

Troubleshooting Exchange Permissions



Contents

- Overview
- Access Denied Errors
- Testing Permissions
- Access Denied: Common Reasons
- Access Denied: Common Scenarios
- Confirming Effective Permissions

Overview

- Quest Products predominantly dictate that permissions be applied to the Exchange Org level so that permissions flow from the root throughout the organisation. By default this cannot be available with the Exchange 2003 GUI. The following article describes the process of adding this feature: <http://support.microsoft.com/kb/259221>. The process of adding the permissions are document well within the Quick Start guide of every applicable Quest Product. Many Windows Management products integrated with Exchange require the need for Send-As & Receive-As rights, amongst other permissions of course. This permission would practically allow the object to open other user's mailboxes and view what is inside and also insert messages into the mailbox. This is a pre-validation test performed on Quest applications whereby we programmatically insert a message into a given mailbox in order to confirm the rights given have been applied successfully, after which we delete the message.

Within the Quick Start Guides, detailed information is given on how to apply permissions, which should always be sufficient. If that is not the case and permissions do not appear to be functioning as they should this document should hopefully explain how to troubleshoot permission issues.

- What tools do I need to troubleshoot?

ADSIEdit: You will need to download ADSIEDIT which is part of the 200x server support tools. These can be downloaded from <http://www.microsoft.com/downloads/details.aspx?FamilyID=96a35011-fd83-419d-939b-9a772ea2df90&DisplayLang=en>. Once installed you will need to register the adsiedit.dll. To do so use the following command via Start - Run 'regsvr32 adsiedit'

MFCMAPI: This is a tool which allows you to connect to the Exchange server, store, mailbox, and public folder levels. It can be downloaded from <http://www.microsoft.com/downloads/details.aspx?FamilyID=55FDFFD7-1878-4637-9808-1E21ABB3AE37&displaylang=en>

- Which type of Quest Products would I likely encounter this problem?

Notes Migrator for Exchange, Groupwise Migrator for Exchange, MessageStats, Archive Manager. Almost all products which have a connection to Microsoft Exchange

Access Denied Errors

- What error(s) defines access denied?

As a general rule Quest Products use CDO (currently version) 1.2.1 MAPI Access to extract or insert data into Exchange. The standard error returned via CDO from MAPI is "MAPI_E_LOGON_FAILED" OR '8004011'. The '8004011' will always mean simply, you do NOT have permission. If you ever see that number it will always mean you do not have permission

Each Quest product under various circumstances will return a different error in full, but the error will always have one common denominator. Sample and typical errors returned from our applications in these circumstances are:

Quest Notes Migrator for Exchange: "MAPI error 80040115 Component: Microsoft Exchange Server-InformationStore Low level error: 000006BE Context: 00000514"

Quest Migration Manager for Exchange: "CSession::Logon Error -2147221231 The information store could not be opened. - MAPI_E_LOGON_FAILED (MAPI 1.0) Low level error: 0x0 File: 'aeWrapHelpers.h' Line: '264'"

Quest Archive Manager ESM Account: "ERROR: Session.OpenMsgStore: MAPI error 8004011D Error: You do not have permission to log on. Component: Microsoft Exchange Server Information Store Context: 00000519"

Quest Archive Manager Journal Account: "17:06:15 Exporting Mailbox: Mailbox - ArchiveMgr_Journal 17:06:15 ERROR: Session.OpenMsgStore: 17:06:15 MAPI error 8004011D 17:06:15 Error: Microsoft Exchange Server 17:06:15 Component: Microsoft Exchange Server information Store 17:06:15 Context: 00000526"

Testing Permissions

- There are many different ways to test and confirm permissions to the Exchange Server, the Exchange Store, and Mailbox Level. The various ways are discussed below.
- *Outlook*

You can simply test permissions by logging into Windows and Outlook as the user account the Exchange permissions are applied to. You must open Outlook and perform the relevant functions to test. For example, if you have Send-As & Receive-As rights, add an additional mailbox within Outlook. If you can view the another mailbox on the relevant mail store and server, you have been granted permissions successfully.
- *MFCMAPI*

You can also download MFCMAPI (<http://www.microsoft.com/downloads/details.aspx?FamilyID=55FDFFD7-1878-4637-9808-1E21ABB3AE37&displaylang=en>). This tool allows you to connect to Exchange at all levels in order to confirm the relevant permissions are present. Instructions come with the product, but to simply logon and display the store:

 1. Log into Windows with the service account you require to test permissions
 2. Run MFCMapi
 3. On the Session menu, click Logon and Display Store Table.
 4. You will be prompted to create a profile or select a profile
 5. Enter details of user's mailbox whose errors are encountered in the log.
 7. You can further click on Mailbox or Public Folders to browse through various mail or Public Folder MAPI Information
- *ADSIEdit*

Using ADSIEdit, you can view the effective rights of a user. This is discussed further below.

Access Denied: Common Reasons

- *Issue 1: The user object with which permissions are assigned, is a member of Domain Admins or Enterprise Admins.*
Resolution: By default these two built-in groups have the Send-As & Receive-As permissions denied. Therefore you must remove the user object from Domain Admins or Enterprise Admins. It would not be common practice to remove the deny from the one of these groups as the permissions are structures this way for a reason.
 - *Issue 2: The user object with which permissions are assigned has a deny applied via Group Policy*
Resolution: Remove the GPO restriction, remove the user from that GPO assignment
 - *Issue 3: The user object with which permissions are assigned, but its Active Directory user object security shows that it does not inherit permissions from its parent preventing permission inheritance*
Resolution: Open ADUC. Confirm 'View – Advanced Features' is selected. Open the user object in question. Select 'Security – Advanced'. Confirm the 'Allow inheritable permissions from the parent to propagate to this object and all child objects', is selected
 - Issue 4: The user object with which permissions are assigned have been assigned correctly, but the Exchange Organisation is not set to inherit the flow of permissions from root to mail store.
Resolution: This means that the Exchange Org may have permissions at Org level, the Mail Store may also have permissions, but the Exchange Server itself does not have permissions. This can be shown by opening adsiedit, selecting an appropriate mail store, selecting 'Properties – Security – Advanced – Effective permissions'. An example of a path in adsiedit is: "Domain.com/Configuration/Services/Microsoft Exchange/Org/Administrative Groups/AdminGroup/Servers/Server Name/Information Store/First Storage Group/Mailbox Store"
- Note: Please see 'Confirming Effective Permissions' section on how to perform the above steps.
- Issue 5: I have permissions, permissions are applied correctly, but still not working
Resolution: With Exchange, especially 2007, permissions can take considerable time to propagate fully. The alternative is to create another user and apply permissions once more

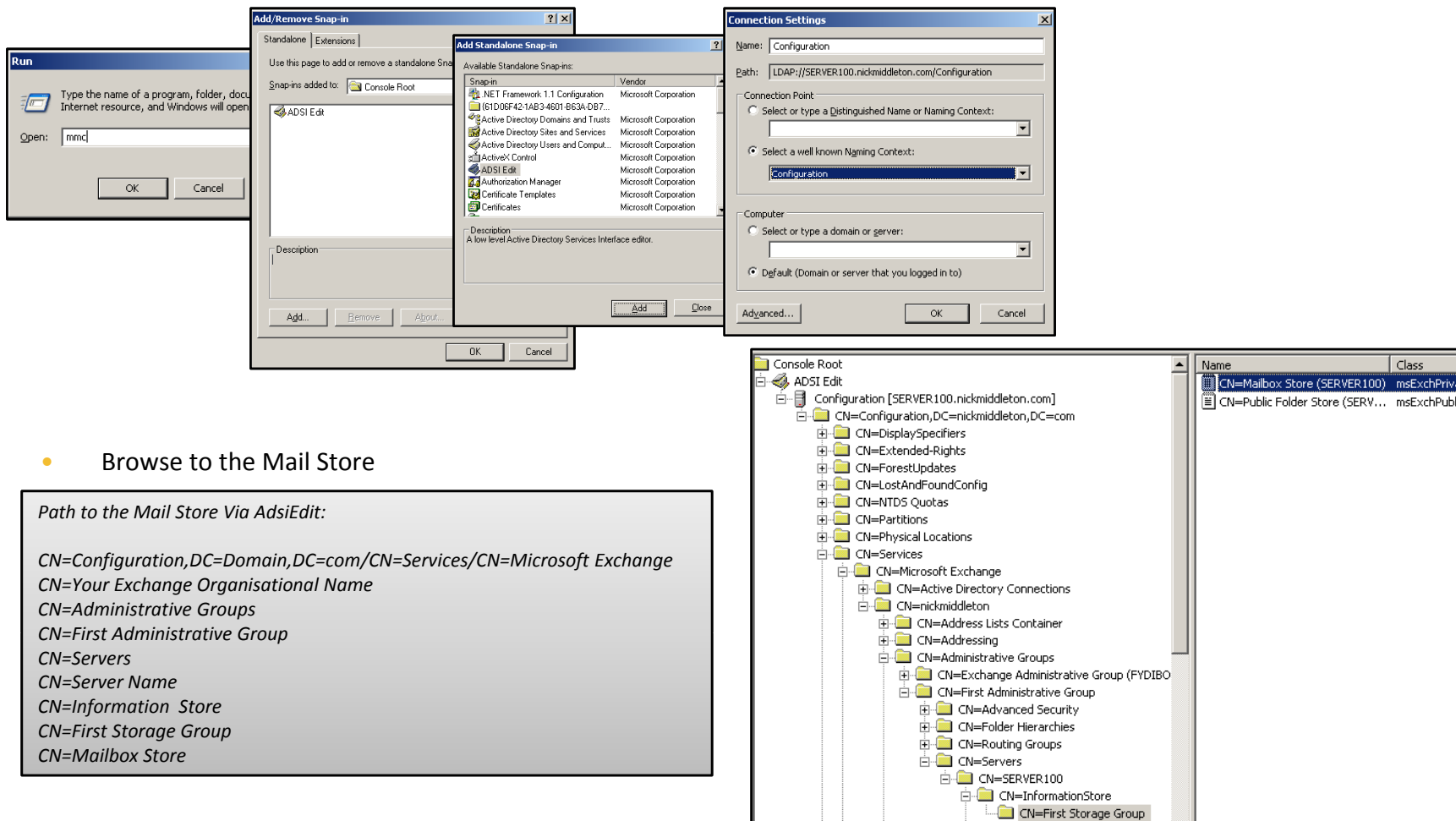
Access Denied: Common Scenarios

- *You are having a problem with one user only, every other user seems to be fine*
Resolution: Open ADUC. Confirm 'View – Advanced Features' is selected. Open the user object in question. Select 'Security – Advanced'. Confirm the 'Allow inheritable permissions from the parent to propagate to this object and all child objects', is selected
- *You are having a problem with more than one user, but not all*
Resolution: Confirm any consistency between the users. Are they on the same store, are they on the same Exchange server? The Exchange Org may have permissions at Org level, the Mail Store may also have permissions, but the Exchange Server itself does not have permissions. This can be shown by opening adsiedit, selecting an appropriate mail store, selecting 'Properties – Security – Advanced – Effective permissions'. In some cases it may be necessary to check every level of *Effective Permissions* from the Exchange Organisation down to the Mail Store itself, such as:
CN=Configuration,DC=Domain,DC=com\CN=Services CN=Microsoft Exchange
 CN=Your Exchange Organisational Name
 CN=Administrative Groups
 CN=First Administrative Group
 CN=Servers
 CN=Server Name
 CN=Information Store
 CN=First Storage Group
 CN=Mailbox Store
- *You are having a problem with all users, not matter what you do nothing works*
Resolution: Most likely the account you are using is a member of Domain Admins or Enterprise Admins. See *Reason 1* previously.

Confirming Effective Permissions

In order to confirm the effective permissions the following is a short summary on how to do this

- Open AdsiEdit.msc
- Add the ADSI Edit Snap-In
- Open the Configuration Container



The image contains four screenshots illustrating the steps to access the Mail Store via ADSI Edit:

- Run Dialog:** Shows the 'Run' dialog box with 'mmc' entered in the 'Open:' field.
- Add Standalone Snap-in:** Shows the 'Add Standalone Snap-in' dialog box with 'ADSI Edit' selected in the 'Snap-ins added to:' list.
- Connection Settings:** Shows the 'Connection Settings' dialog box with 'Configuration' selected in the 'Connection Point' dropdown.
- ADSI Edit Console Tree:** Shows the ADSI Edit console tree with the 'Configuration' container expanded, showing the hierarchy: Configuration [SERVER100.nickmiddleton.com] > CN=Configuration,DC=nickmiddleton,DC=com > CN=Services > CN=Microsoft Exchange > CN=First Storage Group > CN=Mailbox Store (SERVER100).

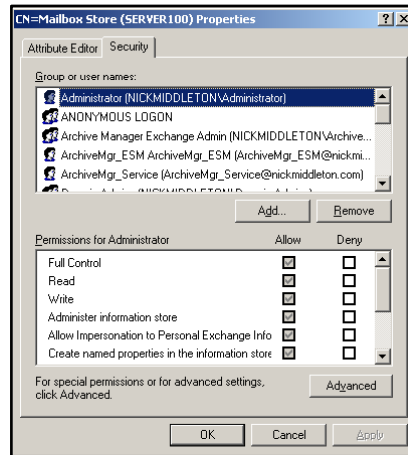
- Browse to the Mail Store

Path to the Mail Store Via AdsiEdit:

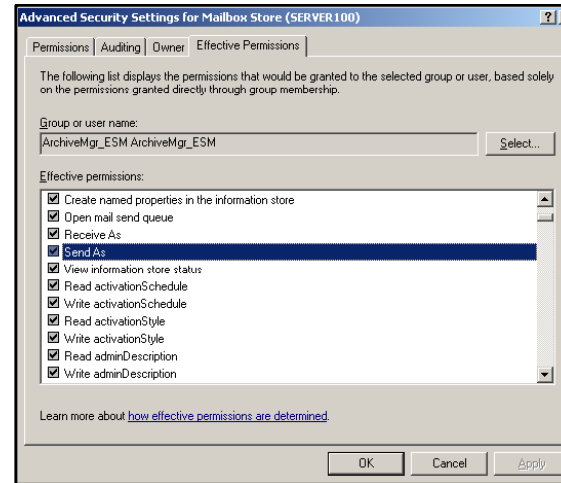
*CN=Configuration,DC=Domain,DC=com/CN=Services/CN=Microsoft Exchange
CN=Your Exchange Organisational Name
CN=Administrative Groups
CN=First Administrative Group
CN=Servers
CN=Server Name
CN=Information Store
CN=First Storage Group
CN=Mailbox Store*

Confirming Effective Permissions..

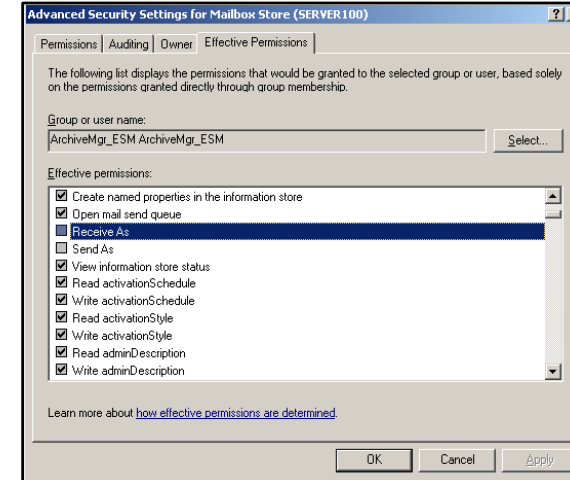
- Mail Store Properties



- Correct Effective Permissions



- Incorrect Effective Permissions



Path to the Mail Store Via AdsEdit:

*CN=Configuration,DC=Domain,DC=com/CN=Services/CN=Microsoft Exchange
 CN=Your Exchange Organisational Name
 CN=Administrative Groups
 CN=First Administrative Group
 CN=Servers
 CN=Server Name
 CN=Information Store
 CN=First Storage Group
 CN=Mailbox Store*

Note: This object 'ArchiveMgr_ESM' in 'correct effective permissions' would have permission from the root of the Exchange Organisation flowing down via inheritance through to the mail store. If, at any of the levels, such as the 'First Administrative Group', the object did not have permissions, the effective rights would show this as per the screenshot 'Incorrect effective permissions'.