



Trusted Exchange 2003™

TREX™ Supplemental Pre-TREX Installation Configuration Notes

*Communications & Power Engineering, Inc.
1040 Flynn Road
Camarillo, California 93012 USA
+1 805 389 7414
www.commpower.com*

Comments on document: e-mail cjpurcell@commpower.com

TREX Export License:
TREX-EXP-CRYPTO-R5-1: CCATS# G038718, ECCN: 5D002
Exceptions: ENC per EAR 740.17 (A) and (B)(3)

Supplemental Notes

Establishing Parent / Child Domain Relationship - Single Forest/Multiple Domains

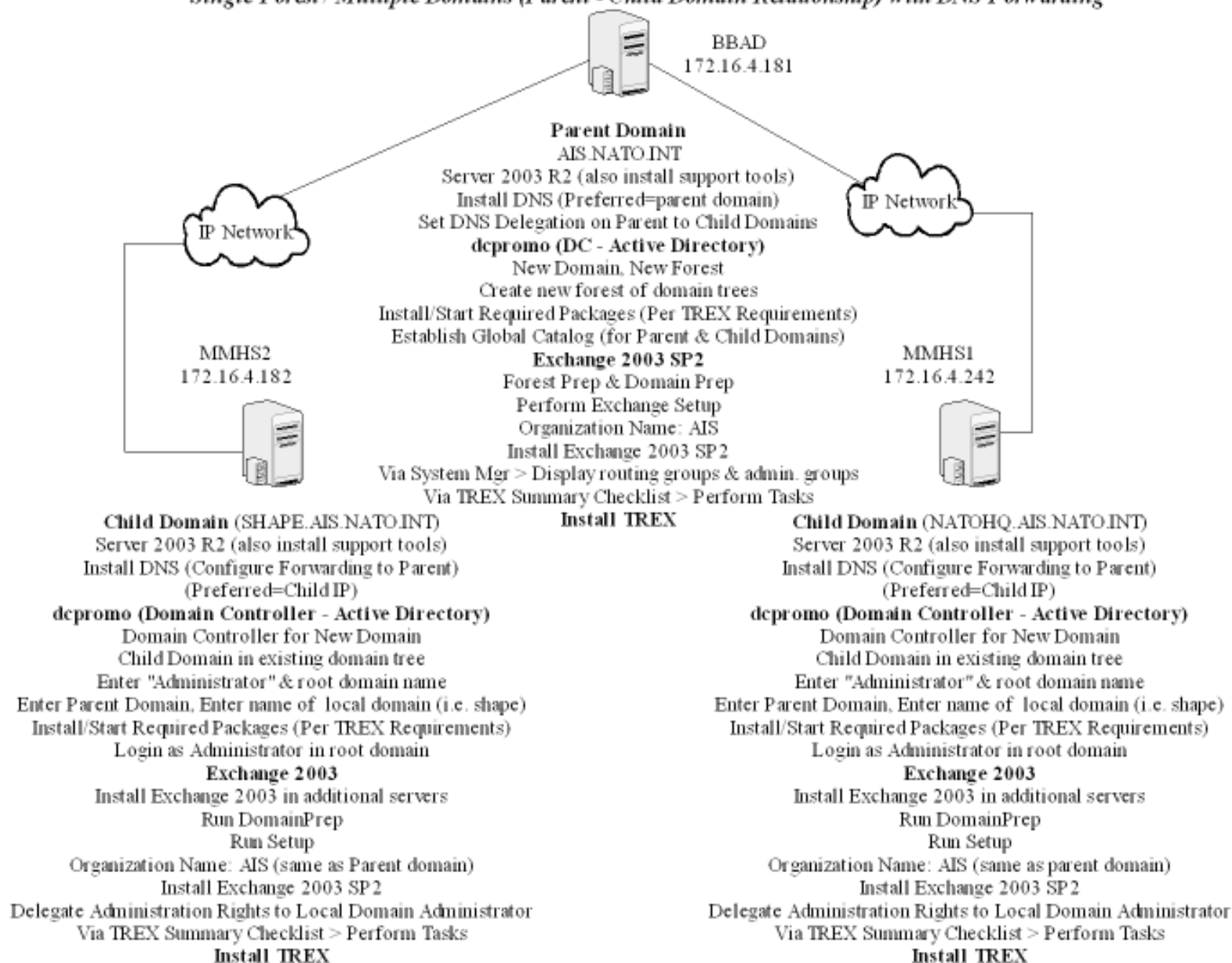
These supplemental notes are used to support the attached figures that summarize the tasks that are required in order to establish relationships in a Single Forest/Single Domain & Single Forest/Multiple Domains environments.

Please Note:

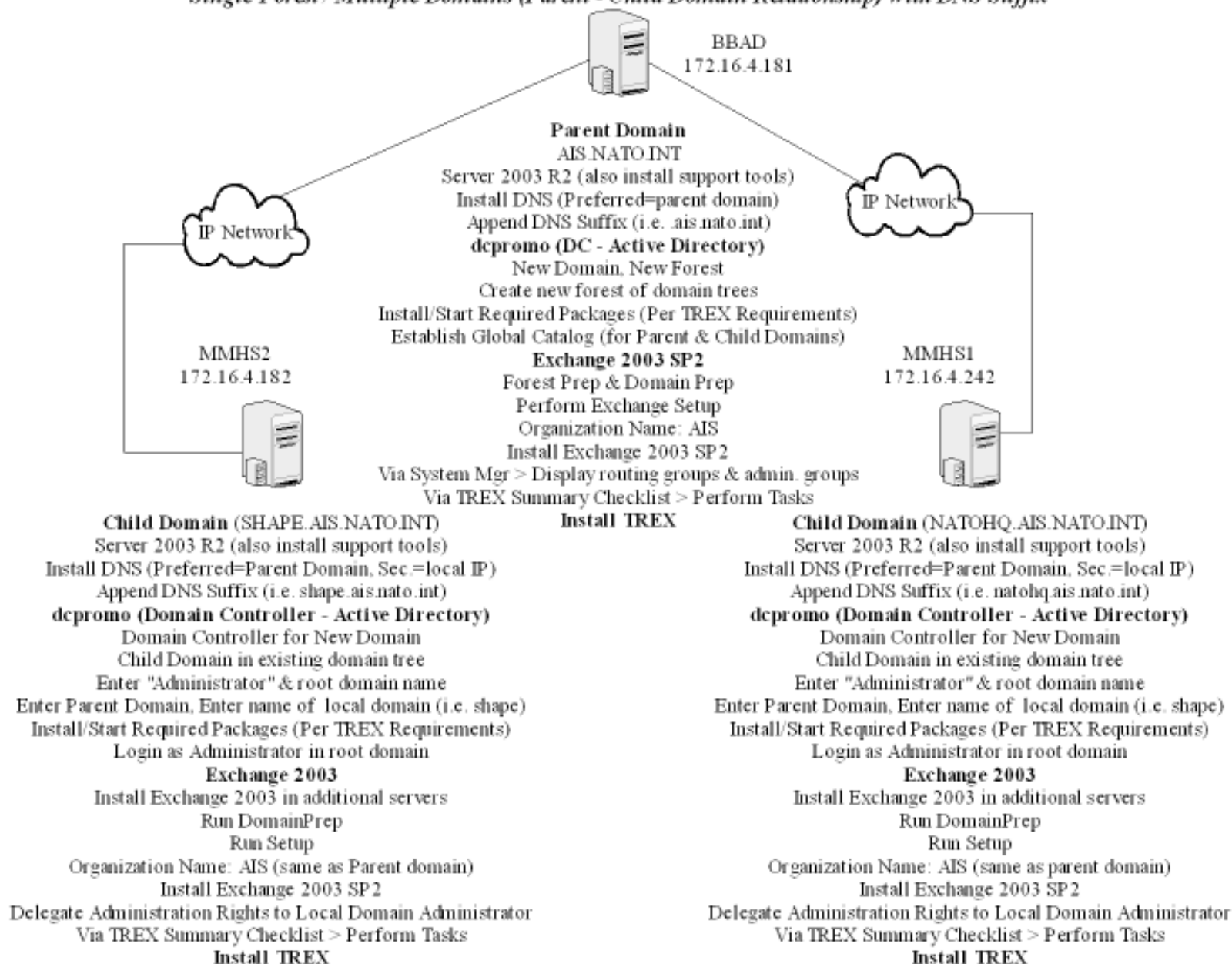
- The first figure represents DNS with forwarding.
- The second figure represents DNS with suffixes.

For those tasks identified on the drawing and not discussed herein, please refer to the document "CommPower TREX Summary Checklist for Preparing a Platform for TREX Operation".

Single Forest / Multiple Domains (Parent - Child Domain Relationship) with DNS Forwarding



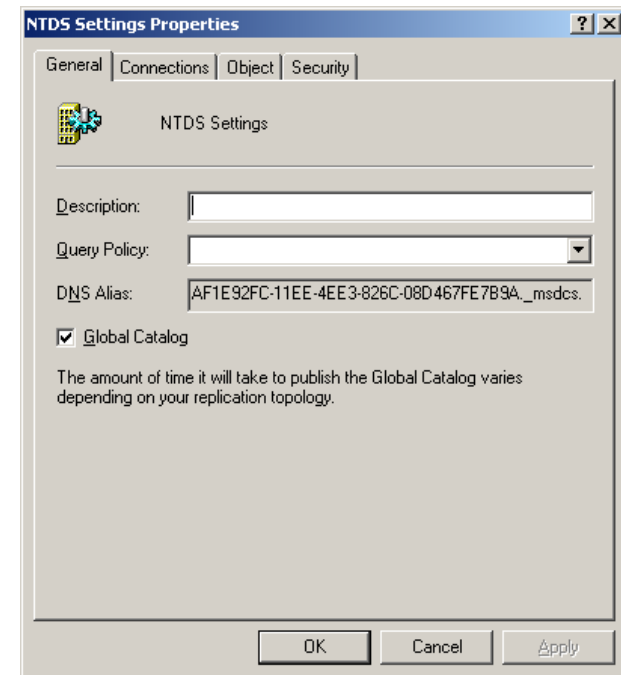
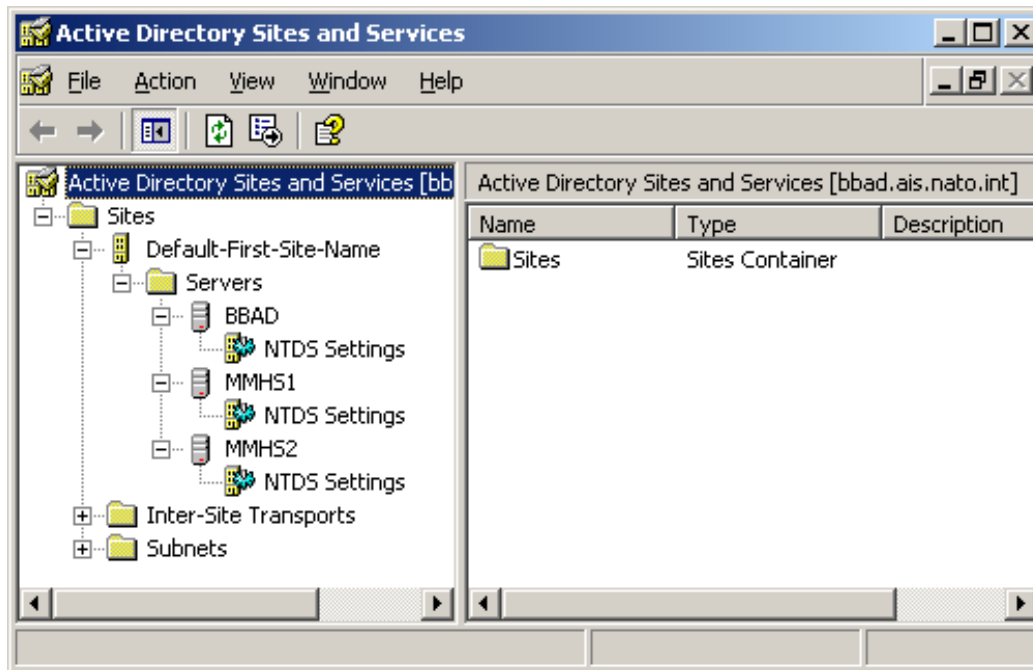
Single Forest / Multiple Domains (Parent - Child Domain Relationship) with DNS Suffix



Global Catalog:

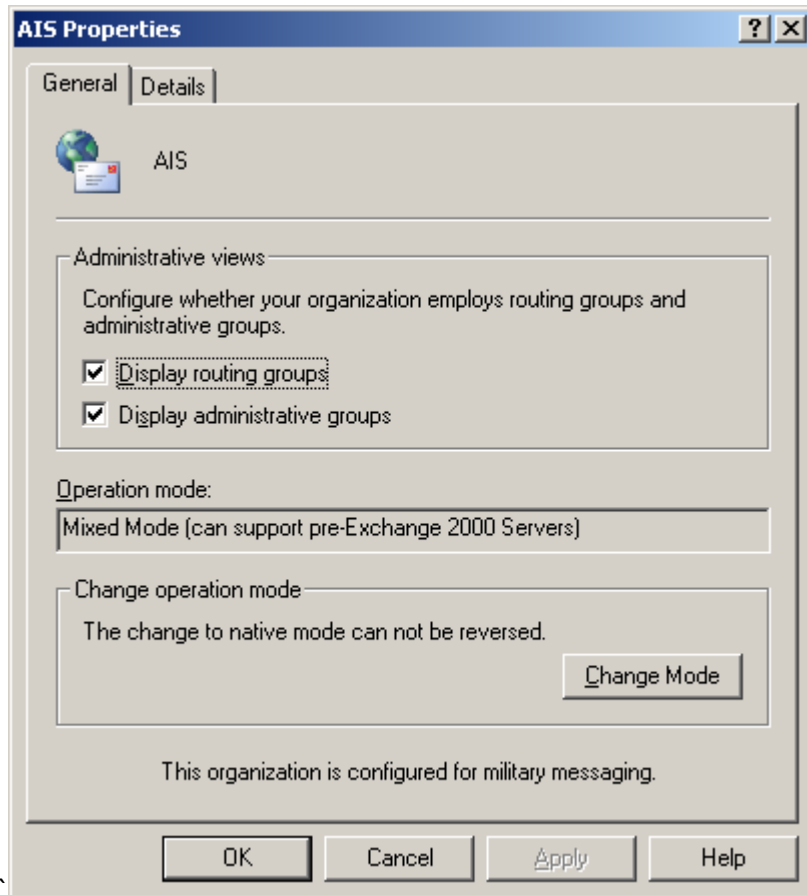
After the applicable systems (Parent Domain & Child Domains) have been promoted to a Domain Controller and Active Directory has been established AND prior to installing Exchange 2003 you must enable Global Catalog.

Active Directory Sites and Services > expand Default-First-Site-Name > expand Servers > expand the Parent Domain & the Child Domains > for the Parent Domain & each Child Domain right click the NTDS Settings and select Properties > for the Parent Domain & each Child Domain enable "Global Catalog"



Displaying Routing Groups & Administrative Groups:

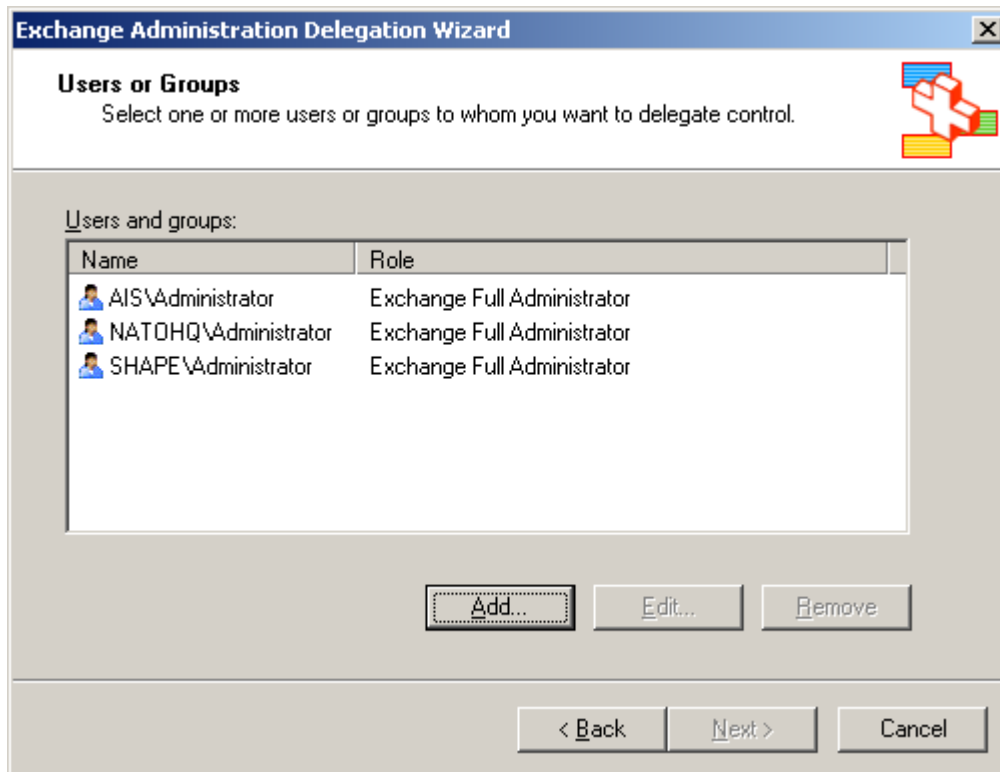
On the Parent Domain, after Exchange 2003 has been installed > System Manager > right click Exchange Organization Name (top entry) > select Properties > enable Display routing groups & administrative groups



Delegate Administrative Rights to Local Domain Administrators:

From each Child Domain login as the Administrator to the Parent Domain > System Manager > right click Exchange Organization Name (top entry) > select Delegate Control > select next > select Add > select Browse > select Location > expand Entire Directory > select applicable Child Domain > type in "Administrator" (in check names box) > select OK > select OK > for "Role" > select Exchange Full Administrator > select OK > select next > select Finish > select OK

You are now able to login to the Child Domain as the Child Domain Administrator with full exchange administrator rights.

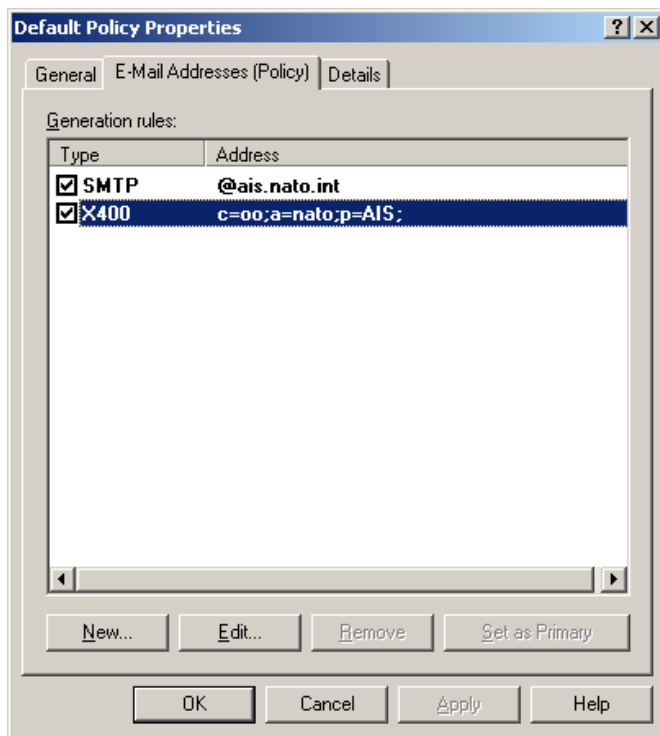


Recipient Default Policy Based on System/Domain:

Within a Parent Domain / Child Domain relationship in a Single Forest/Multiple Domain environment it is required that default recipient policies be established for any system that will have Exchange 2003 installed. This is required in order to establish the correct SMTP & X400 addresses based where the user is being created.

Default Policy for Parent Domain:

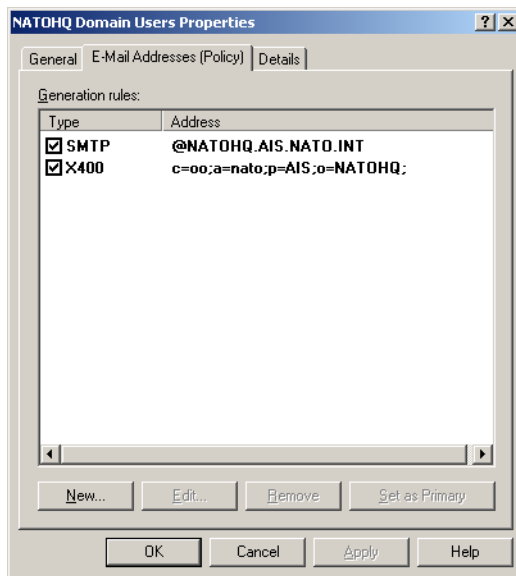
On the Parent Domain > System Manager > expand Recipients > select Recipient Policies > in the System Manager display area > select Default Policy > edit (if applicable) both the SMTP & X400 address for that of the Parent Domain



Creating Default Policies for Child Domains:

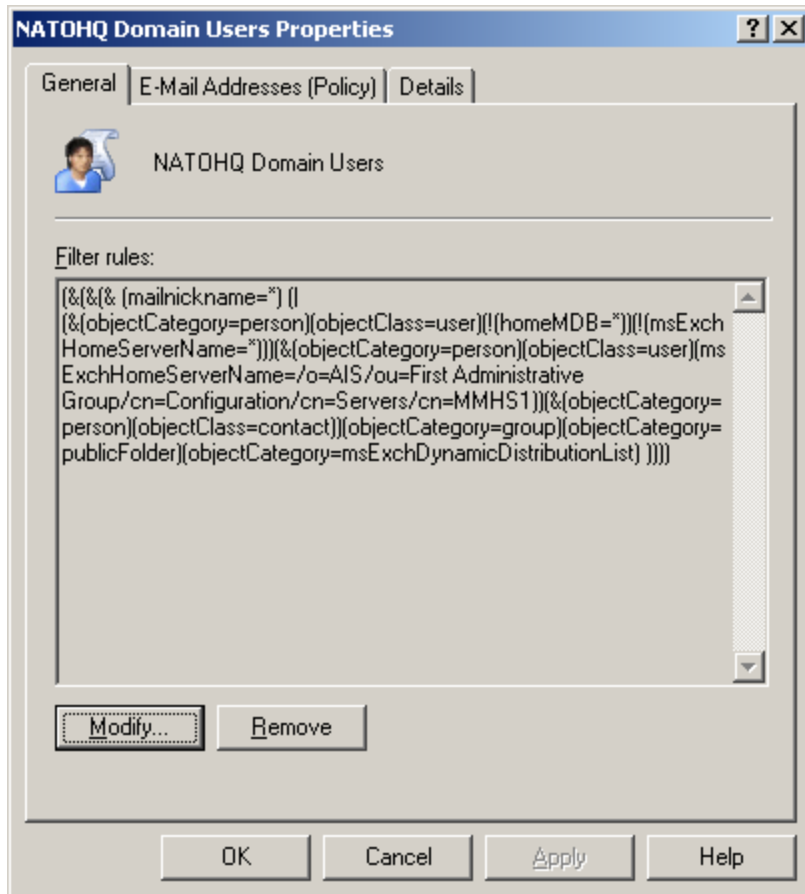
On the Parent Domain > System Manager > expand Recipients > select Recipient Policies > in the System Manager display area > right click and select New > select Recipient Policy > enable E-mail Addresses > select OK > enter the Name of the default policy to be established (i.e. NATOHQ Domain Users) > select Modify > select Storage > select Mailboxes on this server > select Browse > > type in the computer name of the applicable system in check names box (i.e. MMHS1, MMHS2) > select Check Names > the applicable computer name will be underlined > select OK > select "OK > select Apply > select OK

The new recipient policy is displayed along with Default Policy > double click the new policy > select E-Mail Addresses (Policy) > select New > select SMTP Address > in the Address box enter the SMTP address (i.e. @natohq.ais.nato.int) > select OK > set this new SMTP address as the Primary > delete the old SMTP entry > select New > select X.400 Address > select OK > enter the applicable value (c = oo, a = nato, p = <name of the parent organization> (i.e. AIS), o=NATOHQ > select Apply, select OK > set this new X400 address as the Primary > delete the old X400 entry.



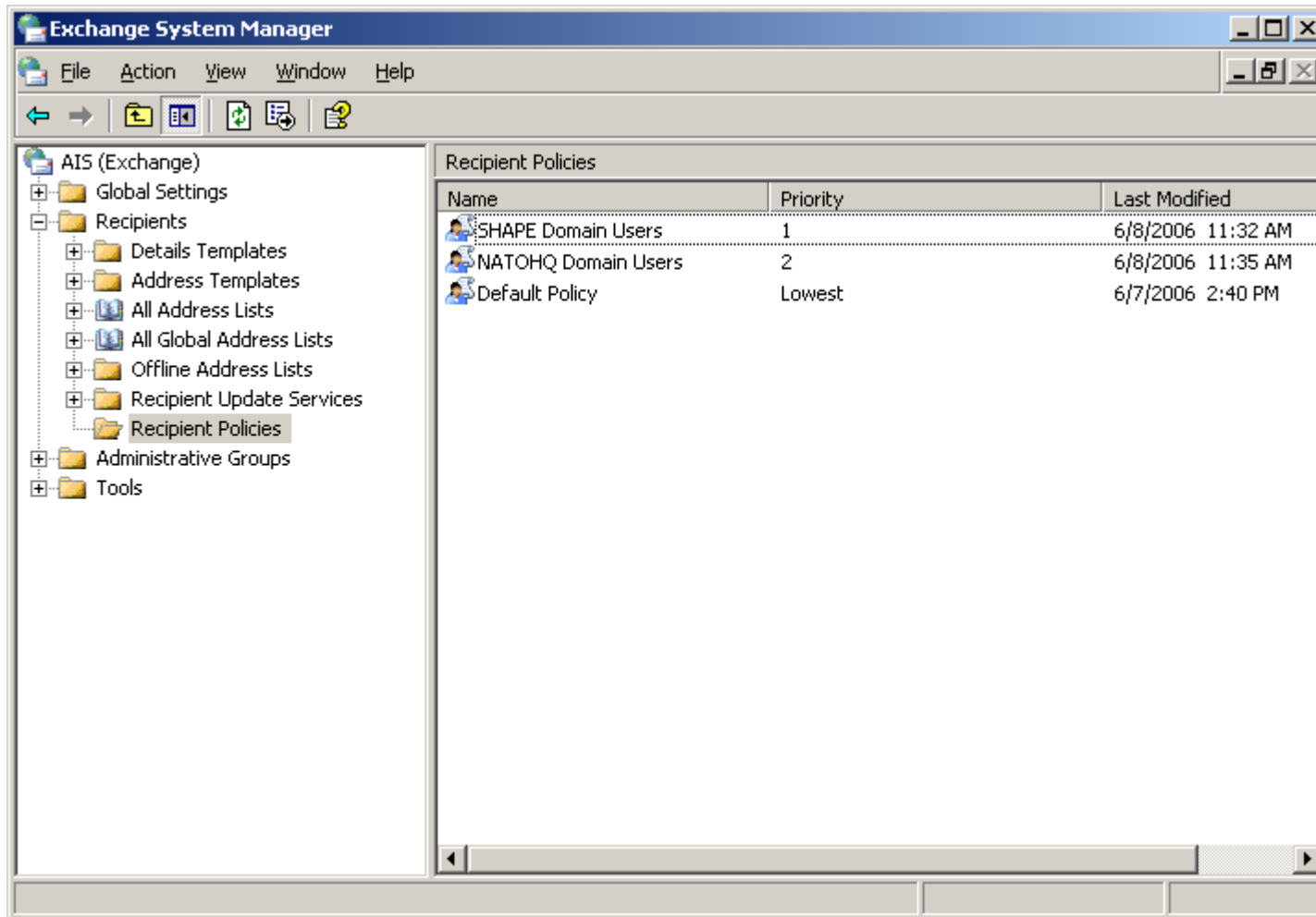
Establish Filter rules for New Policy:

For the new policy > Select the General tab > select Modify > select Storage > select Mailboxes on this server > select browse > select the applicable Child Domain > select OK > select Apply > select OK



Establish Recipient Policy Priority:

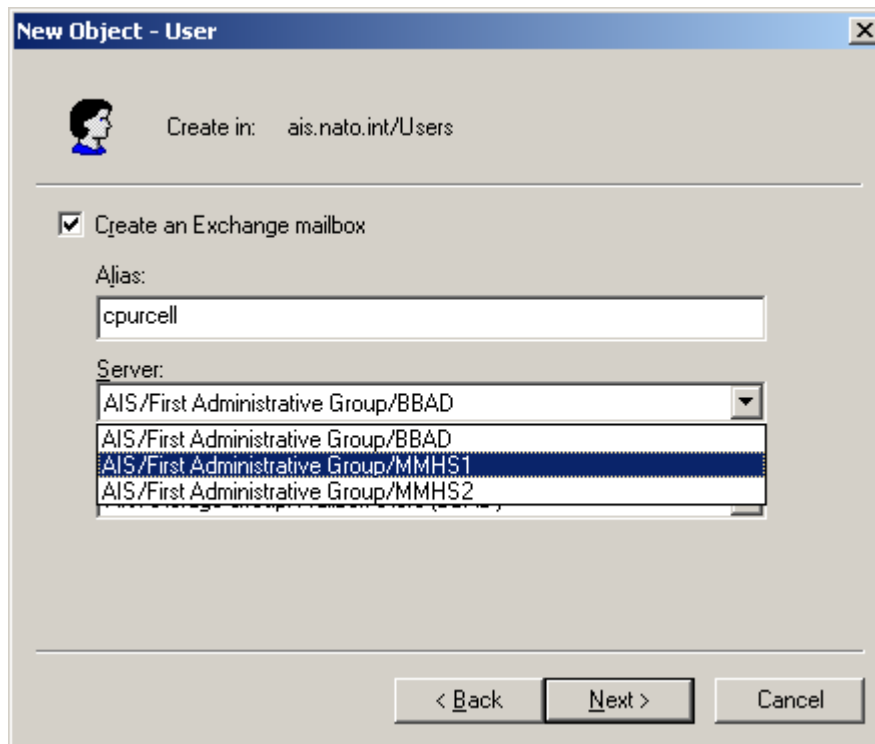
As applicable, change the priority of the policies.



Helpful Hints:

- Via Administrative Tools > Active Directory Users and Computers...

When adding a user be careful when you get to the dialog box (“Create an Exchange mailbox”) page... make sure you select the applicable Server...



New Object - User

Create in: ais.nato.int/Users

Create an Exchange mailbox

Alias:
cpurcell

Server:
AIS/First Administrative Group/BBAD
AIS/First Administrative Group/BBAD
AIS/First Administrative Group/MMHS1
AIS/First Administrative Group/MMHS2

< Back Next > Cancel

Create the Applicable Routing Groups:

In a Parent/Child Domain relationship there must exist a separate "Routing Group" for each system within the Parent/Child domain.

By default, "Routing Groups" for systems in a Parent/Child domain are located under "First Routing Group > Members".

To view the "Members" in the "First Routing Group":

- Via System Manager > expand "Administrative Group > expand Routing Groups > expand First Routing Group > expand Members (the members are the "First Routing Group" are displayed

i.e. BBAD (Parent System)
 MMHS! (Child System)
 MMHS2 (Child System)

If these systems are not within their own "Routing Group", the behavior of Exchange does not provide the routing requirements required by TREX.

In order to create the applicable "Routing Groups" (and subsequent members and connectors) perform the following tasks:

1. Create the new "Routing Group"
2. Move the applicable "Member" to the applicable "Routing Group > Member" folder
3. Create the applicable X400 connectors for each "Routing Group"

Create the new "Routing Group":

In the examples given herein the following information is used to create the applicable "Routing Group":

- Parent domain Node Name is "BBAD". Exchange Address is "ais.nato.int"
- Child domain Node Name is "MMHS1". Exchange Address is "natohq.ais.nato.int"
- Child domain Node Name is "MMHS2". Exchange Address is "shape.ais.nato.int"

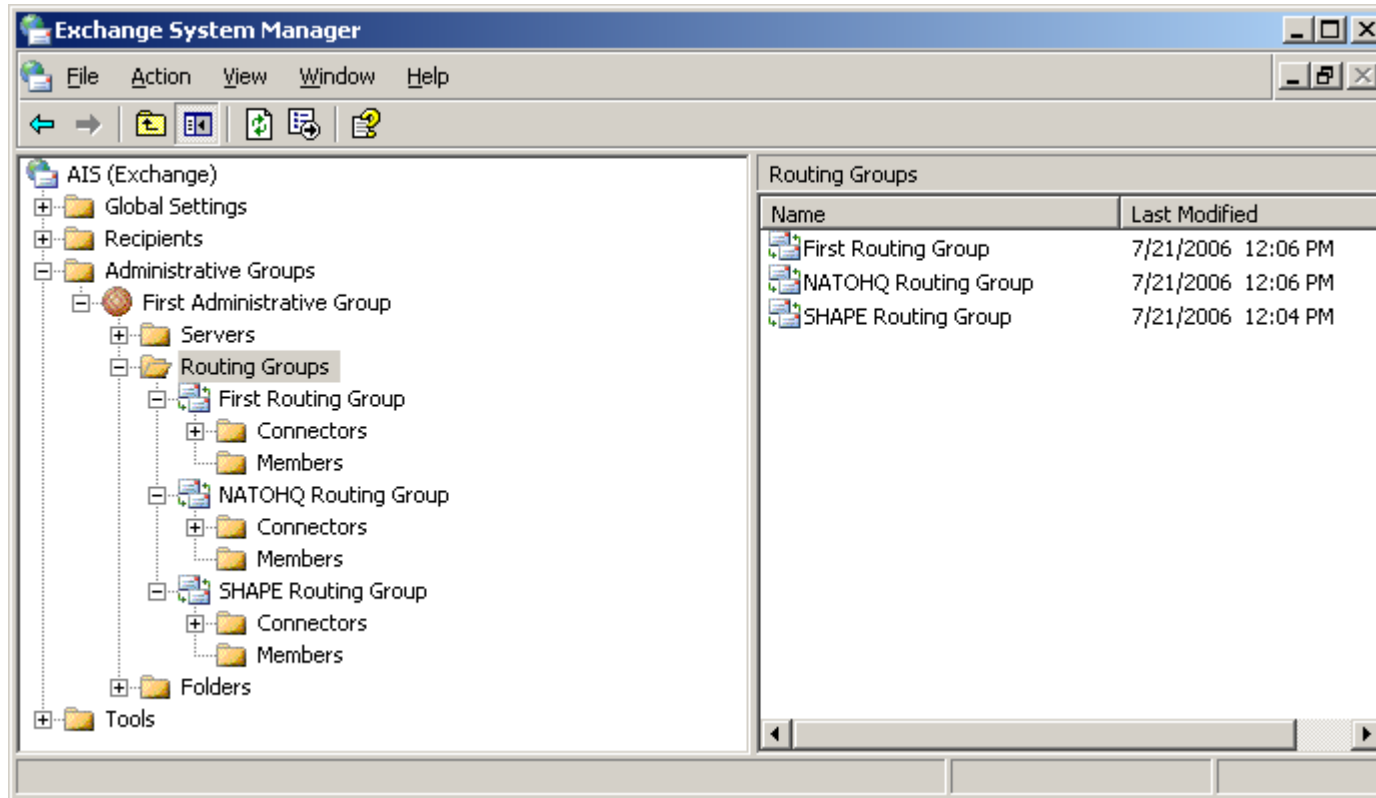
- o Via System Manager > expand "Administrative Group > expand Routing Groups

- o Right click Routing Groups > select New > select Routing Group

- o Define the name of the new "Routing Group" (i.e.)
 - NATOHQ Routing Group
 - SHAPE Routing Group

Create all required routing groups as exemplified in below display.

Please note that the “First Routing Group” remains unchanged. The parent domain (BBAD, “ais.nato.int”) reside under this “Routing Group”.



Cut & Paste “Members”:

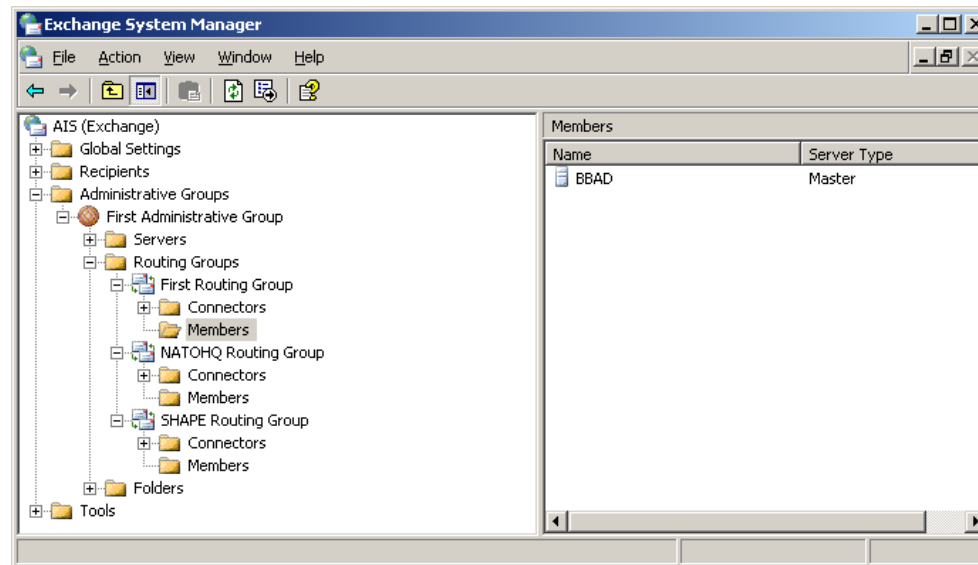
- Expand “First Routing Group” > expand Members

The applicable domain names will be displayed (i.e.):

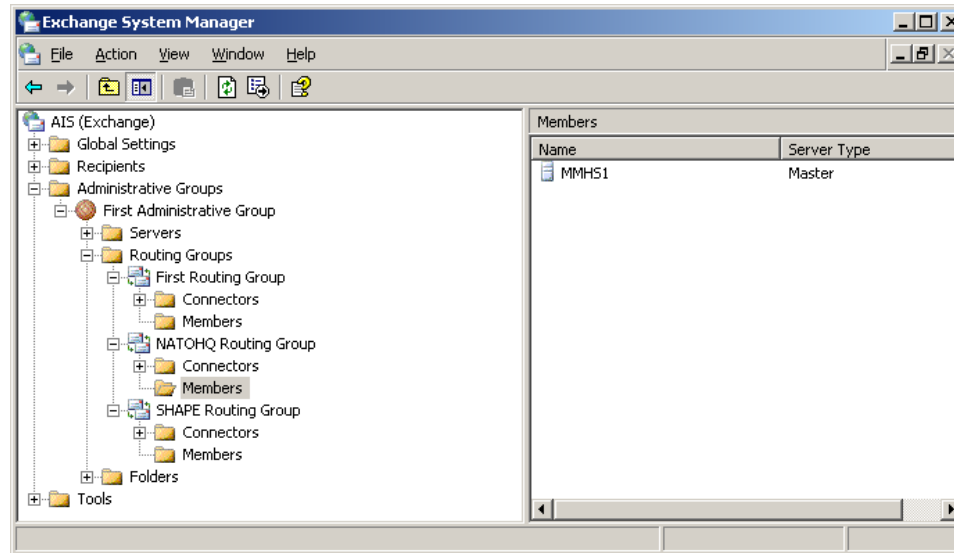
BBAD
MMHS1
MMHS2

- Select and right click “MMHS1” > select Cut
- Expand the “NATOHQ Routing Group” > expand Members > within the Members Folder, Paste “MMHS1”
- Under “First Routing” > expand Members
- Select and right click “MMHS2” > select Cut
- Expand the “SHAPE Routing Group” > expand Members > within the Members Folder, Paste “MMHS2”

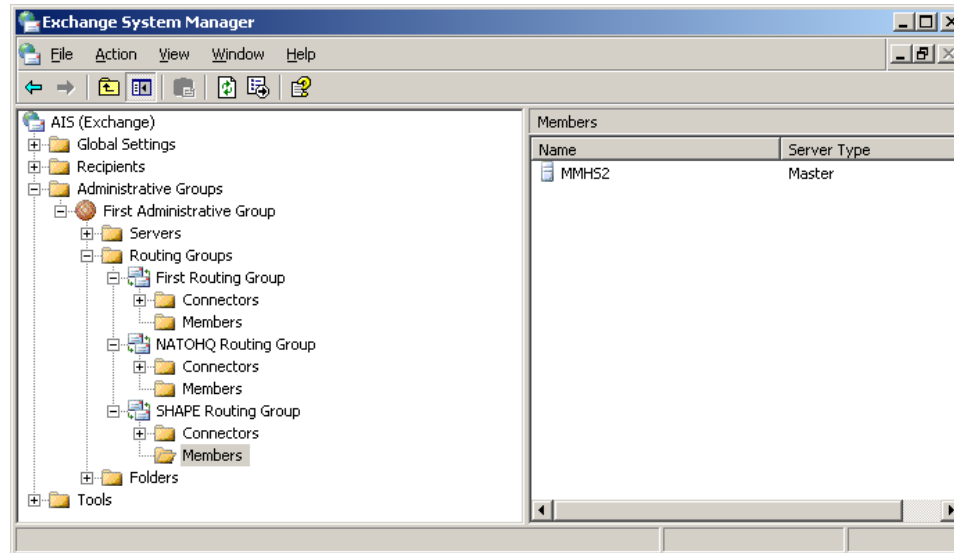
First Routing
Group Members



NATOHQ Routing Group Members

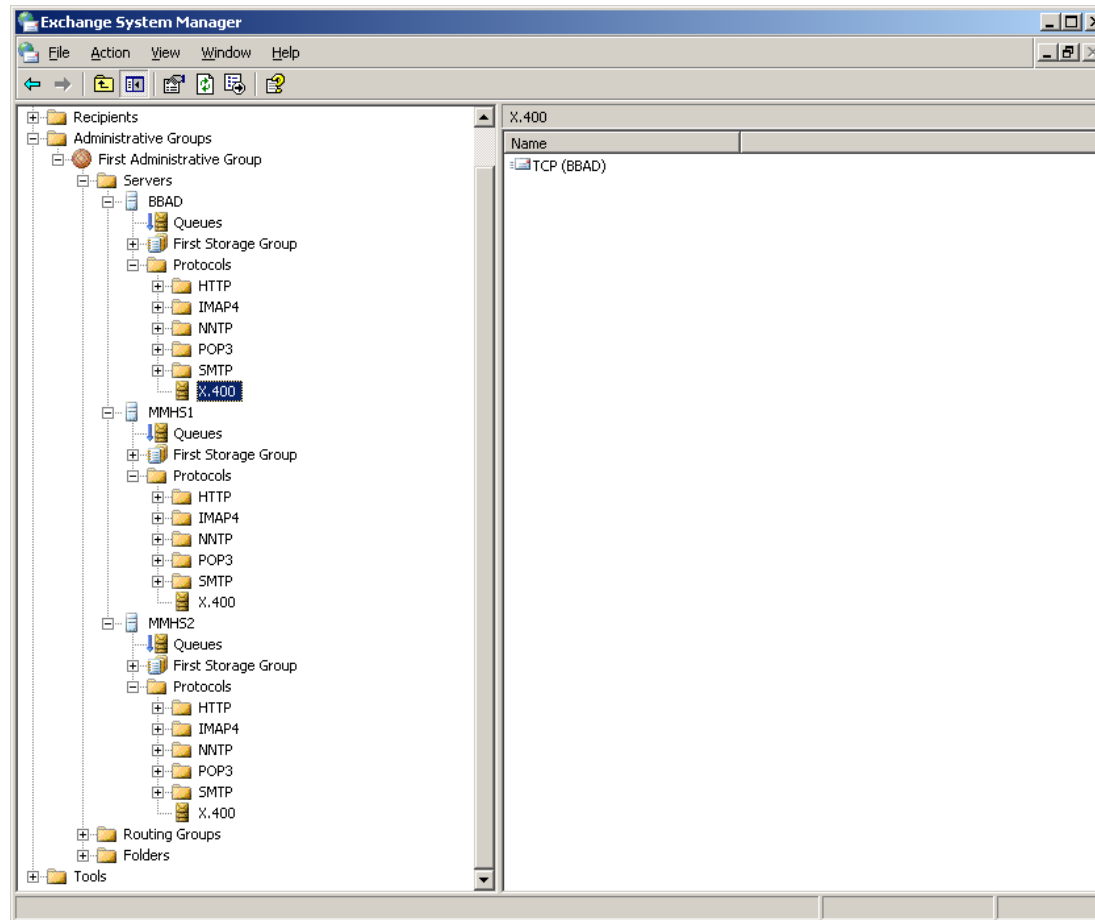


SHAPE Routing Group Members



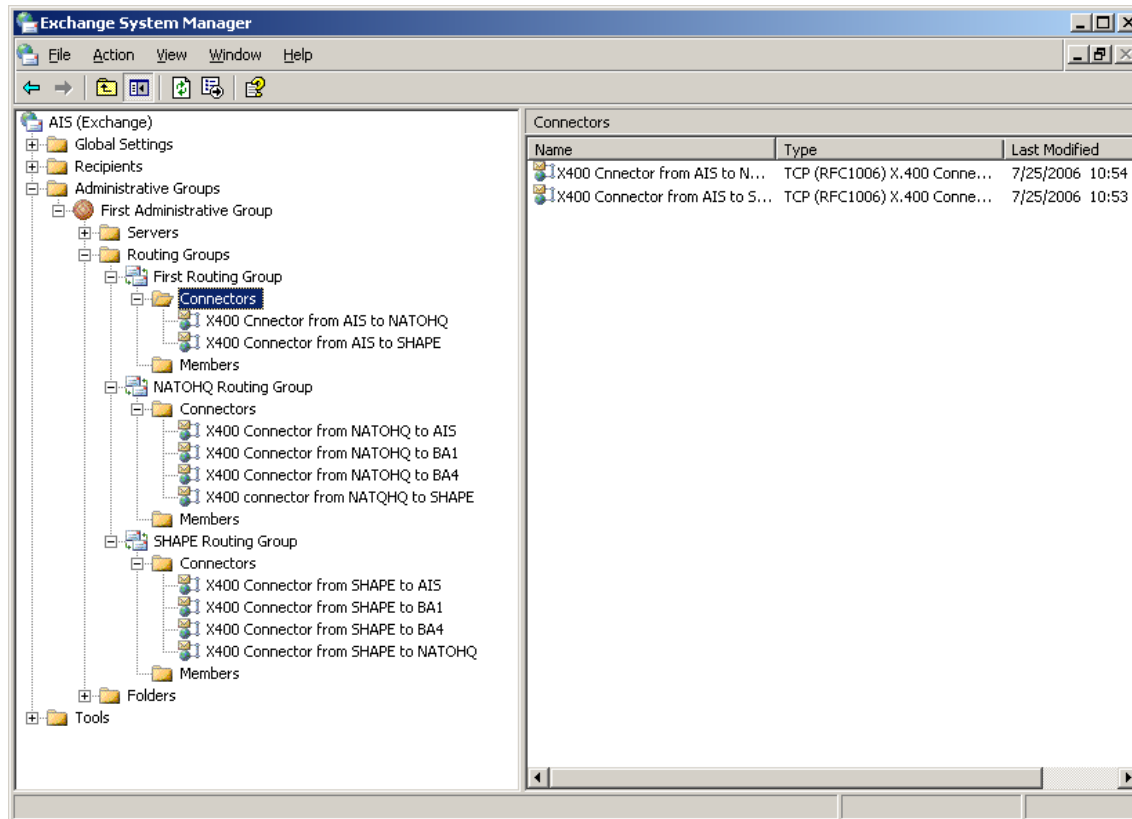
Create X400 Service Transport Stack:

- Per the CommPower TREX Establishing X400 Service Transport Stack & X400 Connectors Guide
 - Create the X400 Service Transport Stack for each domain (i.e. BBAD, MMHS1, MMHS2)



Create X400 Connectors:

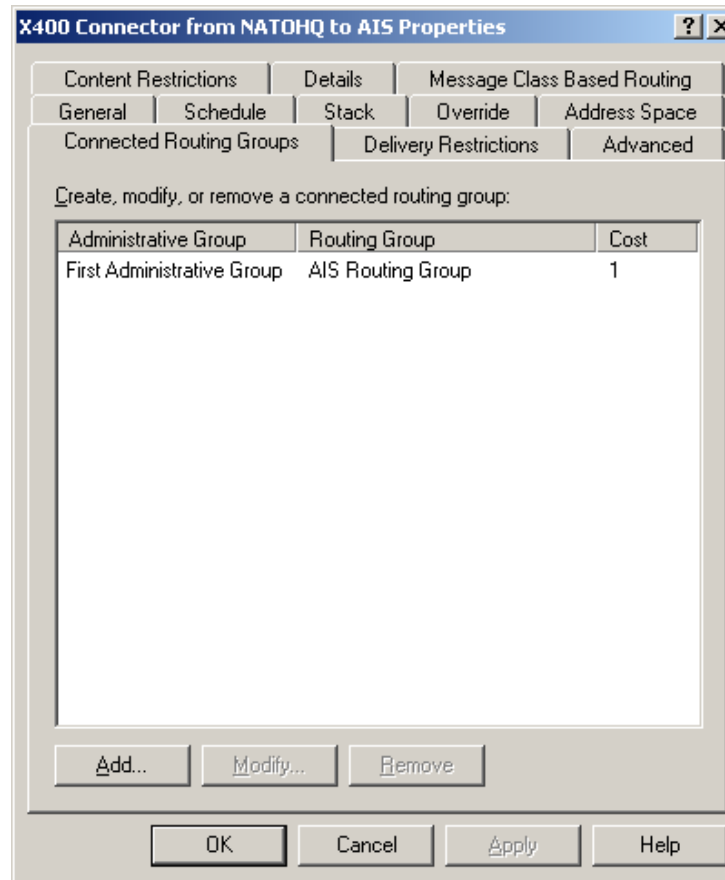
- For each Routing Group > expand Connectors
- Per the CommPower TREX Establishing X400 Service Transport Stack & X400 Connectors Guide
 - Create and configure the applicable X400 Connectors (as exempld herein):



Connected Routing Group:

For X400 Connectors within the same “umbrella” (e.g., SF/MD or SF/SD) must have the “Connected Routing Group” defined.

In the example given below... “X400 Connector from NATOHQ to AIS” the “Connected Routing Group” for NATOHQ would be defined with the “AIS Routing Group”.



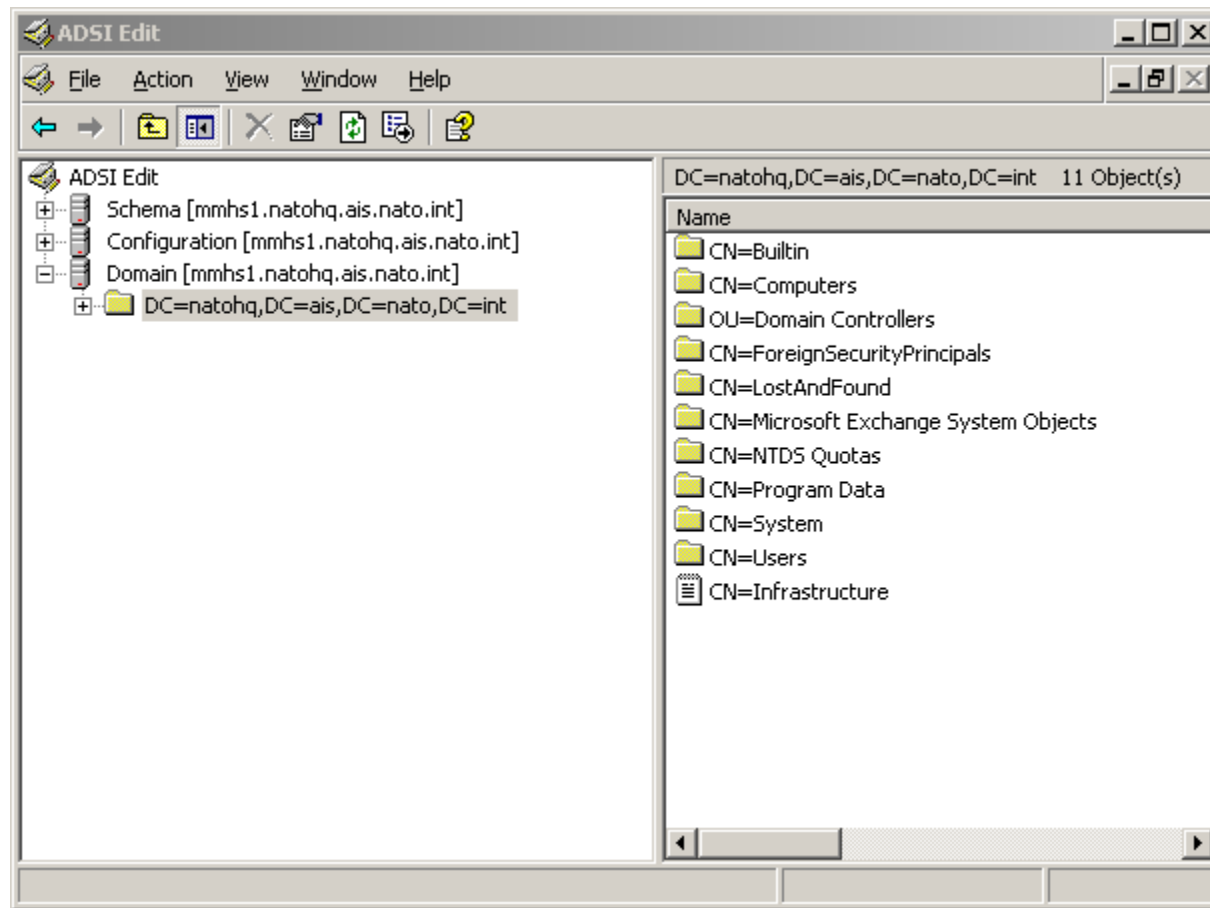
Be sure to define the “Connected Routing Group” for each applicable X400 connector.

Active Directory Permissions for Anonymous Login:

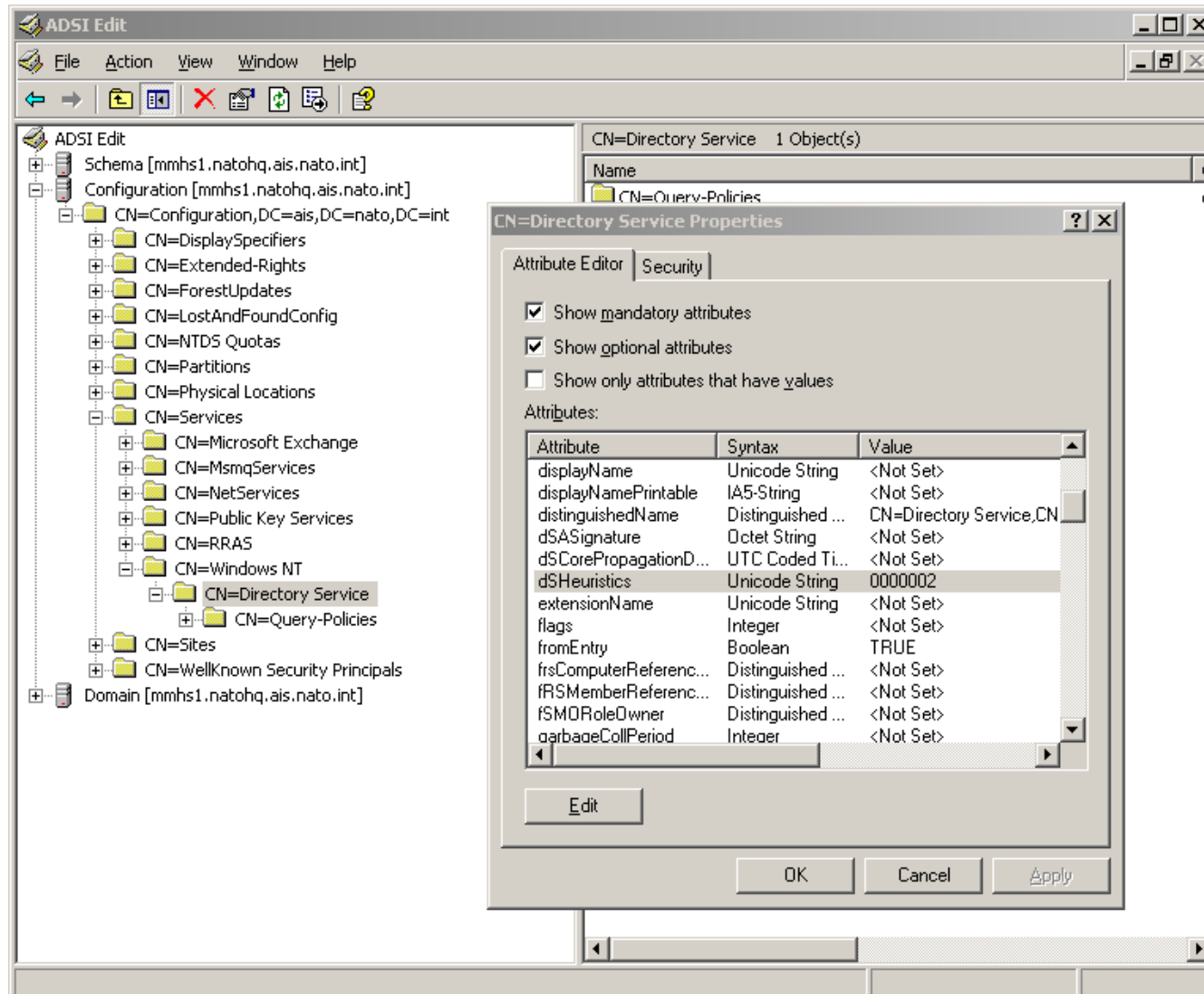
For a SF/MD or SF/SD configuration Active Directory Permissions need to be modified to allow the systems under that particular configuration to access the Active Directory. If these permissions are not defined then access errors will occur within TREX when attempting to access the AD.

Via "adsiedit" → If Domain [domain name] does not exist → right click "ADSI Edit" → select "Connect to" → select "Select a well known Naming Content" → select Domain → select "OK" → right click node under "Domain" → select "Properties" → select "Security" → select "Advanced" → select "Add" → type in "Ano..." → select "Check names" → select "OK" → select "Apply onto" drop down list → select "Container objects" → select/allow "List Contents" → select "OK" → select "Add" → type in "Ano..." → select "Check names" → select "OK" → select "Apply onto" drop down list → select "Organizational Unit objects" → select/allow "List Contents" → select "OK" → select "Add" → type in "Ano..." → select "Check names" → select "OK" → select "Properties" tab → select "Apply onto" drop down list → select "User objects" → select/allow "Read Public Information" (hint... near top of pull down list) → select "OK" → select "Add" → type in "Ano..." → select "Check names" → select "OK" → select "Properties" tab → select "Apply onto" drop down list → select "User objects" → select/allow "Read Phone and Mail Options" → select "OK" → select "Apply" → select "OK" → select "OK" → exit "adsiedit".

“adsiedit” Path:



Setting “dsHeuristics” Value (Authorizes use of Anonymous Login):



Set Value = 0000002

Remote TREX Configuration:

The “LOCAL SERVICE” & “NETWORK SERVICE” accounts must be present in order for “Remote TREX Configuration > Interrogate” to function correctly.

