStore, NearStore, NetCache, NOW NetApp on the Web, SANscreen, SecureShare, SnapDrive, SnapLock, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapValidator, SnapVault, Spinnaker Networks, SpinCluster, SpinFS, SpinHA, SpinMove, SpinServer, StoreVault, SyncMirror, Topio, VFM, VFM (Virtual File Manager), and WAFL are registered trademarks of NetApp, Inc. in the U.S.A. and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The evolution of storage are trademarks of NetApp, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. The NetApp arch logo; the StoreVault logo; ApplianceWatch; BareMetal; Camera-to-Viewer; ComplianceClock; ComplianceJournal; ContentDirector; ContentFabric; Data Motion; EdgeFiler; FlexShare; FPolicy; Go Further, Faster; HyperSAN; InfoFabric; Lifetime Key Management, LockVault; NOW; ONTAPI; OpenKey, RAID-DP; ReplicatorX; RoboCache; RoboFiler; SecureAdmin; SecureView; Serving Data by Design; Shadow Tape; SharedStorage; Simplicore; Simulate ONTAP; Smart SAN; SnapCache; SnapDirector; SnapFilter; SnapMigrator; SnapSuite; SohoFiler; SpinMirror; SpinRestore; SpinShot; SpinStor; vFiler; VPolicy; and Web Filer are trademarks of NetApp, Inc. in the U.S.A. and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of NetApp, Inc. in the U.S.A.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks. NetApp, Inc. NetCache is certified RealSystem compatible.

Introduction	1
Overview	1
Single Mailbox Recovery Administrative Server 6.0 Enhancements.....	1
System Requirements.....	1
Installing Single Mailbox Recovery Administrative Server	3
Installation Recommendations	3
Uninstalling Single Mailbox Recovery Administrative Server	4
Upgrading Single Mailbox Recovery	4
Licensing.....	4
Getting Help.....	5
Online Help	5
Technical Support.....	5
Conventions in this Manual	5
Shortcut Menu	6
Notes and Tips.....	6
 Chapter 1: Administrative Server	 7
Overview	7
Looking at the Single Mailbox Recovery Management Console	7
Menu Bar.....	8
Single Mailbox Recovery Management Console First Run Configuration	11
Server Configuration Page.....	11
Server Configuration Tab.....	11
Active Connections Tab	14
Available Services Tab.....	14
 Chapter 2: Mailbox Permissions Service	 17
Overview	17
Mailbox Permissions Service First Run Configuration	17
Permission Model	18
Horizontal Check.....	18
Vertical Check	20

Examples of Use.....	21
Specific (Internal) Tab	22
Adding a Mailbox.....	22
Adding and Removing a User or Group.....	23
Setting Permissions for a Mailbox	24
Sorting the Permission Order	25
Specific (External) tab	27
Adding a Mailbox.....	27
Adding and Removing a User or Group.....	29
Setting Permissions for a Mailbox	30
Sorting the Permission Order	31
Mailbox Categories Tab.....	32
Setting the Mailbox Category.....	32
Adding and Removing a User or Group.....	32
Setting Permissions for all Mailboxes Internal or External to this Domain.....	34
Sorting the Permission Order	35
All Mailboxes Tab	37
Adding and Removing a User or Group.....	37
Setting Permissions for All Mailboxes.....	39
Sorting the Permission Order	40
Manage Refusals Tab.....	42
Allowing a Refusal.....	42
Clearing, Reloading, and Saving.....	44
Using the Wizard	44
Chapter 3: Application Auditing Service	53
Overview.....	53
Types of Activities that are Logged.....	53
Client Activities that are Logged.....	53
Server-Side Activities that are Logged.....	54
Audit Service First Run Configuration	54
Skip Button.....	54
Advertising on Active Directory	54
Manage Logs Tab.....	55
Log Directory Tree	56
Audit Logs	56

Configuration Tab.....	61
Audit Store Root Path.....	61
24-Hour Log Rollover Time.....	63
Appendix A: Activities to be Logged	65
Client-Side Activities to be Logged.....	65
Single Mailbox Recovery for Exchange User Interface Actions	65
Single Mailbox Recovery for Exchange Command Line Actions	66
Data Wizard.....	67
Single Mailbox Recovery ExtractWizard Actions	67
Server-Side Activities that are Logged	68
Server Log	68
Mailbox Permissions Service Session Log.....	68
Single Mailbox Recovery Management Console Session Log	69
Server Configuration Plug-In	69
Glossary.....	71
Index.....	73

Overview

Welcome to NetApp® Single Mailbox Recovery Administrative Server 6.0. This application is a framework that can host centralized services to multiple clients and provide both client and server support for Single Mailbox Recovery 6.0 and Single Mailbox Recovery ExtractWizard users.

Single Mailbox Recovery Administrative Server includes:

- **Server Configuration:** You can monitor the active connections and available services, change ports, restart or stop server, and elect to be discovered in Active Directory.
- **Mailbox Permissions Service:** In order to reinforce your internal corporate security policies, you can restrict access in Single Mailbox Recovery 6.0 to mailboxes contained within private EDB Exchange mailbox stores based on your authority.
- **Application Auditing Service:** Activities performed as part of Single Mailbox Recovery 6.0 and Single Mailbox Recovery ExtractWizard operations, as well as activities within Single Mailbox Recovery Administrative Server, are logged as part of an “audit trail.”

You can manage these services using the Single Mailbox Recovery Management Console, which is the main interface for using this product.

Single Mailbox Recovery Administrative Server 6.0 Enhancements

Single Mailbox Recovery Administrative Server 6.0 contains all the features and benefits of Single Mailbox Recovery Administrative Server 1.1 plus these exciting new and improved features:

- Support for Microsoft Exchange 2007 SP2 and Exchange 2010

System Requirements

Single Mailbox Recovery Administrative Server requires the following minimum system configuration:

- One of the following operating systems:
 - Windows Server® 2003
 - Windows Server® 2008 Standard
 - Windows Server 2008 Data Center
 - Windows Server 2008 Enterprise
 - Windows® Vista Business
 - Windows Vista Ultimate

- Windows Vista Enterprise

Note: The operating systems are required to have the latest service packs installed.

- The following virtual environments are supported:
 - VMware® Server 1.0x, 2.x
 - VMware® Workstation v6.0x for Windows
 - Microsoft® Virtual Server™ 2005 R2
 - Microsoft® Hyper-V Server™ 2008 R2
 - Microsoft® Virtual PC 2007
 - VMware® ESX 3.5, ESXi

Note: Single Mailbox Recovery Administrative Server is not supported on Windows Vista 64-bit virtual operating systems.

Note: HASP key operation is validated in environments that support USB attached devices and support the NetApp distributed HASP drivers only.

- Microsoft® .NET Framework 3.5: System must have .NET Framework 3.5 installed in order to function.
- Intel® Pentium® 4 class or higher compatible processor
- 2 GB RAM
- 200 MB of free hard disk space for the installation. Additional disk space will be required to store log information as the system runs.
- Monitor with 800 x 600 or higher screen resolution
- High-speed TCP/IP LAN network connection, minimum of 100 Mbps recommended.
- USB port (for Single Mailbox Recovery product licenses requiring HASP key dongle to run application)
- Windows-based domain network environment. The system running Single Mailbox Recovery Administrative Server, and all systems running Single Mailbox Recovery for Exchange and Single Mailbox Recovery ExtractWizard, must be joined to the same Windows-based network domain (or a trusted domain). Users must be logged in as a user of that domain when running Single Mailbox Recovery for Exchange. To ensure correct operation, the Single Mailbox Recovery Administrative Server Administrator should be logged in as a domain user with Administrator rights on the local system running Single Mailbox Recovery Administrative Server, in order to install and configure Single Mailbox Recovery Administrative Server. The domain account will also need authority to update Active Directory (e.g. Domain Admin), if you wish to advertise Single Mailbox Recovery Administrative Server services on Active Directory.
- In order to ensure correct operation of the Single Mailbox Recovery Administrative Server and any Single Mailbox Recovery for Exchange and Single Mailbox Recovery ExtractWizard clients, firewall solutions must be configured to allow communication on the TCP port Single Mailbox Recovery Administrative Server is configured to use. The TCP port number can be configured via the Single Mailbox Recovery Management Console.

Installing Single Mailbox Recovery Administrative Server

.....

Before you install Single Mailbox Recovery Administrative Server, it is recommended that you consider your installation strategy including the availability of Single Mailbox Recovery Administrative Server around the clock, the security Single Mailbox Recovery Administrative Server will be providing and how your installation location could impact the level of security, and your available resources for application installation.

Installation Recommendations

Availability: It is recommended that the Single Mailbox Recovery Administrative Server installation be on a distinct machine from Single Mailbox Recovery. Single Mailbox Recovery Administrative Server is a server and should be available 24/7. If Single Mailbox Recovery Administrative Server is not available, Single Mailbox Recovery and Single Mailbox Recovery ExtractWizard will not function. A workstation with these applications running is far more likely to be rebooted in the course of normal work and shutdown overnight. Single Mailbox Recovery Administrative Server can be run on an Exchange Server but because an Exchange Server is a mission critical system, especially for larger organizations, it isn't recommended but is still up to you to decide.

Security: Single Mailbox Recovery Administrative Server is the provider of security related services (auditing and mailbox permissions), so it would be best practice to separate the user and Administrator roles. Running Single Mailbox Recovery and Single Mailbox Recovery Administrative Server on the same system could compromise the integrity of the security provided by mailbox permissions and auditing functions. However, if the Administrator of Single Mailbox Recovery Administrative Server is also a user of Single Mailbox Recovery, having them both installed on the same machine makes sense.

Resources: Single Mailbox Recovery Administrative Server is a server and needs sufficient resources to run efficiently. If your organization needs to run multiple installations of Single Mailbox Recovery simultaneously, having a dedicated, server type system would service client requests more efficiently. Attempting to run Single Mailbox Recovery Administrative Server on a system running other applications, such as Microsoft® Exchange Server or Single Mailbox Recovery, could result in compromised or slower performance.

To install Single Mailbox Recovery Administrative Server

1. Turn off any disk utility or antivirus program running in the background.
2. Insert the Single Mailbox Recovery Administrative Server CD-ROM into your CD-ROM drive.
3. The installation program will automatically start. If it does not:
 - **For Windows Server 2003 and earlier:** Click **Run** on the **Start** menu, and type D:\autorun.exe or D:\bin\setup.exe, where D is the drive letter of your CD-ROM drive. Click **OK**.
 - **For Microsoft Vista and Windows Server 2008:** Click **Run** on the **Start/All Programs/Accessories** menu, and type D:\autorun.exe or D:\bin\setup.exe, where D is the drive letter of your CD-ROM drive. Click **OK**.
4. Follow the on-screen instructions.

Uninstalling Single Mailbox Recovery Administrative Server

You can uninstall Single Mailbox Recovery Administrative Server by running the uninstall program.

1. Click the **Start** button and then click **Control Panel**. (In Windows 2000 and earlier, you will point to **Settings** before you click Control Panel.)
2. In Control Panel:
 - For Windows Server 2003 and earlier:** Click the **Add or Remove Programs** icon.
 - Click **Single Mailbox Recovery Administrative Server**, and then click **Change/Remove**.
 - Click **Yes** when the confirmation dialog box appears.
 - For Microsoft Vista and Windows Server 2008:** Click Uninstall a program under the Programs heading.
 - Click **Single Mailbox Recovery Administrative Server**, and then click **Uninstall/Change**.
3. Follow the on-screen instructions.

Upgrading Single Mailbox Recovery

Single Mailbox Recovery Administrative Server 6.0 is not compatible with Single Mailbox Recovery Administrative Server 1.1 or earlier license files.

Licensing

All Single Mailbox Recovery Administrative Server editions require an active license file. The purpose of this file is to let you buy only those features you need. Before Single Mailbox Recovery Administrative Server is enabled, it checks the .ini file for three things:

- The license file must be valid for Single Mailbox Recovery Administrative Server 6.0.
- Server name enforcement if applicable.
- Subscription length if applicable.

Note: Only licensed machines can run Single Mailbox Recovery Administrative Server. Single Mailbox Recovery Administrative Server can be licensed for use on one or more specific machines. If you are unable to operate the software, contact your sales representative with the error reason code for further assistance.

Getting Help

.....

NetApp provides you with the following ways to get help for Single Mailbox Recovery Administrative Server:

Online Help

Online Help includes all of the information in the user guide and more, and it lets you quickly access this information by using one of three tabs. The Contents tab offers a hierarchical view of the contents of the user guide. The Search tab offers a full-text search of the user guide. The Index tab offers a keyword-based way to get to specific topics.

To start online Help

Do one of the following:

- On the **Help** menu, click **Contents**.
- Press the **F1** key.

Technical Support

If you have questions or problems not answered in the user guide or the online Help, call our Technical Support group. When reporting an issue, please include any information that might help us diagnose the problem. The following details are often the most helpful:

- The version of Single Mailbox Recovery Administrative Server you are using (on the **Help** menu, click **About**).
- The versions of Windows that you are running.
- The version of Exchange Server that contained the Source EDB file.
- The circumstances and sequence of steps that led to the problem.
- The text of the error messages (if any appeared), and the contents of the **Details** window.
- A list of other Windows programs that you were running when the error occurred.

Contact Information

See “Contact Information” at the beginning of this user guide.

Conventions in this Manual

.....

This manual uses guidelines for commands available on the shortcut menu and in notes and tips.

Shortcut Menu

You can access many of the same commands available on the menu bar by right-clicking the mouse to display a shortcut menu. This manual seeks to teach you how to use commands on the menu bar, and doesn't always specify when you can use the shortcut menu. Once you become familiar with Single Mailbox Recovery Administrative Server, the commands available to you on the shortcut menu should become apparent.

Notes and Tips

The notes and tips in this user guide follow the guidelines offered in the *Microsoft Manual of Style for Technical Publications*, 3rd Edition. Redmond, WA: Microsoft Press, 2004.

ADMINISTRATIVE SERVER

.....

Overview

.....

NetApp® Single Mailbox Recovery Administrative Server activates mailbox permissions and provides auditing services for Single Mailbox Recovery for Exchange and Single Mailbox Recovery ExtractWizard client and server.

When you launch Single Mailbox Recovery 6.0, it attempts to connect to Single Mailbox Recovery Administrative Server if it is activated. Single Mailbox Recovery Administrative Server is located automatically using a Service Connection Point (SCP) in the Active Directory, or a server whose details have been manually provided by you.

After connecting to the server, Single Mailbox Recovery can utilize the services you have opted to activate—mailbox permissions service or application auditing service. These services are configured and monitored using the Single Mailbox Recovery Management Console.

Looking at the Single Mailbox Recovery Management Console

.....

The Single Mailbox Recovery Management Console is the main user interface that allows you to configure and monitor Single Mailbox Recovery Administrative Server and the installed services. You can use the Single Mailbox Recovery Management Console to configure services and determine whether or not they are active and therefore made available to clients.

Multiple clients can simultaneously use the services hosted by the server. At a minimum, it supports 50 concurrent users.

Single Mailbox Recovery Administrative Server opens to the Single Mailbox Recovery Management Console which contains a Server configuration button, the installed services buttons, and configuration pages for each service.

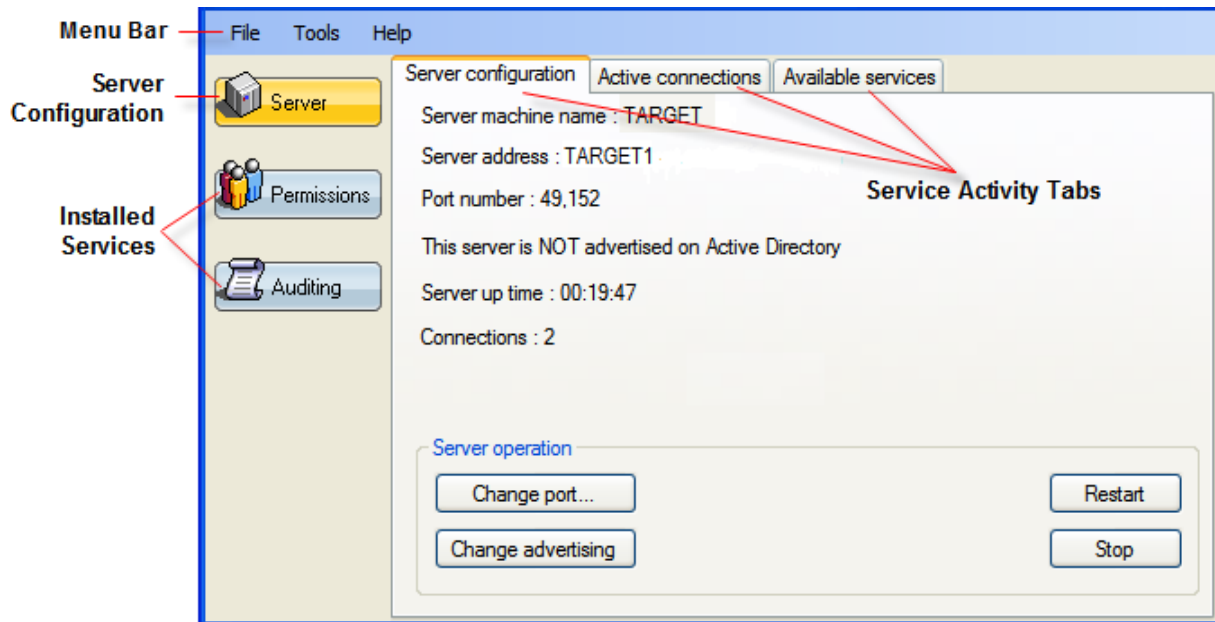


Figure 1-1. Single Mailbox Recovery Management Console main window

Menu Bar

In the menu bar, the options of Plugin Activation and Deactivate plugins are available under the Tools menu.

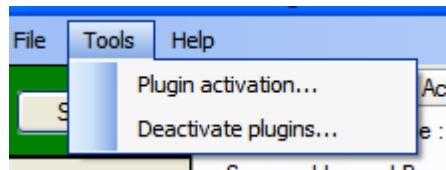


Figure 1-2. Plugin Activation/Deactive Plugins options

PLUGIN ACTIVATION

If you deactivate or skip a plugin during the Single Mailbox Recovery Administrative Server finalization (on Single Mailbox Recovery Management Console first run), you can activate it with the Plugin Activation menu item. Any deactivated/skipped plugins activate as a result of selecting this option.

After selecting this option, Single Mailbox Recovery Management Console checks to see if any plugin is currently active. If the plugin is active, its finalization window appears.

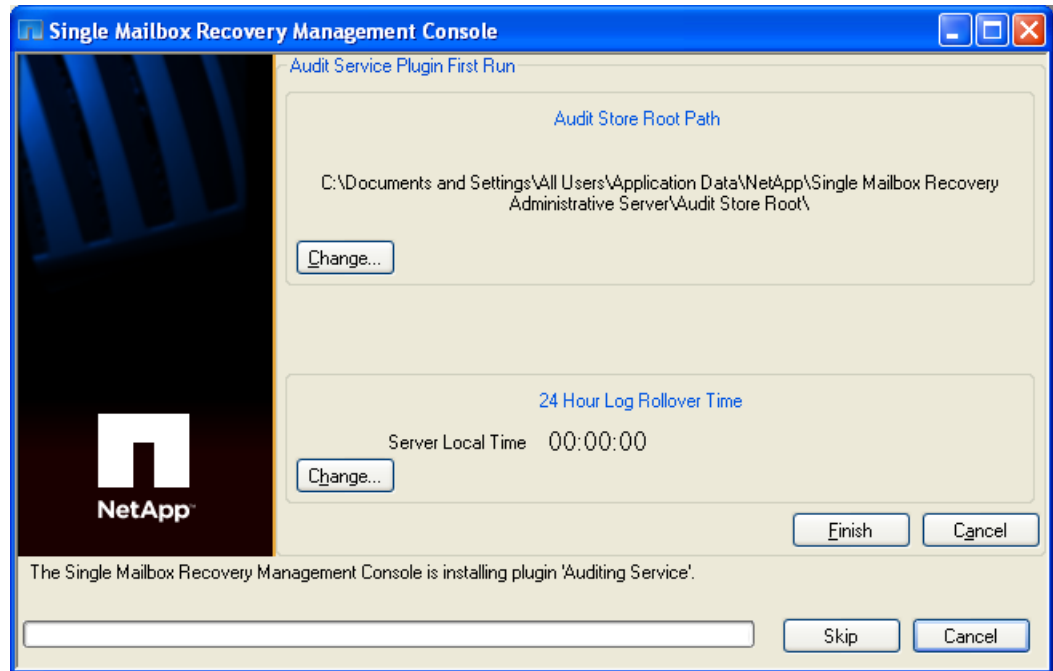


Figure 1-3. Example of finalization window for Auditing

After you click Finish, Single Mailbox Recovery Management Console moves onto the next inactive plugin (if there is one). Once all plugins are activated, a message appears stating that Single Mailbox Recovery Administrative Server needs to be restarted for changes to take effect.

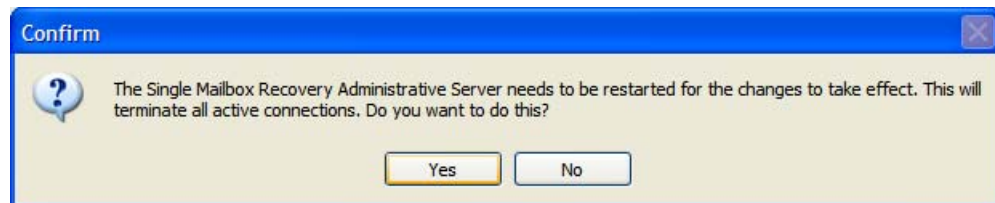


Figure 1-4. Confirm activation message

If you click Yes, the server restarts and the newly activated plugins are available, both for configuration and management within Single Mailbox Recovery Management Console and for client use.

If you click No, the server does not restart and the plugin(s) are not activated until the server is next restarted (for example, by clicking the Restart button on the server configuration page or by rebooting the system). See "Server Operation" on page 12 for more information.

DEACTIVATE PLUGINS

You can use the Deactivate Plugins menu item to deactivate any currently active plugins. The act of deactivation removes the plugin from the Single Mailbox Recovery Management Console so it cannot be configured or managed, and prevents client applications from using the service they provide. After you select Deactivate Plugins from the Tools menu, the Plug-in deactivation window appears.

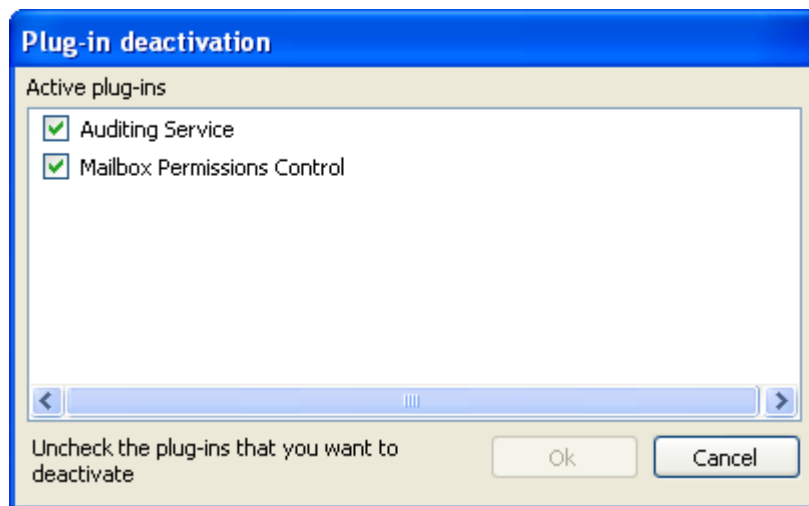


Figure 1-5. Plug-in deactivation window

Deselect the plugin or plugins that you wish to deactivate. After you click OK, a message appears stating that Single Mailbox Recovery Administrative Server needs to be restarted for changes to take effect.

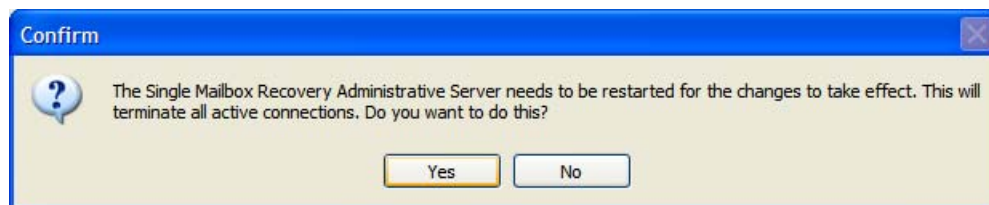


Figure 1-6. Confirm deactivation message

If you click Yes, the server restarts and the deactivated plugin(s) are no longer available, either for configuration/management or for client use. If you click No, the server does not restart and the plugin(s) are not deactivated until the server is next restarted (for example, by clicking the Restart button on the server configuration page or by rebooting the system). See “Server Operation” on page 12 for more information.

Plugin deactivation (skipping during finalization) can be useful if you determine you want just one service but not the other. For example, your organization needs to audit activity, but does not need to enforce access permissions for mailboxes contained within EDB files.

Single Mailbox Recovery Management Console First Run Configuration

.....

After installation, when Single Mailbox Recovery Management Console is run for the first time, it will prompt you to finalize the installation.

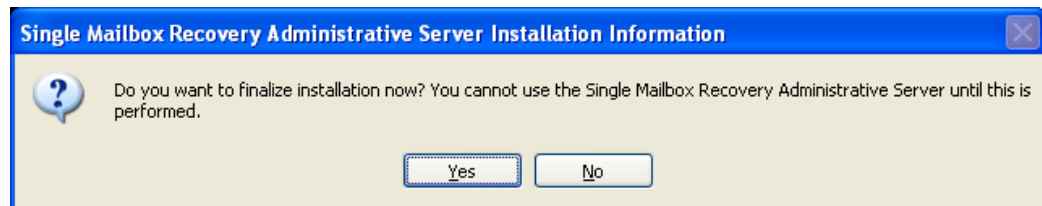


Figure 1-7. Finalize installation

If you click No, Single Mailbox Recovery Management Console closes and clients will not be able to connect. If you click Yes, Single Mailbox Recovery Management Console finalizes each of the plug-ins. For details on the finalization for Mailbox Permissions and Applications Auditing, see “Mailbox Permissions Service First Run Configuration” on page 17 and “Audit Service First Run Configuration” on page 54.

Server Configuration Page

.....

The Server Configuration page is available by clicking the Server button in the main window of Single Mailbox Recovery Administrative Server. The right pane contains three tabs that you can use to configure the server, view the configuration settings, and monitor the activity of the services.

Server Configuration Tab

The *Server Configuration* tab displays your server machine name, the server address, the port number, whether the server is advertised on Active Directory, the server up time which displays how long the Single Mailbox Recovery Administrative Server has been running in the current session, and the number of connections.

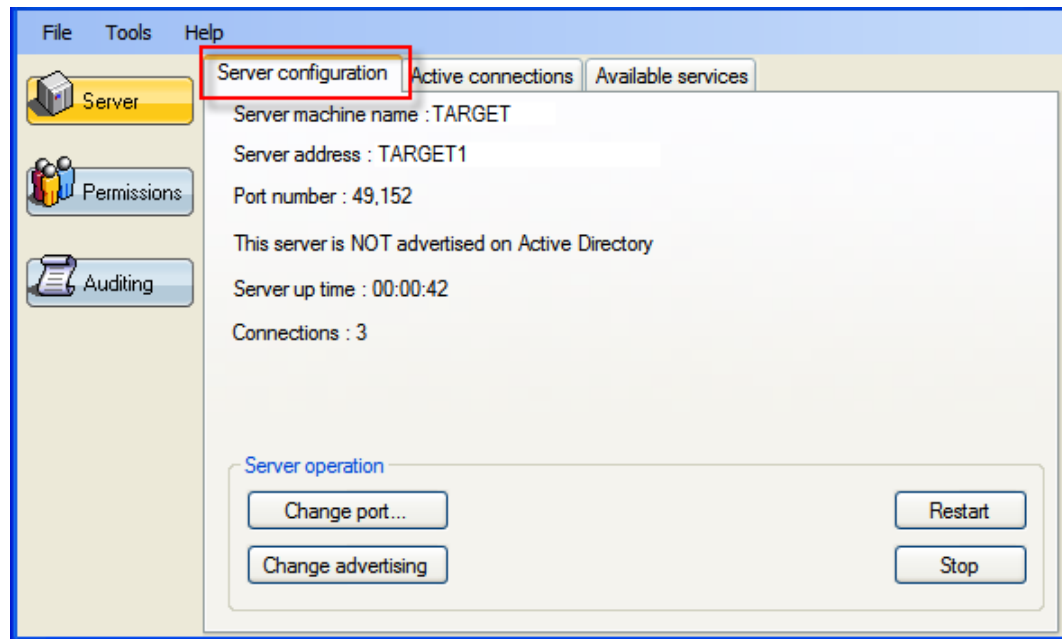


Figure 1-8. Server Configuration tab

SERVER OPERATION

The Server operation section allows you to change the current port, advertise on Active Directory (AD), restart the server, or stop the server connection.

Change port

You can change the server connection port by clicking the Change port button. A confirmation message appears if you have active connections.

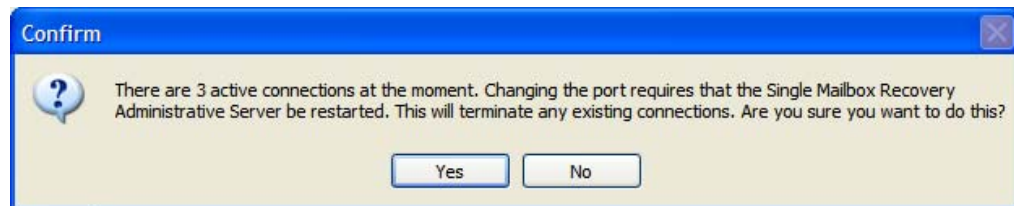


Figure 1-9. Confirmation message for changing ports with active connections

Changing the port number only takes affect when the server is restarted.

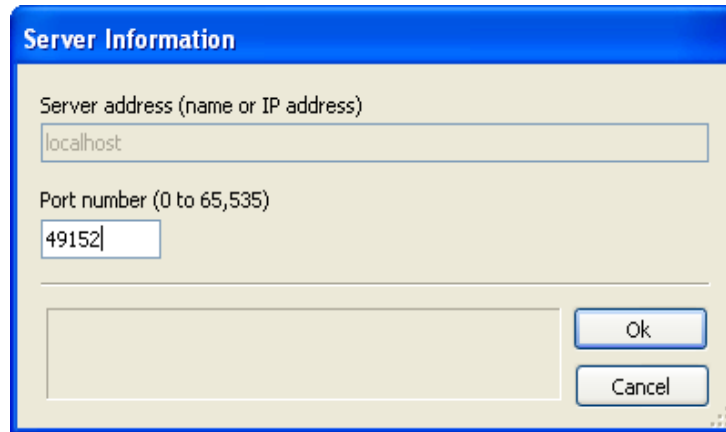


Figure 1-10. Server Information

If the server is currently advertising on Active Directory, the port change immediately updates the Service Connection Point (SCP).

Note: In order to ensure correct operation of the Single Mailbox Recovery Administrative Server and any Single Mailbox Recovery for Exchange and Single Mailbox Recovery ExtractWizard clients, firewall solutions must be configured to allow communication on the TCP port Single Mailbox Recovery Administrative Server is configured to use. The TCP port number can be configured via the Single Mailbox Recovery Management Console.

Change Advertising

Upon the first run, the Single Mailbox Recovery Administrative Server asks you if the Single Mailbox Recovery Administrative Server should be discoverable in Active Directory. You must have the authority to update the Active Directory. With the Change advertising button, this setting can be changed at any time.

A confirmation message appears if you change the setting.

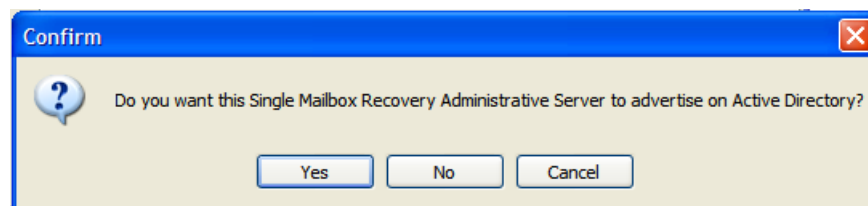


Figure 1-11. Confirm advertising on Active Directory

Restart

You can restart the server with the Restart button, which causes any connected clients to lose their connections to the server and close down. You will be prompted to confirm this action.

Stop

You can terminate the connection to the server by clicking the Stop button. You will be prompted to confirm this action. Once the server is stopped, it cannot be connected to by client applications, and therefore are unable to run. You can start the server again by launching the Single Mailbox Recovery Management Console.

Active Connections Tab

The *Active Connections* tab shows the active connections to the server and allows you to terminate selected connections.

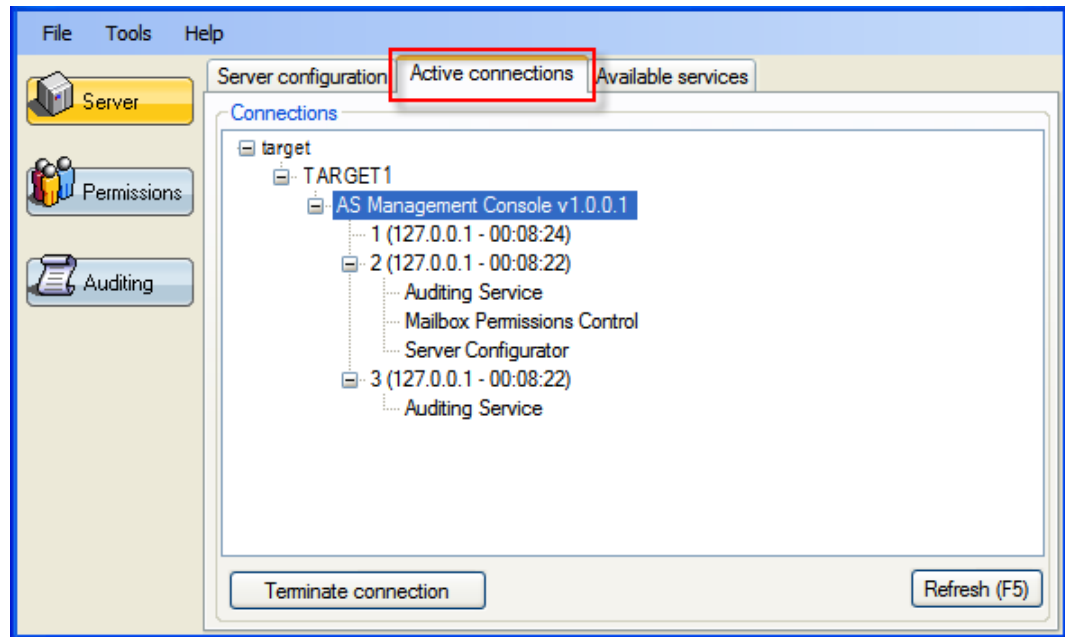


Figure 1-12. Active Connections tab

CONNECTIONS

The Active connections tree displays the user node, the name of the machine that you are currently running on, the application you are connected to, the session number, and the Single Mailbox Recovery Management Console plug-ins that are currently activated.

TERMINATE

You can break the connection to the server by clicking the Terminate connection button.

REFRESH

You can update the information on the page by clicking the Refresh button.

Note: The information on the page is automatically refreshed every 10 seconds.

Available Services Tab

The *Available Services* tab lists all the installed services and shows which connections are currently using them.

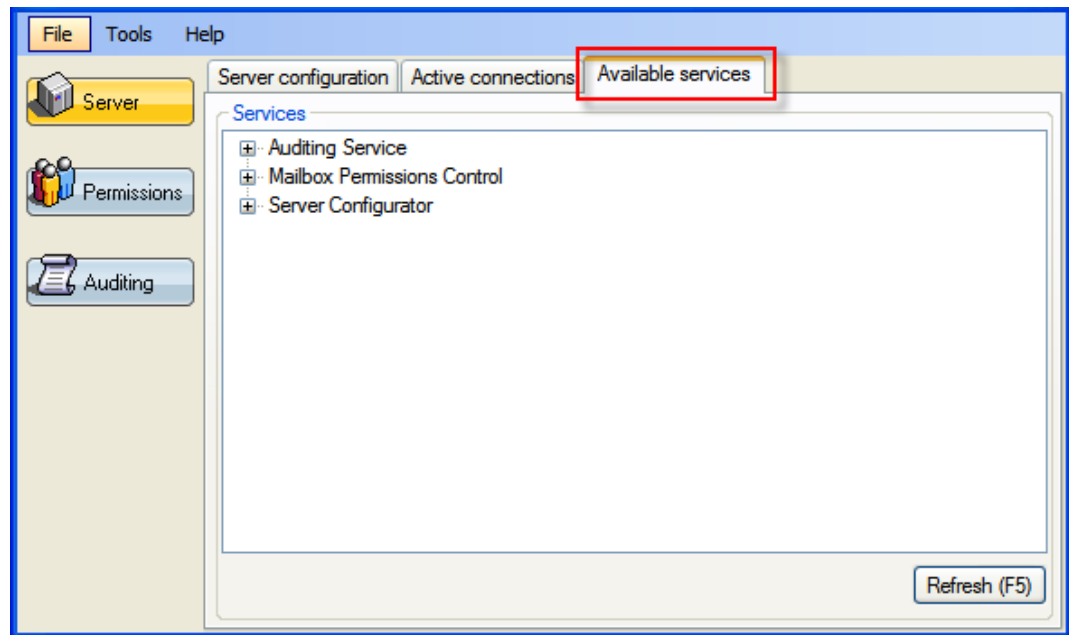


Figure 1-13. Available Services tab

SERVICES

The Available services tab displays the same information as the Active connections tab, but it is arranged by service.

Refresh

You can update the information on the page by clicking the Refresh button.

Note: The information on the page is automatically refreshed every 10 seconds.

MAILBOX PERMISSIONS SERVICE

Overview

NetApp® Single Mailbox Recovery Administrative Server provides you the ability to restrict access to mailboxes contained within private Exchange mailbox stores to clients using Single Mailbox Recovery for Exchange. To assist you in reinforcing your corporate security policies, you can set permissions on internal and external mailboxes to your domain, to groups or individuals, and in any configuration.

Permissions fall into one of five categories:

- **Internal Mailboxes:** These permissions apply to specific mailboxes that exist within the current domain.
- **External Mailboxes:** These permissions apply to specific mailboxes that do not exist within the Administrator's current domain.
- **Mailbox categories:** These permissions apply to mailboxes according to their category.
- **All Mailboxes:** These permissions apply to all mailboxes.
- **Refusals List:** Any mailbox that does not find a match or are denied access end up in this list.

Important Note: The Mailbox Permissions Service is supported for cases in which both server and client systems are joined to the same domain. The Mailbox Permission Service is not supported for scenarios in which the client system(s) are operating in a different domain to the server.

Note: The Mailbox Permissions Service is able to control access to individual mailboxes contained within offline Microsoft Exchange EDB data stores originating from Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007 (including SP1 and SP2), and Microsoft Exchange 2010. Please note that mailboxes contained within an EDB data store from Microsoft Exchange 5.5 cannot be recognized as internal and will therefore always be treated as external.

Mailbox Permissions Service First Run Configuration

When the permissions service plug-in is first installed using the Single Mailbox Recovery Management Console, a wizard appears allowing you to set up some initial permission settings. See "Using the Wizard" on page 44 for more information.

Permission Model

When a user in Single Mailbox Recovery for Exchange 6.0 attempts to access a mailbox contained within a private Exchange mailbox store (EDB file), the access request processes through the permission settings starting with Specific mailboxes (internal or external) and ending up with All mailboxes. Any user denied access at every level or finds no match ends up in the Manage refusals tab. This processing system is called a *Permission Model*.

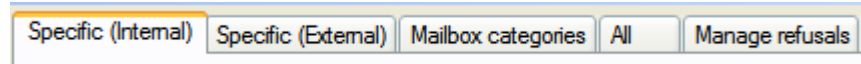


Figure 2-1. Mailbox Permission tabs

Horizontal Check

The *Permission Model* is based on a 3-tier check. The permissions for a particular mailbox or category contain a list of domain users and/or groups, each with a deny or allow permission designation.

Tier 1

- **Specific (Internal) mailbox permissions:** These are mailboxes that are within the Administrator's domain and are in the Active Directory. If permission settings exist for the specific mailbox and the user, whether *Deny* or *Allow*, these determine whether permission is granted or denied. If there is no match (deny or allow), the access request goes to *Mailbox Categories (Tier 2)* permissions.
- **Specific (External) mailbox permissions:** These are mailboxes that are outside the domain and are not in the Active Directory. If permission settings exist for the specific mailbox and the user, whether *Deny* or *Allow*, these determine whether permission is granted or denied. If there is no match (deny or allow), the access request goes to *Mailbox Categories (Tier 2)* permissions.

Tier 2

- **Mailbox Categories permissions (internal or external):** These are internal and external mailboxes grouped by category. If permission settings exist for the user, whether *Deny* or *Allow*, these determine whether permission is granted or denied. If there is no match (deny or allow), the access request goes to *All (Tier 3)* mailboxes.

Tier 3

- **All mailboxes permissions:** This is a catch-all listing of mailboxes that allows you to set permissions for all mailboxes at one time. If permission settings exist for the user, whether *Deny* or *Allow*, these will determine whether permission is granted or denied. If there is no match or permission is denied, the mailbox goes to the *Manage Refusals* list.

-
-
-
-

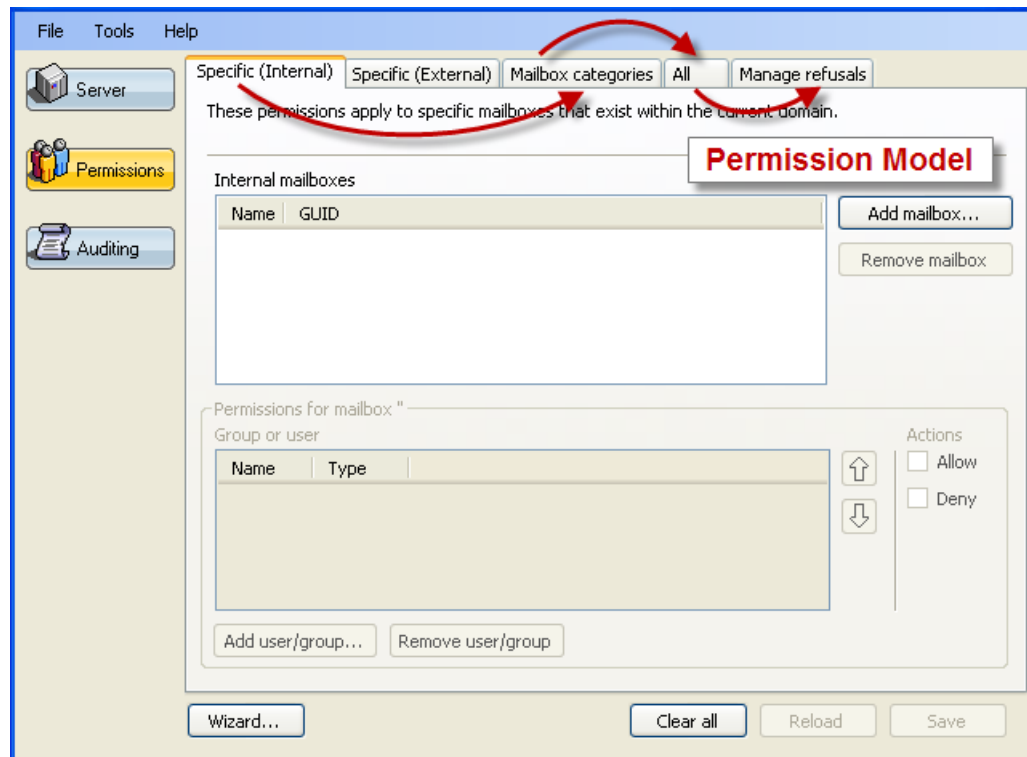


Figure 2-2. Permission Model

Vertical Check

As the requested mailbox name moves through each tab, the access request also processes vertically through the Permissions settings in the Group or user section. The user requesting access to the mailbox moves through the list of domain users and/or group from top to bottom until a match is found, to determine whether access has been allowed or denied.

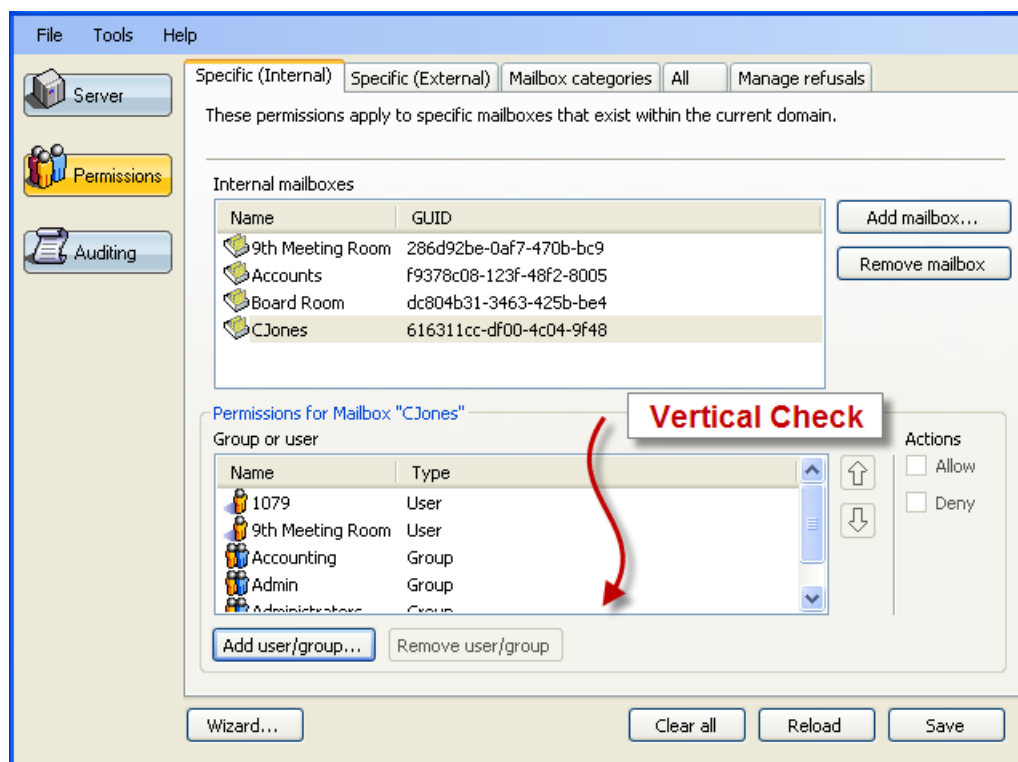


Figure 2-3. Vertical Permission Check

If the access request finds a match, it stops searching and uses whatever permission setting is set for its match.

Note: If there is a match further down the list in another group and the permission is a different setting, the access request only uses the first hit of that match.

If the access request does not find a match in one tier, it continues on through each tier and the permissions settings for each tier. If there is no match in any tier or Group or user list, or it finds a match and the permission setting is “Deny,” it lands in the Manage Refusals list.

MANAGE REFUSALS LIST TAB

Any access request that moves through the 3-tier check and was not matched at any level or was matched and the permission setting is “Deny,” the mailbox ends up in the Manage Refusals list. Temporary or permanent permission can be set for any mailbox in the Manage Refusals list. See “Manage Refusals Tab” on page 42 for more information.

Examples of Use

1. **Scenario #1:** The Administrator sets the “Any” user permission setting on “Deny” in the All mailboxes tab. All mailboxes are inaccessible as a result. The Administrator needs access to the CEO’s mailbox in an EDB file.

The CEO is internal to the Administrator’s domain, and access should only be provided to this mailbox, while all other mailboxes remain inaccessible. He adds the CEO’s mailbox into the Specific (Internal) mailbox list using the “Add Mailbox” button on that page. He then adds his user name to the users and/or group list using the “Add user/group...” button and sets the permission to “Allow.”

Since the CEO’s mailbox is listed on the specific internals list and this is processed first, when the Administrator uses Single Mailbox Recovery for Exchange to open the EDB containing mailboxes from within his domain, the CEO’s mailbox is accessible while all other mailboxes are inaccessible.
2. **Scenario #2:** The Administrator runs Single Mailbox Recovery for Exchange and attempts to open an EDB containing a mailbox belonging to Paul Smith, an executive who is internal to the Administrator’s domain. It is inaccessible. It passes through the Specific Internal group or user listings and no match is found. It then processes through the Mailbox Categories and no match is found. It then moves to the All tab and processes through the Group or users list and no match is found. It ends up in the Manage Refusals list.

The client using Single Mailbox Recovery for Exchange is performing some transactions requiring that Paul Smith’s mailbox be accessible. Since the Administrator does not want access to Paul Smith’s mailbox to be permanent, the temporary access is set for a day. The client performs his tasks on Single Mailbox Recovery for Exchange and when the time limit expires, Paul Smith’s mailbox automatically reverts back to being inaccessible.
3. **Scenario #3:** The Administrator sets permissions so that he is allowed access to all external mailboxes in the Mailbox Category tab. These are mailboxes that are outside the Administrator’s domain. The Administrator runs Single Mailbox Recovery for Exchange and opens an EDB containing mailboxes from within the domain.

Single Mailbox Recovery for Exchange denies access to all mailboxes in this EDB. The Administrator then opens an EDB containing mailboxes from another organization. Single Mailbox Recovery for Exchange allows access to all mailboxes in this EDB.

Specific (Internal) Tab

The Specific (Internal) tab presents a list of known internal mailboxes. By selecting one from the list, the permissions associated with that mailbox can be viewed and/or edited.

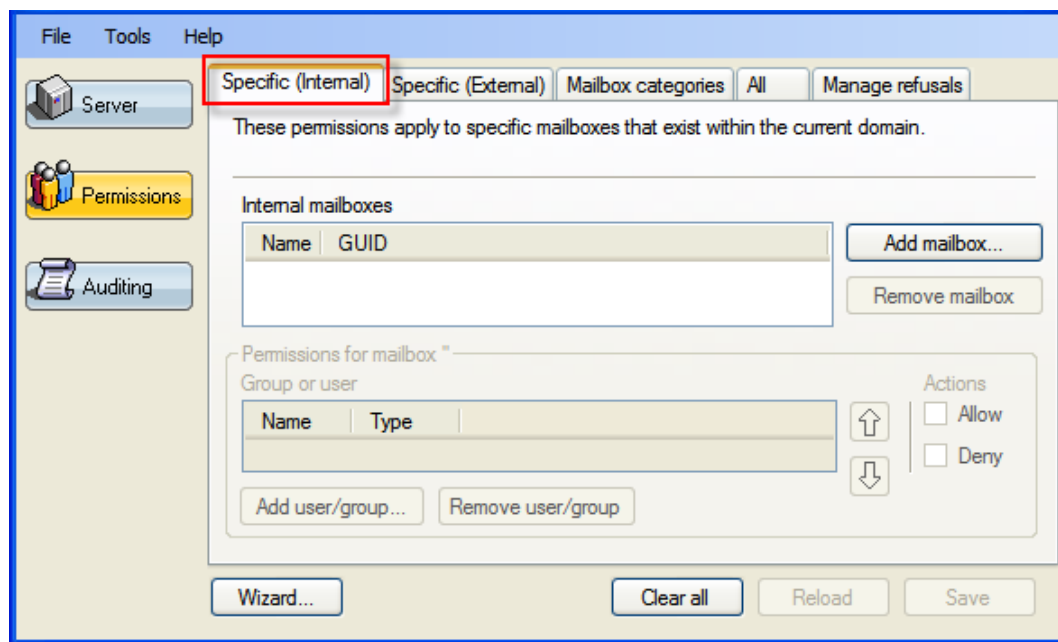


Figure 2-4. Internal Mailbox tab

Adding a Mailbox

You can add a mailbox to the Internal mailbox list. This list is used to apply permissions in the Permissions for mailbox section.

You can filter the list to help you in finding specific users in a large organization. The list is populated with all of the live mailboxes found in the domain. You may select one or more of these mailboxes to add to the list.

To add internal mailboxes

1. Click the **Specific (Internal)** tab.
2. Click **Add Mailbox**. The **Choose Internal Mailboxes to Add** window appears.

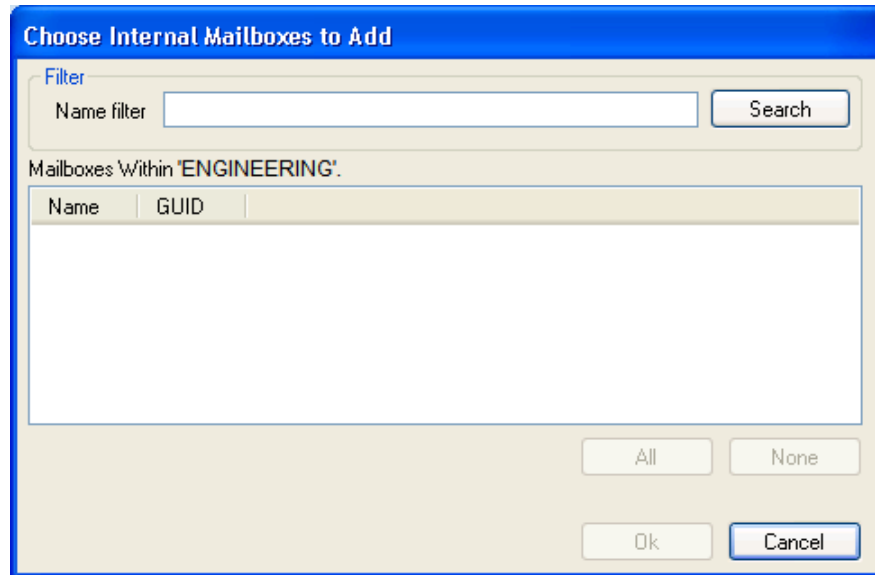


Figure 2-5. Choose Internal Mailboxes to Add

3. Enter a **Name Filter** and click **Search**. The list populates with mailboxes based on the filter you entered.
4. Do one of the following:
 - Click **All** to select the whole list of mailboxes.
 - Select mailboxes individually.
 - Deselect mailboxes list by clicking **None**.
5. Click **OK**. The **Internal mailboxes** list is populated with selected mailboxes.
6. To remove a mailbox, click once on the mailbox and click **Remove mailbox**.
7. Click **Save**.

Adding and Removing a User or Group

You can add a new group or user to the Group or user box in the Permissions for Mailbox section.

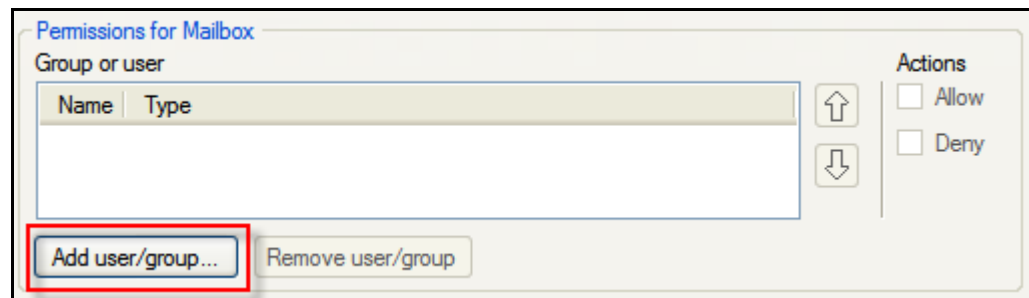


Figure 2-6. Add user/group button

To add a user or group

1. Click **Add user/group**. The **Add Groups or Users** window appears.

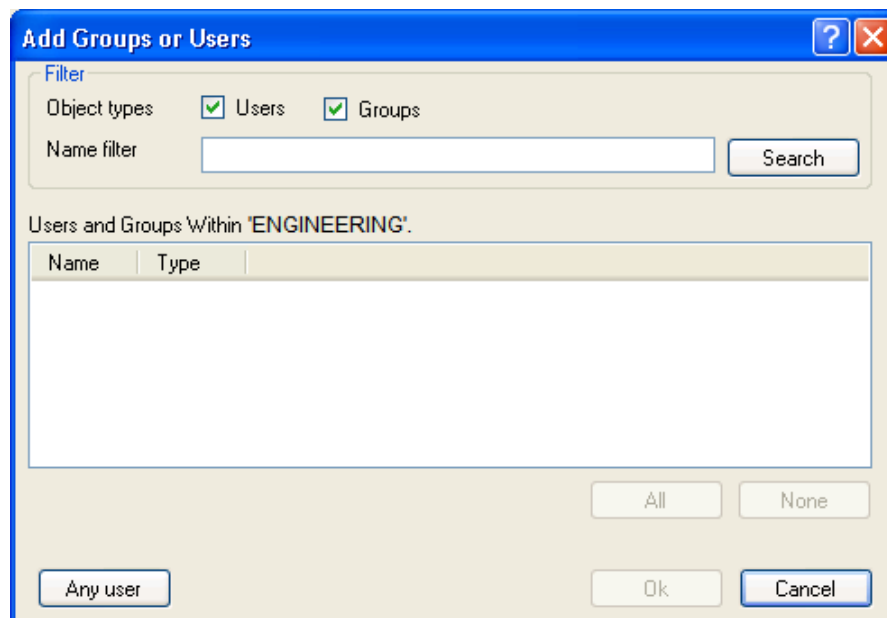


Figure 2-7. Add Groups or Users window

2. Select or deselect the **Object types** you want to search, **Users** and/or **Groups**.
3. Do one of the following:
 - Enter a **Name filter** to narrow down the list and click **Search**.

Note: Single Mailbox Recovery Administrative Server inserts an “*” to create a wild card search.

- Click **Any user**. The **Add Groups and Users** window closes and **Any** is listed in the **Group or user** box.
4. In the populated list, do one of the following:
 - Click **All** to select the whole list of users and groups.
 - Select users and groups individually.
 - Deselect users and groups list by clicking **None**.
 5. Click **OK**.
 6. Click **Save**.

To remove a user or group

1. Select one or more groups or users by clicking once in the **Group or user** box. Multiple groups or users can be selected using the **Shift** or **Ctrl** key.
2. Click **Remove user/group**.
3. Click **Save**.

Setting Permissions for a Mailbox

The Permissions for Mailbox section is used to set permissions for groups or users, add or remove groups or users, or change the order on which they are processed through.

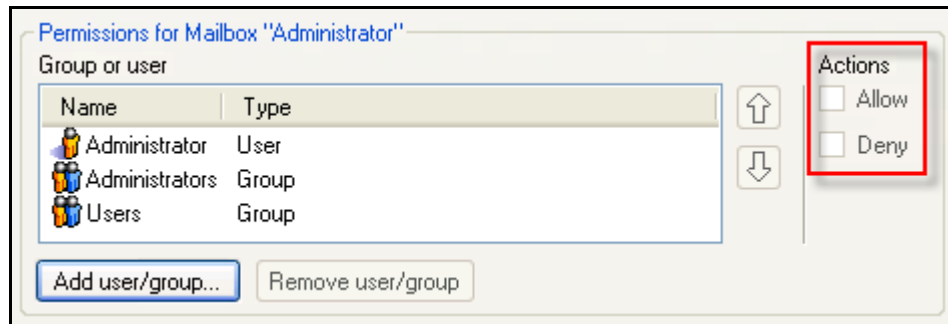


Figure 2-8. Permissions for Mailbox section

Group or user

The Group or user box lists the Name of the group or user and the Type, Group or User.

To set permissions on a group or user

1. Click once on a group or user in the **Group or user** box.

Note: Multiple users can be selected by holding down the Shift key.

2. Select **Allow** or **Deny** under **Actions**.

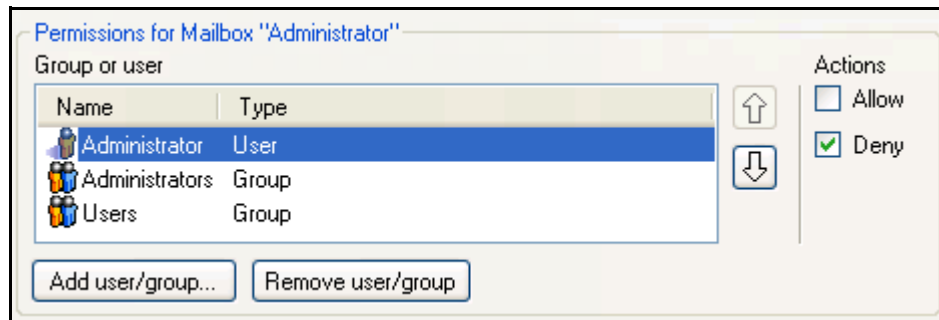


Figure 2-9. Permissions applied to group or user

Sorting the Permission Order

You can change the order of Groups or users using the up and down arrows. The order of the group or user affects the order in which the permission model processes. For example, in the Figure below, if user “Administrator” has the permission setting of “Allow” and the group “Any” is set to “Deny,” since “Administrator” is listed first, it will be “hit” first.

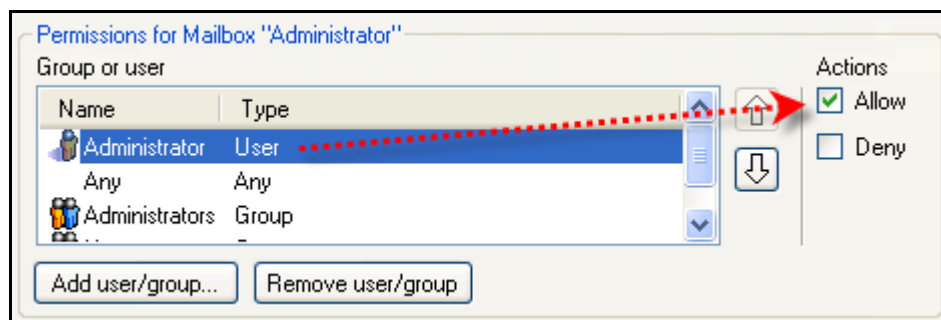


Figure 2-10. "Administrator" is listed first in Group or user box and the permission setting is "Allow."

In the next Figure, the group "Any" has been moved to the top of the list and is hit first. Any group or user listed beneath "Any," even if their permission setting is "Allow," do not get hit since "Any" was hit first and its setting is "Deny." Therefore, any group or user, no matter what their permission setting, are denied permission to access.



Figure 2-11. The Group "Any" has been moved to the top of the list and the permission setting is "Deny."

Specific (External) tab

External Mailboxes are mailboxes not found within the Administrator's domain that are not detailed in Active Directory. The Specific (External) mailboxes tab presents a list of known external mailboxes. By selecting one from the list, the permissions associated with that mailbox can be viewed and/or edited.

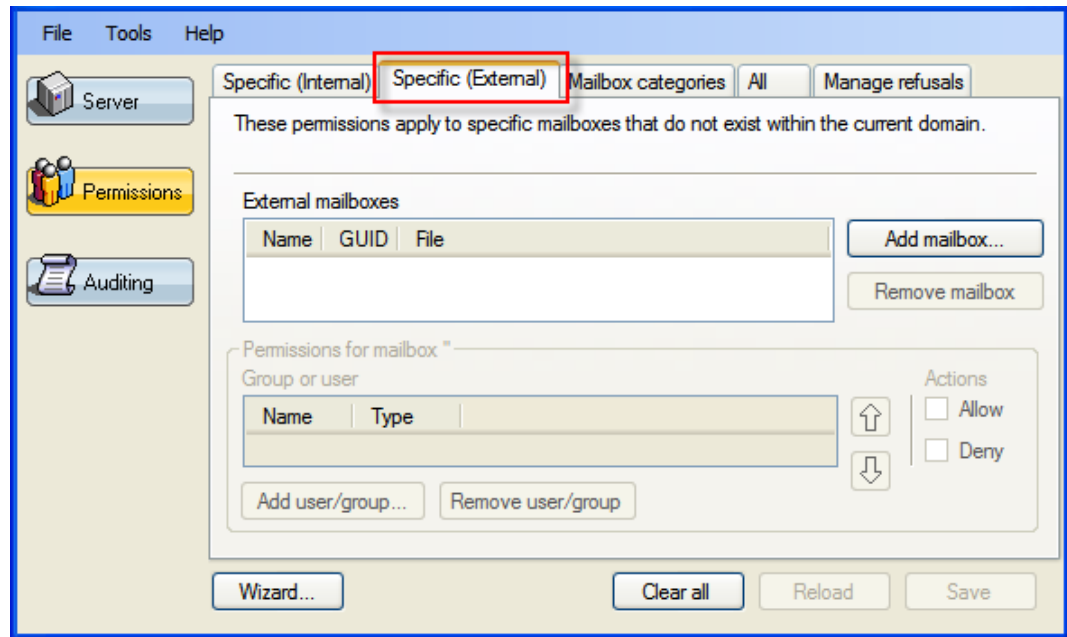


Figure 2-12. External Mailbox tab

Adding a Mailbox

You can add external mailboxes to the External Mailbox list. You can use this list to apply permissions in the Permissions for mailbox section.

To add an external mailbox

1. Select the **Specific (External)** tab.
2. Click **Add mailbox**. The **Select an EDB** window appears.

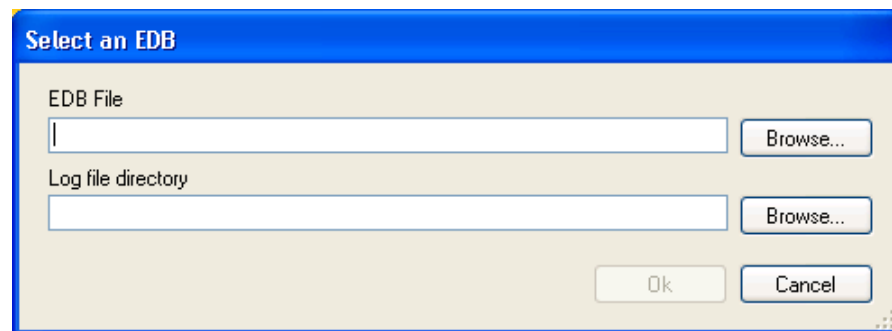


Figure 2-13. Select an EDB

3. Do one of the following:
 - **Browse** for an **EDB File**.
 - Browse for a **Log file directory**.
4. Click **OK**. The EDB file is opened. During this time a progress window appears:

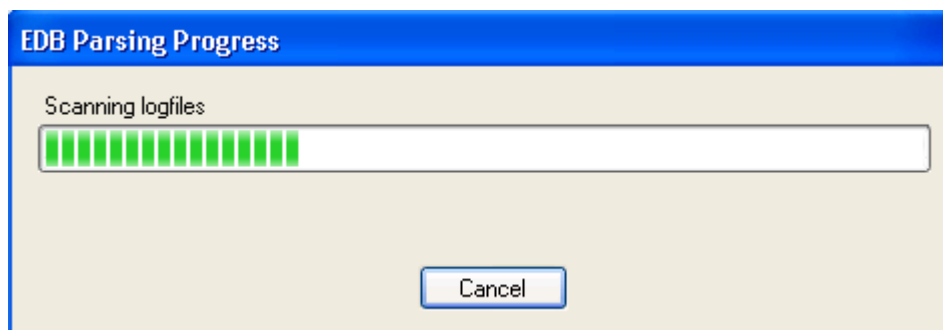


Figure 2-14. EDB Parsing Progress window

5. Upon completion of loading the EDB file, the **Choose External Mailboxes to Add** window appears.

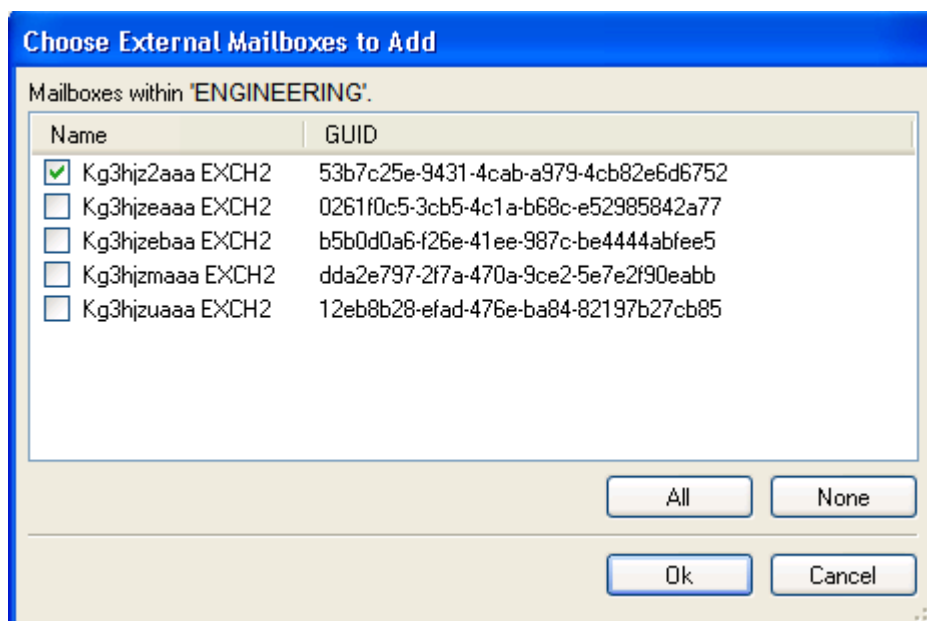


Figure 2-15. Choose External Mailboxes to Add window

6. Do one of the following:
 - Click **All** to select the whole list of mailboxes.
 - Select mailboxes individually.
 - Deselect mailbox list by clicking **None**.
7. Click **OK**. The External mailboxes list is populated with selected mailboxes.
8. Click **Save**.

To remove an external mailbox

1. Select one or more external mailbox(es) in the list.
2. Click **Remove mailbox**.
3. Click **Save**.

Adding and Removing a User or Group

You can add a new group or user to the Group or user box in the Permissions for Mailbox section.

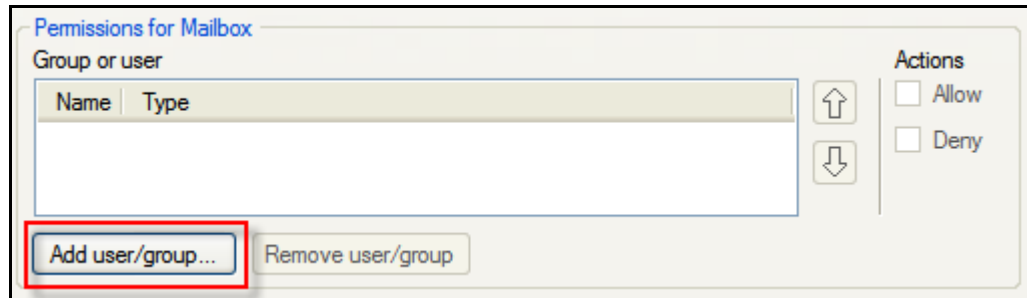


Figure 2-16. Add user/group button

To add a user or group

1. Click **Add user/group**. The **Add Groups or Users** window appears.

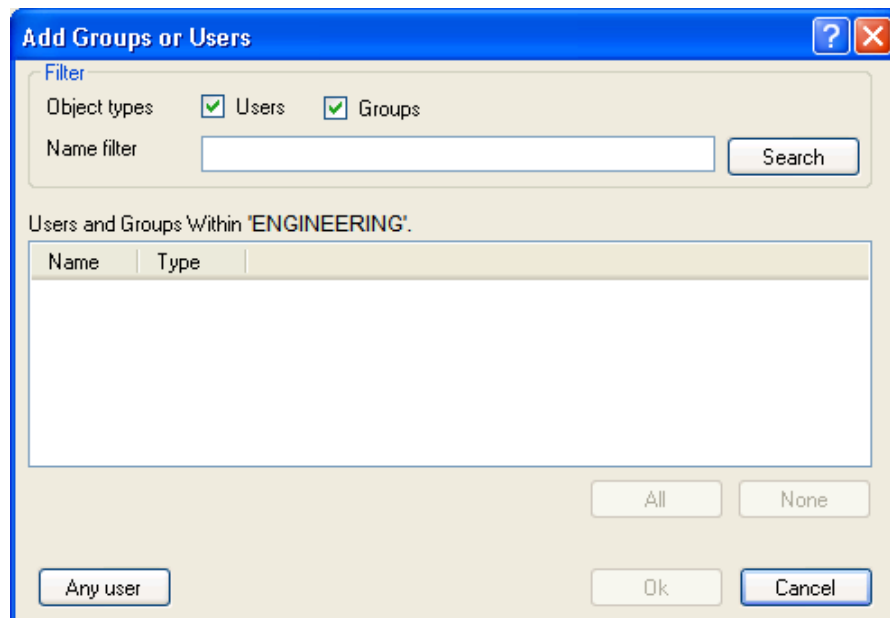


Figure 2-17. Add Groups or Users window

2. Select or deselect the **Object types** you want to search, **Users** and/or **Groups**.
3. Do one of the following:
 - Enter a **Name filter** to narrow down the list and click **Search**.

- Click **Any user**. The **Add Groups and Users** window closes and **Any** is listed in the **Group or user** box.
4. In the populated list, do one of the following:
 - Click **All** to select the whole list of users and groups.
 - Select users and groups individually.
 - Deselect users and groups list by clicking **None**.
 5. Click **OK**.
 6. Click **Save**.

To remove a user or group

1. Select one or more groups or users by clicking once in the **Group or user** box. Multiple groups or users can be selected using the **Shift** or **Ctrl** key.
2. Click **Remove user/group**.
3. Click **Save**.

Setting Permissions for a Mailbox

The Permissions for Mailbox section is used to set permissions for groups or users, add or remove groups or users, or change the order on which they are processed through.

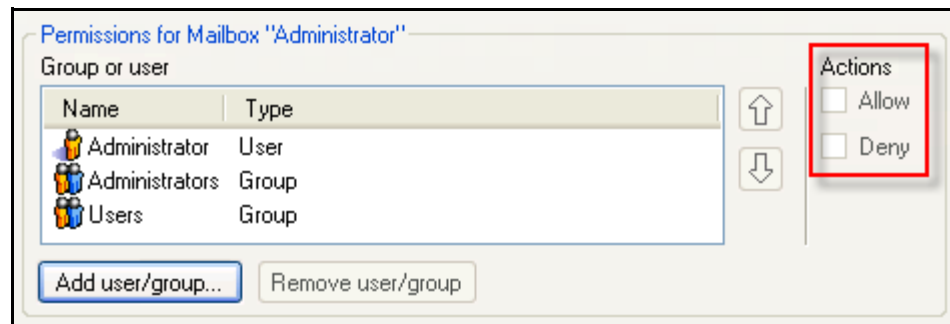


Figure 2-18. Permissions for Mailbox section

Group or user

The Group or user box lists the Name of the group or user and the Type, Group or User.

To set permissions on group or user

1. Click once on a group or user in the **Group or user** box.

***Note:** Multiple users can be selected by holding down the Shift key.*
2. Select **Allow** or **Deny** under **Actions**.

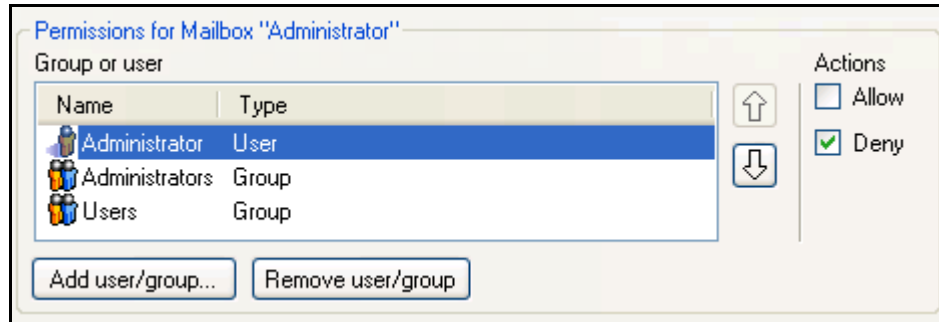


Figure 2-19. Permissions applied to group or user

Sorting the Permission Order

You can change the order of Groups or users by using the up and down arrows. The order of the group or user affects the order in which the permission model processes. For example, in the next Figure, if user “Administrator” has the permission setting of “Allow” and the group “Any” is set to “Deny,” since “Administrator” is listed first, it will be “hit” first.

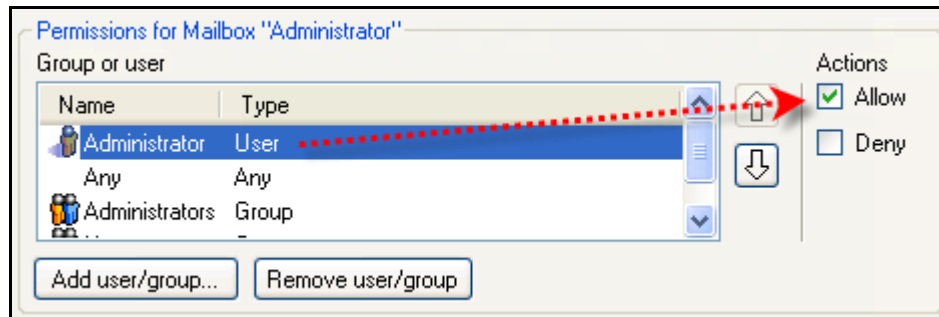


Figure 2-20. “Administrator” is listed first in Group or user box and the permission setting is “Allow.”

In the next Figure, the group “Any” has been moved to the top of the list and is hit first. Any group or user listed beneath “Any,” even if their permission setting is “Allow,” do not get hit since “Any” was hit first and its setting is “Deny.” Therefore, any group or user, no matter what their permission setting, are denied permission to access.



Figure 2-21. The Group “Any” has been moved to the top of the list and the permission setting is “Deny.”

Mailbox Categories Tab

You can set permissions to mailboxes categorized by Internal or External to the domain in the Mailbox Categories tab. These are permissions that apply to all mailboxes of a specific category.

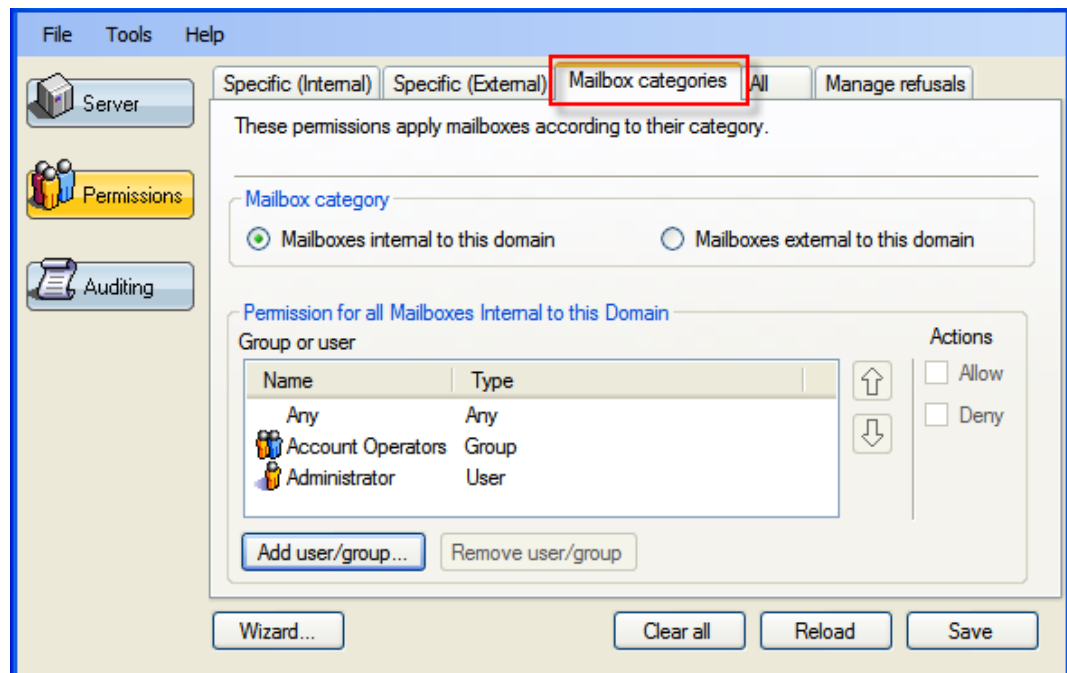


Figure 2-22. Mailbox Categories tab

Setting the Mailbox Category

Select the Mailbox Category you wish to apply permission for:

- Mailboxes internal to this domain, or
- Mailboxes external to this domain.

Adding and Removing a User or Group

You can add a new group or user to the Group or user box in the Permission for all Mailboxes Internal (or External) to this Domain section.

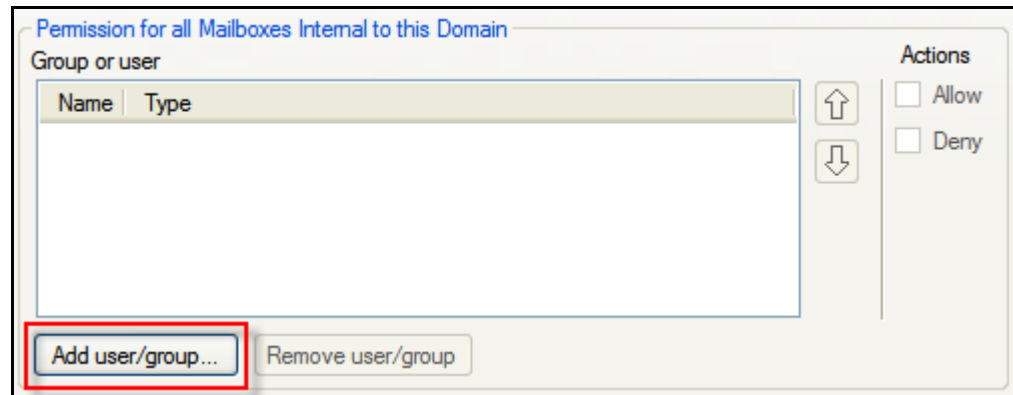


Figure 2-23. Add user/group button

To add a user or group

1. Click **Add user/group**. The **Add Groups or Users** window appears.

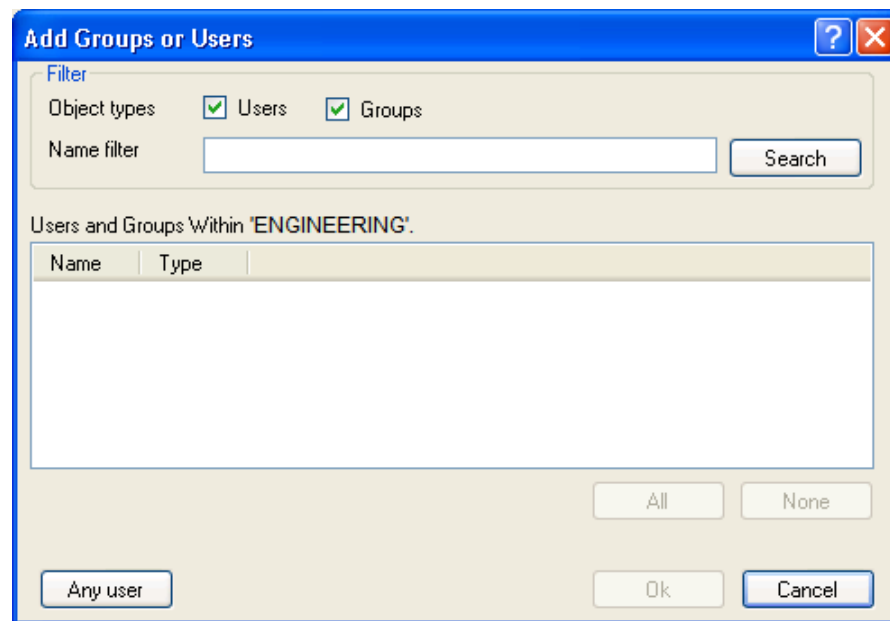


Figure 2-24. Add Groups or Users window

2. Select or deselect the **Object types** you want to search, **Users** and/or **Groups**.
3. Do one of the following:
 - Enter a **Name filter** to narrow down the list and click **Search**.
 - Click **Any user**. The **Add Groups and Users** window closes and **Any** is listed in the **Group or user** box.
4. In the populated list, do one of the following:
 - Click **All** to select the whole list of users and groups.
 - Select users and groups individually.
 - Deselect users and groups list by clicking **None**.

5. Click **OK**.
6. Click **Save**.

To remove a user or group

1. Select one or more groups or users by clicking once in the **Group or user** box. Multiple groups or users can be selected using the **Shift** or **Ctrl** key.
2. Click **Remove user/group**.
3. Click **Save**.

Setting Permissions for all Mailboxes Internal or External to this Domain

You can use this section to set permissions for groups or users, add or remove groups or users, or change the order on which they are processed through.

Group or user

The Group or user box lists the Name of the group or user and the Type, Group or User.

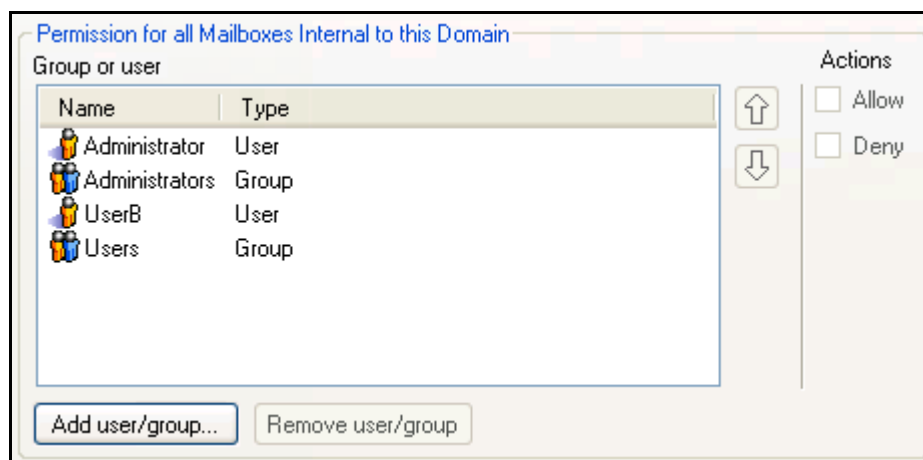


Figure 2-25. Permission for all Mailboxes (Internal or External)

To set permissions on a group or user

1. Click once on a group or user in the **Group or user** box.
Note: Multiple users can be selected by holding down the Shift key.
2. Select **Allow** or **Deny** under **Actions**.

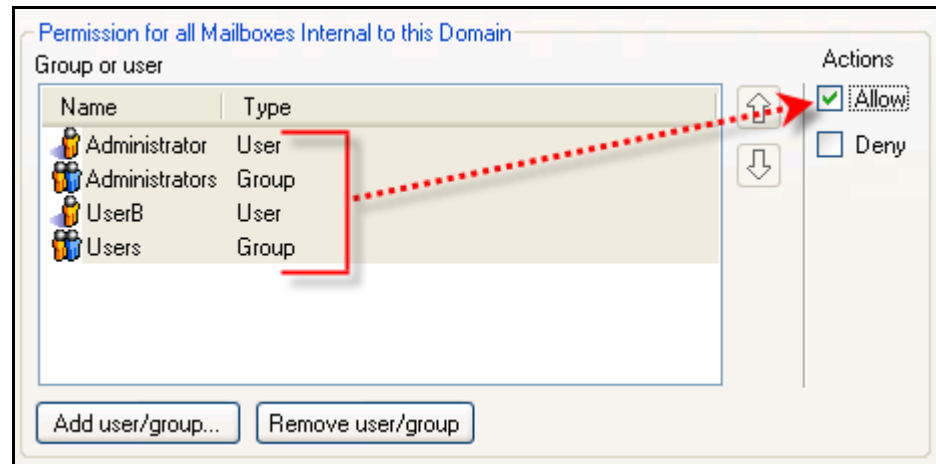


Figure 2-26. Permissions applied to group or user

Sorting the Permission Order

You can change the order of Groups or users by using the up and down arrows. The order of the group or user affects the order in which the permission model processes. For example, in the next Figure, if user "Administrator" has the permission setting of "Allow" and the group "Any" is set to "Deny," since "Administrator" is listed first, it will be "hit" first.

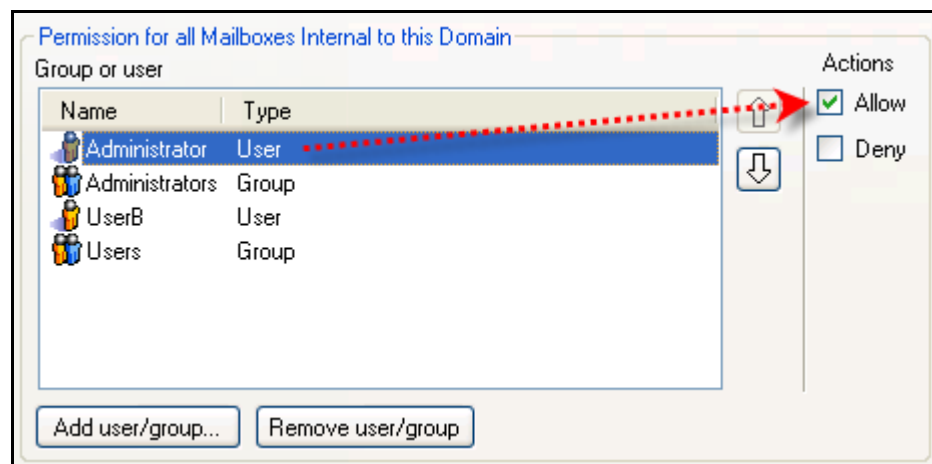


Figure 2-27. The "Administrator" user is at the top of the list and the Action is set to "Allow" permission.

In the next Figure, the group "Any" has been moved to the top of the list and is hit first. Any group or user listed beneath "Any," even if their permission setting is "Allow," do not get hit since "Any" was hit first and its setting is "Deny." Therefore, any group or user, no matter what their permission setting, are denied permission to access.

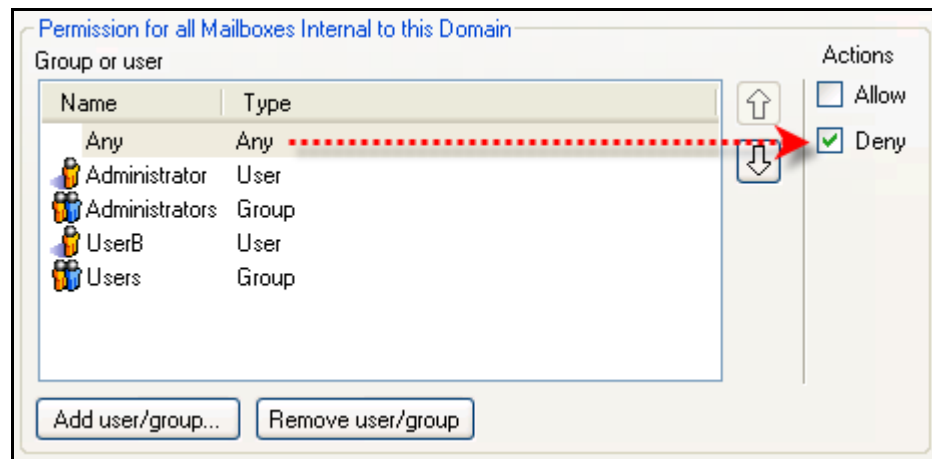


Figure 2-28. The Group “Any” has been moved to the top of the list and the Action is set to “Deny” permission.

All Mailboxes Tab

All Mailboxes is a general mailbox category that allows permissions to be set at a high level (e.g., allow a user or group to access any mailbox).

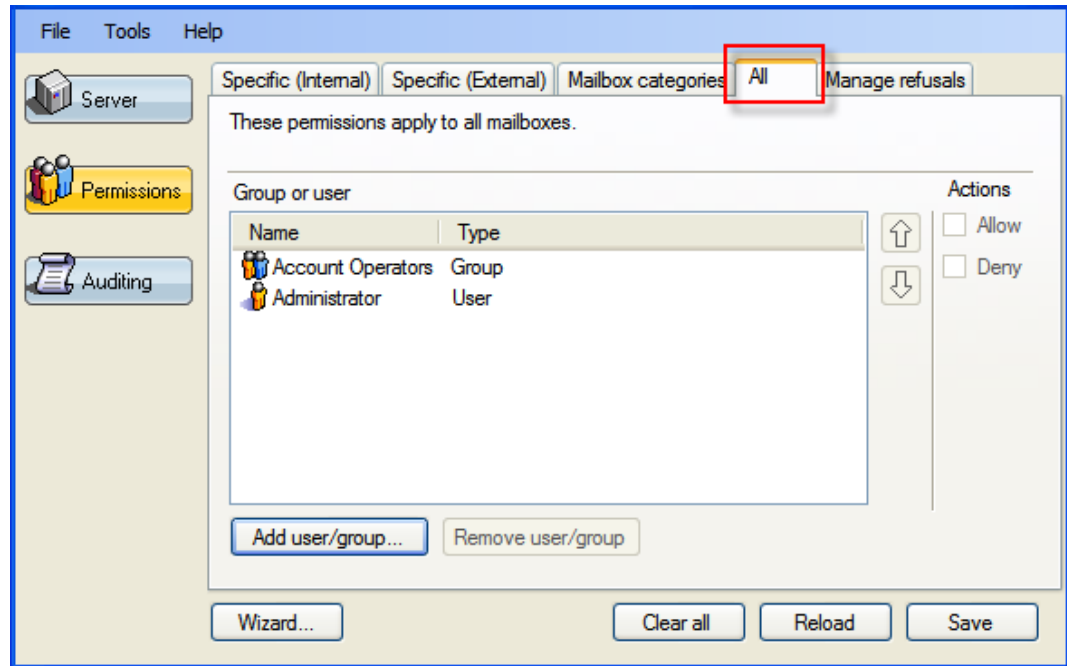


Figure 2-29. All mailboxes tab

Adding and Removing a User or Group

You can add a new group or user to the Group or user box in the All mailboxes tab.

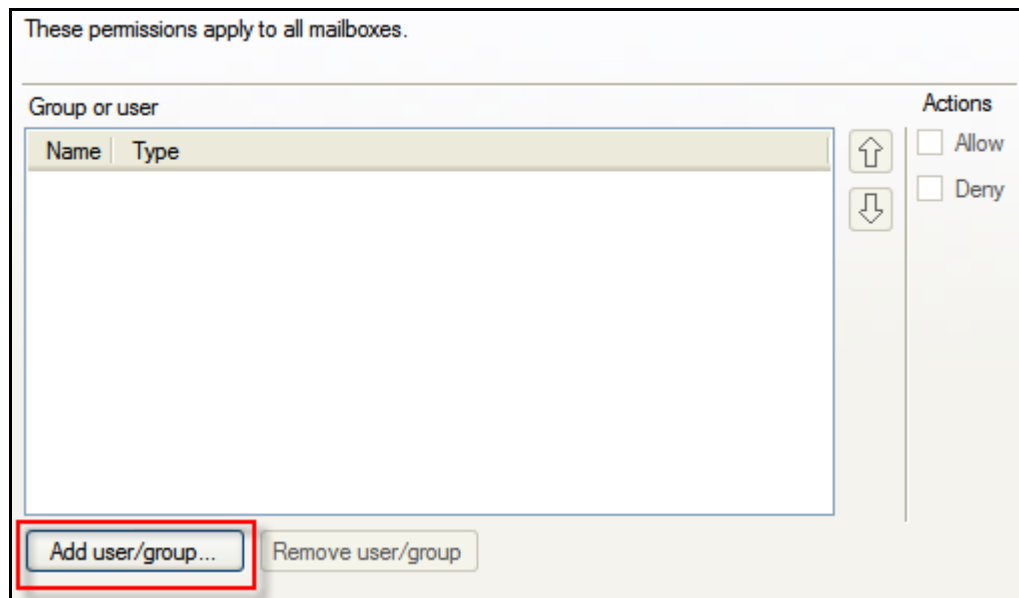


Figure 2-30. Add user/group button

To add a user or group

1. Click **Add user/group**. The **Add Groups or Users** window appears.

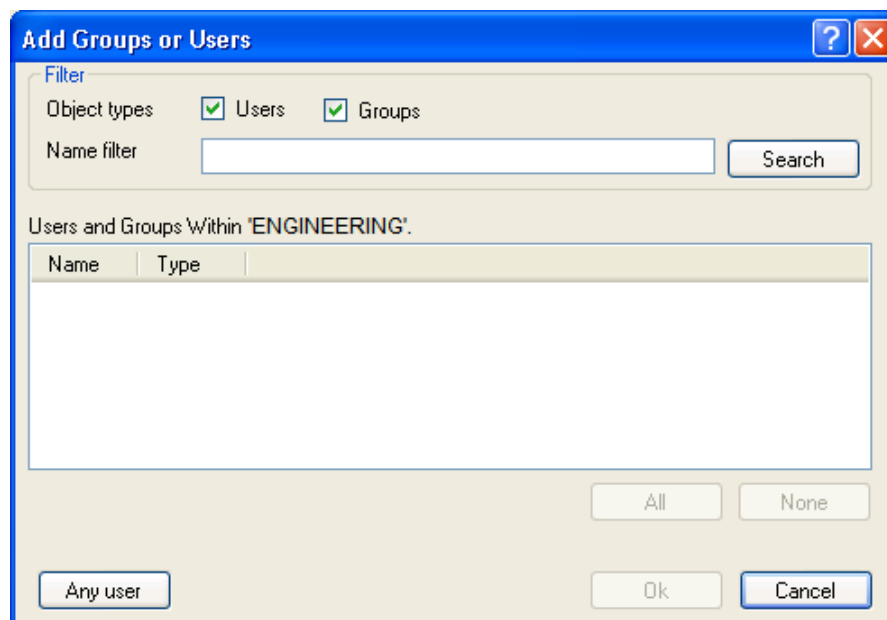


Figure 2-31. Add Groups or Users window

2. Select or deselect the **Object types** you want to search, **Users** and/or **Groups**.
3. Do one of the following:
 - Enter a **Name filter** to narrow down the list and click **Search**.

- Click **Any user**. The Add Groups and Users window closes and **Any** is listed in the **Group or user** box.
- 4. In the populated list, do one of the following:
 - Click **All** to select the whole list of users and groups.
 - Select users and groups individually.
 - Deselect users and groups list by clicking **None**.
- 5. Click **OK**.
- 6. Click **Save**.

To remove a user or group

1. Select one or more groups or users by clicking once in the **Group or user** box. Multiple groups or users can be selected using the **Shift** or **Ctrl** key.
2. Click **Remove user/group**.
3. Click **Save**.

Setting Permissions for All Mailboxes

You can use this section to set permissions for groups or users, add or remove groups or users, or change the order on which they are processed through.

Group or user

The Group or user box lists the Name of the group or user and the Type, Group, or User.

These permissions apply to all mailboxes.

Group or user		Actions	
Name	Type		
Administrator	User	☐	Allow
Administrators	Group	☐	Deny
UserB	User		
Users	Group		

Figure 2-32. Group or user box

To set permissions on group or user

1. Click once on a group or user in the **Group or user** box.

Note: Multiple users can be selected by holding down the Shift key.

2. Select **Allow** or **Deny** under **Actions**.

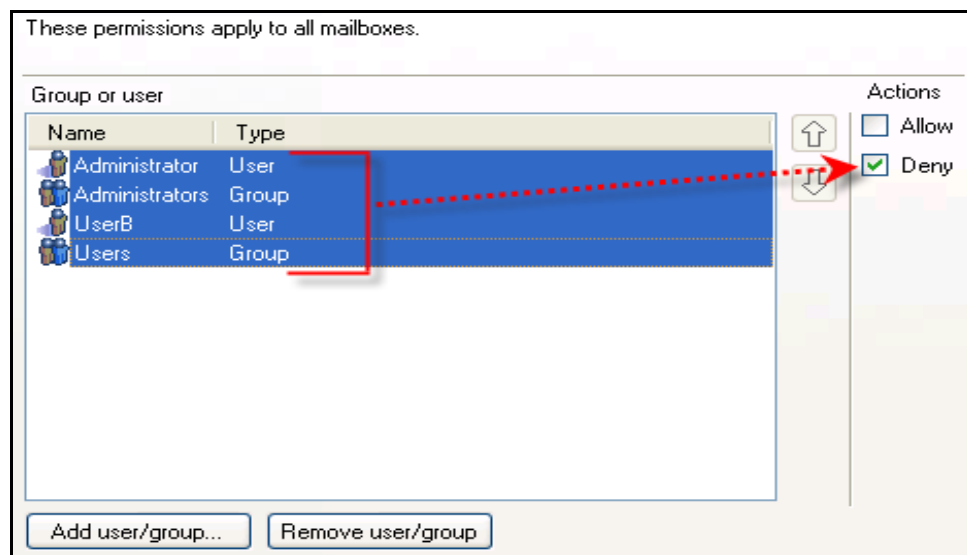


Figure 2-33. Permissions applied to group or user

Sorting the Permission Order

You can change the order of Groups or users by using the up and down arrows. The order of the group or user affects the order in which the permission model processes. For example, in the next Figure, if user "Administrator" has the permission setting of "Allow" and the group "Any" is set to "Deny," since "Administrator" is listed first, it will be "hit" first.

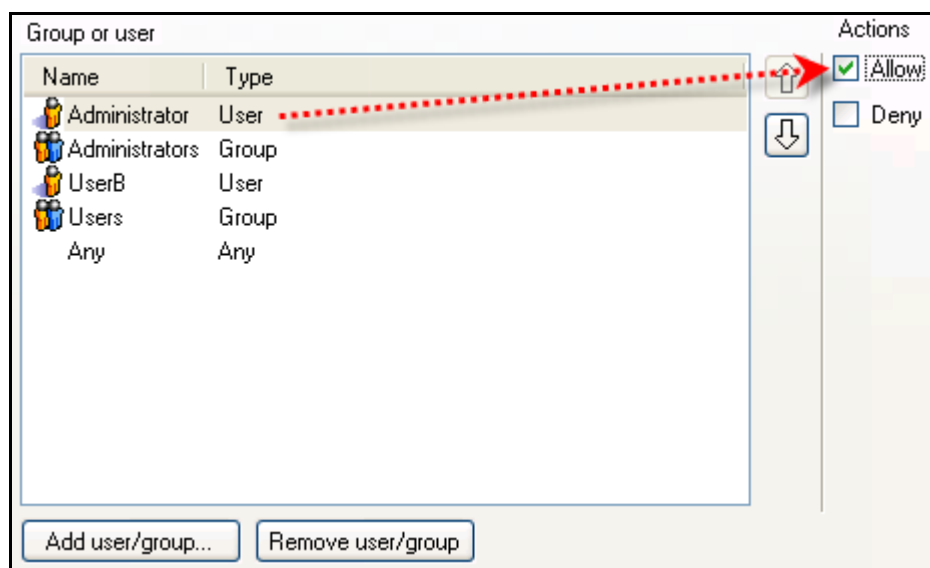


Figure 2-34. The "Administrator" is at the top of the list and the Action is set to "Allow" permission.

In the next Figure, the group “Any” has been moved to the top of the list and is hit first. Any group or user listed beneath “Any,” even if their permission setting is “Allow,” do not get hit since “Any” was hit first and its setting is “Deny.” Therefore, any group or user, no matter what their permission setting, are denied permission to access.

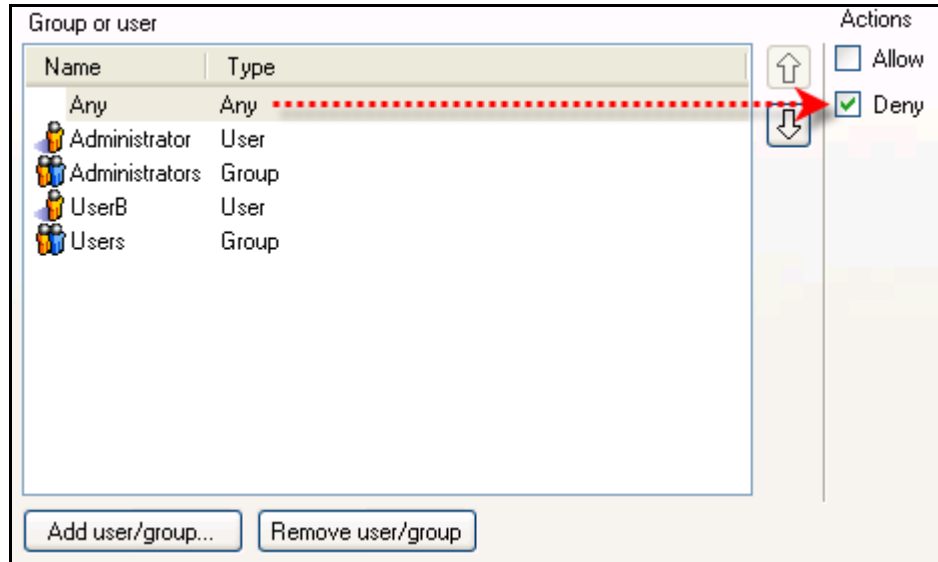


Figure 2-35. The Group “Any” has been moved to the top of the list and the Action is set to “Deny” permission.

Manage Refusals Tab

You can change the permission setting on a mailbox that has failed access attempts either through a “Deny” permission setting or by not finding a match. The server maintains a list of all the failed mailbox access attempts. These are listed in the Manage Refusals tab of the Single Mailbox Recovery Management Console:

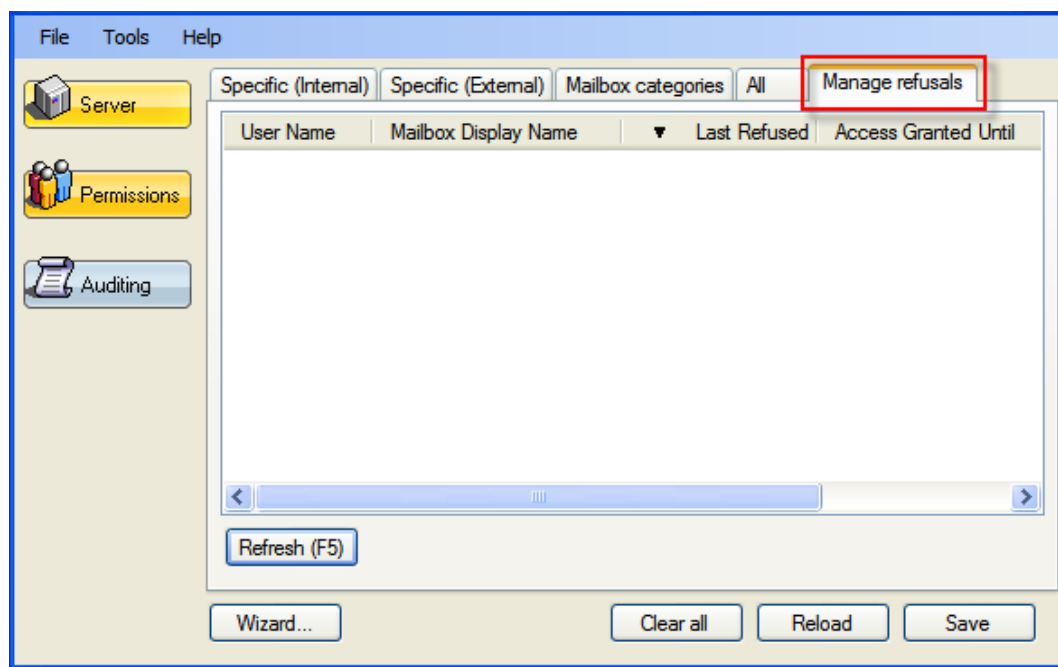


Figure 2-36. Manage Refusals tab

The tab lists the following information:

- **User name:** Name of the user that attempted the access.
- **Mailbox display name:** Name of the mailbox on which access was attempted.
- **Last refused:** Date and time of the last failed attempt.
- **Access granted until:** Date and time up to which access will be allowed.
- **Mailbox file:** The path to the file where the mailbox originated.
- **GUID:** The unique identification of the mailbox.

Allowing a Refusal

There are two ways you can allow a refused mailbox access. A refusal can be temporarily allowed or permanently allowed.

Permanently allowing a refusal involves generating a permission entry for that access attempt.

Temporarily allowing a refusal requires that the user indicate the duration of the access.

To allow a refusal

1. In the **Manage Refusals** tab, right-click a user name. A shortcut menu appears.

2. Do one of the following:

- On the shortcut menu, click **Permanently allow**. The mailbox moves to the appropriate tab.
- On the shortcut menu, click **Temporarily allow**.

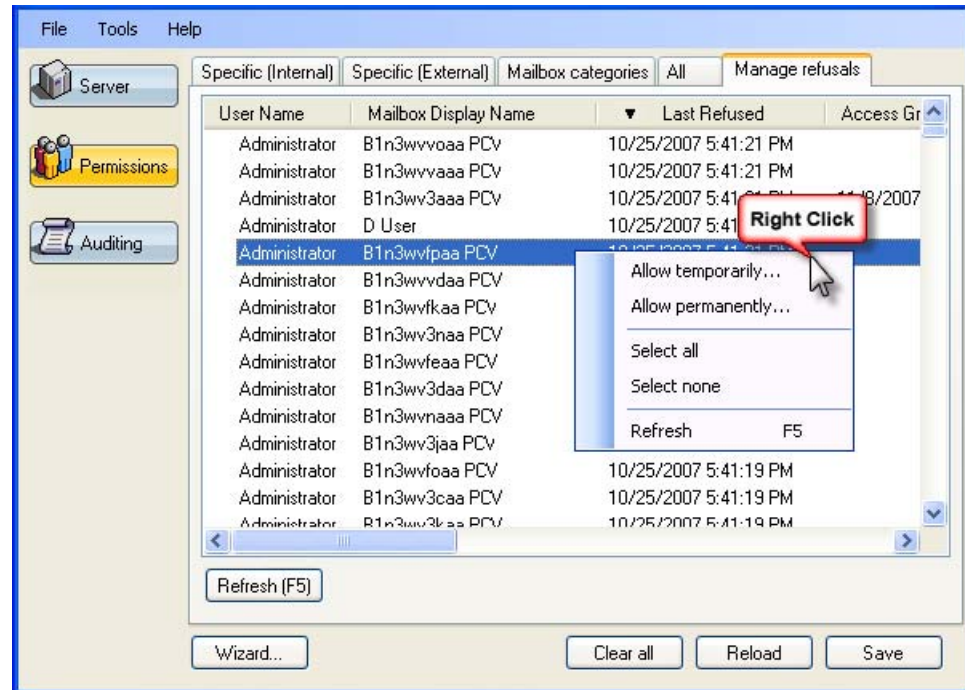


Figure 2-37. Right-click the mailbox to give temporary or permanent permission

- The **Choose duration of temporary allow** window appears.

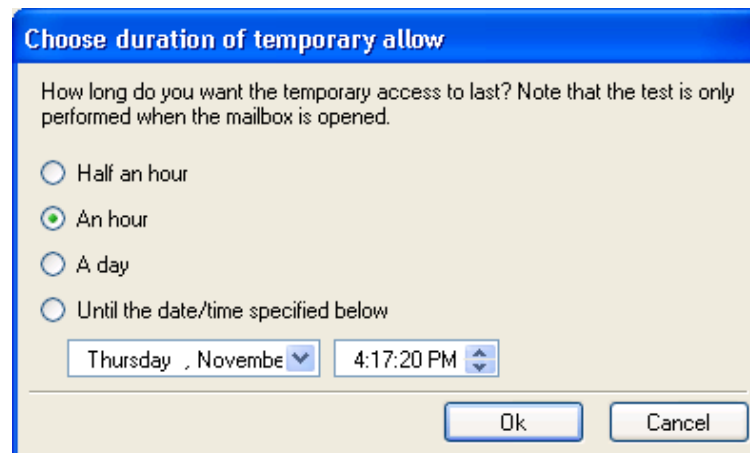


Figure 2-38. Choose the duration of temporary refusal allow

3. If you selected **Temporarily allow**, select one of the following:

- Half an hour
- An hour

- A day
 - Until the date/time specified below—Using the drop-down arrows, select the date and time you want the temporary access to end.
4. Click **OK**. The time and date of the temporary access appears in the Access Granted Until column.

Specific (Internal)		Specific (External)	Mailbox categories	All	Manage refusals
User Name	Mailbox Display Name	▼	Last Refused	Access Granted Until	
Administrator	B1n3wvvoaa PC2003		10/25/2007 5:41:21 PM		
Administrator	B1n3wvvaaa PC2003		10/25/2007 5:41:21 PM		
Administrator	B1n3wv3aaa PC2003		10/25/2007 5:41:21 PM	11/8/2007 5:25:16 PM	
Administrator	D User		10/25/2007 5:41:21 PM		
Administrator	B1n3wvfpaa PC2003		10/25/2007 5:41:21 PM		
Administrator	B1n3wvvdad PC2003		10/25/2007 5:41:20 PM		
Administrator	B1n3wvfkaa PC2003		10/25/2007 5:41:20 PM	11/8/2007 5:37:03 PM	
Administrator	B1n3wv3naa PC2003		10/25/2007 5:41:20 PM		

Figure 2-39. The Temporarily Allow date and time appears in the Access Granted Until column

5. Click **Save**.

Clearing, Reloading, and Saving

The Clear all, Reload, and Save buttons are located on the bottom edge of the Single Mailbox Recovery Management Console.

CLEAR ALL

You can use the Clear all button to clear out all the mailboxes and settings in the Single Mailbox Recovery Management Console.

RELOAD

The Reload button loads the stored permissions set which removes any changes made since the last Save.

SAVE

The Save button saves the current (modified) permissions set. You need to click Save to activate any changes made to the permission settings.

Using the Wizard

You can set the initial permissions for your organization using a wizard which opens when the permissions plug-in is being installed. These settings can be modified later from the Permissions tabs.

1. Click **Wizard** on the main window of Single Mailbox Recovery Administrative Server. The wizard opens with a Welcome page.

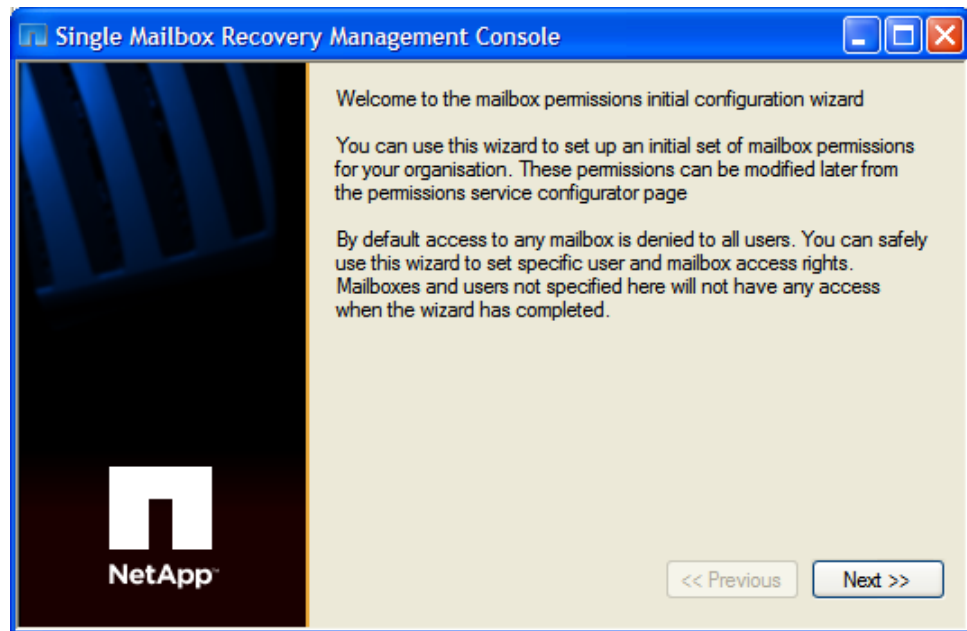


Figure 2-40. Welcome page

2. Click **Next**. The second page of the wizard used for specifically denying access to everyone appears.

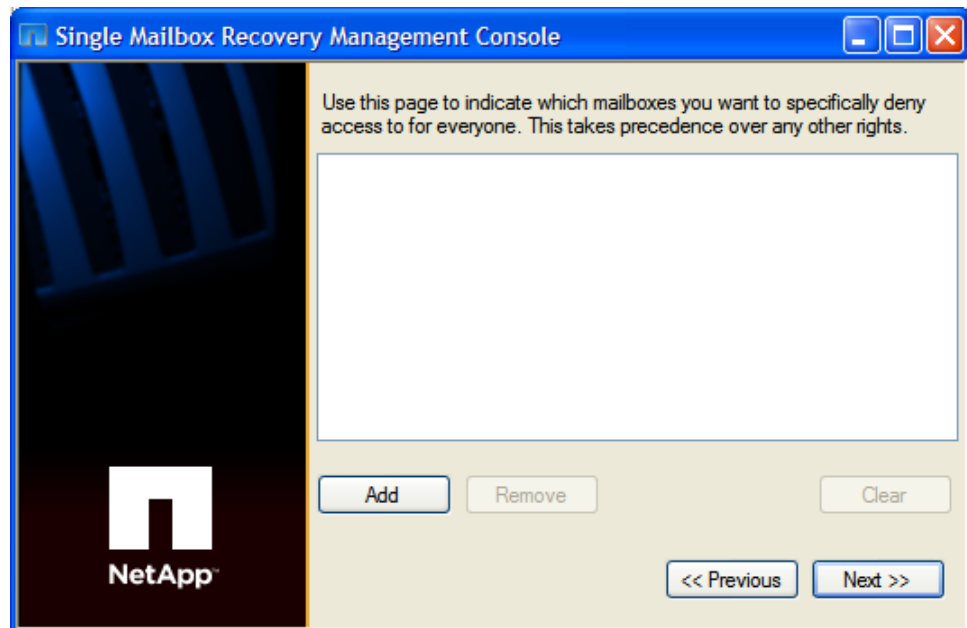


Figure 2-41. Deny access for everyone

Note: This page of the wizard can offer protection to mailboxes the Administrator does not want anyone to access. For example, the CEO's mailbox in Example #1 at "Examples of Use" on page 21. The Administrator should ensure any sensitive or important mailboxes are listed here.

- Click **Add** to list which mailboxes you want to specifically deny access for everyone. The **Choose Internal Mailboxes to Add** window appears.

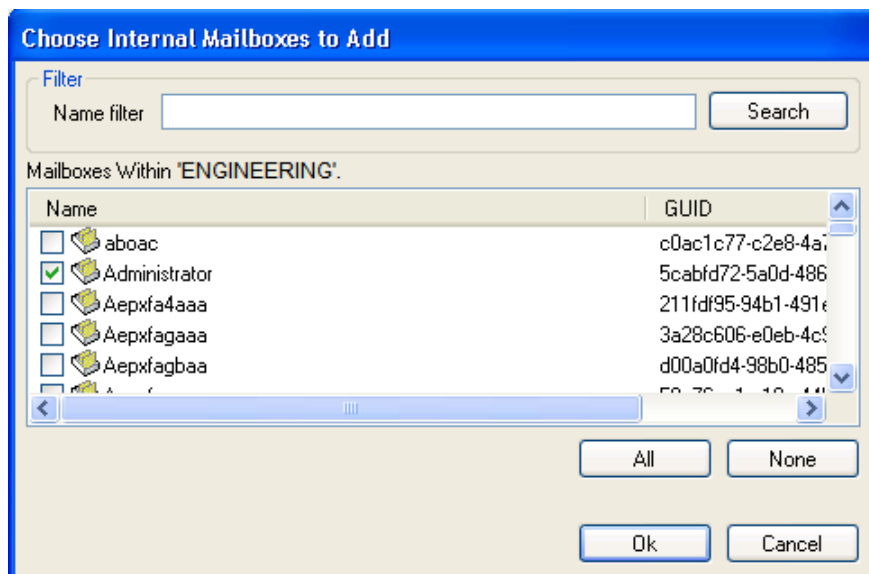


Figure 2-42. Choose Internal Mailboxes

- Enter a **Name filter** to narrow down the list and click **Search**.
- In the populated list, do one of the following:
 - Click **All** to select the whole list of mailboxes.
 - Select mailboxes individually.
 - Deselect mailbox list by clicking **None**.
- Click **OK**.
 - Use the **Remove** option to delete any mailboxes from the list.
 - Click **Clear** to delete the entire list from the page.
- Click **Next**. The add access to internal mailboxes page of the wizard appears.

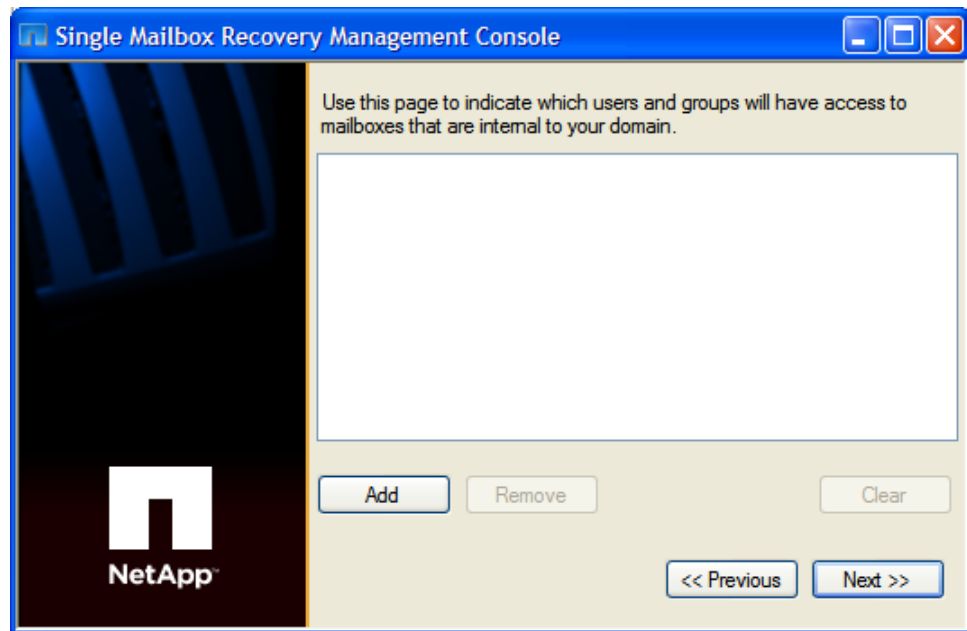


Figure 2-43. Access to internal mailboxes

Note: This page of the wizard is there to allow access to any other mailboxes in the domain, with the exception of the mailboxes chosen on the second page of the wizard. Those users will have access to all other mailboxes internal to the domain. The Administrator should ensure only those users or groups specifically authorized to use Single Mailbox Recovery for Exchange and access company mailboxes located in the EDB files are listed.

8. Click **Add** to list users and groups that will have access to the mailboxes internal to your domain. The **Add Groups or Users** window appears.

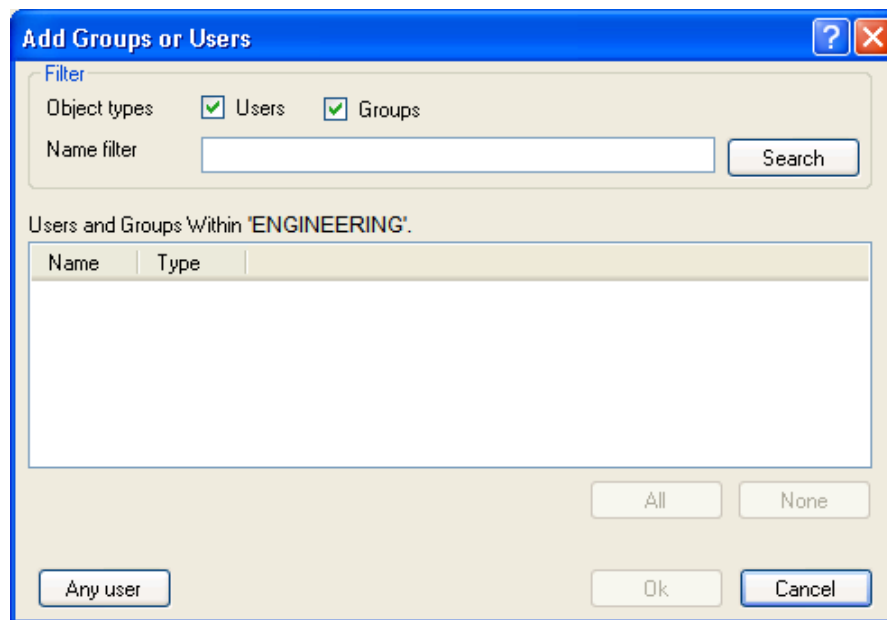


Figure 2-44. Add Groups or Users

9. Select or deselect the **Object types** you want to search, **Users** and/or **Groups**.
10. Do one of the following:
 - Enter a **Name filter** to narrow down the list and click **Search**.
 - Click **Any user**. The **Add Groups and Users** window closes and **Any** is listed in the **Group or user** box.
11. In the populated list, do one of the following:
 - Click **All** to select the whole list of mailboxes.
 - Select mailboxes individually.
 - Deselect mailbox list by clicking **None**.
12. Click **OK**.
 - Use the **Remove** option to delete any mailboxes from the list.
 - Click **Clear** to delete the entire list from the page.
13. Click **Next**. The add access to external mailboxes page in the wizard appears.

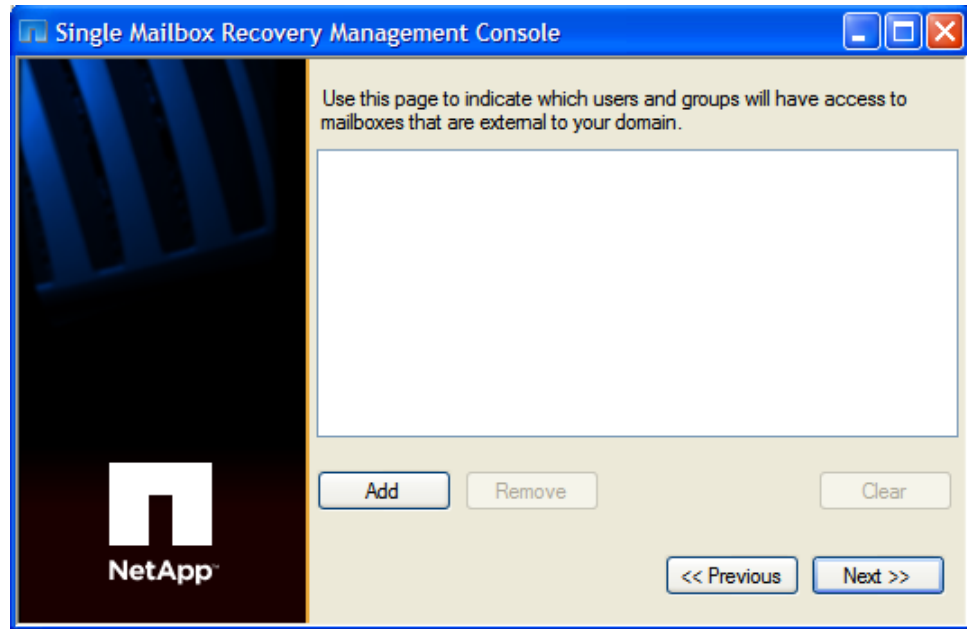


Figure 2-45. Access to external mailboxes

Important Note: This page of the wizard allows access to any mailboxes external to the domain at your choosing. In a large organization, the email system may be distributed along operational or geographic lines and therefore a mailbox external to the Administrator's domain may still be internal to the organization as a whole. Carefully select users you want to have access to mailboxes external to your domain. An option is to leave this list empty and specifically add mailboxes later.

14. Click **Add** to list users and groups that will have access to mailboxes that are external to your domain. The **Add Groups or Users** window appears.

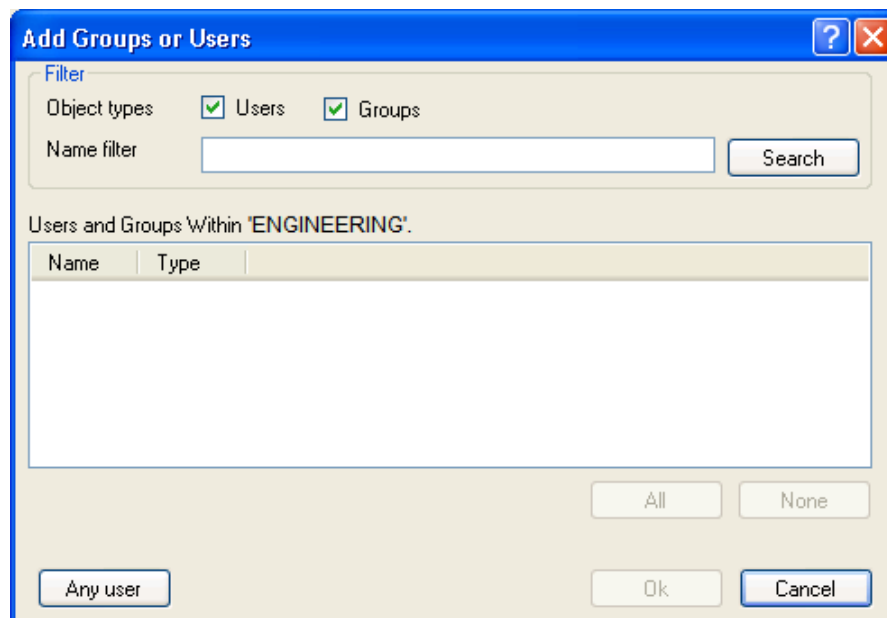


Figure 2-46. Add Groups or Users

15. Select or deselect the **Object types** you want to search, **Users** and/or **Groups**.
16. Do one of the following:
 - Enter a **Name filter** to narrow down the list and click **Search**.
 - Click **Any user**. The **Add Groups and Users** window closes and **Any** is listed in the **Group or user** box.
17. In the populated list, do one of the following:
 - Click **All** to select the whole list of mailboxes.
 - Select mailboxes individually.
 - Deselect mailbox list by clicking **None**.
18. Click **OK**.
 - Use the **Remove** option to delete any mailboxes from the list.
 - Click **Clear** to delete the entire list from the page.
19. Click **Next**. The initial configuration of mailbox access permissions is complete.

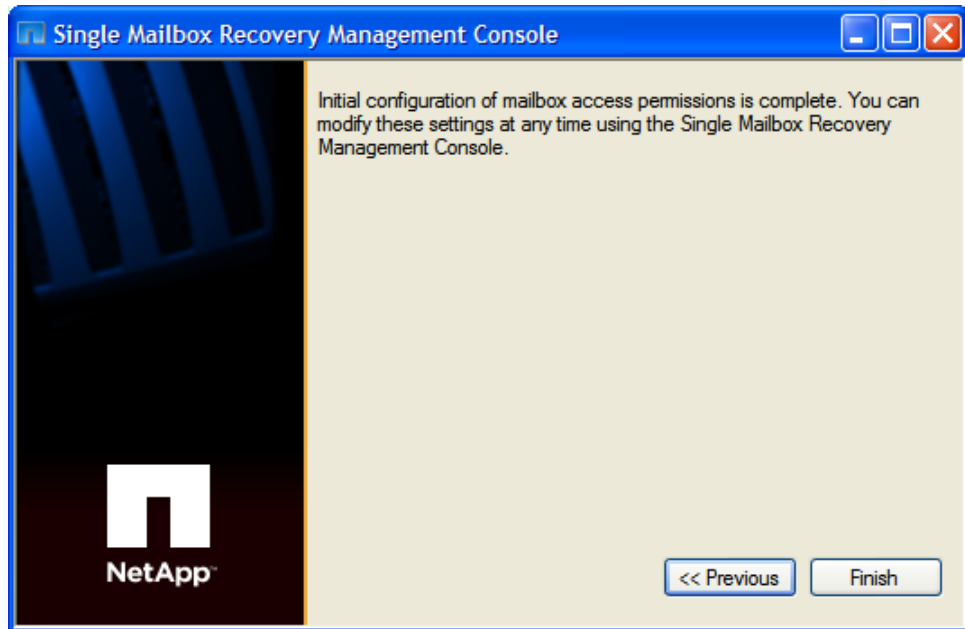


Figure 2-47. Mailbox Access Permissions complete

20. Click **Finish**.

Note: These settings can be modified at a later time. If you use the wizard to modify the settings later, any previous settings are cleared. A message appears stating that running the wizard will clear all the existing permissions.

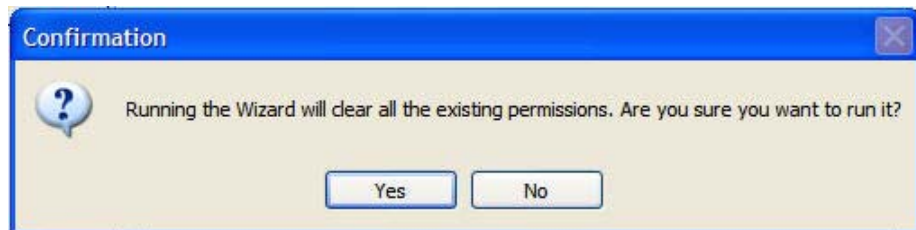


Figure 2-48. Confirmation message to clear all existing permission settings.

APPLICATION AUDITING SERVICE

Overview

The Application Auditing Service is a service plug-in that you can load into Single Mailbox Recovery Management Console. It is used to generate audit log files which record actions performed by users. Audit log files are protected so that tampering is detected.

Activities performed in Single Mailbox Recovery for Exchange 6.0 and Single Mailbox Recovery ExtractWizard, as well as the Single Mailbox Recovery Management Console and Mailbox Permissions Service, are logged as part of an audit trail.

Audit log files contain audit entries which are grouped by session. A session encompasses the actions performed by a particular user on a particular machine using a particular application.

Types of Activities that are Logged

Activities performed by users are logged as a single *stand alone* activity or as part of a larger *transaction* process activity. Both client and server associated activities are logged.

- **Stand alone Activities:** For example, clicking “Next” on a wizard page.
- **Transaction Activities:** Activities that are logged as a pair of entries, the first entry of the pair specifying what is about to happen, and the second entry of the pair specifying the result. For example, copying a folder containing 50 sub-folders and 1000 messages pasting them to a target file. The copying process of each message is not logged, only the initial copy and result of the copy operation as a whole are logged.

Client Activities that are Logged

All activities affecting the source or target store are logged. In addition, all activities that affect what is viewable by you on the screen are logged.

In Single Mailbox Recovery for Exchange 6.0 and Single Mailbox Recovery ExtractWizard, the types of activities logged are those initiated from the user interface, command line interface, and Data Wizard.

See [Appendix A: Activities to be Logged](#) for a list of Client activities that are logged.

Server-Side Activities that are Logged

On the server side, activities are logged for the Server, Mailbox Permissions Service, and the Single Mailbox Recovery Management Console.

See [Appendix A: Activities to be Logged](#) for a list of Server-Side activities that are logged.

Audit Service First Run Configuration

When the audit service plug-in is first installed using the Single Mailbox Recovery Management Console, a configuration screen allows you to change the audit store root path and the 24-hour log rollover time. See “Configuration Tab” on page 61 for more information.

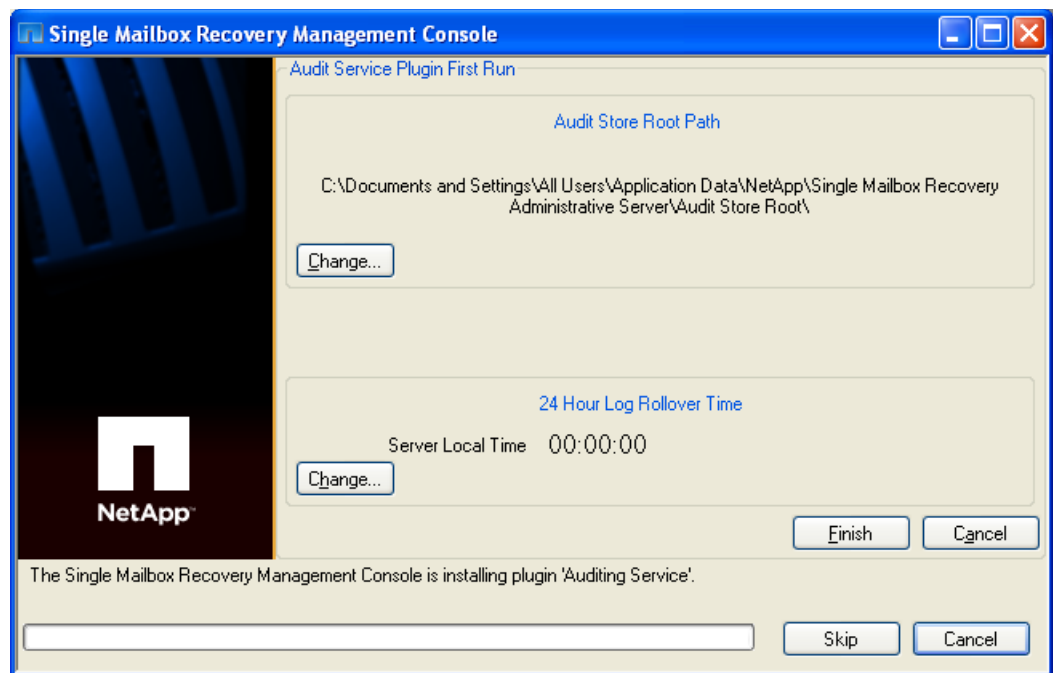


Figure 3-1. Audit Service First Run

Skip Button

The “Skip” button can be used to skip finalization of the current plug-in. If a plug-in’s finalization is skipped, it will not be available for configuration in the Single Mailbox Recovery Management Console and its service not provided to clients, as it is deactivated. Skipped plug-ins can be activated using the Tools\Plug-in Activation menu item at any time after finalization.

Advertising on Active Directory

After finalizing (or Skipping) each plug-in, you are prompted as to whether you want to advertise in Active Directory.



Figure 3-2. Active Directory Advertising message

See “Server Operation” on page 12 for more information.

Manage Logs Tab

In the audit log file main window, you are presented with the directory tree of log files. You can view, copy, validate, and delete audit logs. When you select “View Log,” the log is first verified, and then displays in a browser window.

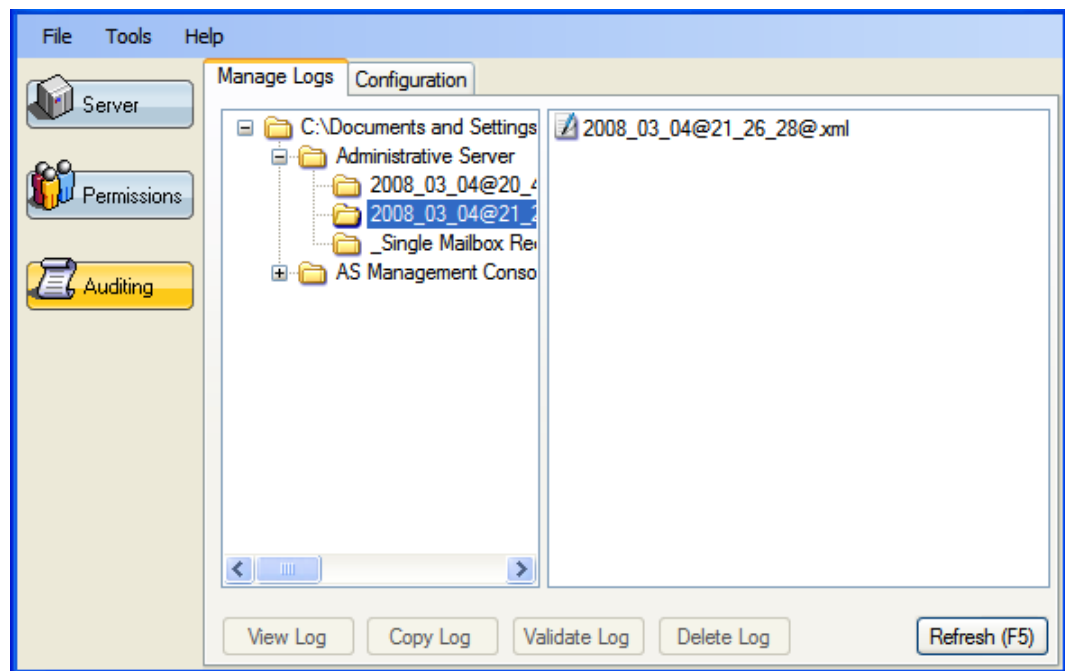


Figure 3-3. Manage Logs tab

Note: The date and time used to form the name of the folder and log file are based on UTC (GMT+0), not local time.

Log Directory Tree

The left pane displays the log directory tree. It displays the root node, then the services that have connected, such as Single Mailbox Recovery for Exchange and Single Mailbox Recovery Management Console. Each service displays the user and the audit sessions with the date and time in the title.

Note: A session log's folder name is determined by using client application name (e.g. Single Mailbox Recovery for Exchange) followed by the date and time the session started (in UTC – GMT+0, not local time-zone). In cases when two clients connect within the same second, the folder name of the second connection will be suffixed with a lower case letter 'a.' If a third connection occurred within the same second it would be suffixed with 'b' and so on.

Audit Logs

The right pane displays the audit session logs.

- If the icon at the beginning of the log is  and/or the log file name has a "@" at the end, it indicates the session is still running and therefore the log is incomplete.
- If the icon is , it indicates the session is complete.

Note: A session log's name is determined using the date and time the session started (in UTC – GMT+0, not local time-zone) with an .xml file extension. Over time, log files will grow and so in order to prevent logs from growing so large that they become unwieldy, new 'rollover' logs are created. The naming convention for these 'rollover logs' is the original date and time name with a '_1' suffix for the first rollover log, a '_2' suffix for the second rollover log, and so on.

REFRESH

You can update the information on the page by clicking the Refresh button.

VIEW LOG

You can open an audit log by selecting a log in the right pane and clicking the View Log button. It opens after a validation is performed. If the validation fails, the log is still viewable but a warning message is displayed.

Single Mailbox Recovery Audit Session

Detailed Report

File Data

This File	Previous File	Next File	File End Reason
C:\Documents and Settings\All Users\Application Data\Single Mailbox Recovery Administrative Server\Audit Store Root\Administrative Server\2008_03_04@20_42_00\2008_03_04@20_42_00.xml	no file	no file	Session Ended

Session Data

Application Name	User Name	Machine Name	Session Start Time	Session End Time	Session End Reason
Administrative					Closed -

Figure 3-4. Audit Session sample

Session Data

This section includes:

- **Application Name:** The name of the application or service being audited (for example, Single Mailbox Recovery for Exchange).
- **User Name:** Name of the user logged in and running the application.
- **Machine Name:** The network name for the computer.
- **Session Start Time:** Start of the Single Mailbox Recovery Audit Session for that application.
- **Session End Time:** End of the Single Mailbox Recovery Audit Session for that application.
- **Session End Reason:** The reason the session was ended: "Closed - Client Closed Session," the application closed; "Closed - Connection Lost," the connection failed unexpectedly (for example, network failure).

Activity Data

Total Activity Entries 39

Activity Id: 1

Server Time	Client Time	Action	Action Modifier	Transaction Id
20:42:00	8:42:00 PM	The Single Mailbox Recovery Administrative Server has started.	Standalone	0

Parameter Name	Parameter Value
Service	Auditing Service (1)
Service	Mailbox Permissions Control (2)
Service	Server Configurator (3)
Server is finalised	True
Server connection port	49152
Server is advertised on ADS	False

Activity Id: 2

Server Time	Client Time	Action	Action Modifier	Transaction Id
20:42:00	8:42:00 PM	Connection started	Standalone	0

Parameter Name	Parameter Value
----------------	-----------------

Figure 3-5. Activity Data in the Audit Log

Activity Data

This section logs:

- **Total Activity Entries:** The total number of activities entered by the user.
- **Activity Id:** Sequential number assigned to user activity.
- **Server Time:** The time of day according to the server.
- **Client Time:** The time of day according to the client.
- **Action:** The type of activity based on the audit activities listed in [Appendix A: Activities to be Logged](#).
- **Action Modifier:** Either Stand alone or Transaction. See “Types of Activities that are Logged” on page 53.
- **Transaction Id:** Sequential number assigned to the transactional activity. A Transactional Id of “0” indicates a stand alone activity.
- **Parameter Name:** The type of of parameter being audited.
- **Parameter Value:** The value of the type of parameter being audited.

Show Summary Report

You can request a Summary Report of the entire audit session by clicking the Show Summary Report button located at the bottom of the audit log.

Address	127.0.0.1
Server connection ID	5
Client application name	AS Management Console v1.0.0.1

Activity Id: 38

Server Time	Client Time	Action	Action Modifier	Transaction Id
21:26:27	9:26:27 PM	Terminating all connections	Stop	1

No parameters

Activity Id: 39

Server Time	Client Time	Action	Action Modifier	Transaction Id
21:26:27	9:26:27 PM	Server is shutting down.	Standalone	0

No parameters

Figure 3-6. Show Summary Report

The Summary Report displays the same header information as the audit log.

Single Mailbox Recovery Audit Session

Summary Report

File Data

This File	Previous File	Next File	File End Reason
C:\Documents and Settings\All Users\Application Data\Single Mailbox Recovery Administrative Server\Audit Store Root\Administrative Server\2008_03_04@20_42_00\2008_03_04@20_42_00.xml	no file	no file	Session Ended

Session Data

Application Name	User Name	Machine Name	Session Start Time	Session End Time	Session End Reason
Administrative					Closed - Client

Figure 3-7. Summary Report

The Activity Data list displays every transaction in the audit session describing the basics of each activity.

Activity Data					
Total Activity Entries					39
ActivityId	Server Time	Client Time	Action	Action Modifier	Transaction Id
1	20:42:00	8:42:00 PM	The Single Mailbox Recovery Administrative Server has started.	Standalone	0
2	20:42:00	8:42:00 PM	Connection started	Standalone	0
3	20:42:03	8:42:03 PM	Connection started	Standalone	0
4	20:42:03	8:42:03 PM	Open service session	Standalone	0
5	20:42:03	8:42:03 PM	Open service session	Standalone	0
6	20:42:03	8:42:03 PM	Open service session	Standalone	0

Figure 3-8. Activity Data in Summary Report

COPY LOG

The Copy Log button copies the log file to an alternate location that you designate. It does not create or maintain a link to the file.

VALIDATE LOG

The Validate Log button displays the result of the validation of the file. If the validation fails, the log still displays but with a warning message.

DELETE LOG

The Delete Log button deletes a log file.

Configuration Tab

.....

The Configuration tab allows you to set or edit the audit store root path and the 24-hour log rollover time.

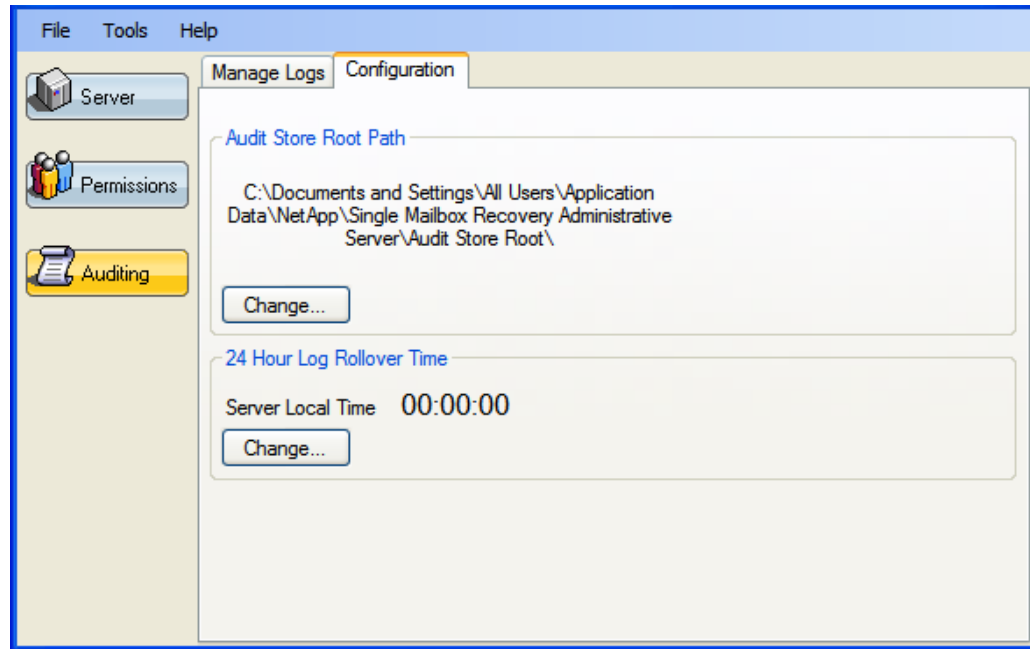


Figure 3-9. Auditing Configuration tab

Audit Store Root Path

You can change the location where the audit logs are stored in the Audit Store Root Path section.

To change the audit store root path

1. Click **Change**. The **Browse For Folder** window is displayed.



Figure 3-10. Select a different root path

2. Click **OK**. A **Change audit service store root** message appears.

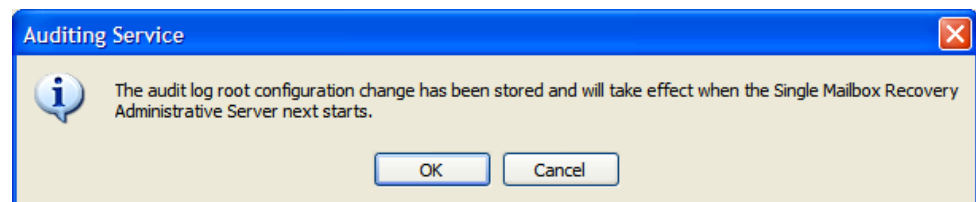


Figure 3-11. Change audit service store root confirmation

3. Click **OK**. The **Audit Store Root Path** change takes affect the next time the server is restarted. This can be achieved using the Restart button on the Server configuration page. See "Server Operation" on page 12. Until the server is restarted, a warning message appears.

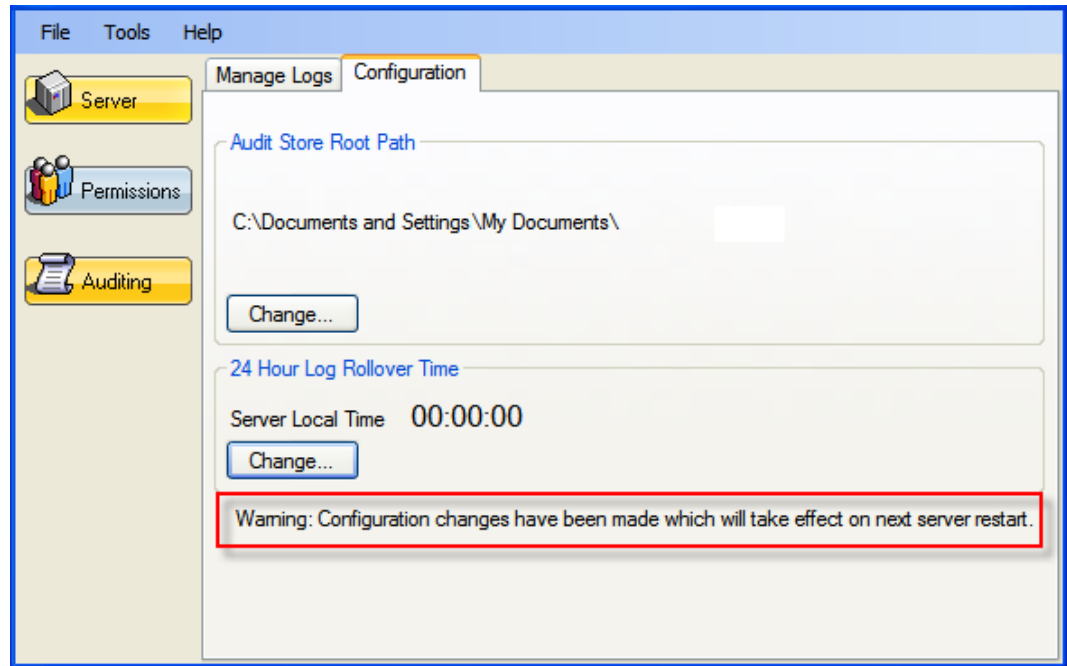


Figure 3-12. Example of warning message

24-Hour Log Rollover Time

This setting allows you to set the time of day the audit log rolls over into a new day.

To change the 24-hour log rollover time

1. Click **Change**. The **Audit Service - Change 24 Hour Log Rollover Time** window appears.

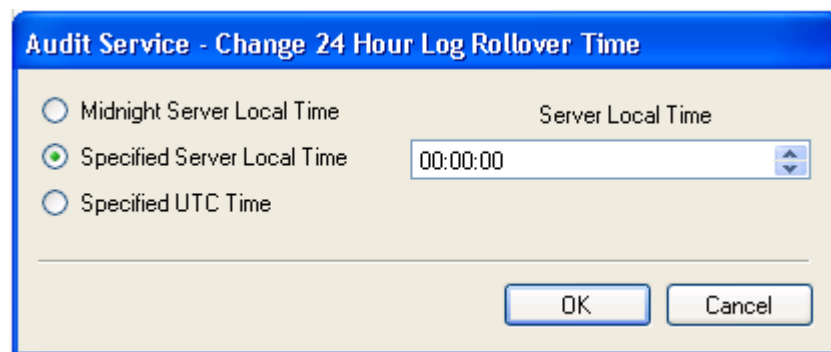


Figure 3-13. Change 24-Hour Log Rollover Time

2. Select one of the following:
 - **Midnight Server Local Time:** Selecting this option automatically sets the rollover time to midnight in the local time of the server location.
 - **Specified Server Local Time:** Selecting this option allows you to set the local time of the server to which you want the audit logs to rollover.

- **Specified UTC Time:** Selecting this option allows you to set the rollover time for the audit logs based on the Greenwich Universal time instead of the server local time.
3. Change the **Server Local Time**, if desired.
 4. Click **OK**. A Single Mailbox Recovery Administrative Server **Auditing Service** message appears:

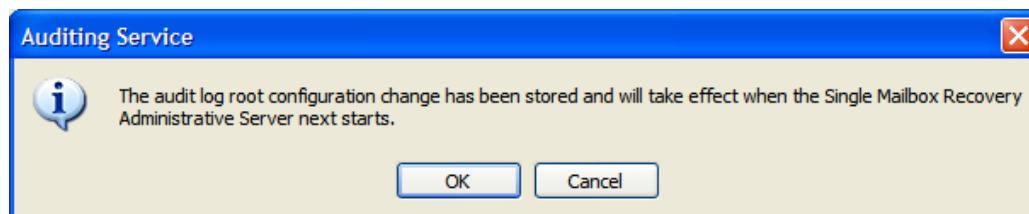


Figure 3-14. Audit log roll time configuration change message

5. The 24-Hour Log Rollover Time change takes affect the next time the server is restarted. You can do this by using the Restart button on the Server configuration page. See "Server Operation" on page 12 for more information. Until the server is restarted, a warning message appears.

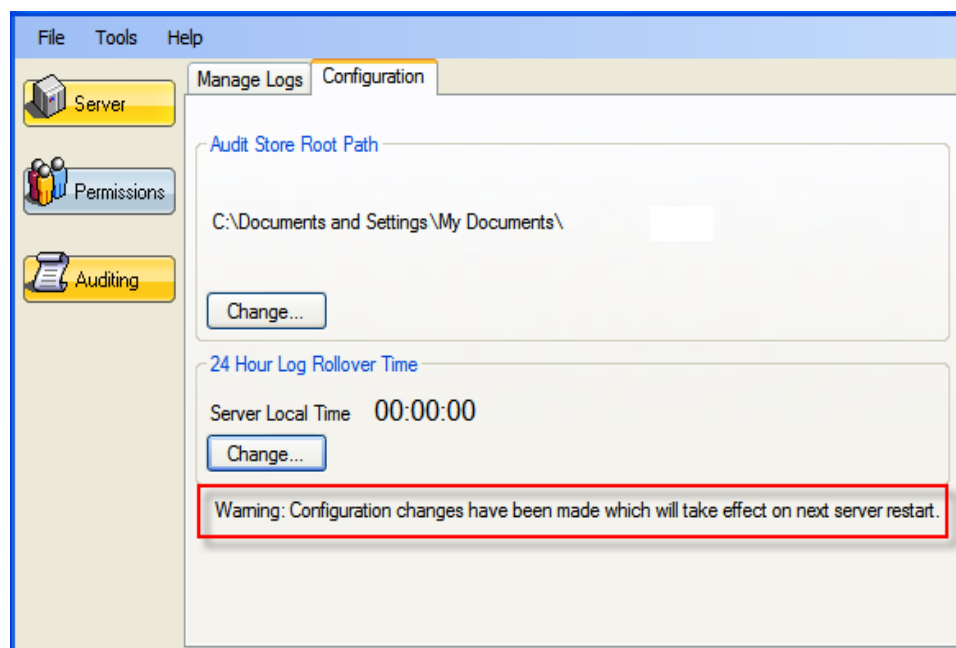


Figure 3-15. Example of warning message

ACTIVITIES TO BE LOGGED

Client-Side Activities to be Logged

All activities affecting the Source or Target store are logged. In addition, all activities that affect what is viewable by you on the screen are logged.

In Single Mailbox Recovery for Exchange 6.0 and Single Mailbox Recovery ExtractWizard, the types of activities logged are those initiated from the user interface, the command line interface, and Data Wizard.

Single Mailbox Recovery for Exchange User Interface Actions

This list displays any action taken on the Single Mailbox Recovery user interface that is recorded in the Application Audit Service.

- **Session Start from GUI:** Single Mailbox Recovery is starting up in GUI mode.
- **Session End:** Single Mailbox Recovery is shutting down.
- **Open Datastore:** A datastore (Source or Target) is about to be opened.
- **Open Target Exchange Server:** A Target exchange server was opened. The audit parameters vary depending if the connection is made to a single mailbox or all mailboxes.
- **Paste Messages:** Messages are pasted from a Source into a Target, either by a prior copy to the clipboard or by a drag and drop.
- **Select Folder:** A folder node in the tree is selected.
- **Paste Folder:** A folder is pasted from a Source into a Target.
- **Delete Folder:** Delete a folder in a Target.
- **Delete Message:** Delete a message in a Target. If multiple messages are selected and deleted, there will be one audit entry for each.
- **Delete Source From Content Analysis Store (CAS):** Delete a Source from a Target CAS. If multiple Sources are selected and deleted, there will be one audit entry for each.
- **Rename Folder:** Rename a folder in a Target.
- **New Folder:** Create a new folder in a Target.
- **Preferences Changed:** The application preferences have been changed. There are three separate property pages of preferences. If a preference on one page changes, the new values of all of the preferences on that same page are audited. All three pages are audited under the same audit action, however the parameters associated with the audit action vary depending on which page was changed.

- **Export Messages:** Messages are exported from a Source into a file.
- **Export Folder:** A folder is exported from a Source to a file.
- **Integrity Check:** Integrity check a folder in a Source.
- **Create Reports Started:** “Generate Reports” was clicked on the “Create Reports” dialog. The audit parameters vary slightly depending on the date selections.
- **Create Reports Finished:** The “Create Reports” dialog operation completed.
- **Report Saved:** The report created using “Create Reports” dialog was saved to file.
- **Find Start:** “Find Now” was clicked on the “Find In Source” dialog. This has two different sets of audit parameters depending on if we are searching in previous search results. When searching in previous results, the search subfolders and search folder paths parameters are omitted.
- **Find Complete:** The “Find In Source” dialog find operation completed.
- **Find Criteria Saved:** The find criteria were saved to file.
- **Save Search Results:** The find report was saved to file. This actually saves two files, a summary report and a detailed report. The filenames to save to are automatically generated. A separate audit entry is made for each as either may fail.
- **Message View Launched:** Launch the message view window in one of three possible view types.
- **Tree Datastore Expanded:** A datastore root node in the tree is expanded.
- **Datastore Closed:** A datastore is closed.
- **Expand Folder Tree:** A folder node in the tree is expanded.
- **View Message:** The contents of a message has been viewed, either from the message window or the message preview pane.
- **View Attachment:** A message attachment was viewed.
- **Save Attachment:** A message attachment was saved.
- **Wizard Page Activated:** A wizard page was activated. This applies to both the Data Wizard and the Mailbox Creation Wizard.
- **Wizard Button Clicked:** A button on a wizard page was activated. This applies to both the Data Wizard and the Mailbox Creation Wizard. For all buttons, there are always three audit parameters (wizard name, page name, button name), as shown below.

Single Mailbox Recovery for Exchange Command Line Actions

- **Session Start from Command Line:** Single Mailbox Recovery for Exchange is starting up in command line mode.
- **List Mailboxes:** The mailboxes in a Source are listed via command line switches.
- **Paste Folder:** A folder is pasted from a Source into a Target via command line switches.
- **Export Folder:** A folder is pasted from a Source to a file via command line switches.
- **Integrity Check:** Integrity check a folder in a Source via command line switches.
- **Command Line Processed:** The command line was processed (this is a transaction audit that surrounds command line processing and can return useful error information if the command line parameters were invalid).

Data Wizard

Data Wizard page activations are audited. This records the wizard name and the wizard page name as parameters. Data Wizard button clicks are audited. This records the wizard name, the wizard page name and the wizard button name as parameters. This audits all button clicks with the exception of the “Next” button. The “Next” button clicks are treated as a special case. Each Data Wizard page is provided with a dedicated function to audit its “Next” button click.

Single Mailbox Recovery ExtractWizard Actions

This list displays any action taken in Single Mailbox Recovery ExtractWizard that is recorded in the Application Auditing Service.

- **Single Mailbox Recovery ExtractWizard Start Up:** Single Mailbox Recovery ExtractWizard is starting up.
- **Single Mailbox Recovery ExtractWizard Exit:** Single Mailbox Recovery ExtractWizard is shutting down.
- **Wizard Page Activated:** A wizard page was activated.
- **Wizard Button Clicked:** A button on a wizard page was activated. For all buttons, there are always two audit parameters (wizard page name, button name), as shown below. For the “Next” button, there may be additional audit parameters, specific to the wizard page. The specific cases are also shown below.
- **Choose Method Page Next Button Clicked:** Extra parameters for “Next” button, Choose Method Page, direct method
- **Choose Source Page Next Button Clicked:** Extra parameters for “Next” button, Choose Source Page, disk
- **Choose Connection Parameters Page Next Button Clicked:** Extra parameters for “Next” button, Choose Connection Parameters Page, exchange2kx
- **Choose Tape Device Page Next Button Clicked:** Occurs between Choose Source page and Catalog Options page when user selects tape and more than one tape device exists on their system.
- **Catalog Options Page Next Button Clicked:** Extra parameters for “Next” button, Catalog Options Page
- **Catalog Progress Page Next Button Clicked:** Extra parameters for “Next” button, Catalog Progress Page
- **Info Store File Selection Page Next Button Clicked:** Extra parameters for “Next” button, Info Store File Selection Page
- **Info Store Destination Page Next Button Clicked:** Extra parameters for “Next” button, Info Store Destination Page
- **Extraction Progress Page Next Button Clicked:** Second to last page of wizard.
- **Emulation Progress Page Next Button Clicked:** Second to last page of wizard.
- **Extraction Results Page Activated:** Last page of wizard (Note: It logs additional information on page activation, not on Next/Finish button click). Logs the same information as is displayed in the results page. If extracted, this includes a listing of which files were successful/failed.

Server-Side Activities that are Logged

.....

On the server side, activities are logged for the Server, Mailbox Permissions Service, and the Single Mailbox Recovery Management Console.

Server Log

This list displays any action taken on the connected server that is recorded in the Application Auditing Service.

- **Server start-up:** Start of the Single Mailbox Recovery Administrative Service.
- **Server shutdown:** End of the Single Mailbox Recovery Administrative Service.
- **Terminating Connections:** This transactional action occurs when the server is about to start terminating a number of connections and when it completes the process.
- **Terminating a Single Connection:** This action occurs when the server closes a connection.
- **Write a Service Message:** This action occurs when a service requests that a message be written to the server audit log.
- **Open a Service:** This action occurs when a client has requested access to a service.
- **Disconnect from a Service:** This action occurs when a service session is being closed. Note that sessions can be closed because the client has indicated that it no longer needs them or because the server (perhaps at the request of the Single Mailbox Recovery Management Console) has chosen to terminate the session.
- **Stop the Server:** This occurs when the server is stopping.
- **Register a Client:** This action occurs when a new client has established a connection to the server.
- **Unregister a Client:** This action occurs when the server has finished communicating with a client. This can either be at the client's request or because the server (perhaps at the request of the Single Mailbox Recovery Management Console) has chosen to terminate the connection.
- **Change Server Configuration:** This action occurs when a request to change the server configuration has been processed.

Mailbox Permissions Service Session Log

This list displays any action taken in the Mailbox Permissions Service that is recorded in the Application Auditing Service.

- **Permissions Have Been Read:** This action occurs whenever the configurator or the service load permissions settings from disk.
- **Permissions Have Been Retired:** This action occurs when the service reloads the permissions set because the MC has told it to. It keeps a record of the outgoing permissions set.
- **Permissions Have Been Updated:** This action occurs when the service reloads the permissions set because the MC has told it to. It keeps a record of the incoming permissions set.
- **Permissions Test Performed:** This action occurs on the service when a client requests a permissions test, i.e., wants to know if they should open a mailbox.

- **Permissions Have Been Written:** This action occurs when the service writes the current permissions set to disk because the MC has told it to. It keeps a record of the newly read permissions set.
- **Permissions Have Changed:** This action occurs when the configurator has written the current permission set to disk and those permissions are now in effect for clients. In other words it occurs when the user clicks the “save” button.
- **A Refusal Has Been Converted Into a Temporary Allow:** This action occurs when the configurator has just converted a refusal into a temporary allow.
- **A Refusal Has Been Converted Into a Permanent Allow:** This action occurs when the configurator has just converted a refusal into a permanent allow.
- **Permissions Auditing Has Ended:** This action occurs when the service is shutting down.

Single Mailbox Recovery Management Console Session Log

This list displays any action taken in the Single Mailbox Recovery Management Console user interface that is recorded in the Application Auditing Service.

- **Console Start:** This action occurs when the Single Mailbox Recovery Management Console is ready for normal operation.
- **Console End:** This action occurs when the Single Mailbox Recovery Management Console is shutting down.
- **Server Restarted:** This action occurs after the server has been restarted and a connection re-established to it.
- **First-time Run:** This action occurs when the Single Mailbox Recovery Management Console has just completed first-time run functionality.
- **Deactivate Plug-ins:** This action occurs when the Single Mailbox Recovery Management Console is deactivating one or more plug-ins.

Server Configuration Plug-In

This list displays any action taken in the Server Configuration page that is recorded in the Application Auditing Service.

- **Terminate Connection:** This action occurs when the user chooses to terminate a connection.
- **Set Server Port:** This action occurs when the user changes the server port.
- **Set Active Directory Advertising:** This action occurs when the user changes whether or not the server is advertised on Active Directory.

Term	Description
Any User	Any User is a special entity. This matches against any user regardless of group or name. It is used to terminate further permission checking. This must always be the last entry in a permission list.
Client	The Client is the software making use of services being hosted on the Server. Note that the Single Mailbox Recovery Management Console acts as a client of the Server to achieve its tasks.
Multiplicity	It is pointless to have a user or group appear explicitly twice within a single list. You can implicitly match with one or more groups that are listed but a user or group can only be specifically mentioned once.
Server	This is an application running on a remote machine. It manages the connection with the client and hosts multiple services. A server package is a self-contained chunk of information being exchanged between the client and the server
Service	This is a plug-in module that the server loads. A service package is information being exchanged between a client and an individual service.

Numerics

24-hour log rollover time
changing 54, 61

A

Active Directory
advertising 11, 13
updating 13
Activity Data 58
advertising
changing 13
All mailboxes
permissions 18
allowing access
permanently 42
temporarily 42
audit log
changing rollover time 63
copying 60
deleting 60
validating 60
viewing 56
audit logs
changing location 61
audit store root path
changing 54, 61

C

changes
activating 44
complete log 56
connection
terminating 13, 14
connections
active 14
conventions in this manual
menu commands and shortcuts
5
notes and tips 6
shortcut menu 6

D

denying access 45
directory tree 55

E

external mailbox
permissions 18
removing 29
external mailboxes
adding 27

F

failed access attempts 42
first run configuration 17, 54

G

getting help 5
group or user
adding 23
setting permissions 25

H

Help
online Help 5

I

incomplete log 56
installed services
list 14
internal mailbox
permissions 18

K

Keyboard Shortcuts 3

L

list
filtering 22
logged activities
stand alone 53
transaction 53

M

mailbox
adding 22
removing 23
Mailbox Categories
permissions 18

mailboxes

clearing 44

Menu Commands and Shortcuts 6

Midnight Server Local Time 63

N

Notes and Tips 6

O

online Help 5

P

permanently allow 43
Permission Model 18
horizontal check 18
vertical check 20
permission order
changing 25
permission settings 18
permissions
applying 22
editing 22, 27
saving 44
setting 24
sorting order 25
viewing 22, 27
port
changing 12

R

refusal
allowing 42
refusals
managing 42

S

server
restarting 12, 13
stopping 12, 13
Service Connection Point
updating 13
services
available 15
Session Data 57
settings

- clearing 44
- modifying 51
- Shortcut Menu 6
- Specified Server Local Time 63
- Specified UTC Time 64
- stored permissions
 - reloading 44
- Summary Report
 - showing 58
- system requirements 1

T

- technical support 5
- temporarily allow 43
- temporary refusal allow
 - choosing duration 43

U

- user or group
 - removing 24

W

- wizard
 - using 44