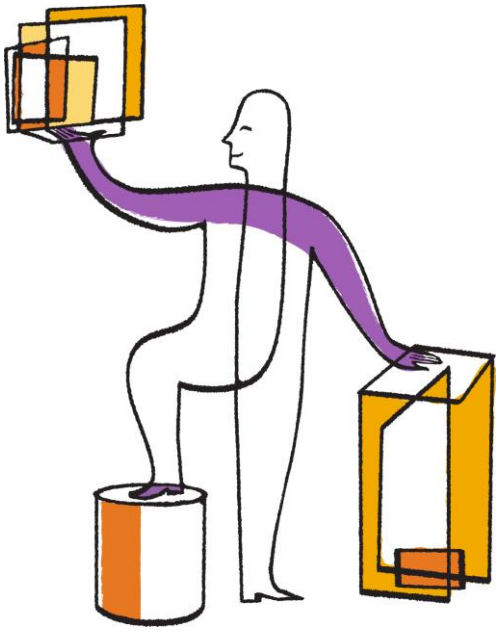
Single Mailbox Recovery 7.2

Administrative Server Administration Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-10652_A0
December 2015

Notice to Users

Single Mailbox Recovery software 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 Administration Guide, or will be available on the website. In that event, please read the release notes or Read Me file before using the product.

Contents

Contents i

Introduction 1

Overview 1

Release Notes 1

Getting Help 1

Conventions in this Manual 2

Chapter 1: Single Mailbox Recovery Administrative Server 3

Overview 3

Looking at the Single Mailbox Recovery Management Console 3

Single Mailbox Recovery Management Console First Run Configuration 6

SMBR/SMAS Integration 6

Server Configuration Page 9

Chapter 2: Mailbox Permissions Service 14

Overview 14

Multi-Tenant Background 14

Mailbox Permissions Service First Run Configuration 15

Permission Model 15

Horizontal Check 15

Vertical Check 17

Examples of Use 18

Specific (Internal) Tab 26

Location Column 27
Adding a Mailbox 28
Adding and Removing a User or Group 28
Setting Permissions for a Mailbox 30
Sorting the Permission Order 30
Specific (External) Tab 31
Adding a Mailbox 32
Adding and Removing a User or Group 34
Setting Permissions for a Mailbox 35
Sorting the Permission Order 36
Mailbox Categories Tab 36
Setting the Mailbox Category 37
Adding and Removing a User or Group 37
Setting Permissions for Mailboxes Matching the Selected Category 40
Sorting the Permission Order 41
All Mailboxes Tab 42
Adding and Removing a User or Group 42
Setting Permissions for All Mailboxes 44
Sorting the Permission Order 45
Manage Refusals Tab 46
Allowing a Refusal 47
Clearing, Reloading, and Saving 48
Using the Wizard 49

Chapter 3: Application Auditing Service 56

Overview 56

Types of Activities that are Logged 56

Client Activities that are Logged 56

Server-Side Activities that are Logged 56

Audit Service First Run Configuration 57

Skip Button 57

Advertising on Active Directory 57

Manage Logs Tab 58

Log Directory Tree 58

Audit Logs 58

Configuration Tab 63

Audit Store Root Path 63

24-Hour Log Rollover Time 65

Chapter 4: Settings Service 67

Overview 67

Setting the Security Values 67

Adding or Removing a User or Group 69

Appendix A: Activities to be Logged 71

Client-Side Activities to be Logged 71

Single Mailbox Recovery User Interface Actions 71

Single Mailbox Recovery Command Line Actions 72

Data Wizard 73

Single Mailbox Recovery ExtractWizard Actions 73

Logged Server-Side Activities 74

Server Log 74

Mailbox Permissions Service Session Log 75

Settings Service Session Log 76

Single Mailbox Recovery Management Console Session Log 76

Server Configuration Plug-In 77

Glossary 78

Copyright Information 80

Trademark Information 81

How to Send Comments About Documentation and Receive Update Notifications 82

Index 83

Introduction

Overview

Welcome to NetApp® Single Mailbox Recovery Administrative Server 7.2. This application is a framework that can host centralized services to multiple clients and provide both client and server support for Single Mailbox Recovery 7.2 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 7.2 to mailboxes contained within private EDB Exchange mailbox stores based on your authority.
- **Application Auditing Service:** Activities performed as part of Single Mailbox Recovery 7.2 and Single Mailbox Recovery ExtractWizard operations, as well as activities within Single Mailbox Recovery Administrative Server, are logged as part of an "audit trail."
- **Settings Service:** Provides you the ability to centrally administer the Single Mailbox Recovery application's security preferences.

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

Release Notes

The *NetApp® Single Mailbox Recovery 7.2 Administrative Server Release Notes* document contains additional information about the Single Mailbox Recovery Administrative Server, including:

- System requirements
- Upgrading from previous versions
- Technical support

Getting Help

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

- Online Help
- Technical Support

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.

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 does not 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.

Chapter 1: Single Mailbox Recovery Administrative Server

Overview

Single Mailbox Recovery Administrative Server activates mailbox permissions, centralizes administration of certain application settings, and provides auditing services for Single Mailbox Recovery and Single Mailbox Recovery ExtractWizard clients.

When you launch Single Mailbox Recovery 7.2, 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, including mailbox permissions service, application auditing service, or settings 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.

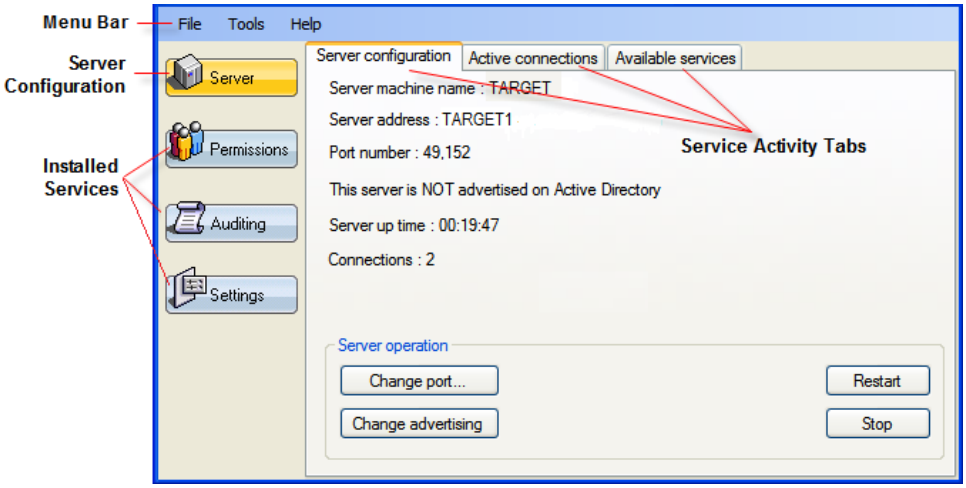


Figure 1-1: Single Mailbox Recovery Management Console main window

Menu Bar

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

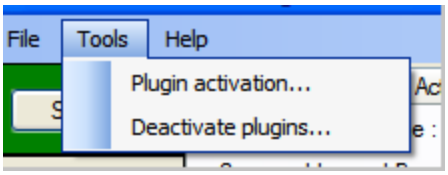


Figure 1-2: Plugin Activation/Deactive Plugins options

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 inactive. If the plugin is inactive, its finalization window appears.

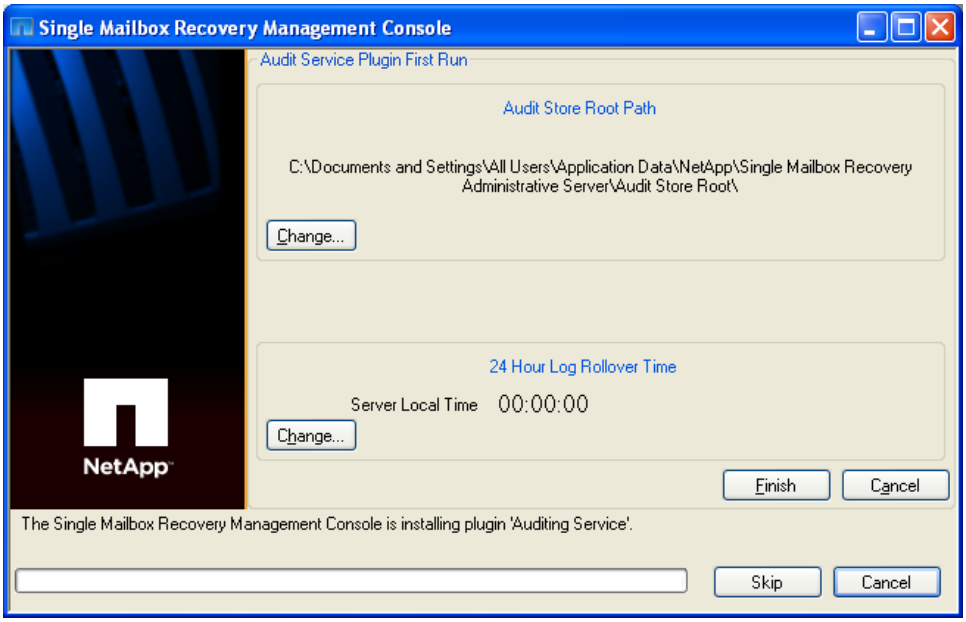


Figure 1-3: Example of finalization window for Auditing

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.

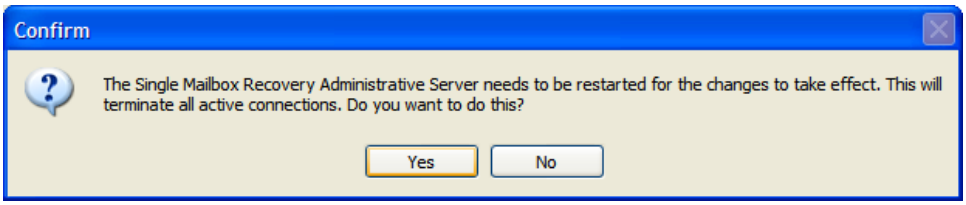


Figure 1-4: Confirm deactivation message

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). For more information, see **"Server Operation" on page 10**.

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.

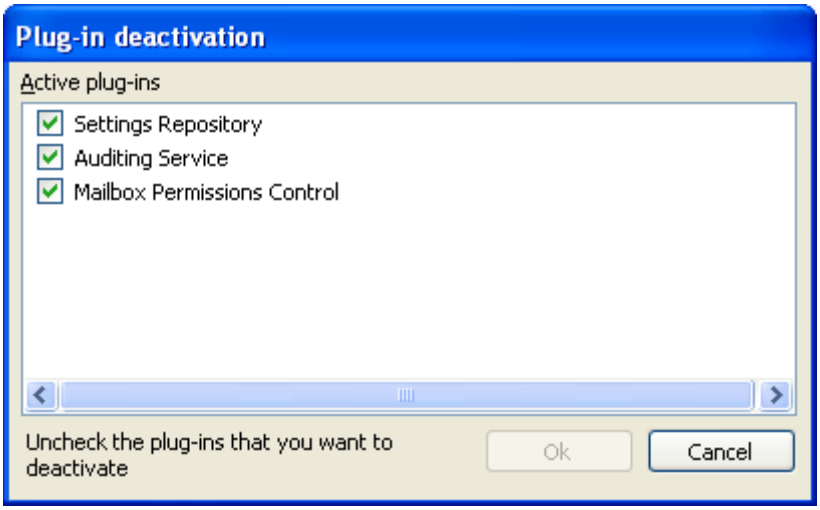


Figure 1-5: Plug-in deactivation window

Clear the plugin or plugins that you want 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.

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). For more information, see **"Server Operation" on page 10**.

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

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.

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 plugins. For details on the finalization for Mailbox Permissions and Applications Auditing, see **"Mailbox Permissions Service First Run Configuration" on page 15** and **"Audit Service First Run Configuration" on page 57**.

SMBR/SMAS Integration

When you launch Single Mailbox Recovery (SMBR), it attempts to connect to Single Mailbox Recovery Administrative Server (SMAS) if it is activated. The local SMBR client should have the SMAS option enabled in its license file to search for an SMAS server.

Note: *This is a license option that must be obtained through your NetApp Account Representative.*

SMAS can be installed and running; however, if the SMBR client does not locate the SMAS server, then none of the SMAS server's functions are available to that SMBR client.

The administrator can choose to deploy the SMAS service in the following two ways:

1. SMAS service is advertised on the Active Directory

When the user selects the Active Directory (AD) to "advertise" the presence of the SMAS server, SMBR will send an inquiry over the network and the AD will respond to the inquiry with the SMAS server name and the port number.

SMAS is located automatically by using a Service Connection Point (SCP) in the AD, or a server whose details you have provided. The SCP is an AD object created to respond to SMBR and SMAS server queries with the SMAS server name and listening port number. The AD SCP entry for SMAS is under the SMAS server in ADSIEdit.

If the SMAS computer is not a domain controller, it appears under CN=Computers. If SMAS is installed on the domain controller, it appears under CN=Domain Controllers.

The AD query looks for the keyword beginning with "SMASf669"

2. SMAS service is not advertised on the Active Directory

If the user selects to not advertise over the AD, there is no entry in the AD.

In this case, when SMBR is launched, the user is prompted to enter the details to create the connection point manually. SMBR will then directly connect to the specified SMAS server name and port number itself.

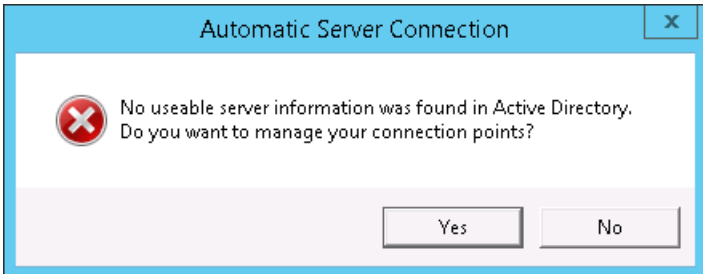


Figure 1-6: In SMBR, the user is prompted to select one of the options.

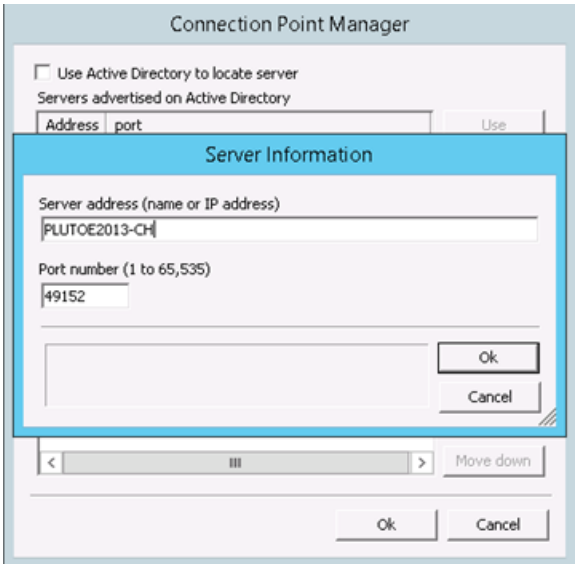


Figure 1-7: In SMBR, the user is prompted to enter the server information.

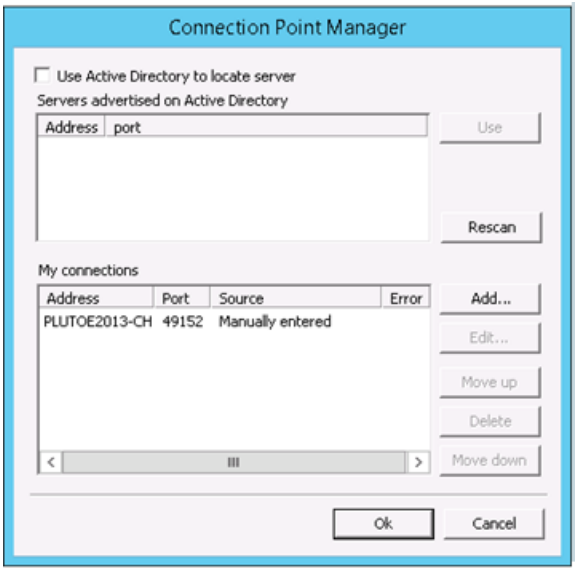


Figure 1-8: In SMBR, the Connection Point Manager displays the newly entered values.

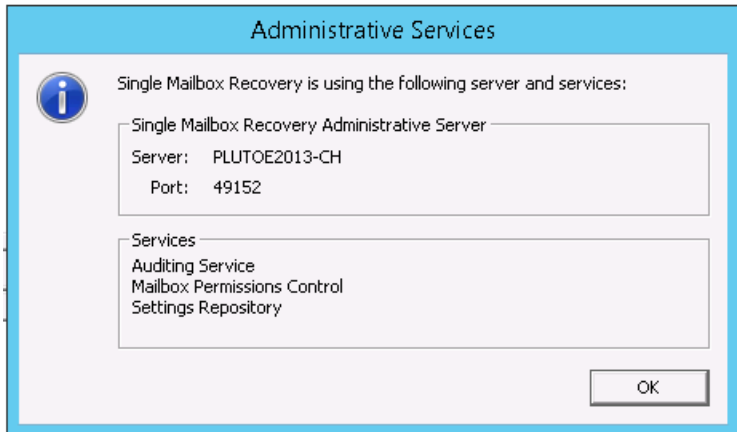


Figure 1-9: In SMBR, the entered server responds to the SMAS service request.

The advantage of advertising over the AD is that the local user does not need to know the SMAS server and port information.

After connecting to the server, Single Mailbox Recovery can use the activated services, including the mailbox permissions service, application auditing service, and settings service. These services are configured and monitored using the Single Mailbox Recovery Management Console.

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.

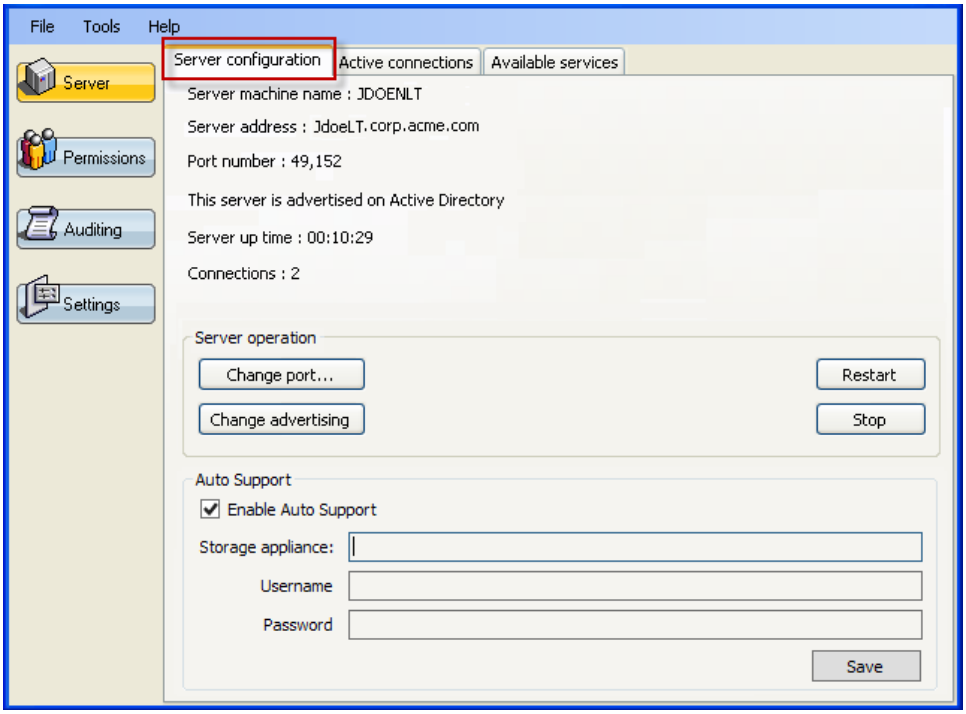


Figure 1-10: Server Configuration tab

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.

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

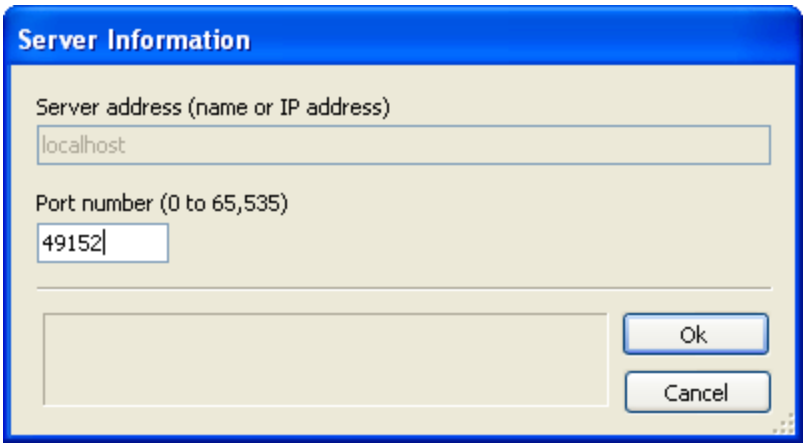


Figure 1-11: Server Information

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 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.

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.

Auto Support (ASUP)

Use the Auto Support section to govern whether messages about the following Single Mailbox Recovery Administrative Server tasks, when performed, are sent to a NetApp storage appliance:

- Start of the Management Console
- Abnormal exit of Management Console

  Note: *The NetApp storage appliance can be configured to automatically forward this to NetApp.*

- Start, restart and stop of the Single Mailbox Recovery Administrative Server service.

Enable Auto Support

Select this option to log Single Mailbox Recovery Administrative Server usage information and customer configuration data to the NetApp storage appliance specified below.

Storage appliance

Enter the name or IP address of the NetApp storage appliance where the Auto Support messages are logged.

Username

Username for account with permissions required to log an ASUP message on the NetApp storage appliance.

Password

Password for account with permissions required to log an ASUP message on the NetApp storage appliance.

Active Connections Tab

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

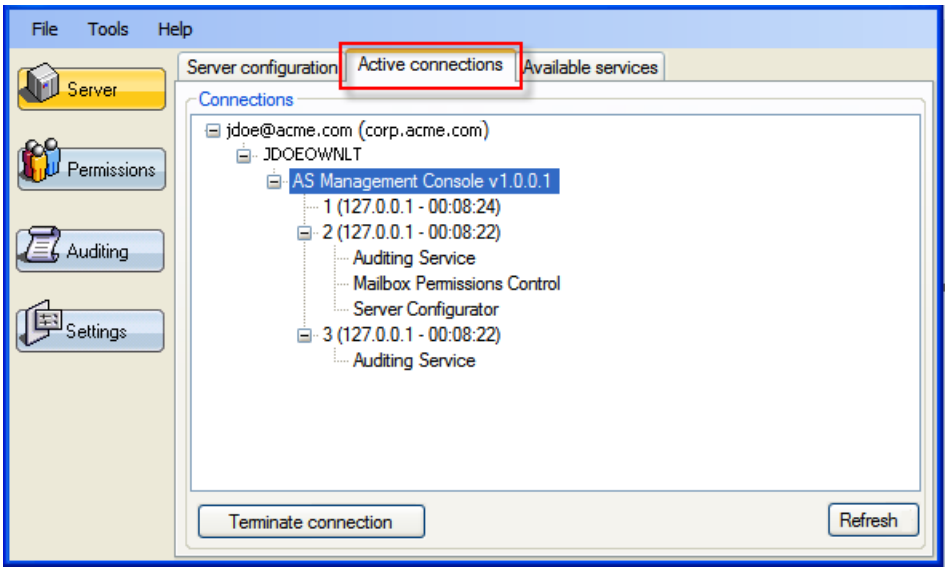


Figure 1-12: Active Connections tab

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 plugins 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.

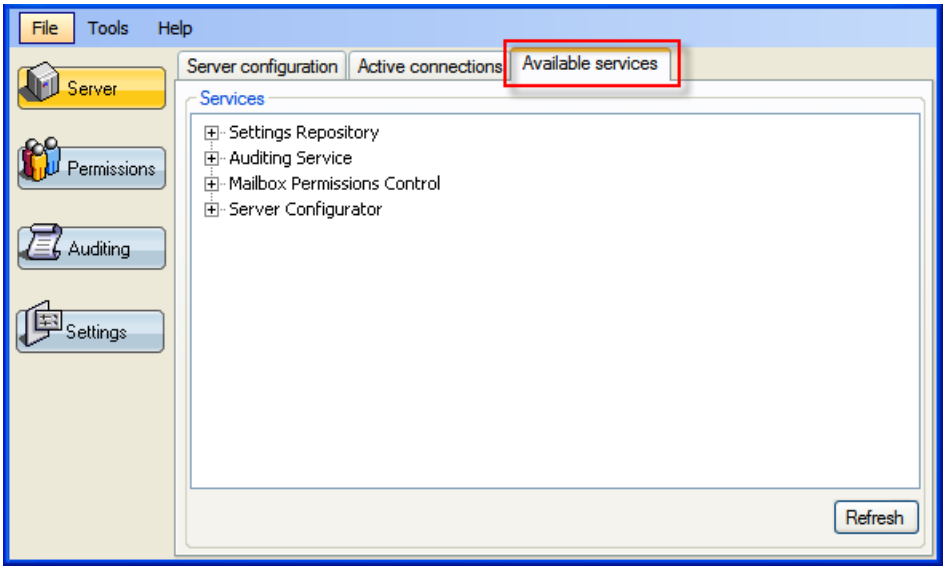


Figure 1-13: Active Connections tab

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.*

Chapter 2: Mailbox Permissions Service

Overview

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. To assist you in reinforcing your corporate security policies, you can set permissions on internal and external mailboxes to your forest, 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 forest.
- **External Mailboxes:** These permissions apply to specific mailboxes that do not exist within the current forest.
- **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: *The Mailbox Permissions Service is supported for cases in which both server and client systems are joined to domains in the same forest (where domains have a two-way trust relationship). The Mailbox Permission Service is not supported for scenarios in which the client system(s) are operating in a different forest 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 and later. 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.*

Multi-Tenant Background

The mailbox permissions service includes support for both:

1. Multi-domain environments – and –
2. Microsoft Exchange Server 2010 and later multi-tenant features, specifically:
    a. /hosting deployments of Microsoft Exchange Server with Exchange Hosted Organizations (Microsoft Exchange Server 2010 SP1 only)
    b. Address Book Policies

The support for these features includes identifying the location of mailboxes, users, and groups, and the ability to define rules to grant or deny permission to mailboxes associated with domains, Microsoft Exchange Server hosted organizations, and Address Book Policies. This support allows existing domain and multi-tenant configurations to be leveraged when creating permission rules to grant or deny access to mailboxes opened by Single Mailbox Recovery.

Mailbox Permissions Service First Run Configuration

When the permissions service plugin is first installed using the Single Mailbox Recovery Management Console, a wizard appears allowing you to set up some initial permission settings. For more information, see **"Using the Wizard" on page 49**.

Permission Model

When a user in Single Mailbox Recovery 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*.

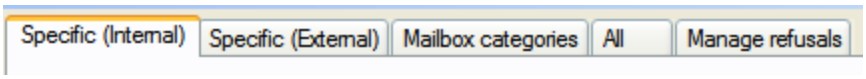


Figure 2-1: Mailbox Permission tabs

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 in the forest, each with a deny or allow permission designation.

Tier 1

- **Specific (Internal) mailbox permissions:** These are mailboxes that are within the Administrator's forest 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 forest 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:** These are categories of mailboxes present in the environment. Specific entries exist for the different categories of mailboxes that are internal to the forest in which they are located (by the domain/sub-domain, Microsoft Exchange Server 2010 SP1 Hosted Organization, or Microsoft Exchange Server 2010 SP2 and later Address Book Policy). Specific entries also exist for general categories of mailboxes that are internal and external to the forest. If permission settings exist in a category matching the mailbox for the user, whether Deny or Allow, these settings are used to determine whether permission is granted or denied. If there is no match (Deny or Allow), the access request applies 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.

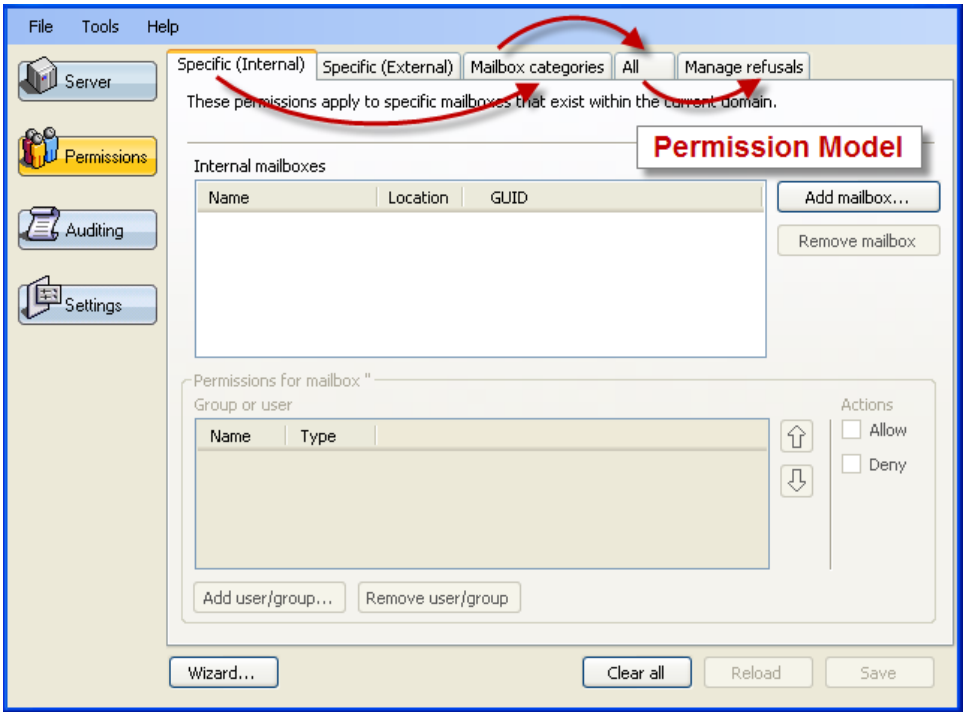


Figure 2-2: Permission Model

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 groups in the forest from top to bottom until a match is found, to determine whether access has been allowed or denied.

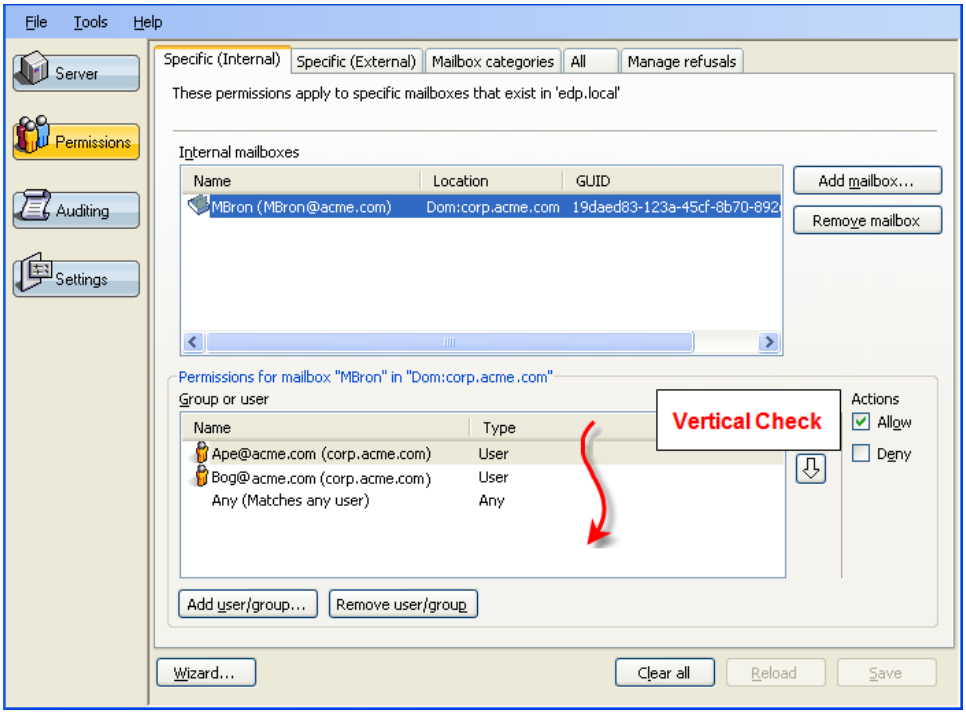


Figure 2-3: Vertical Permission Check

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. For more information, see **"Manage Refusals Tab" on page 46**.

Examples of Use

Scenario #1

The Administrator sets the "Any" user permission setting on "Deny" in the All mailboxes tab. All mailboxes are inaccessible as a result.

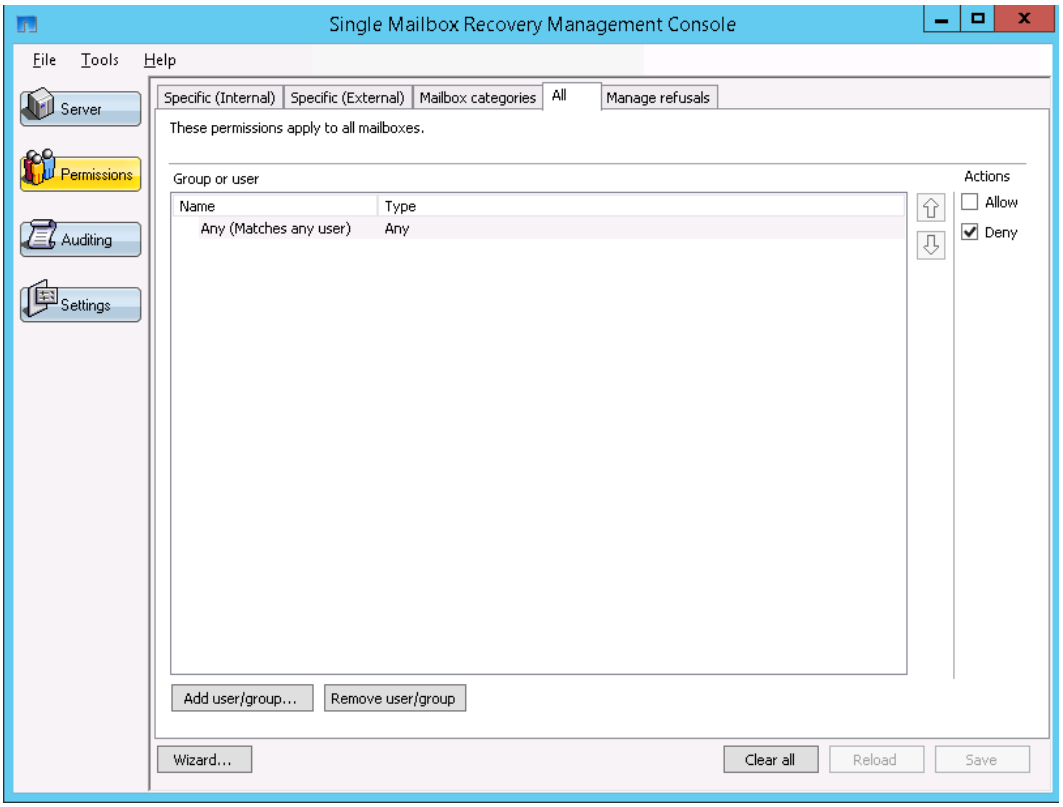


Figure 2-4: All mailboxes are made inaccessible.

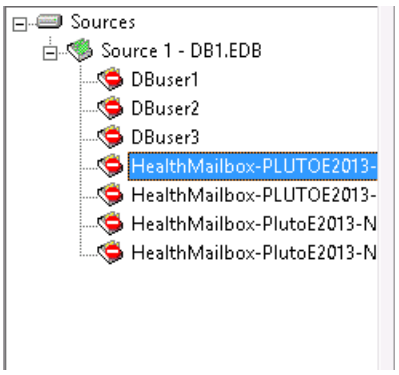


Figure 2-5: All mailboxes are inaccessible.

The Administrator needs access to the DBuser2's mailbox in an EDB file. The DBuser2 is internal to the Administrator's forest, and access should only be provided to this mailbox, while all other mailboxes remain inaccessible. He adds the DBuser2'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."

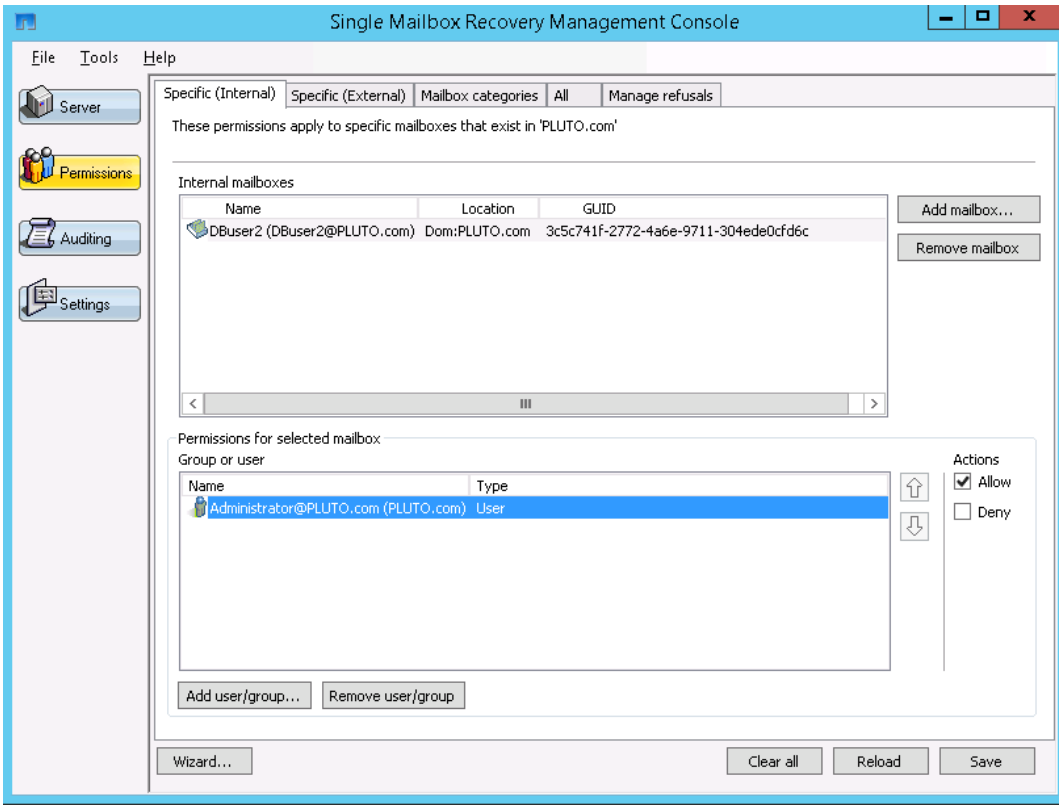


Figure 2-6: A specific internal mailbox is made accessible.

Since the DBuser2's mailbox is listed on the specific internals list and this is processed first, when the Administrator uses Single Mailbox Recovery to open the EDB containing mailboxes from within his forest, the DBuser2's mailbox is accessible while all other mailboxes are inaccessible.

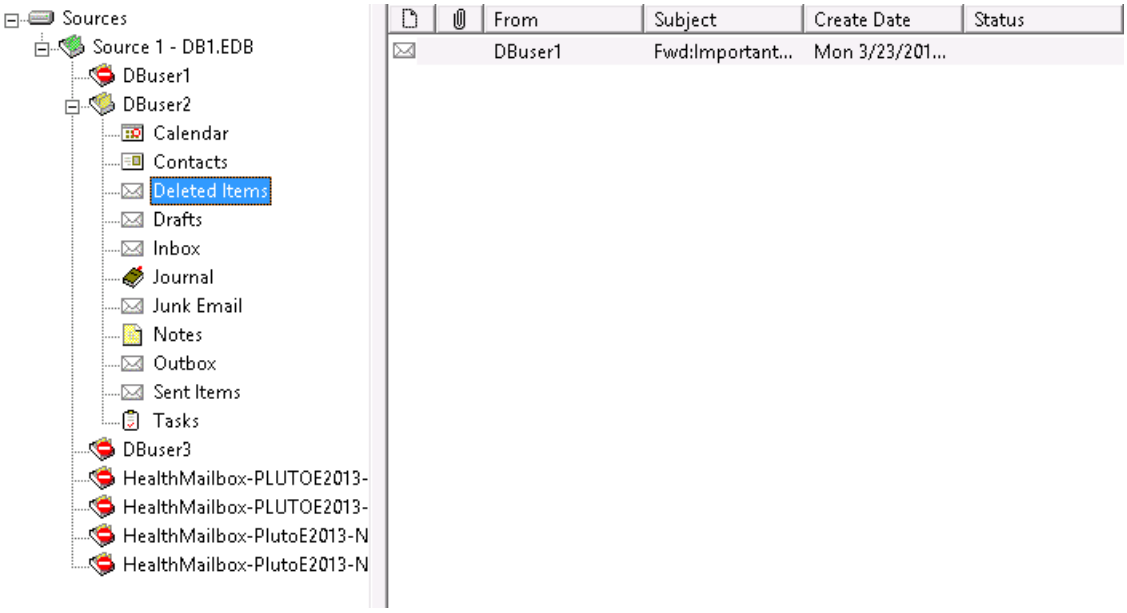


Figure 2-7: A specific internal mailbox is accessible.

Scenario #2

The Administrator runs Single Mailbox Recovery and attempts to open an EDB containing a mailbox belonging to DBuser2, an executive who is internal to the Administrator's forest. 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.

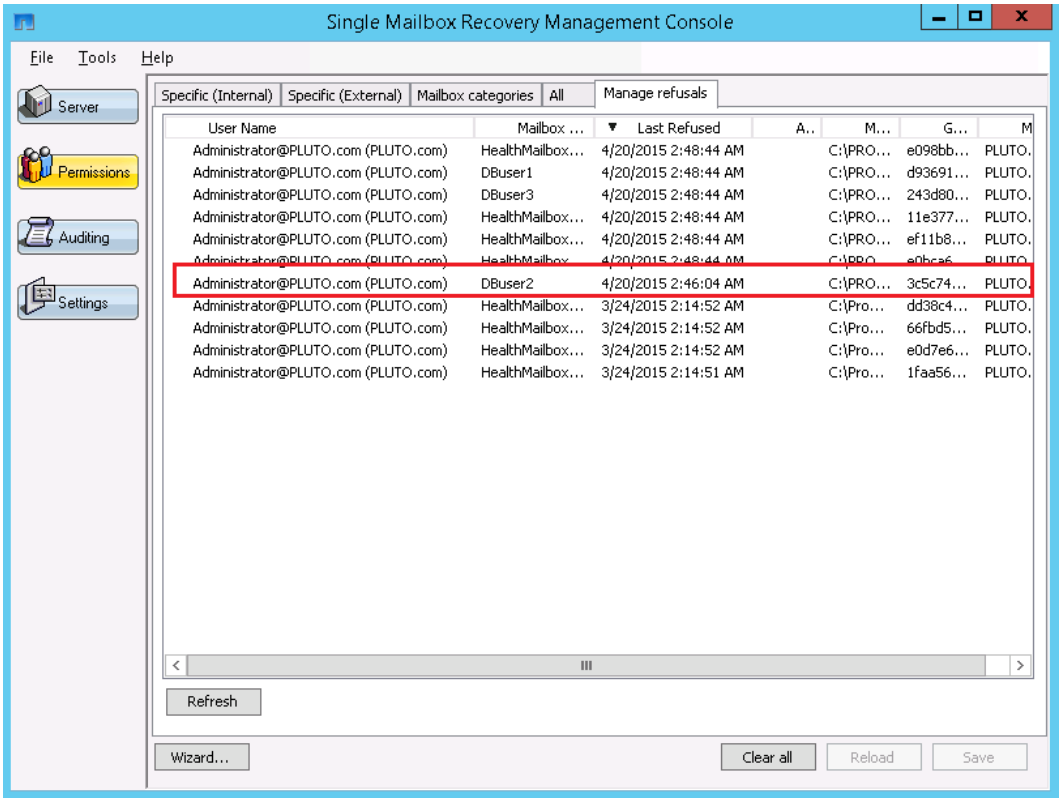


Figure 2-8: A specific internal mailbox is inaccessible.

The client using Single Mailbox Recovery is performing some transactions requiring that DBuser2's mailbox be accessible. Since the Administrator does not want access to DBuser2's mailbox to be permanent, the temporary access is set for a day. The client performs his tasks on Single Mailbox Recovery and when the time limit expires, DBuser2's mailbox automatically reverts back to being inaccessible.

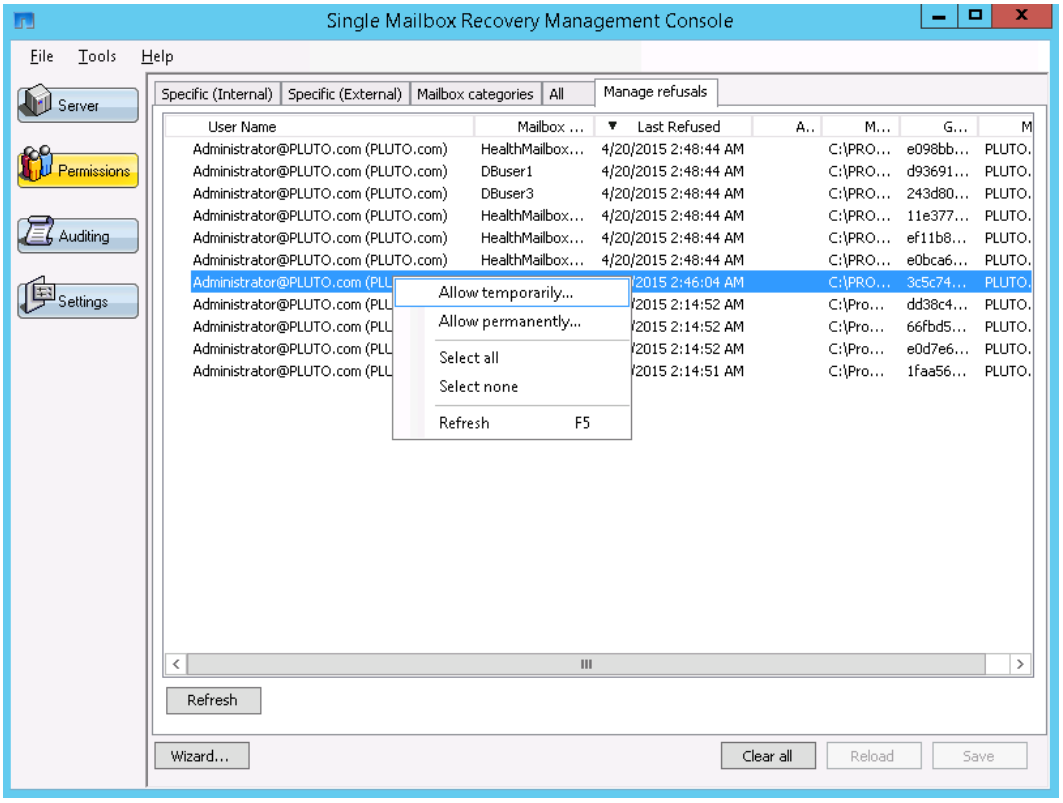


Figure 2-9: The specific internal mailbox is made accessible temporarily.

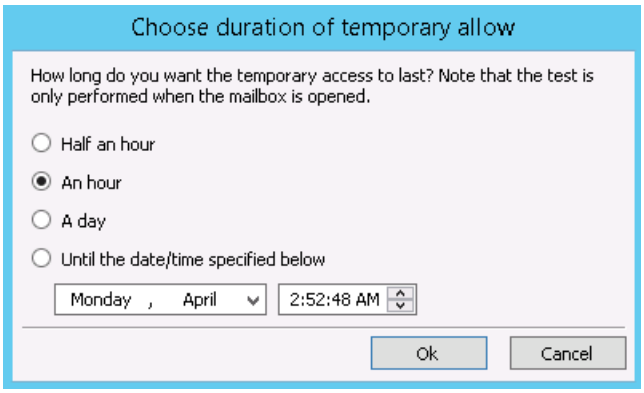


Figure 2-10: The specific internal mailbox is made accessible temporarily.

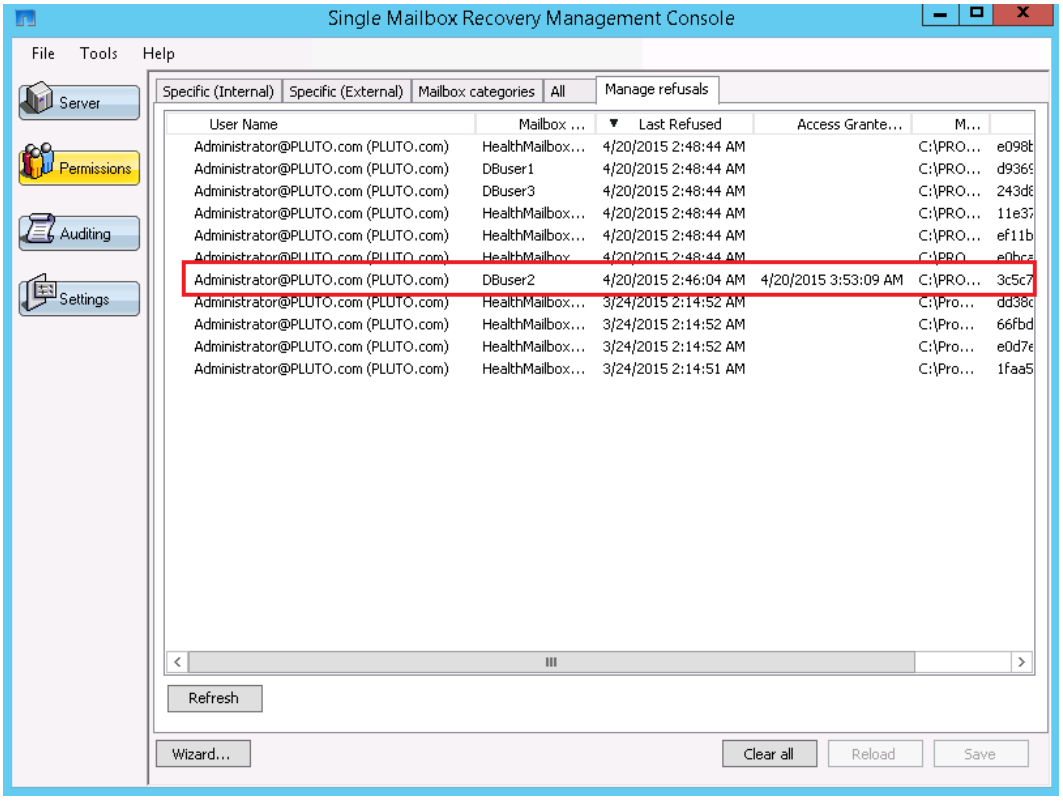


Figure 2-11: The specific internal mailbox is made accessible temporarily.

Scenario #3

The Administrator sets permissions so that he is allowed access to all internal mailboxes in the Mailbox Category tab. When he runs Single Mailbox Recovery and opens an EDB containing mailboxes from within the forest, Single Mailbox Recovery allows access to all mailboxes in this EDB. When he opens an EDB containing mailboxes from another environment, Single Mailbox Recovery denies access to all mailboxes in this EDB as they are external to the forest.

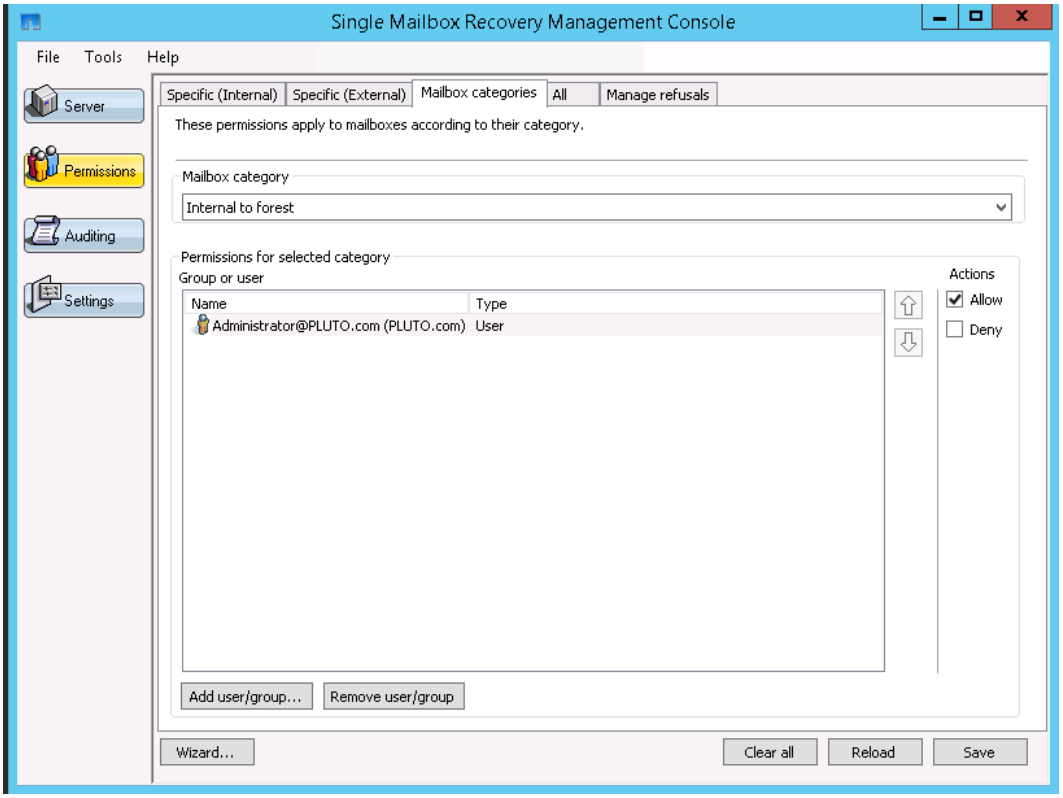


Figure 2-12: All the mailboxes internal to the forest are made accessible.

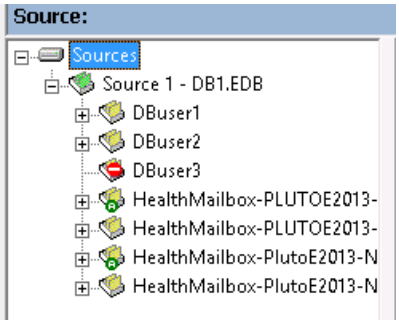


Figure 2-13: All the mailboxes internal to the forest are accessible.

Scenario #4

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 forest. The Administrator runs Single Mailbox Recovery and opens an EDB containing mailboxes from within the forest.

Single Mailbox Recovery denies access to all mailboxes in this EDB. The Administrator then opens an EDB containing mailboxes from another environment. Single Mailbox Recovery allows access to all mailboxes in this EDB as they are external to the forest.

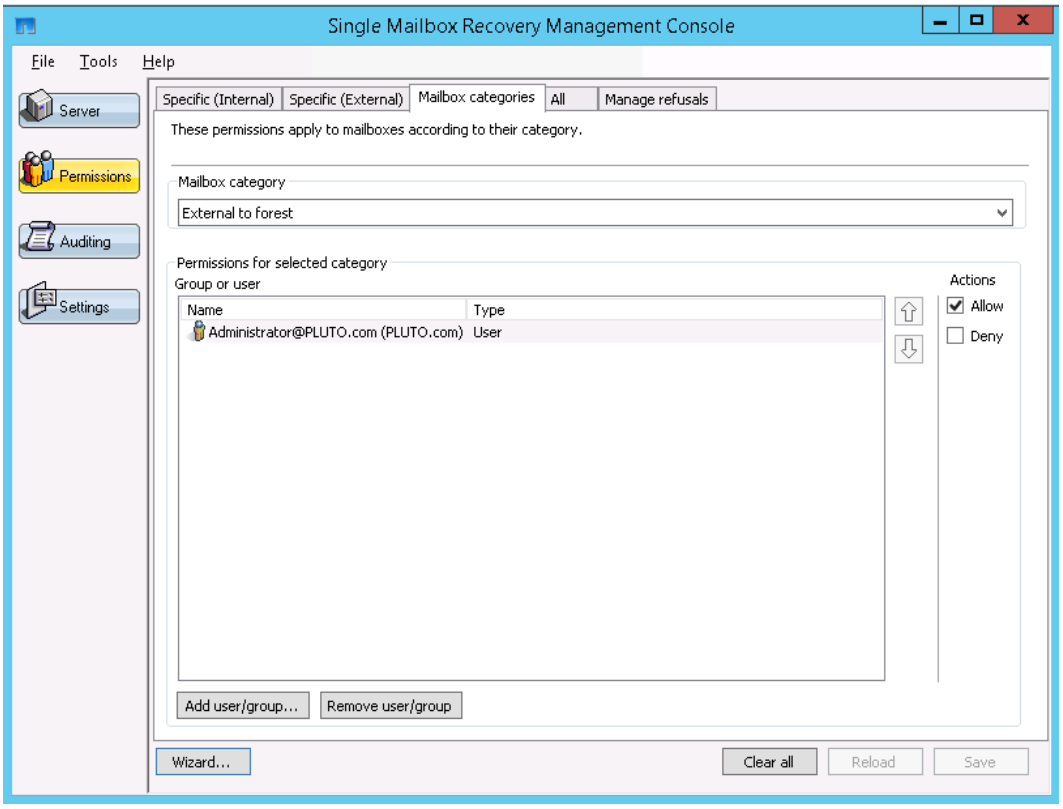


Figure 2-14: All the mailboxes that are external to the forest are made accessible.

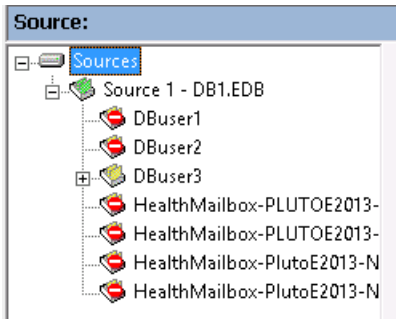


Figure 2-15: All the mailboxes that are external to the forest are accessible.

Scenario #5

The Administrator has freshly installed the Single Mailbox Recovery Administrative Server and has no mailboxes permission rules defined. As a result, all mailboxes are inaccessible. The Administrator has Address Book Policies defined for a number of different groups within his organization and has created group specific administrator users. Each group administrator should be allowed access to the mailboxes within their group. For example, 'Group Administrator ABP1' should be able to access mailboxes listed in the Global Address List (GAL) for the Address Book Policy, 'ABP1'.

On the ‘Mailbox categories’ tab, the Administrator opens the Mailbox category list, selects “Internal to ABP ‘ABP1’”and then adds the ‘Group Administrator ABP1’ user name to the users and/or group list by clicking "Add user/group..." and sets the permission to "Allow."

When the ‘Group Administrator ABP1’ user runs Single Mailbox Recovery and opens an EDB containing mailboxes from the organization as a whole, only those mailboxes that are listed in the ABP1 Address Book Policy GAL are accessible. All other mailboxes are not accessible. Since no other mailbox permissions are defined when another user runs Single Mailbox Recovery and opens the same EDB, no mailboxes can be accessed.

Scenario #6

The Administrator clears mailbox permissions. All mailboxes are inaccessible as a result. The Administrator’s environment has deployed Microsoft Exchange Server 2010 with the ‘/hosting’ switch and has a number of Microsoft Exchange Server Hosted Organizations defined. The Administrator has created hosted organization specific administrator users. Each hosted organization administrator should be allowed access to the mailboxes within their hosted organization. ‘Hosted Organization 1 Administrator’ should be able to access mailboxes from ‘Hosted Organization 1’ and ‘Hosted Organization 2 Administrator’ should be able to access mailboxes from ‘Hosted Organization 2’.

On the ‘Mailbox categories’ tab, the Administrator opens the Mailbox category list and selects “Internal to organization ‘Hosted Organization 1’”. He then adds the ‘Hosted Organization 1 Administrator’ user name to the users and/or group list by clicking "Add user/group..." and sets the permission to "Allow." He then repeats this process for ‘Hosted Organization 2’.

When the ‘Hosted Organization 1 Administrator’ user runs Single Mailbox Recovery and opens an EDB containing mailboxes from the environment as a whole, only the mailboxes from ‘Hosted Organization 1’ can be accessed. All other mailboxes are denied. When the ‘Hosted Organization 2 Administrator’ user runs Single Mailbox Recovery and opens that same EDB, only those mailboxes that are from ‘Hosted Organization 2’ can be accessed; he cannot access mailboxes from ‘Hosted Organization 1’ or anywhere else, just as ‘Hosted Organization 1 Administrator’ cannot access mailboxes from ‘Hosted Organization 2’.

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.

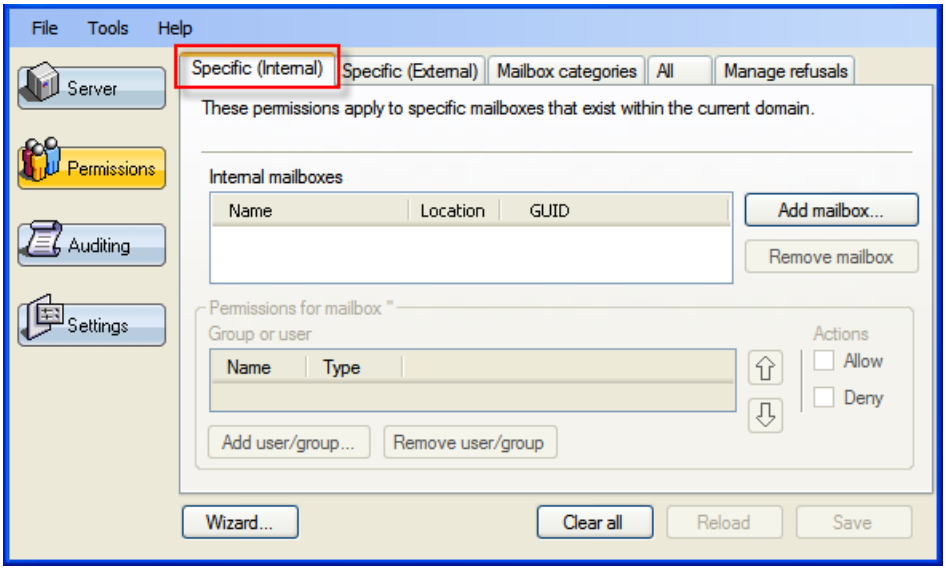


Figure 2-16: Specific (Internal) tab

Location Column

The Location column provides information relating to the location of a mailbox. This column is present in the following:

- Specific (Internal) page
- Choose Internal Mailboxes dialog box
- Manage Refusals page

The location of a mailbox is determined in order of the following criteria:

1. Address book policy (ABP) with a Global Address List (GAL) that includes the mailbox owner.
2. Hosted organization membership
3. Domain membership.

The association of an ABP takes precedence over membership of a hosted organization which takes precedence over membership of a domain.

The location column consists of a prefix and location details in the form '<Location:><Details>' as follows:

Abp: Mailbox owner is listed by the Global Address List of named address book policy or policies.

Org: Mailbox owner is a member of the named hosted organization.

Dom: Mailbox owner is a member of the named domain.

For example: 'Abp:ABP1', 'Org:HostedOrg1', 'Dom:domain.com'.

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 forest, along with their location. 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.

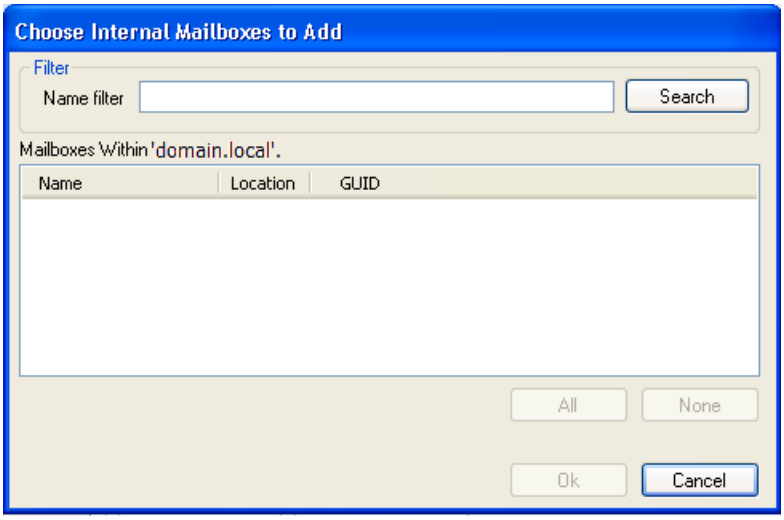


Figure 2-17: Choose Internal Mailboxes to Add

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.
   - Clear mailboxes list by clicking **None**.
5. Click **OK**. The **Internal mailboxes** list is populated with selected mailboxes.
6. 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.

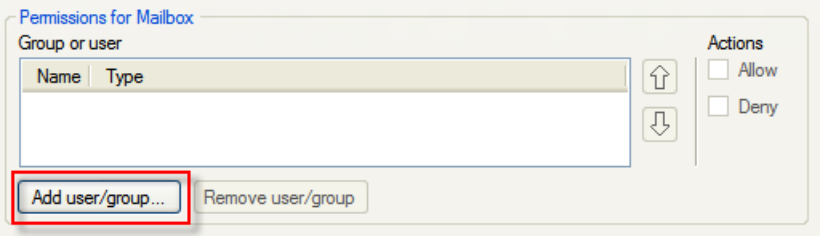


Figure 2-18: Add user/group button

To add a user or group

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

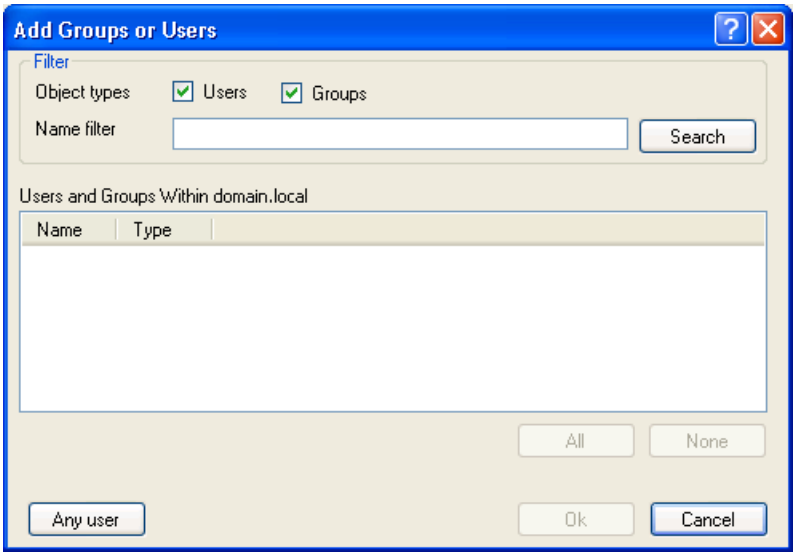


Figure 2-19: Add Groups or Users window

2. Select or clear 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.
   - Clear 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.

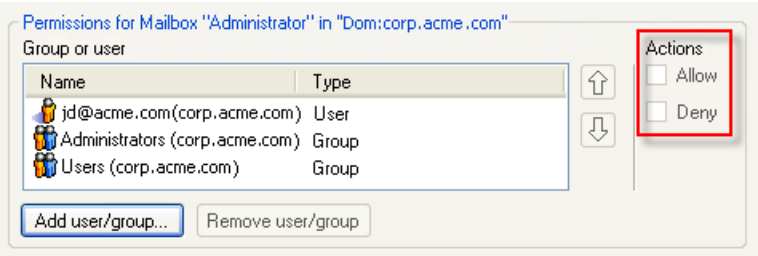


Figure 2-20: Permissions for Mailbox section

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**.

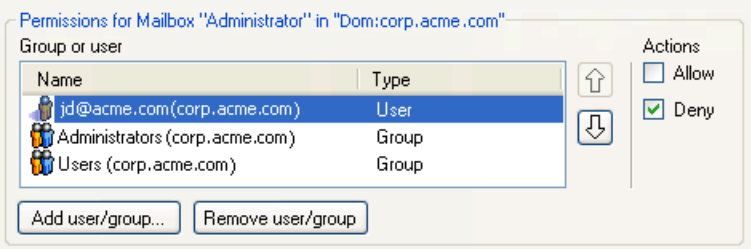


Figure 2-21: Permissions applied to group or user

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.

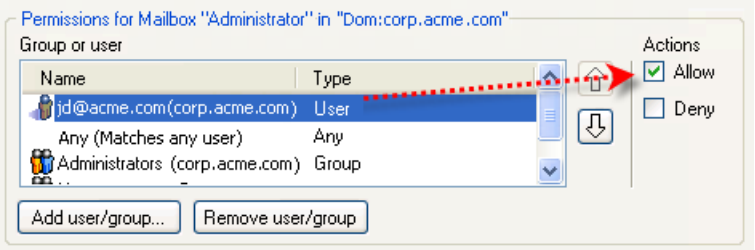


Figure 2-22: "Administrator" is listed first in Group or user box and the permission setting is "Allow."

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 the permission setting is "Allow," does not get hit since "Any" was hit first and its setting is "Deny." Therefore, any group or user, no matter what the permission setting, is denied permission to access.

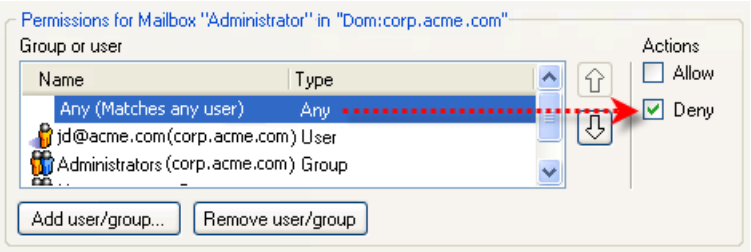


Figure 2-23: The Group "Any" has been moved to the top of the list and the permission setting is "Deny."

Specific (External) Tab

External Mailboxes are mailboxes not found within the Administrator's forest 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.

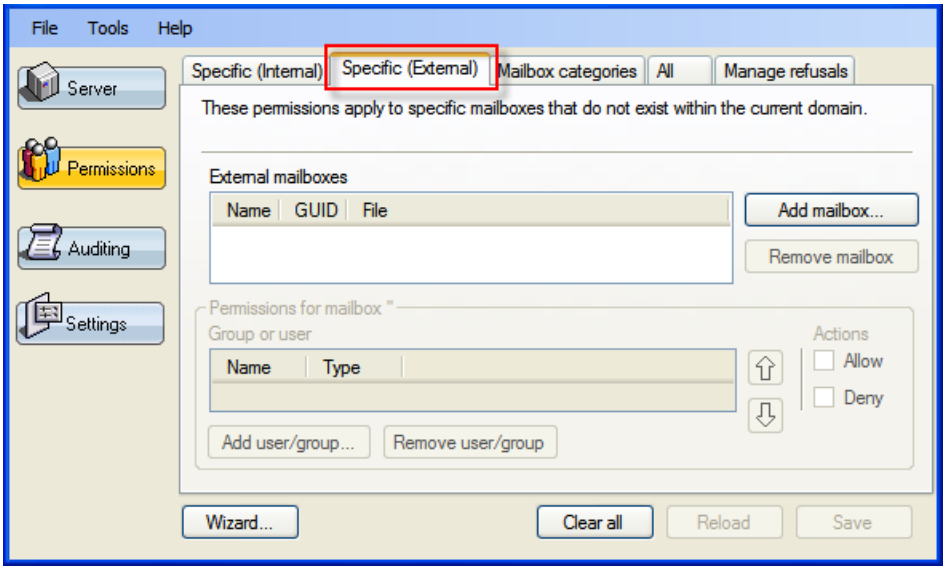


Figure 2-24: Specific (External) tab

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.

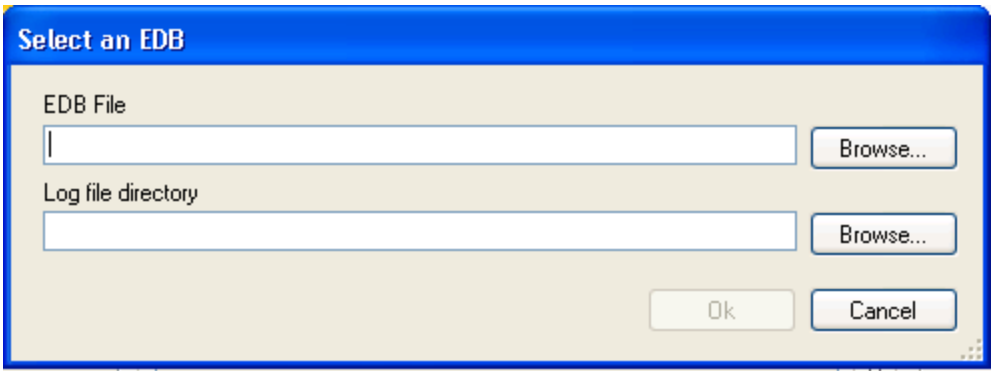


Figure 2-25: Select an EDB

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:

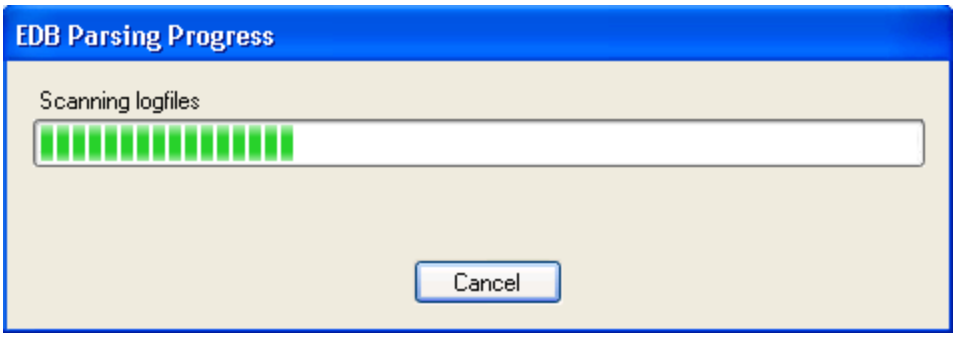


Figure 2-26: EDB Parsing Progress window

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

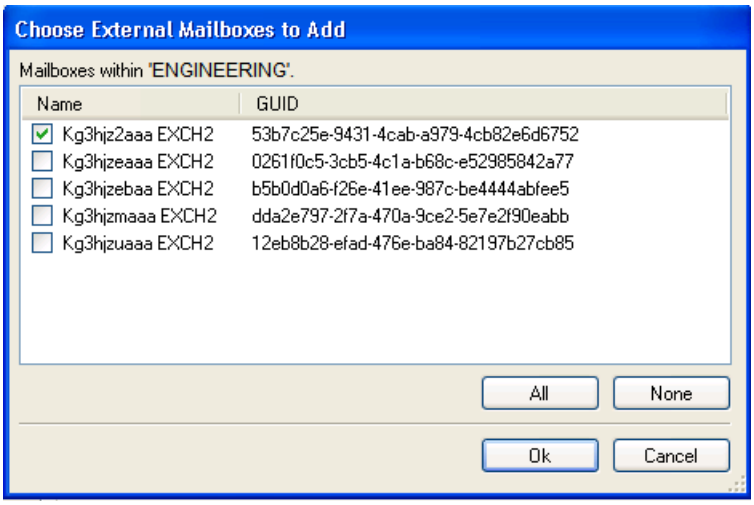


Figure 2-27: Choose External Mailboxes to Add window

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

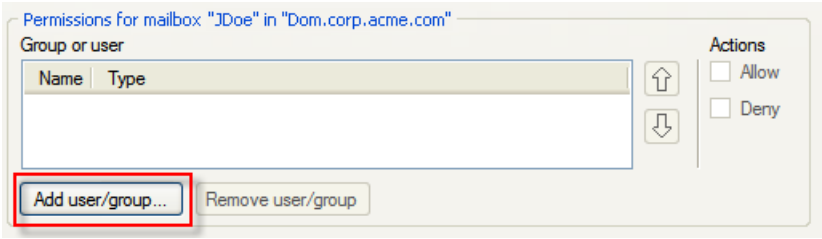


Figure 2-28: Add user/group button

To add a user or group

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

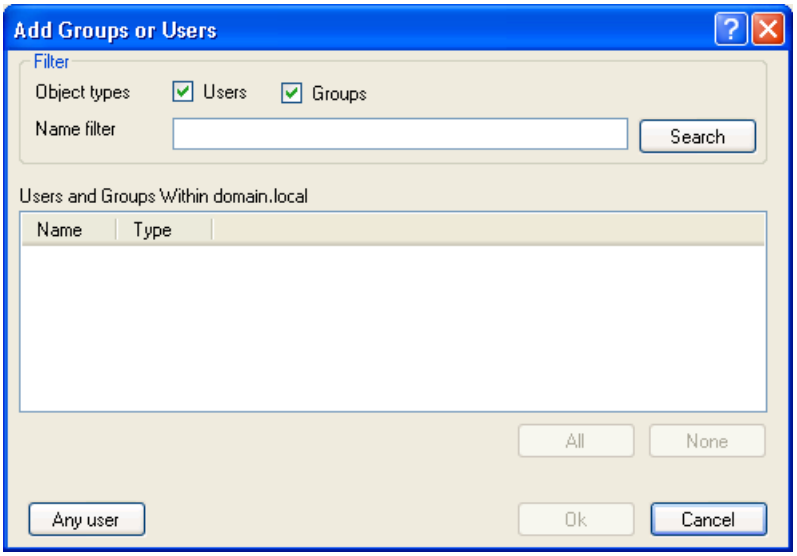


Figure 2-29: Add Groups or Users window

2. Select or clear 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.
   - Clear 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.

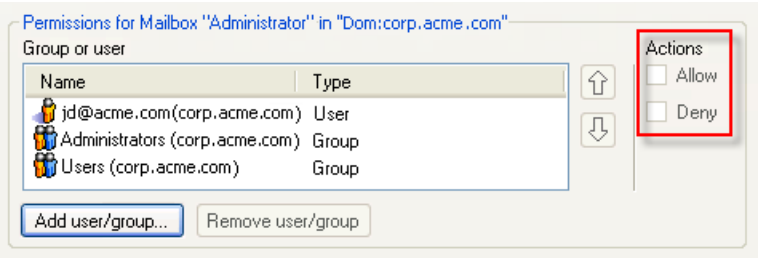


Figure 2-30: Permissions for Mailbox section

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**.

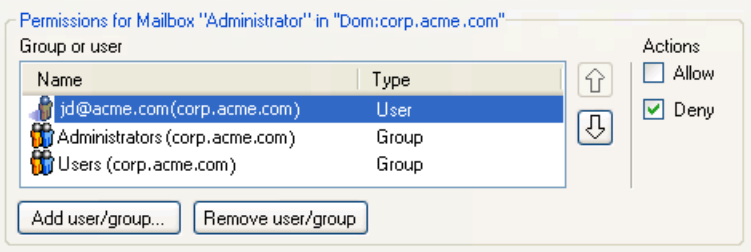


Figure 2-31: Permissions applied to group or user

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.

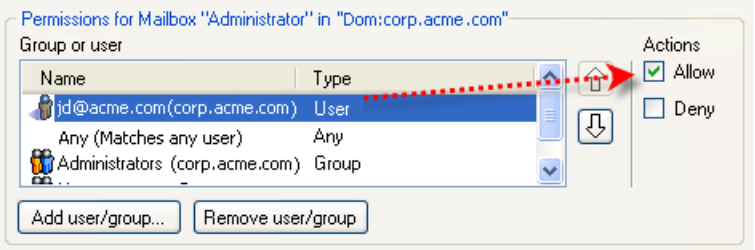


Figure 2-32: "Administrator" is listed first in Group or user box and the permission setting is "Allow."

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 the permission setting is "Allow," does not get hit since "Any" was hit first and its setting is "Deny." Therefore, any group or user, no matter what the permission setting, is denied permission to access.

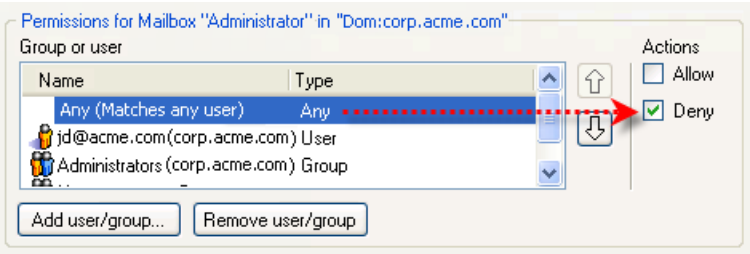


Figure 2-33: The Group "Any" has been moved to the top of the list and the permission setting is "Deny."

Mailbox Categories Tab

Using the Mailbox Categories tab, you can set permissions to mailboxes categorized by their location. For more information about locations, see **"Location Column" on page 27**.

The mailbox categories available in a specific environment are dependent on the configuration and deployed features in that environment. Operation in a multi-domain forest or when multi-tenant features like Address Book Policies and Exchange Hosted Organizations are in use will affect the categories listed.

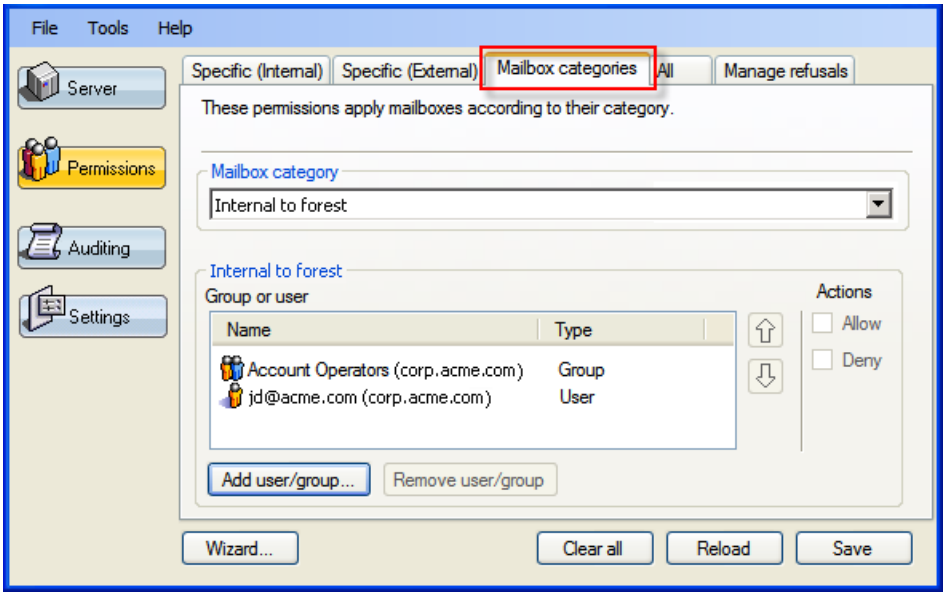


Figure 2-34: Mailbox categories tab

Setting the Mailbox Category

Select the Mailbox Category to which you want the permission to apply from the following:

- **Internal to ABP 'xxx':** Referenced by this specific Address Book Policy Global Address List.
- **Internal to any ABP:** Referenced by any Address Book Policy Global Address List.
- **Internal to organization 'xxx':** Member of a specific Microsoft Exchange Server hosted organization.
- **Internal to any organization:** Member of any Microsoft Exchange Server hosted organization.
- **Internal to domain 'xxx' but not configured in an ABP or organization:** Member of a specific domain, but not referenced by an Address Book Policy Global Address List or member of a Microsoft Exchange Server hosted organization.
- **Internal to forest but not configured in an ABP or organization:** Member of any domain in the forest, but not referenced by an Address Book Policy Global Address List or member of a Microsoft Exchange Server hosted organization.
- **Internal to forest:** Member of any domain in the forest.
- **External to forest:** Member of a domain outside the forest.

Adding and Removing a User or Group

You can add a new group or user to the Group or user box to the selected category.

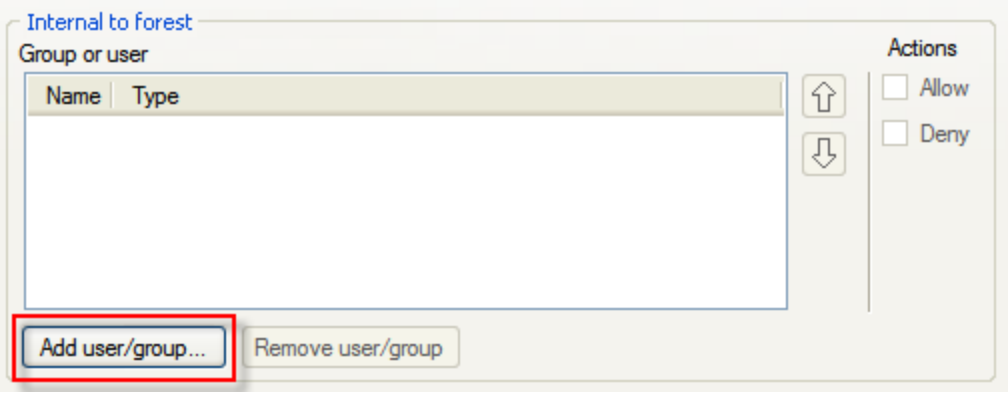


Figure 2-35: Add user/group button

To add a user or group

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

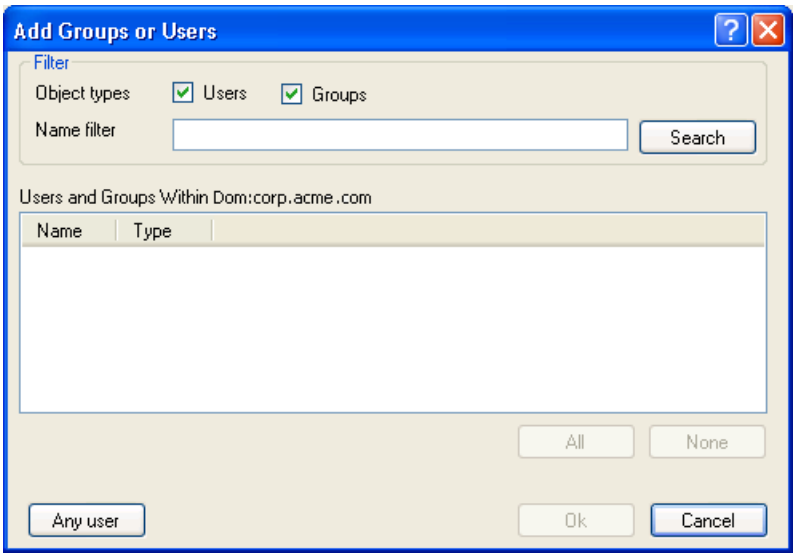


Figure 2-36: Add Groups or Users window

2. Select or clear 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.
   - Clear 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**.

A note on user and group naming and identification

In common with all controls within the Mailbox Permissions service that list users and groups information is displayed in a standardized form designed to disambiguate.

Users are identified by their User Principal Name (UPN) followed by additional information in parenthesis. The UPN is used to disambiguate and ensure the user can be uniquely identified. In parenthesis following the user name additional information is provided as follows:

- '<UPN> (<domain.name,<Loc:><LocationName>)' – where
  - <UPN> is the User Principal Name (e.g. user@domain.com)
  - <domain.name> is the domain where the user is defined (e.g. domain.com).
  - <Loc:><LocationName> can be:
    - Org:<Exchange Hosted Org Name>
    - Abp:<Assigned ABP>
  - e.g. john.doe@company.com (corp.company.com)
  - e.g. administrator@org1.com (hosted.local,Org:org1)
  - e.g. administrator@domain.local (domain.local,Abp:Abp_1)

Groups are identified by their name followed by additional information in parenthesis. The additional information is used to disambiguate and ensure the group can be uniquely identified. In parenthesis following the user name additional information is provided as follows:

- '<Group name> (<info>)'
  - <Group name> is the name of group.
  - Where <info> can be:
    - The domain where the user is defined (e.g. domain.com).
    - 'Well known SID' – In multi-domain environments this is shown when the group is an inbuilt security group identified by a well-known SID. Each domain will likely

have its own instance of a well-known group so Single Mailbox Recovery Administrative Server aggregates them into a single object to avoid confusion.

- The special 'Any' group provided to match any user will display as 'Any (Matches any user)'

- e.g. Administrators (corp.company.com)
- e.g. Account Operators (Well known SID)
- e.g. Any (Matches any user)

Note: *If permissions are set for a user or group and that user or group is later deleted it will no longer be recognized. In this scenario the user/group name will be: '<user/group name> (Ext:)'.*

Setting Permissions for Mailboxes Matching the Selected Category

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.

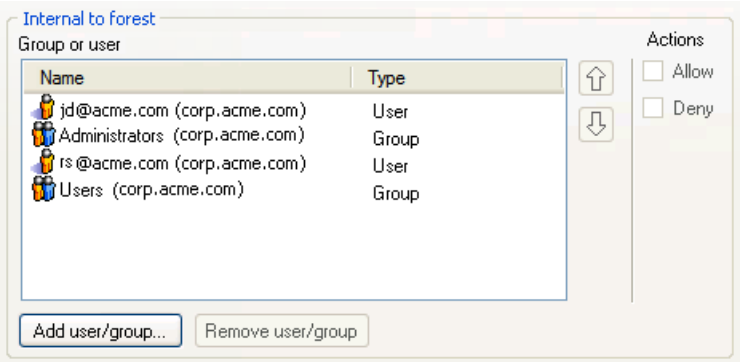


Figure 2-37: Permission for the category "Internal to forest" (any mailbox that is a member of any domain in the forest)

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**.

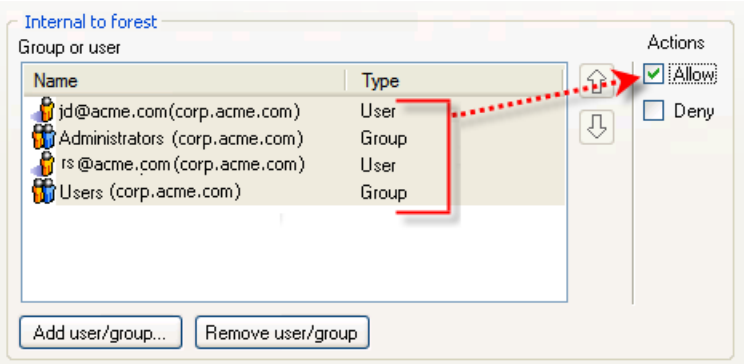


Figure 2-38: Permissions applied to group or user

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.

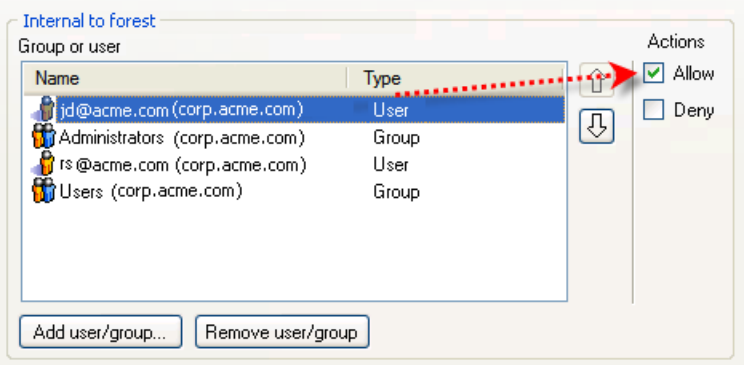


Figure 2-39: The "Administrator" user is at the top of the list and the Action is set to "Allow" permission.

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 the permission setting is "Allow," does not get hit since "Any" was hit first and its setting is "Deny." Therefore, any group or user, no matter what the permission setting, is denied permission to access.

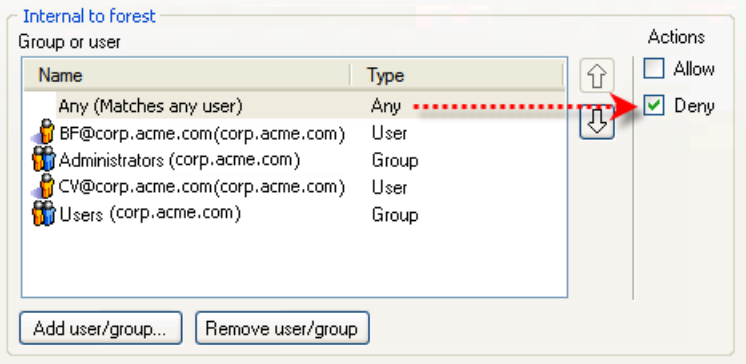


Figure 2-40: The Group "Any" has been moved to the top of the list and the Action is set to "Deny" permission.

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).

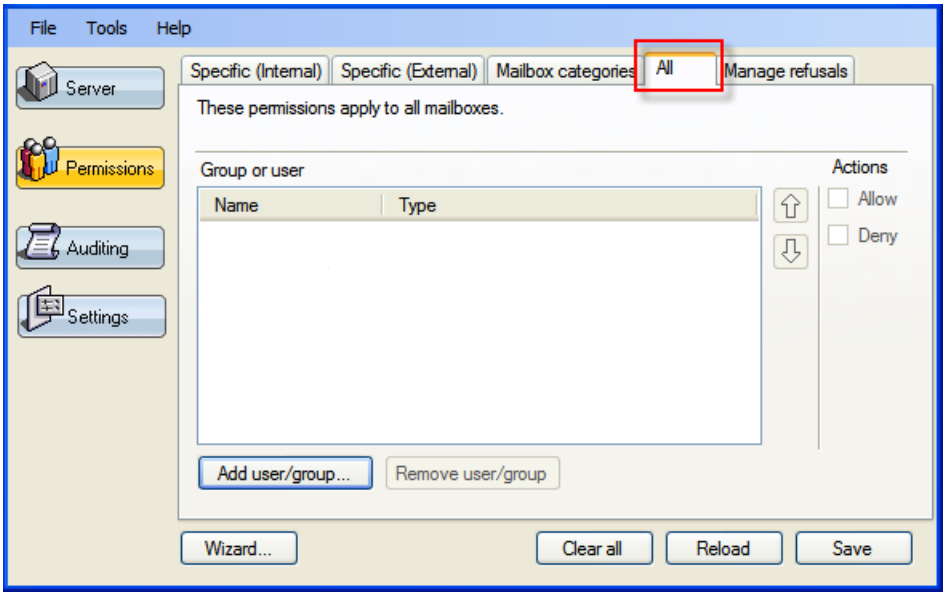


Figure 2-41: All mailboxes tab

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.

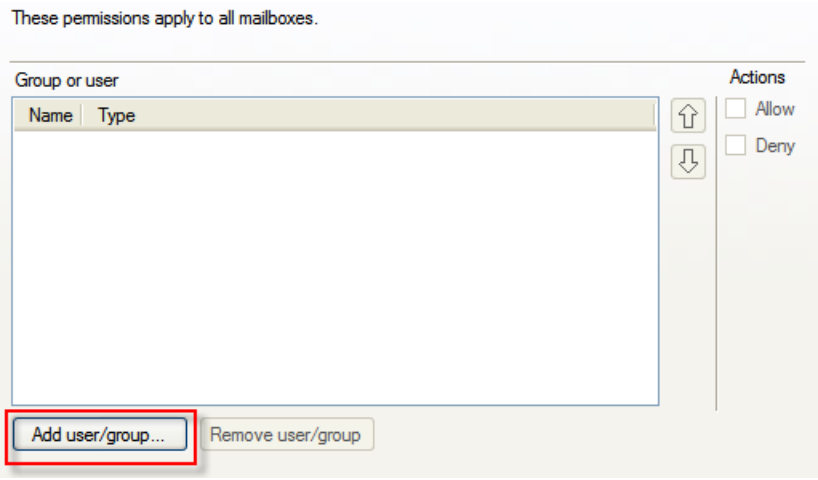


Figure 2-42: Add user/group button

To add a user or group

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

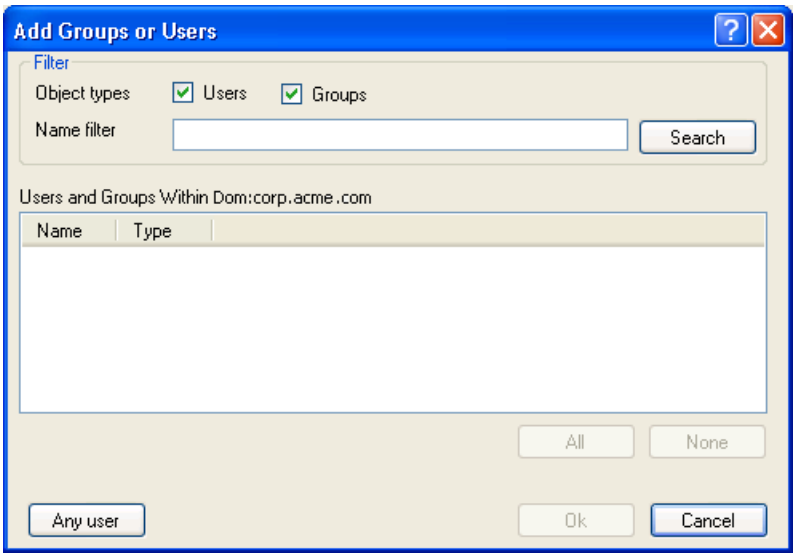


Figure 2-43: Add Groups or Users window

2. Select or clear 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.

- Clear 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.

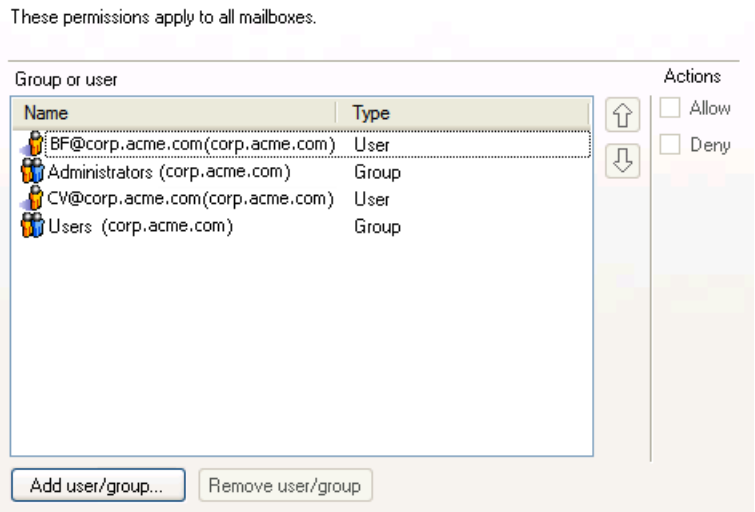


Figure 2-44: Group or user box

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**.

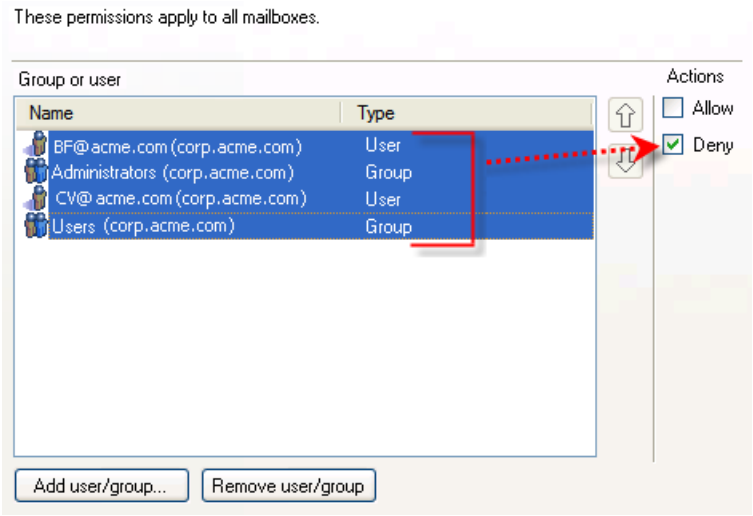


Figure 2-45: Permissions applied to group or user

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.

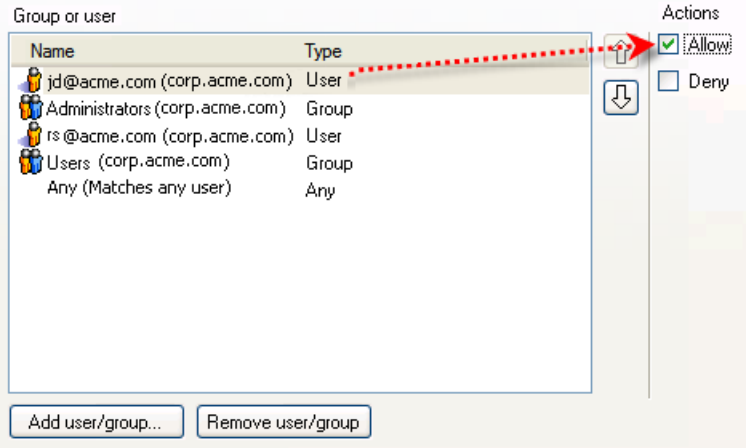


Figure 2-46: The "Administrator" is at the top of the list and the Action is set to "Allow" permission.

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 the permission setting is "Allow," does not get hit since "Any" was hit first and its setting is "Deny." Therefore, any group or user, no matter what the permission setting, is denied permission to access.

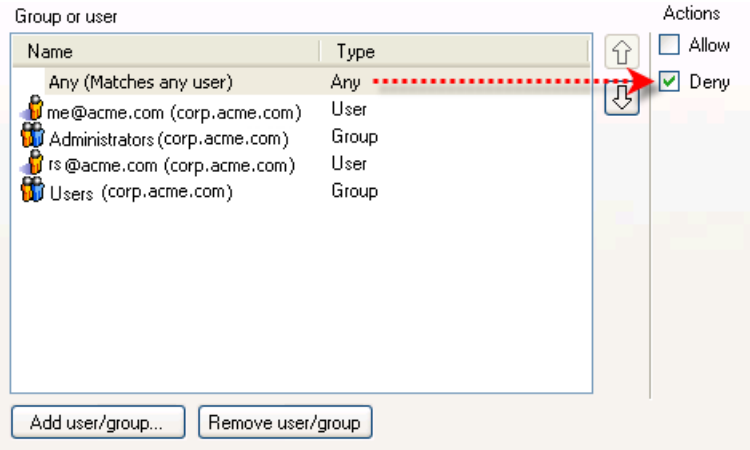


Figure 2-47: The Group "Any" has been moved to the top of the list and the Action is set to "Deny" permission.

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.

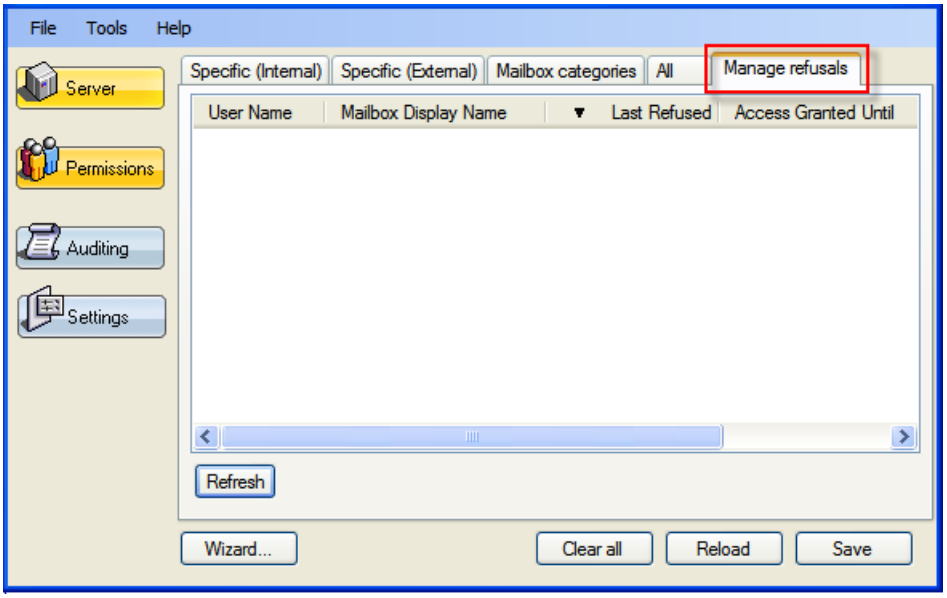


Figure 2-48: Manage refusals tab

The Manage refusals tab displays 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.
- **Mailbox Location:** The location of the mailbox. For more information, see **"Location Column" on page 27**.

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**.

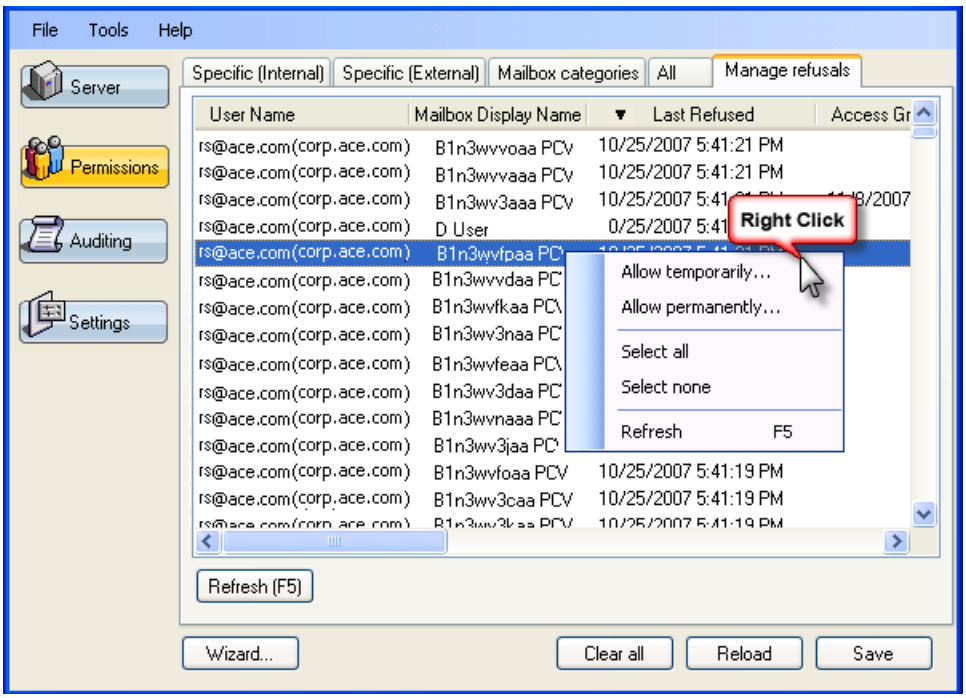


Figure 2-49: Right-click the mailbox to give temporary or permanent permission

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

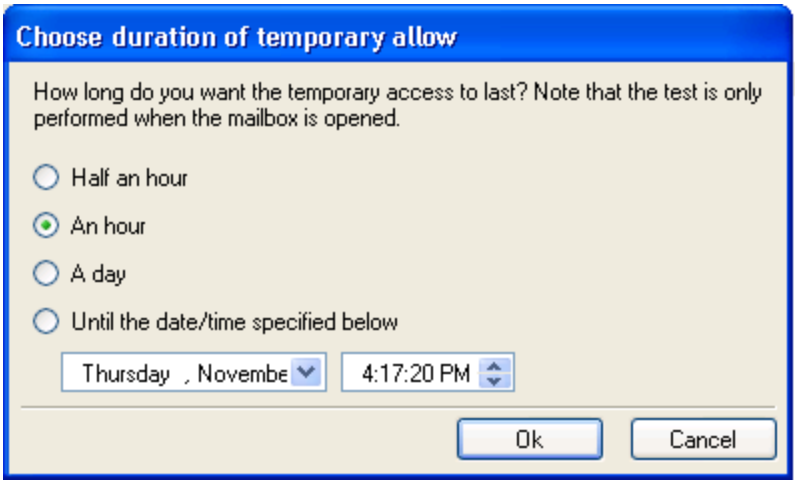


Figure 2-50: Choose the duration of temporary refusal allow

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.

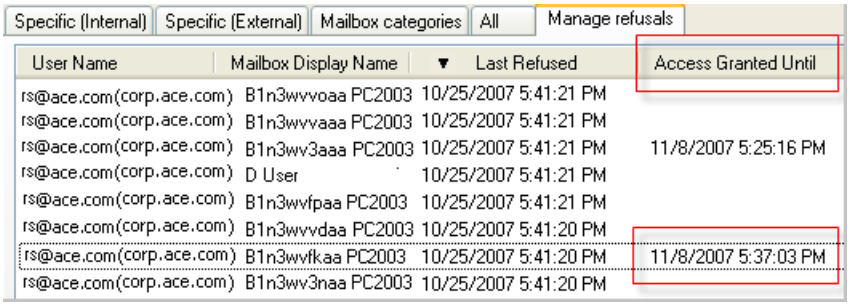


Figure 2-51: The Temporarily Allow date and time appears in the Access Granted Until column

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 plugin 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.

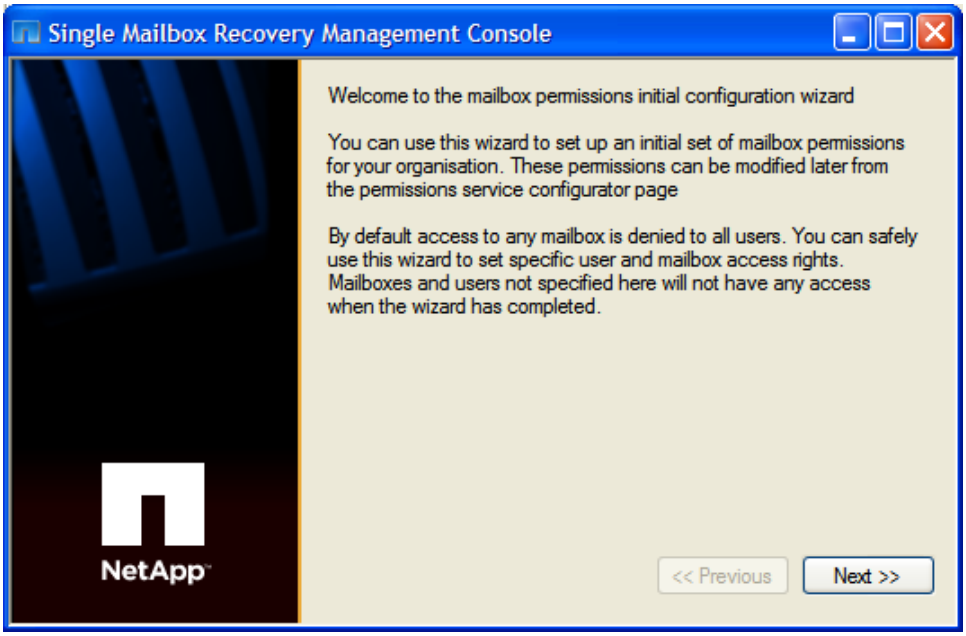


Figure 2-52: Welcome page

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

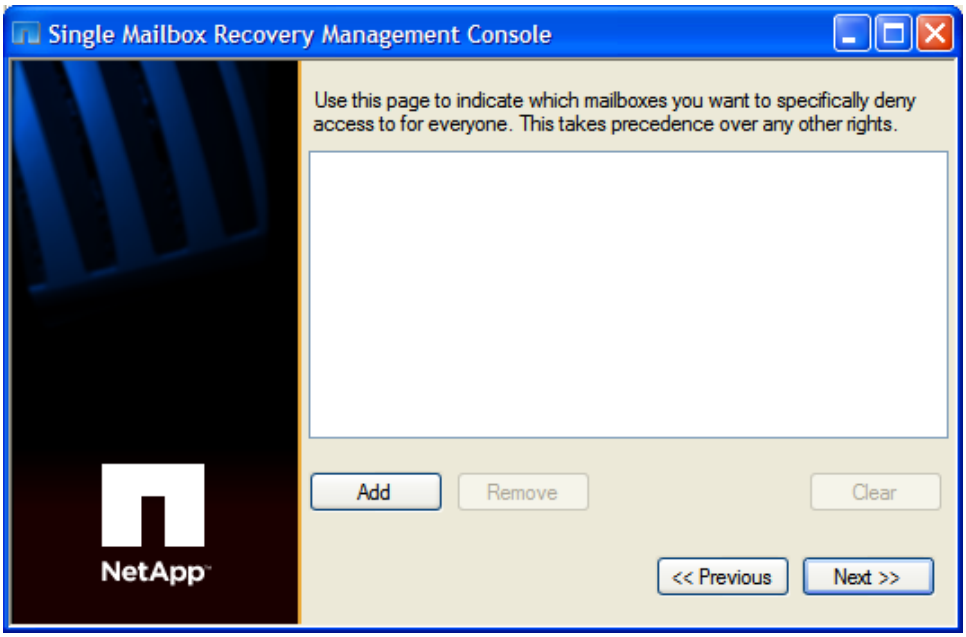


Figure 2-53: Deny access for everyone

Note: *This page of the wizard can offer protection to mailboxes the Administrator does not want anyone to access. The Administrator should ensure any sensitive or important mailboxes are listed here. For example, the CEO's mailbox in Example #1 at* ***"Examples of Use" on page 18****.*

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

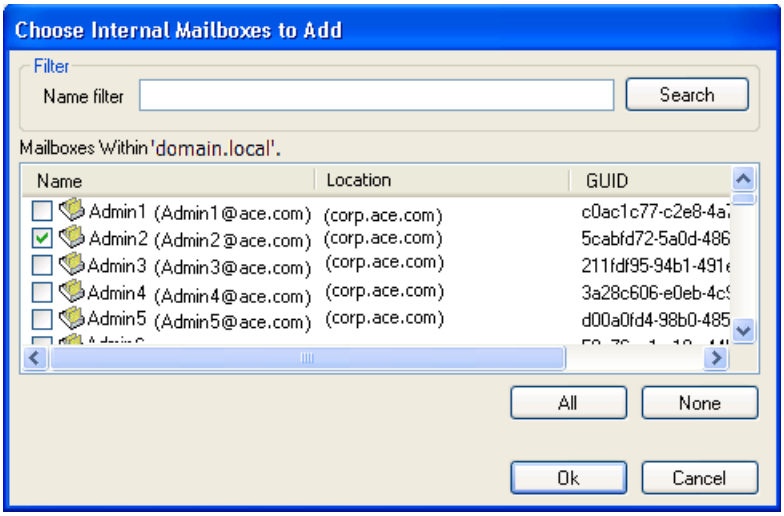


Figure 2-54: Choose Internal Mailboxes

4. Enter a **Name filter** to narrow down the list and click **Search**.
5. In the populated list, do one of the following:
   - Click **All** to select the whole list of mailboxes.

- Select mailboxes individually.
- Clear mailbox list by clicking **None**.

6. Click **OK**.
   - Use the **Remove** option to delete any mailboxes from the list.
   - Click **Clear** to delete the entire list from the page.
7. Click **Next**. The add access to internal mailboxes page of the wizard appears.

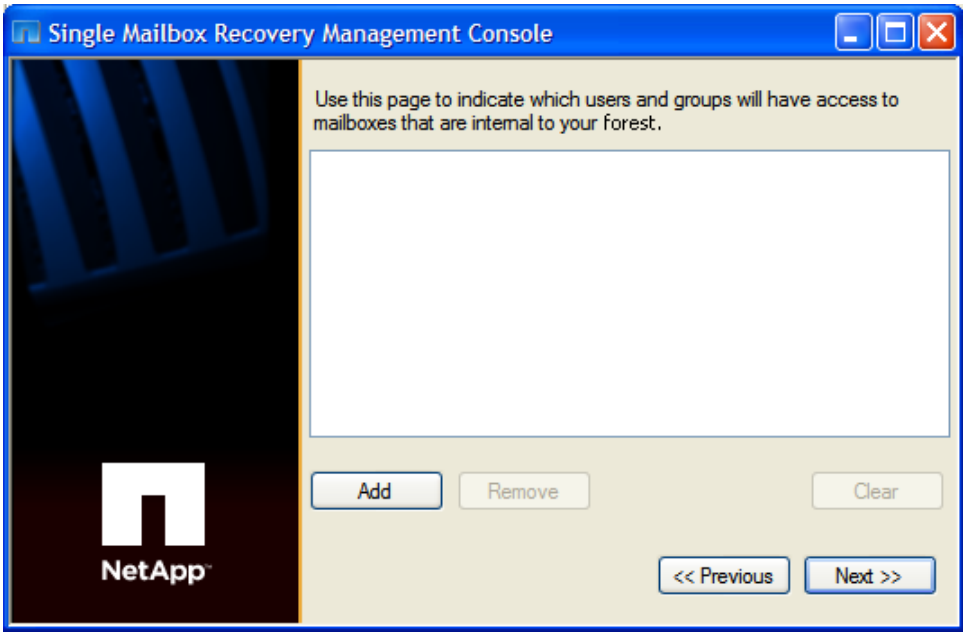


Figure 2-55: Access to internal mailboxes

Note: *This page of the wizard is there to allow access to any other mailboxes in the forest, 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 forest. The Administrator should ensure only those users or groups specifically authorized to use Single Mailbox Recovery 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 forest. The **Add Groups or Users** window appears.

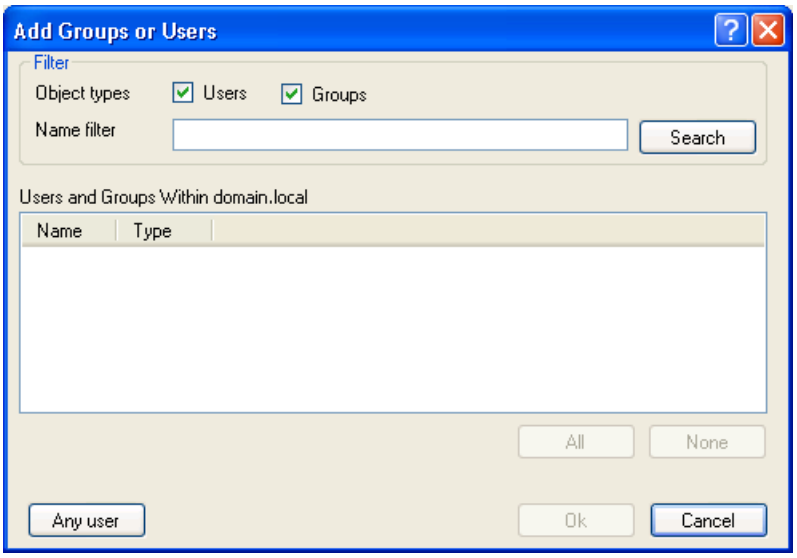


Figure 2-56: Add Groups or Users

9. Select or clear 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.
    - Clear 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.

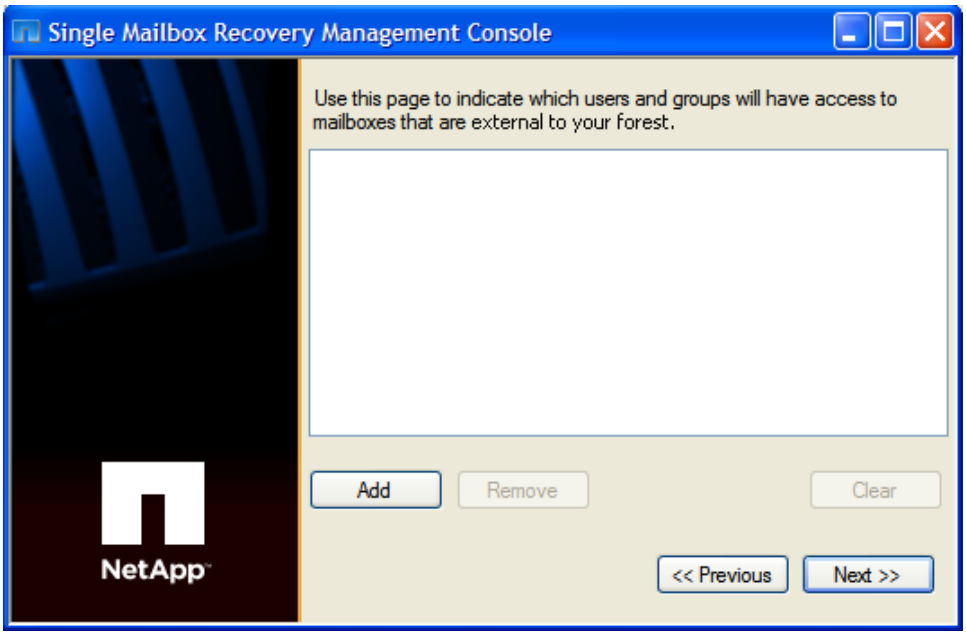


Figure 2-57: Access to external mailboxes

Important: *This page of the wizard allows access to any mailboxes external to the forest 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 forest may still be internal to the organization as a whole. Carefully select users you want to have access to mailboxes external to your forest. 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 forest. The **Add Groups or Users** window appears.

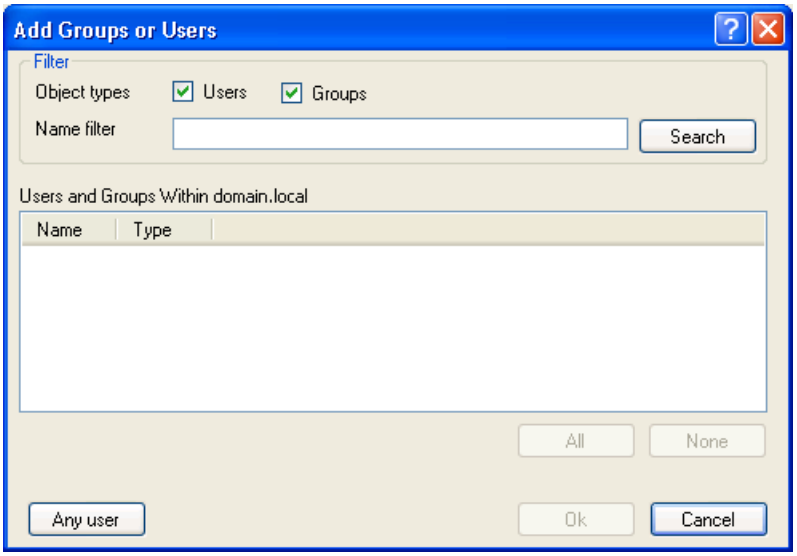


Figure 2-58: Add Groups or Users

15. Select or clear 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.
    - Clear 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.

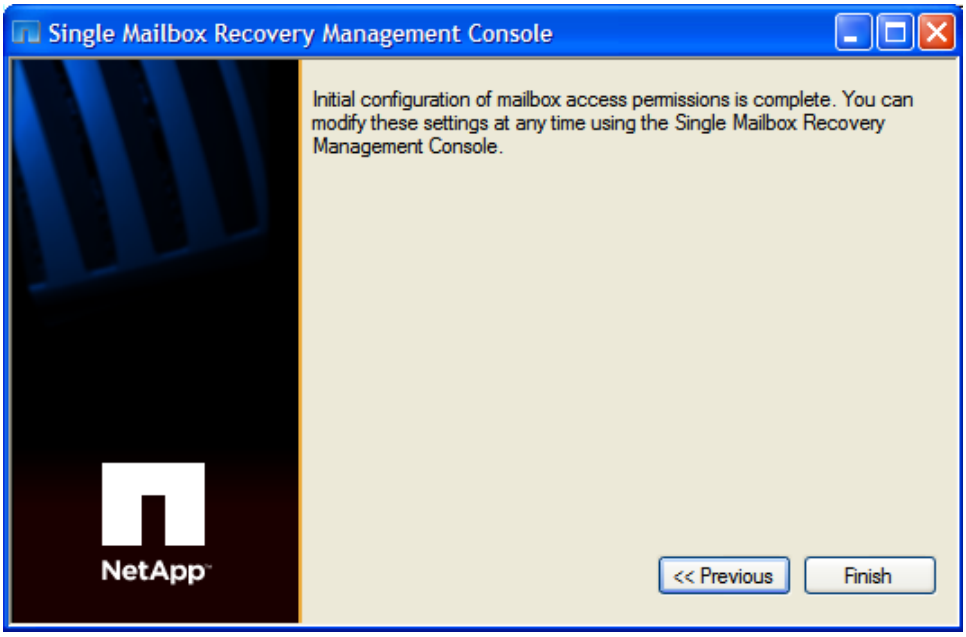


Figure 2-59: Mailbox Access Permissions complete

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.*

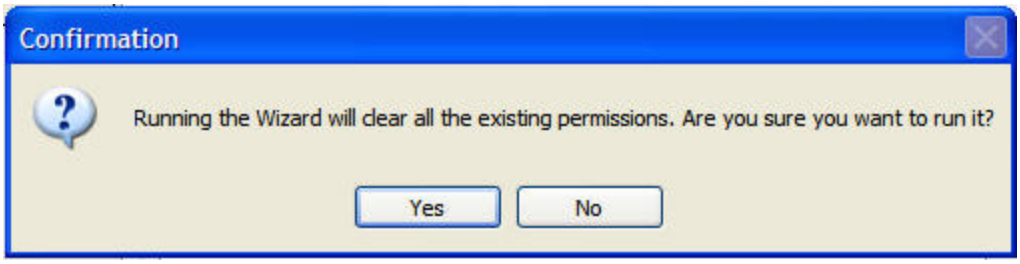


Figure 2-60: Confirmation message to clear all existing permission settings.

Terminate

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

Chapter 3: Application Auditing Service

Overview

The Application Auditing Service is a service plugin 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 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 and 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 and Single Mailbox Recovery ExtractWizard, the types of activities logged are those initiated from the user interface, command line interface, and Data Wizard.

See **"Activities to be Logged" on page 71** 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 **"Activities to be Logged" on page 71** for a list of Server-Side activities that are logged.

Audit Service First Run Configuration

When the audit service plugin 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. For more information, see **"Configuration Tab" on page 63**.

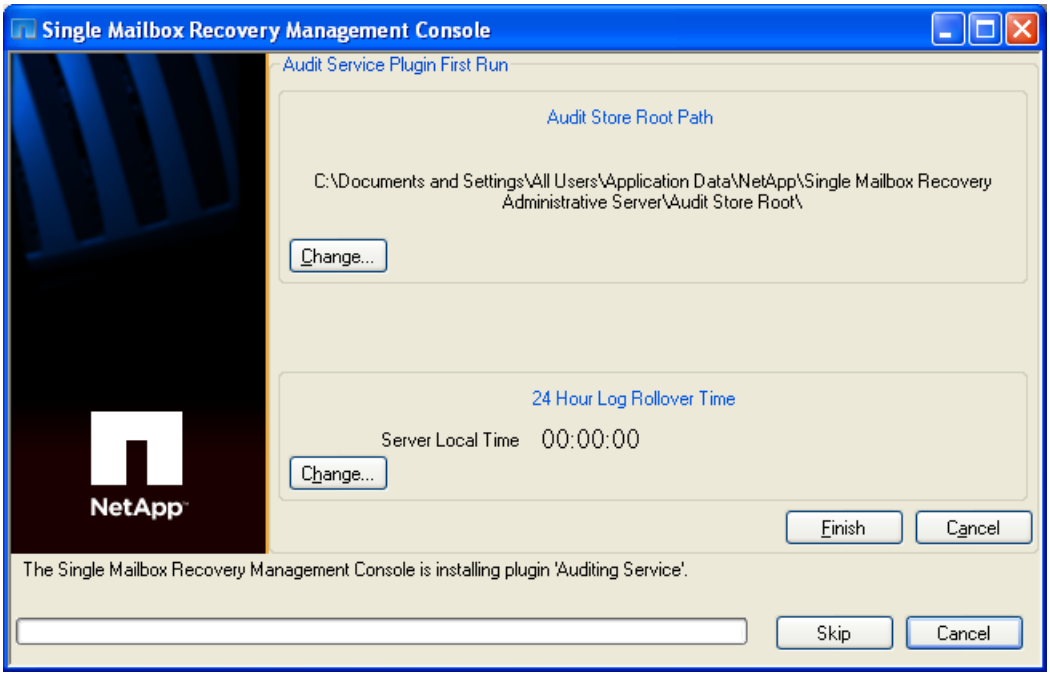


Figure 3-1: Audit Service First Run

Skip Button

The "Skip" button can be used to skip finalization of the current plugin. If a plugin'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 plugins can be activated using the Plug-in Activation command on the Tools menu item at any time after finalization.

Advertising on Active Directory

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

Figure 3-2: Active Directory Advertising message

For more information, see **"Server Operation" on page 10**.

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.

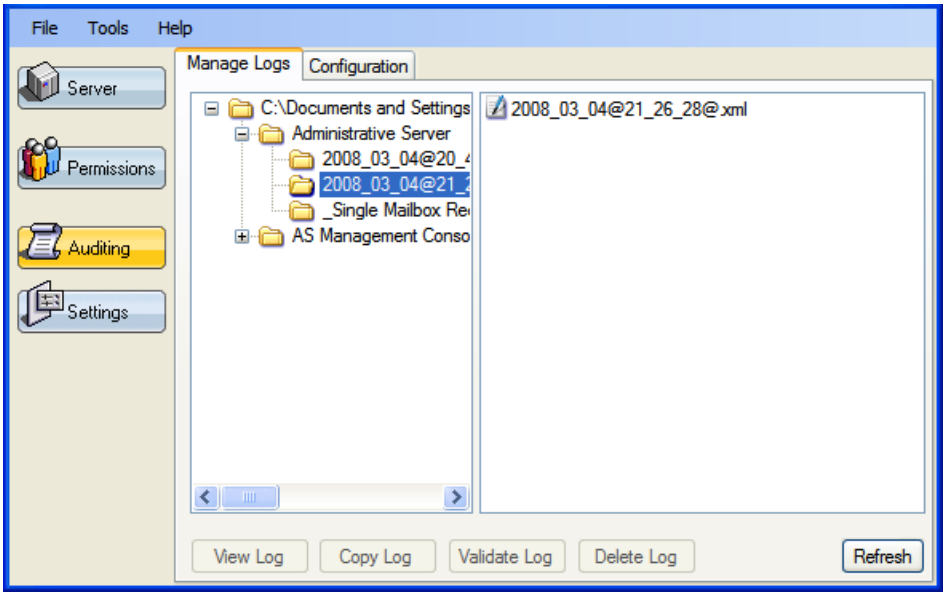


Figure 3-3: Manage Logs tab

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

Note: *A session log's folder name is determined by using client application name (e.g. Single Mailbox Recovery) 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).

- **User Name:** Name of the user logged in and running the application. The user name is the Unique Principal Name (UPN) of the user with the domain name in parenthesis; for example, user.name@location.com (domain.local).
- **Machine Name:** The network name for the computer.
- **Session Start Time:** Start of the Single Mailbox Recovery Administrative Server Audit Session for that application.
- **Session End Time:** End of the Single Mailbox Recovery Administrative Server 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 **"Activities to be Logged" on page 71**.
- **Transaction Id:** Sequential number assigned to the transactional activity. A Transactional Id of "0" indicates a stand alone activity.
- **Parameter Name:** The type 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

Show Summary Report

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 -

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	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.

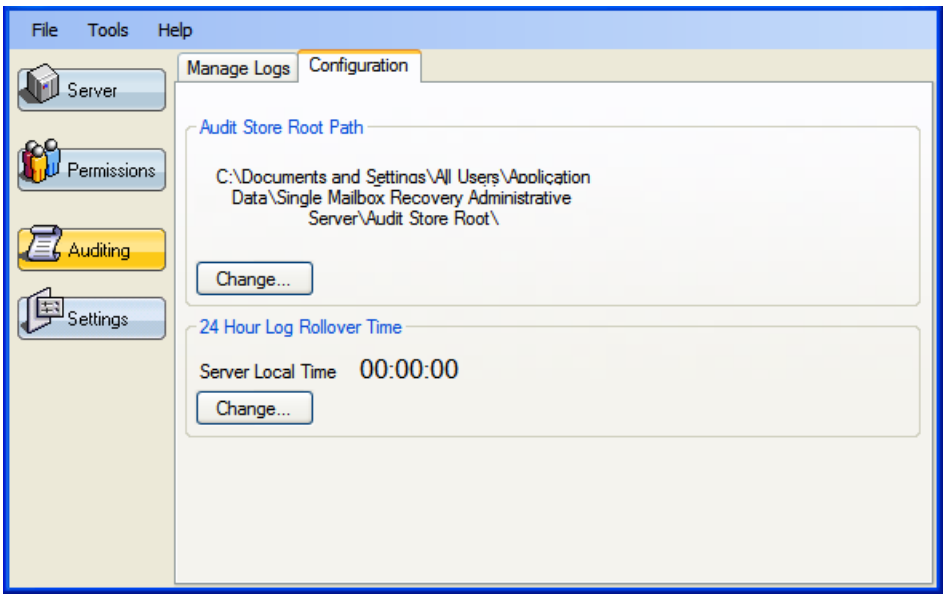


Figure 3-9: Configuration tab

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.

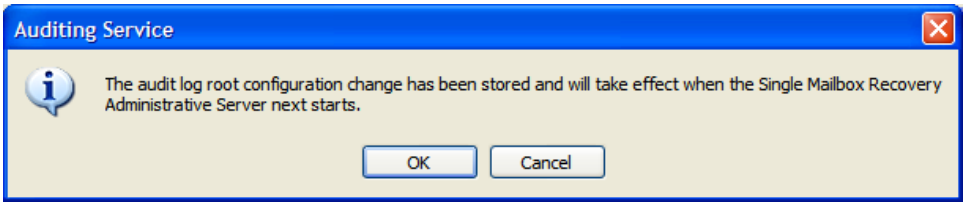


Figure 3-11: Change audit service store root confirmation

3. Click **OK**. The **Audit Store Root Path** change takes effect the next time the server is restarted. This can be achieved using the Restart button on the Server configuration page. For more information, see **"Server Operation" on page 10**.

   Until the server is restarted, a warning message appears.

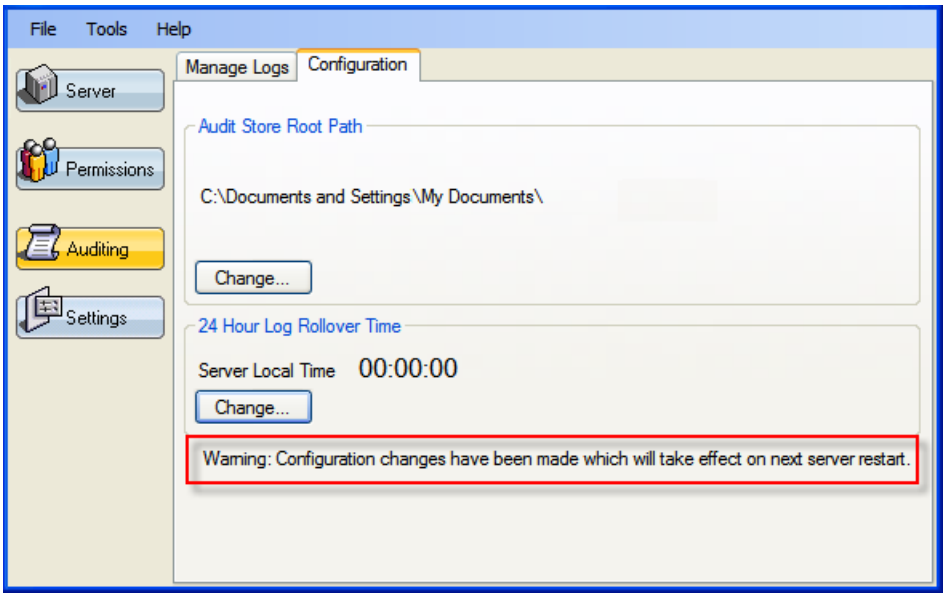


Figure 3-12: Example of warning message

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.

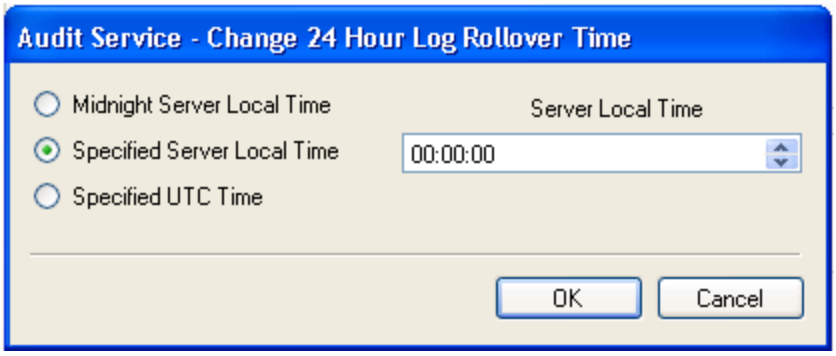


Figure 3-13: Change 24-Hour Log Rollover Time

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.

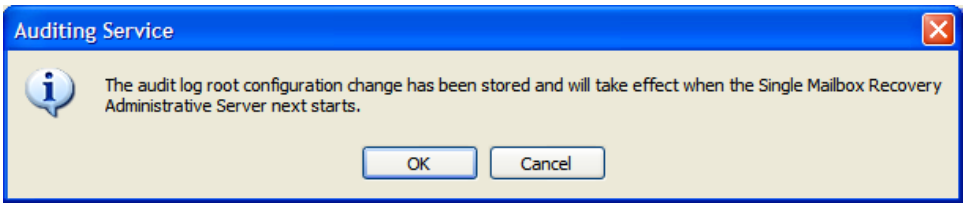


Figure 3-14: Audit log roll time configuration change message

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. Until the server is restarted, a warning message appears. For more information, see **"Server Operation" on page 10**.

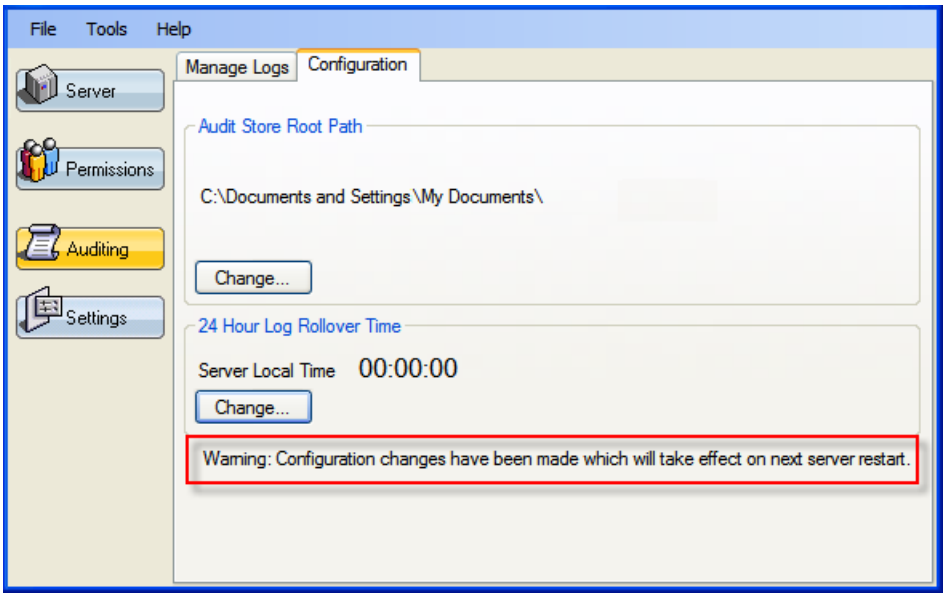


Figure 3-15: Example of warning message

Chapter 4: Settings Service

Overview

The Settings Service is a service plugin that you can load into Single Mailbox Recovery Management Console. It is used to centrally administer security preferences in the Single Mailbox Recovery application.

The Security tab on the Preference dialog box in Single Mailbox Recovery controls the level of information available to the user when restoring mailboxes and governs the tasks that person can perform. The Settings service on Single Mailbox Recovery Administrative Server enables you to centrally administer and lock the default security values on the Security tab for certain users or groups.

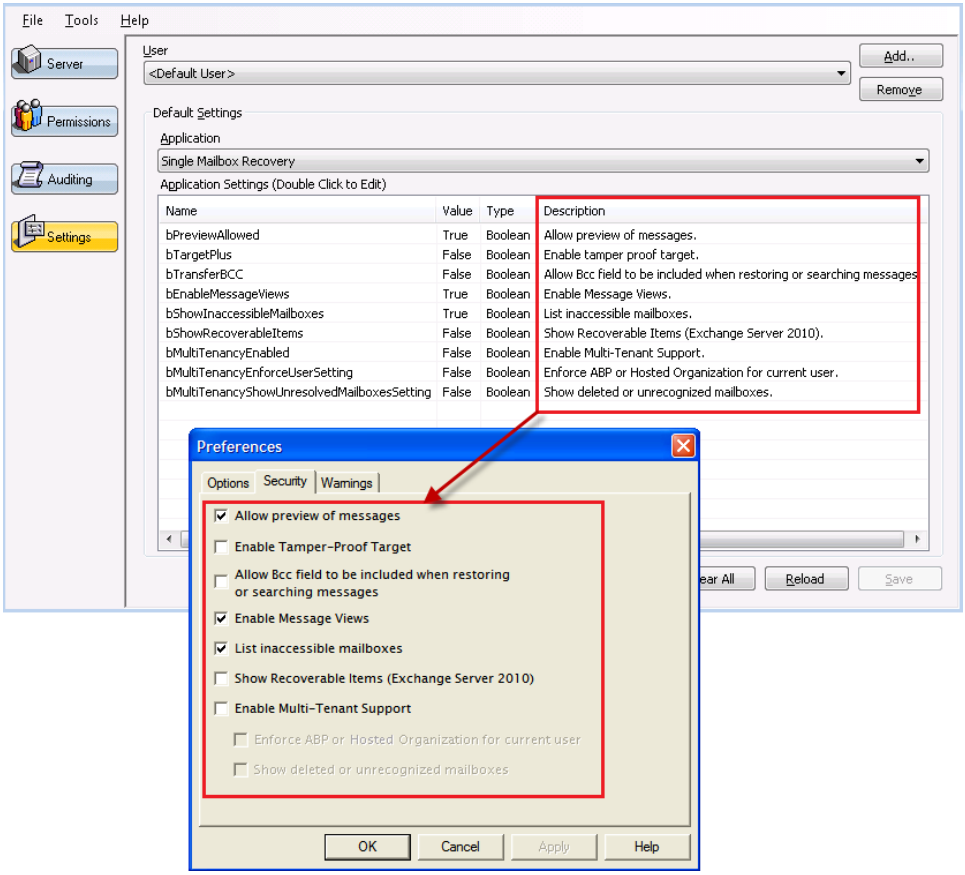


Figure 4-1: Security Settings centrally administered from the Settings service

Setting the Security Values

The Settings page enables you to centrally administer and lock the default security values in Single Mailbox Recovery for users or groups.

To set the security values

1. In the left pane, click **Settings**.

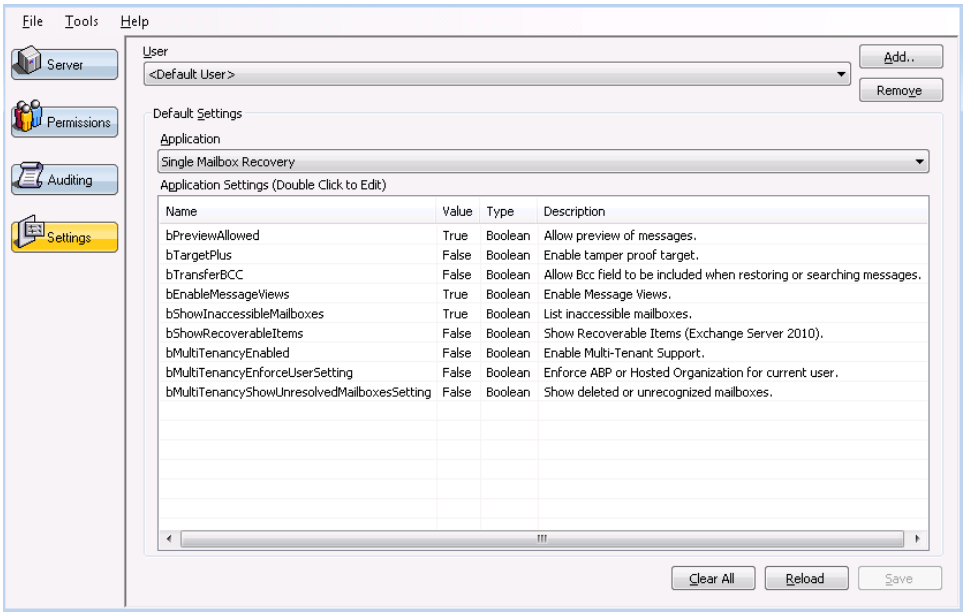


Figure 4-2: Settings page

2. In the **User** box, select the user or group you want to assign the default security values.

   Note: *Click **Add** to add users using the Add Groups or Users dialog box. For more information, see* ***"Adding or Removing a User or Group" on page 69****.*

   Note: *Selecting <Default User> displays the settings used by default when no settings are provided for the user or group.*

3. In the **Application** box, the default value "Single Mailbox Recovery" is selected.
4. In the **Application Settings** list, double-click the security setting you want to change for the selected user, group, or <Default User>.
5. In the **Setting Editor** dialog box, view the **Name** and **Information** of the selected security setting.

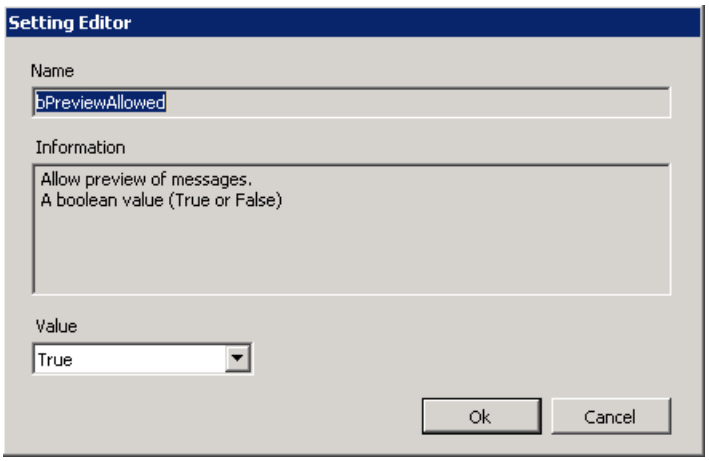


Figure 4-3: Setting Editor dialog box

6. In the **Value** field, do one of the following:
   - Select **True** to activate the setting.
   - Select **False** to de-activate the setting.
7. Click **OK** to set the Value in the Application Settings list.
8. If you want to change additional security values, repeat steps 4 through 7.

   Note: *You can click **Clear All** to return the Application Settings to the default security values or click **Reload** to return the Application Settings to the most recently saved security values for the selected user.*

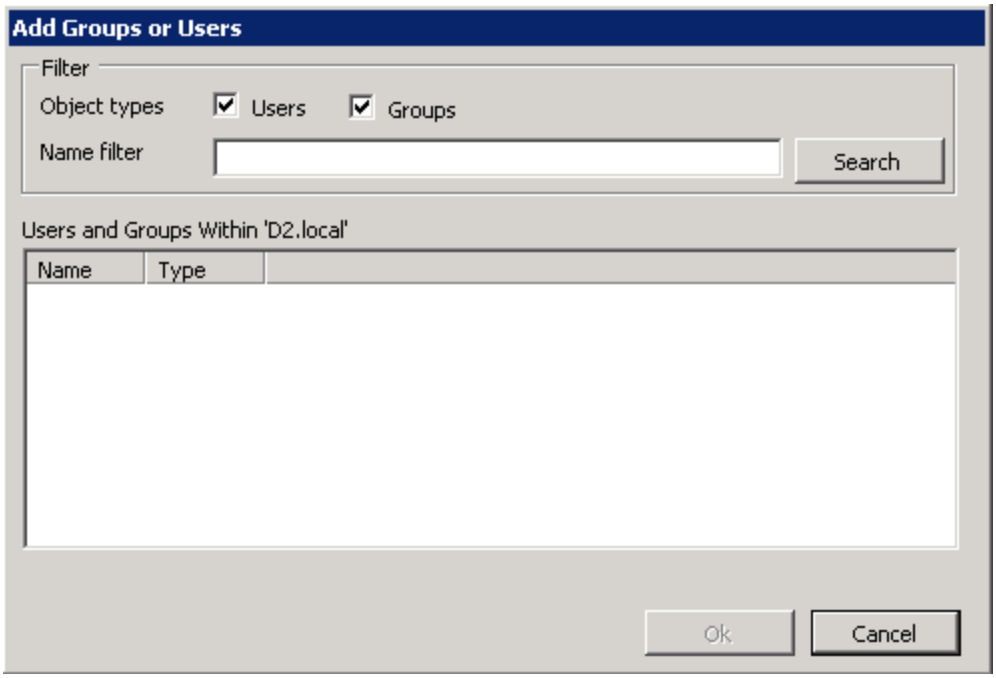
9. When you have completed the setting the security values for the selected User, click **Save**.

Adding or Removing a User or Group

You can add a group or user to the User box on the Settings page with the Add Groups or Users dialog box.

To add a user or group

1. On the **Settings** page to the right of the **User** box, click **Add**.



Add Groups or Users dialog box

2. In the **Add Groups or Users** dialog box, use the **Filter** group to select or clear the Objects types you want to search: **Users** and/or **Groups**.
3. Do one of the following:
   - Enter a name filter to narrow the list and click **Search**.
   - Click **Search** and view all the selected object types within the forest.
4. In the populated list, do one of the following:
   - Double-click the group or user you want to add.
   - Select the group or user you want to add and click **Ok**.

The selected group or user appears in the User Box on the Settings page.

To remove a user or group

- On the Settings page, use the **User** box to select the user or group you want to remove and click **Remove**.

The selected group or user clears from the User Box on the Settings page. For more information, see **"A note on user and group naming and identification" on page 39**.

Appendix A: 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 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 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 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:** Performs an 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 content 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 Command Line Actions

- **Session Start from Command Line:** Single Mailbox Recovery 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 form 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.

Logged Server-Side Activities

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 Server.
- **Server shutdown:** End of the Single Mailbox Recovery Administrative Server.
- **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.

Settings Service Session Log

This list displays any action taken in the Settings Service that is recorded in the Application Settings Service.

- **Settings have been loaded:** This action occurs when the Settings service loads the settings.
- **A setting has been read and returned to the client application:** This action occurs when a client application requests a setting.
- **The settings service is closing:** This action occurs when the Settings service closes.

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 plugins.
- **Settings have been loaded:** This action occurs when the Settings service loads the settings.
- **A user or group has been added:** This action occurs when the Settings service adds a user or group.
- **The settings for a group or user have been removed:** This action occurs when the Settings service removes a user or group.
- **A setting has been changed:** The action occurs when the Settings service changes a setting.
- **Settings have been saved:** This action occurs when the Settings service saves the settings.
- **Settings have been cleared:** This action occurs when the Settings service clears the settings.

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.

Glossary

Term	Description
ABP	Address Book Policies. A feature that allows users to restrict the users and mailboxes they can view when sending emails in an environment using Microsoft Exchange Server 2010 SP2 and later. Users can be assigned ABPs. ABPs include a Global Address List (GAL) that defines the mailboxes a user assigned an ABP can view.
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.
Exchange Hosted Organization(or **Hosted Organization)**	An organizational unit created in an environment that has deployed Microsoft Exchange Server 2010 SP1 or SP2 using the /hosting switch (Hosting Mode). Users and associated mailboxes created in a hosted organization can only see other users and mailboxes created in the same hosted organization.
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.

Term	Description
Multi-Tenancy Support	Support included in Single Mailbox Recovery and Single Mailbox Recovery Administrative Server for multi-tenant deployments of Microsoft Exchange Server 2010 and later. Specifically support is provided for environments that are utilizing the Microsoft Exchange Server 2010 SP1, SP2 Hosting Mode or Microsoft Exchange Server 2010 SP2 and later Address Book Policy feature. Support includes the ability to limit the source and target mailboxes a user can access based on Exchange Hosted Organizations or Address Book Policies. For information regarding Hosting Mode using the "/hosting" switch, see http://technet.microsoft.com/en-us/library/ff923272.aspx and http://social.technet.microsoft.com/wiki/contents/articles/1110.exchange-2010-sp1-information-for-hosted-service-providers.aspx. For information regarding Address Book Policies, see http://technet.microsoft.com/en-us/library/hh529948.aspx and http://technet.microsoft.com/en-us/library/hh529916.aspx.
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 plugin module that the server loads. A service package is information being exchanged between a client and an individual service.

Copyright Information

Copyright © 1994-2015 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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.

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. 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).

Trademark Information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at http://www.netapp.com/us/legal/netapptmlist.aspx.

Document version number: 7.2.0.3

How to Send Comments About Documentation and Receive Update Notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

2

24-hour log rollover time
  changing 57, 63

A

Active Directory
  advertising 9-11
  updating 11
Activity Data 60
Address Book Policies 78
address book policy 25, 27, 37
advertising
  changing 11
All mailboxes
  permissions 16
allowing access
  permanently 47
  temporarily 47
Application Auditing Service 56
audit log
  changing rollover time 65
  copying 62
  deleting 63
  validating 63
  viewing 59
audit logs
  changing location 63
audit store root path
  changing 57, 63
auto support 11

C

changes
  activating 49
complete log 59
connection
  terminating 11-12, 55
connections
  active 12
conventions in this manual
  notes and tips 2
  shortcut menu 2

D

denying access 49
directory tree 58

E

external mailbox
  permissions 15
  removing 33
external mailboxes
  adding 32

F

failed access attempts 46
first run configuration 15, 57

G

getting help 1
global address list 27
group or user
  adding 28
  setting permissions 30, 35

H

Help
  online Help 2

I

incomplete log 58
installed services
  list 12
internal mailbox
  permissions 15

L

list
  filtering 28
Location column 27

logged activities
  stand alone 56
  transaction 56

M

mailbox
  adding 28
Mailbox Categories
  permissions 16
Mailbox Category
  setting 37
Mailbox Permissions Service 14
mailboxes
  clearing 49
Menu Commands and Shortcuts 2
Midnight Server Local Time 65
Mult-Tenant
  background 14
Multi-Tenant Support 79

N

Notes and Tips 2

O

online Help 2

P

permanently allow 47
Permission Model 15
  horizontal check 15
  vertical check 17
permission order
  changing 30
permission settings 15
permissions
  applying 28
  editing 26, 31
  saving 49
  setting 30, 35
  sorting order 30
  viewing 26, 31
port
  changing 10

R

refusal
  allowing 47
refusals
  managing 46
Release Notes 1

S

server
  restarting 10-11
  stopping 10-11
Server Configuration Page 9
Service Connection Point
  updating 10
services
  available 13
Session Data 59
Setting Service 67
settings
  clearing 49
  modifying 54
Shortcut Menu 2
Specified Server Local Time 65
Specified UTC Time 65
stored permissions
  reloading 49
Summary Report
  showing 61

T

technical support 2
temporarily allow 47

U

user or group
  removing 30

W

wizard
  using 49