# DELEGATED SERVICE PROXY ACCOUNT FOR CA IM TO MANAGE ACTIVE DIRECTORY DOMAIN 2008+

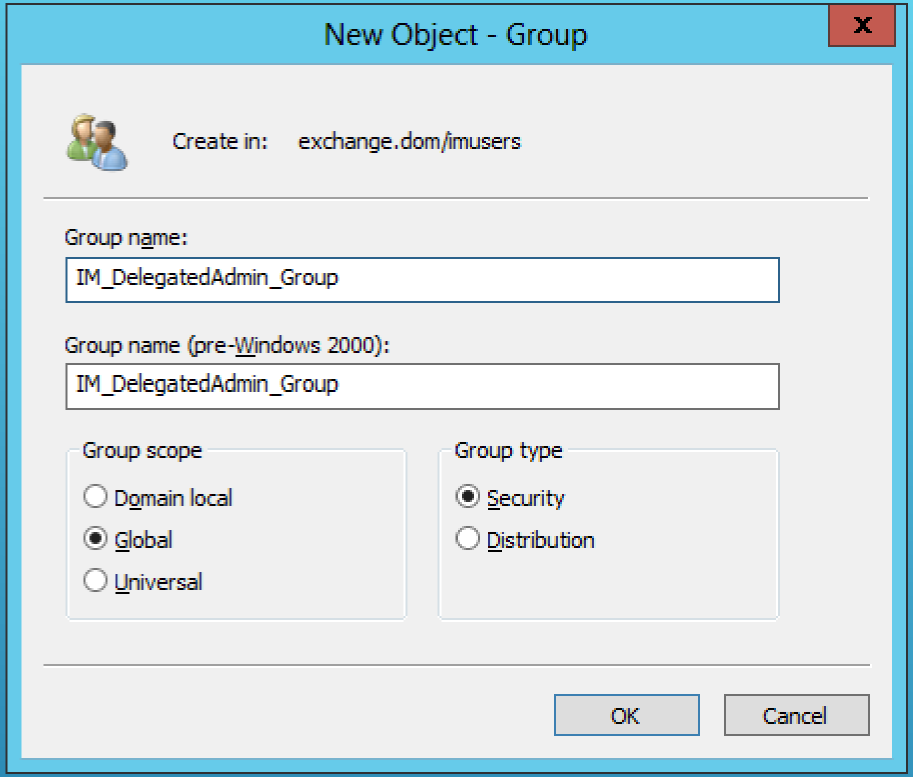
Alan Baugher

Dec 2013

- Client’s active directory domain(s) follows the security policies standard of least privileged access, such that two (2) accounts are created for users that will access the Active Directory solution with higher access than a standard AD users account.

- Active Directory’s default delegation model prevents delegation access from having equal or higher access than Enterprise/Domain Admins built-in accounts, to avoid creating a security gap; that a newly delegated admin could reset other admins passwords to gain higher privileges via account takeover.
  - This default delegation is enforced by AD domain polices.
  - This default delegation is typically enforce by client domain policies for non-built-in accounts. This needs to be validated for each client.

# ASSUMPTIONS



New Object - Group

Create in: exchange.dom/imusers

Group name: IM_DelegatedAdmin_Group

Group name (pre-Windows 2000): IM_DelegatedAdmin_Group

Group scope

○ Domain local

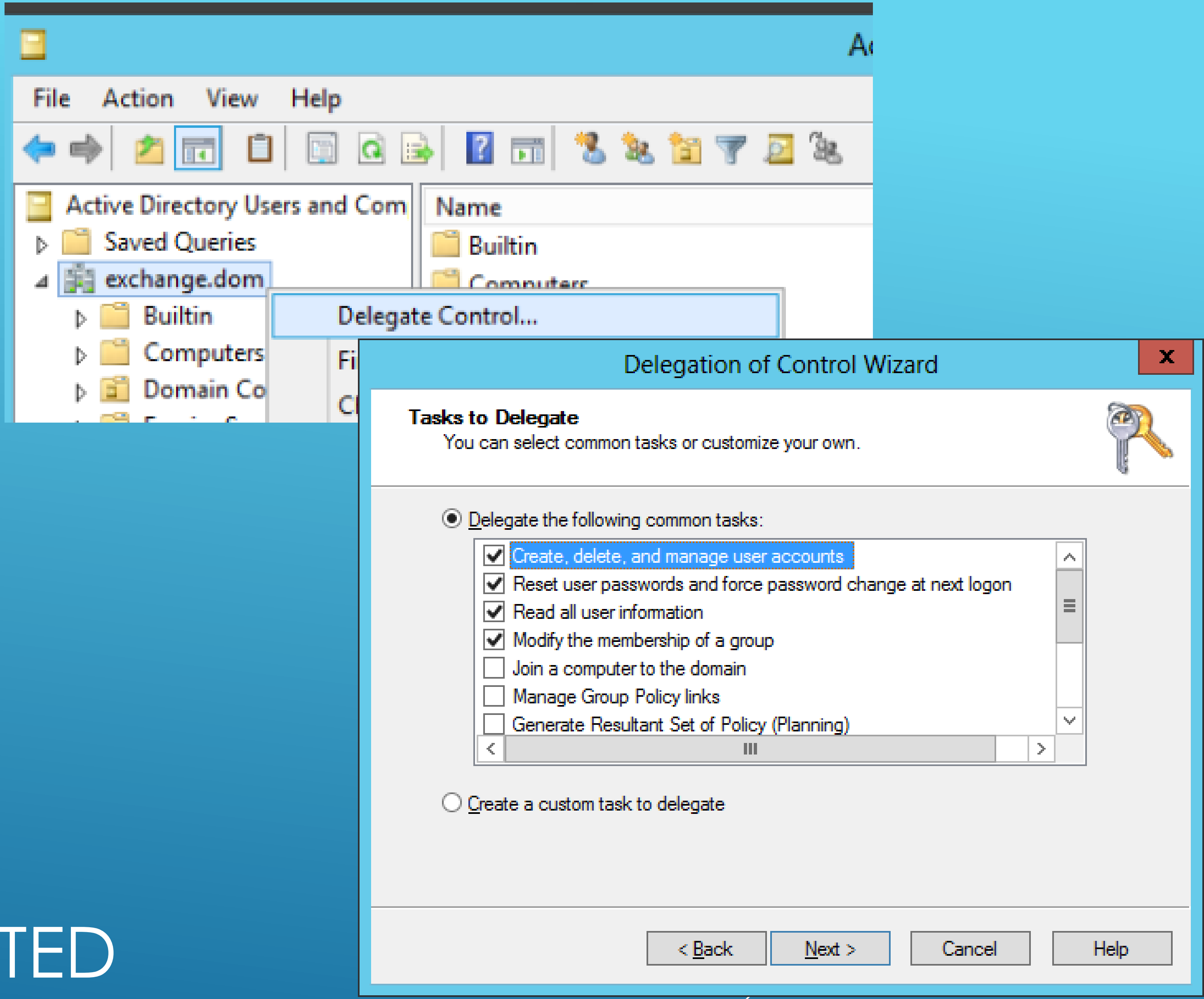
● Global

○ Universal

Group type

● Security

○ Distribution



Delegation of Control Wizard

**Tasks to Delegate**

You can select common tasks or customize your own.

● Delegate the following common tasks:

☑ Create, delete, and manage user accounts

☑ Reset user passwords and force password change at next logon

☑ Read all user information

☑ Modify the membership of a group

□ Join a computer to the domain

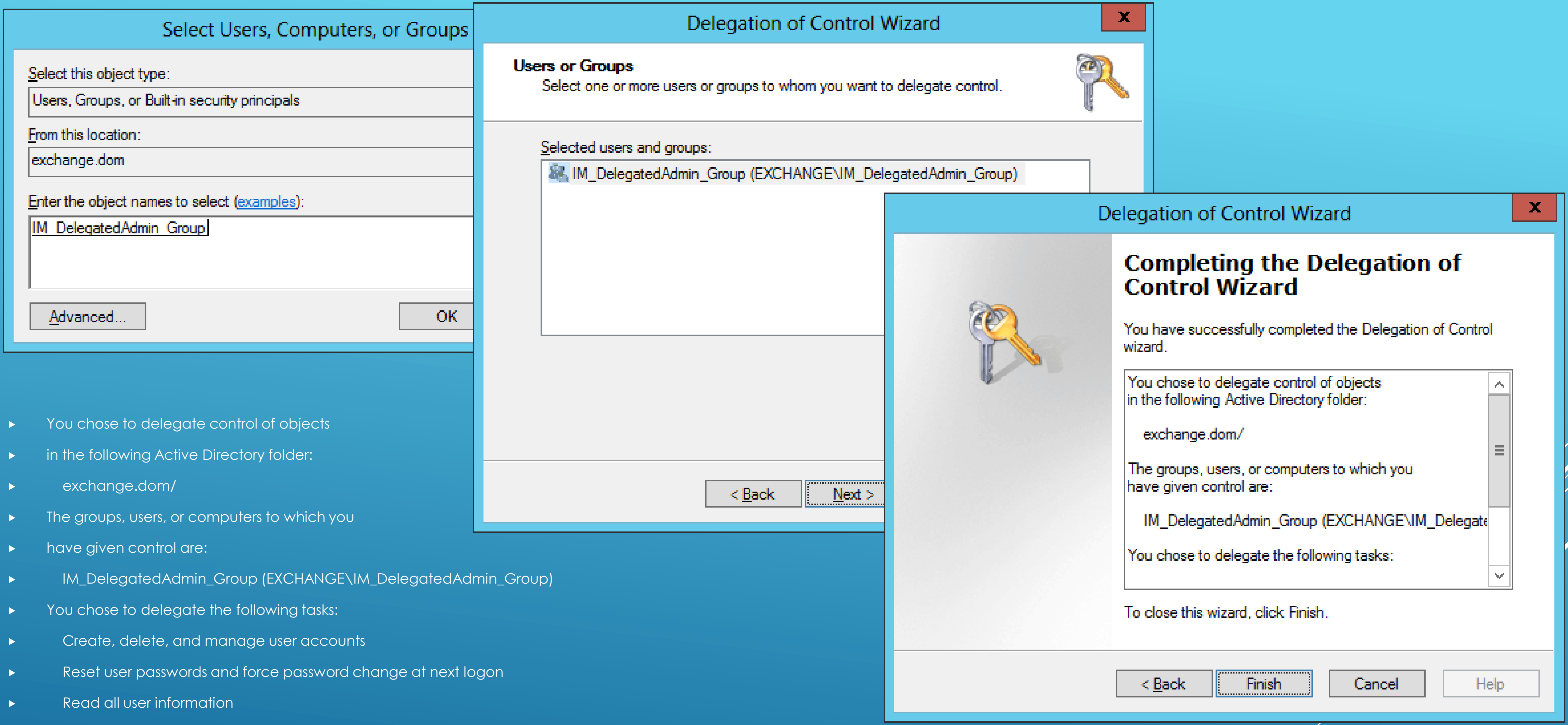
□ Manage Group Policy links

□ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate

# CREATE A NEW DELEGATED ADMIN GROUP & ASSIGN DELEGATED CONTROL TO THE ROOT OF ACTIVE DIRECTORY DOMAIN

# ASSIGN CRUD SERVICES TO NEW GROUP



Select Users, Computers, or Groups

Select this object type:

Users, Groups, or Built-in security principals

From this location:

exchange.dom

Enter the object names to select (examples):

IM_DelegatedAdmin_Group

Delegation of Control Wizard

**Users or Groups**

Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

IM_DelegatedAdmin_Group (EXCHANGE\IM_DelegatedAdmin_Group)

Delegation of Control Wizard

**Completing the Delegation of Control Wizard**

You have successfully completed the Delegation of Control wizard.

You chose to delegate control of objects
in the following Active Directory folder:

exchange.dom/

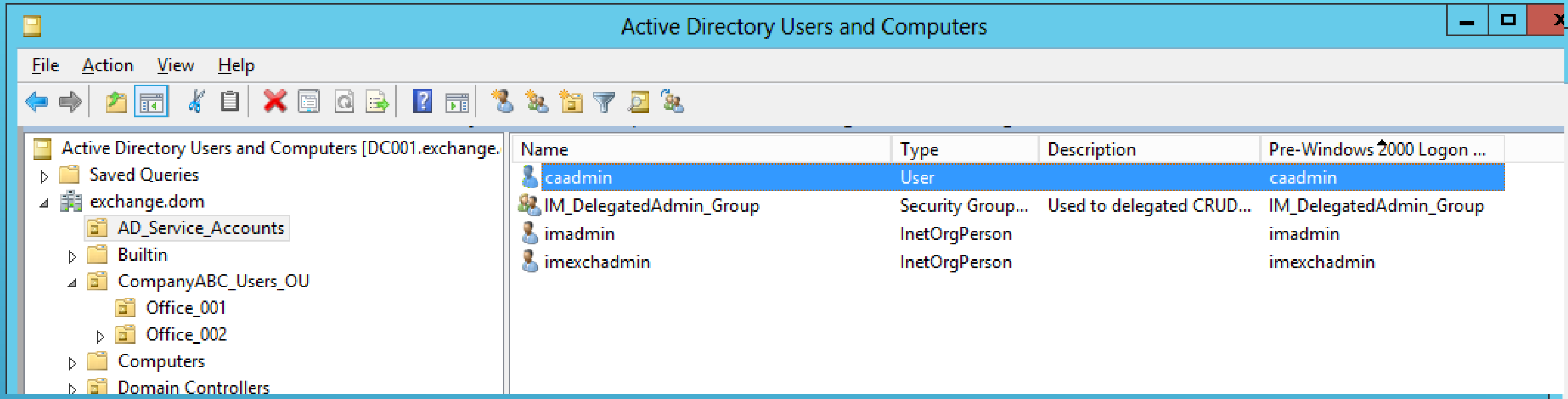
The groups, users, or computers to which you
have given control are:

IM_DelegatedAdmin_Group (EXCHANGE\IM_Delegate

You chose to delegate the following tasks:

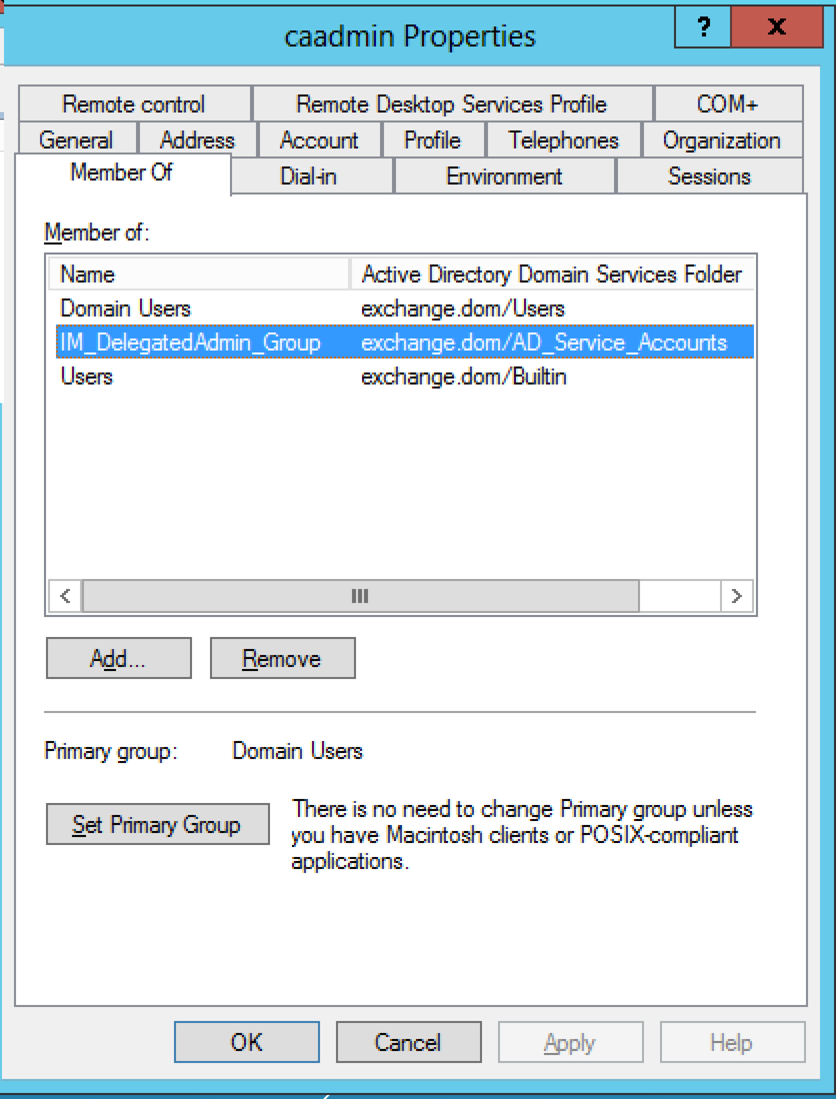
To close this wizard, click Finish.

- You chose to delegate control of objects
- in the following Active Directory folder:
- exchange.dom/
- The groups, users, or computers to which you
- have given control are:
- IM_DelegatedAdmin_Group (EXCHANGE\IM_DelegatedAdmin_Group)
- You chose to delegate the following tasks:
- Create, delete, and manage user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Modify the membership of a group



- Active Directory Users and Computers [DC001.exchange.
  - Saved Queries
  - exchange.dom
    - AD_Service_Accounts
    - Builtin
    - CompanyABC_Users_OU
      - Office_001
      - Office_002
    - Computers
    - Domain Controllers

| Name | Type | Description | Pre-Windows 2000 Logon ... |
|---|---|---|---|
| caadmin | User | | caadmin |
| IM_DelegatedAdmin_Group | Security Group... | Used to delegated CRUD... | IM_DelegatedAdmin_Group |
| imadmin | InetOrgPerson | | imadmin |
| imexchadmin | InetOrgPerson | | imexchadmin |



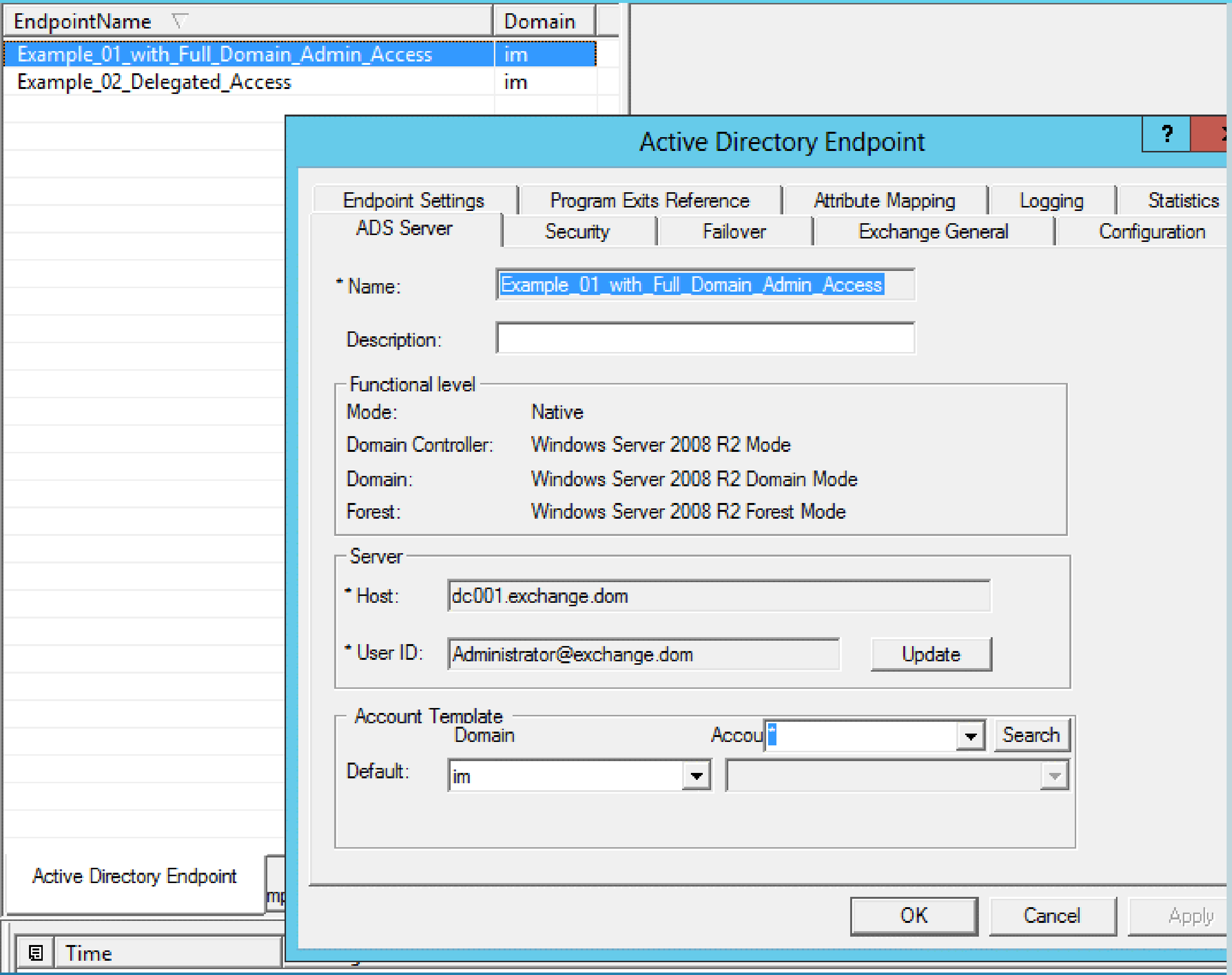
Member of:

| Name | Active Directory Domain Services Folder |
|---|---|
| Domain Users | exchange.dom/Users |
| IM_DelegatedAdmin_Group | exchange.dom/AD_Service_Accounts |
| Users | exchange.dom/Builtin |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

# CREATE USER AND ASSIGN MEMBERSHIP TO NEW AD GROUP



| EndpointName | Domain |
|---|---|
| Example_01_with_Full_Domain_Admin_Access | im |
| Example_02_Delegated_Access | im |

Active Directory Endpoint

* Name: Example_01_with_Full_Domain_Admin_Access

Description:

Functional level

| | |
|---|---|
| Mode: | Native |
| Domain Controller: | Windows Server 2008 R2 Mode |
| Domain: | Windows Server 2008 R2 Domain Mode |
| Forest: | Windows Server 2008 R2 Forest Mode |

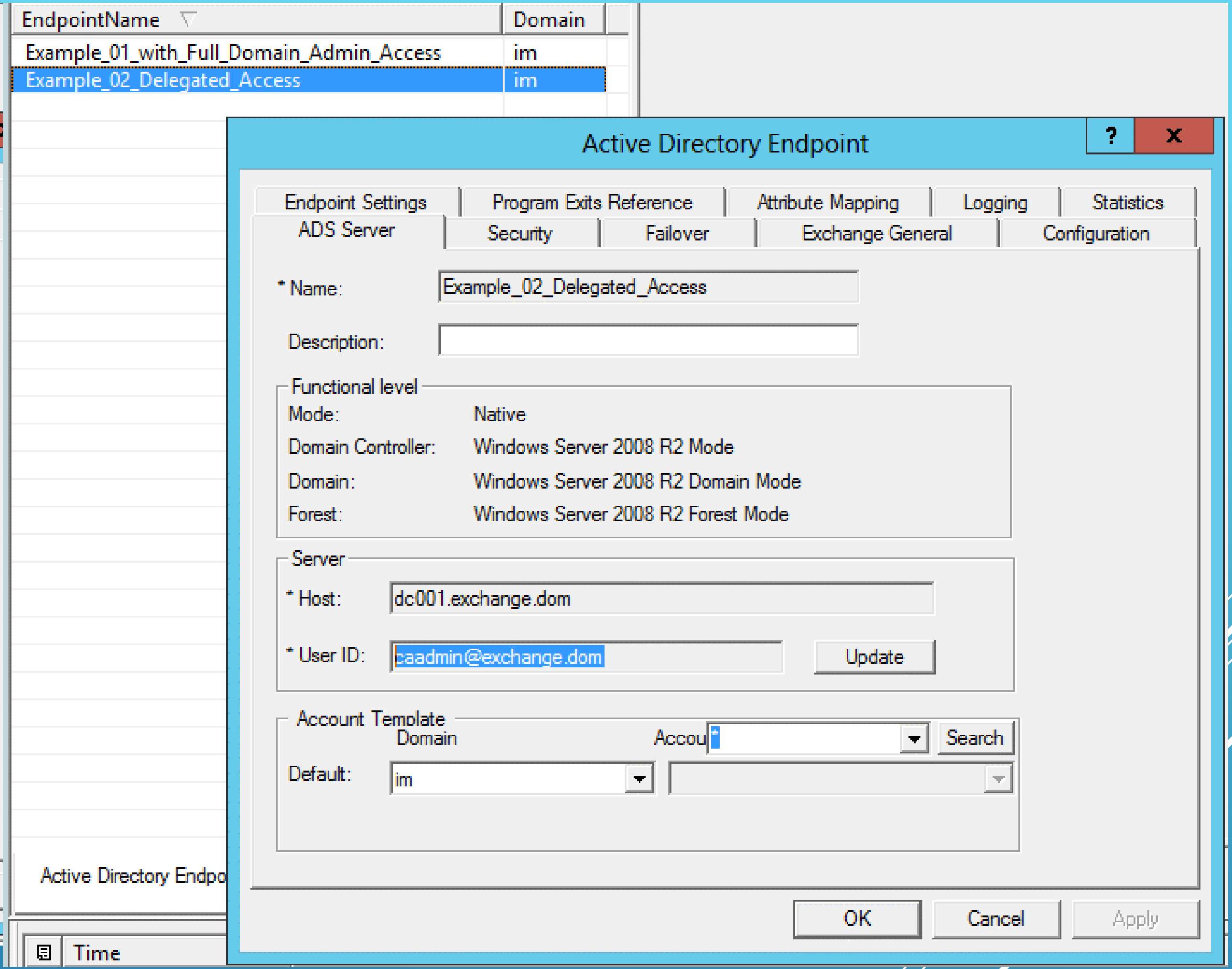
Server

* Host: dc001.exchange.dom

* User ID: Administrator@exchange.dom

Account Template

Default: Domain im



| EndpointName | Domain |
|---|---|
| Example_01_with_Full_Domain_Admin_Access | im |
| Example_02_Delegated_Access | im |

Active Directory Endpoint

* Name: Example_02_Delegated_Access

Description:

Functional level

| | |
|---|---|
| Mode: | Native |
| Domain Controller: | Windows Server 2008 R2 Mode |
| Domain: | Windows Server 2008 R2 Domain Mode |
| Forest: | Windows Server 2008 R2 Forest Mode |

Server

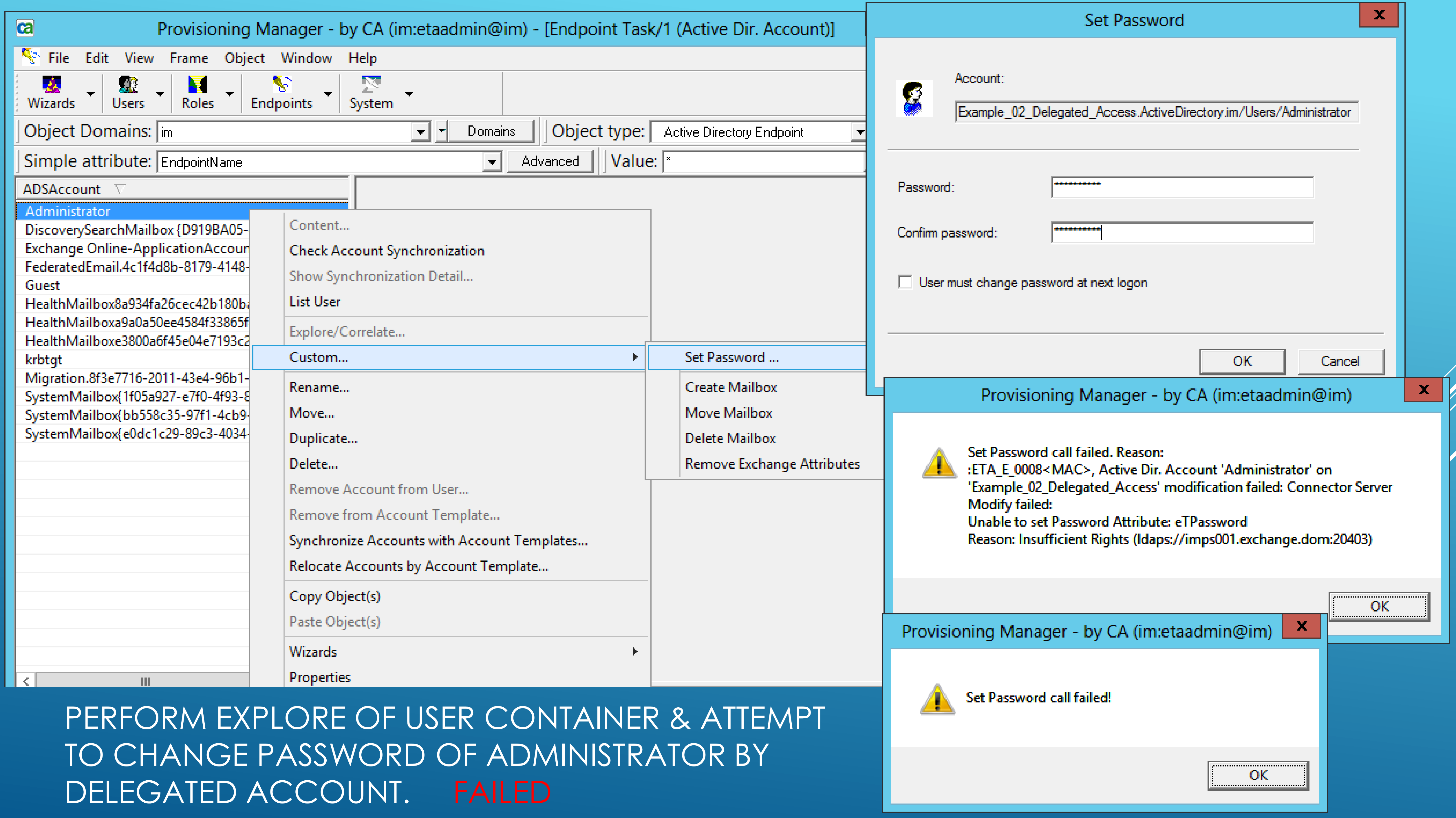
* Host: dc001.exchange.dom

* User ID: caadmin@exchange.dom

Account Template

Default: Domain im

# DEFAULT ADMINISTRATOR VERSUS DELEGATED ADMIN ACCOUNT


Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Dir. Account)]
File
Edit
View
Frame
Object
Window
Help
Wizards
Users
Roles
Endpoints
System
Domains
Advanced
ADSAccount
Content...
Check Account Synchronization
Show Synchronization Detail...
List User
Explore/Correlate...
Custom...
Rename...
Move...
Duplicate...
Delete...
Remove Account from User...
Remove from Account Template...
Synchronize Accounts with Account Templates...
Relocate Accounts by Account Template...
Copy Object(s)
Paste Object(s)
Wizards
Properties
Set Password ...
Create Mailbox
Move Mailbox
Delete Mailbox
Remove Exchange Attributes
Set Password
OK
Cancel
Provisioning Manager - by CA (im:etaadmin@im)
OK
Provisioning Manager - by CA (im:etaadmin@im)
OK

Object Domains: im

Object type: Active Directory Endpoint

Simple attribute: EndpointName

Value: *

Administrator
DiscoverySearchMailbox{D919BA05-
Exchange Online-ApplicationAccour
FederatedEmail.4c1f4d8b-8179-4148-
Guest
HealthMailbox8a934fa26cec42b180b
HealthMailboxa9a0a50ee4584f33865f
HealthMailboxe3800a6f45e04e7193c2
krbtgt
Migration.8f3e7716-2011-43e4-96b1-
SystemMailbox{1f05a927-e7f0-4f93-8
SystemMailbox{bb558c35-97f1-4cb9-
SystemMailbox{e0dc1c29-89c3-4034-

Account: Example_02_Delegated_Access.ActiveDirectory.im/Users/Administrator

Password: ***********

Confirm password: ***********

☐ User must change password at next logon

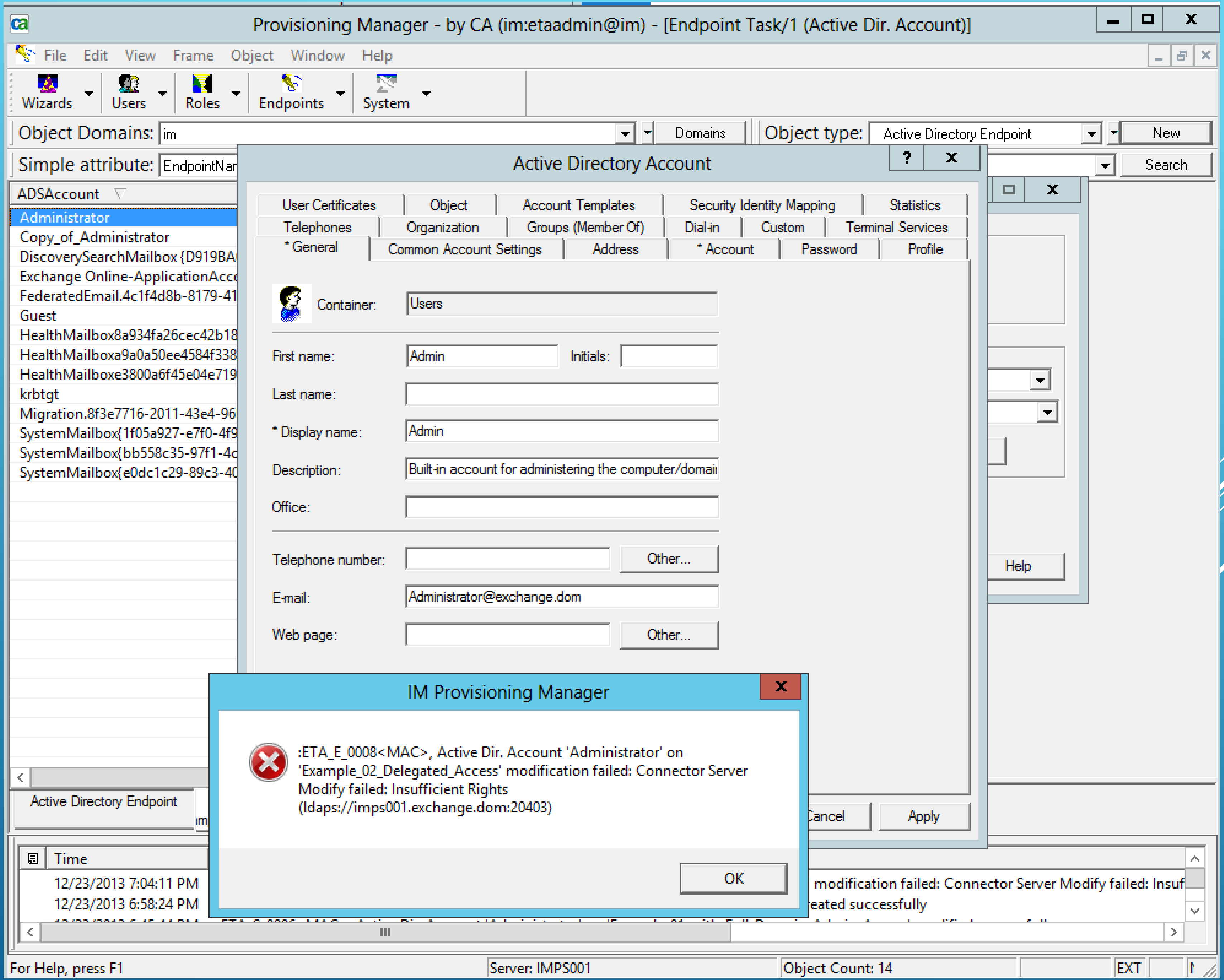
Set Password call failed. Reason:
:ETA_E_0008<MAC>, Active Dir. Account 'Administrator' on 'Example_02_Delegated_Access' modification failed: Connector Server Modify failed:
Unable to set Password Attribute: eTPassword
Reason: Insufficient Rights (ldaps://imps001.exchange.dom:20403)

Set Password call failed!

PERFORM EXPLORE OF USER CONTAINER & ATTEMPT TO CHANGE PASSWORD OF ADMINISTRATOR BY DELEGATED ACCOUNT. FAILED

# ATTEMPT A MODIFY OPERATION - CHANGE FIRST NAME FIELD OF ADMINISTRATOR

FAILED



Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Dir. Account)]

Object Domains: im

Object type: Active Directory Endpoint

Simple attribute: EndpointNar

ADSAccount

Administrator
Copy_of_Administrator
DiscoverySearchMailbox {D919BA
Exchange Online-ApplicationAcc
FederatedEmail.4c1f4d8b-8179-41
Guest
HealthMailbox8a934fa26cec42b18
HealthMailboxa9a0a50ee4584f338
HealthMailboxe3800a6f45e04e719
krbtgt
Migration.8f3e7716-2011-43e4-96
SystemMailbox{1f05a927-e7f0-4f9
SystemMailbox{bb558c35-97f1-4c
SystemMailbox{e0dc1c29-89c3-40

Active Directory Account

Container: Users

First name: Admin

Initials:

Last name:

* Display name: Admin

Description: Built-in account for administering the computer/domai

Office:

Telephone number:

E-mail: Administrator@exchange.dom

Web page:

IM Provisioning Manager

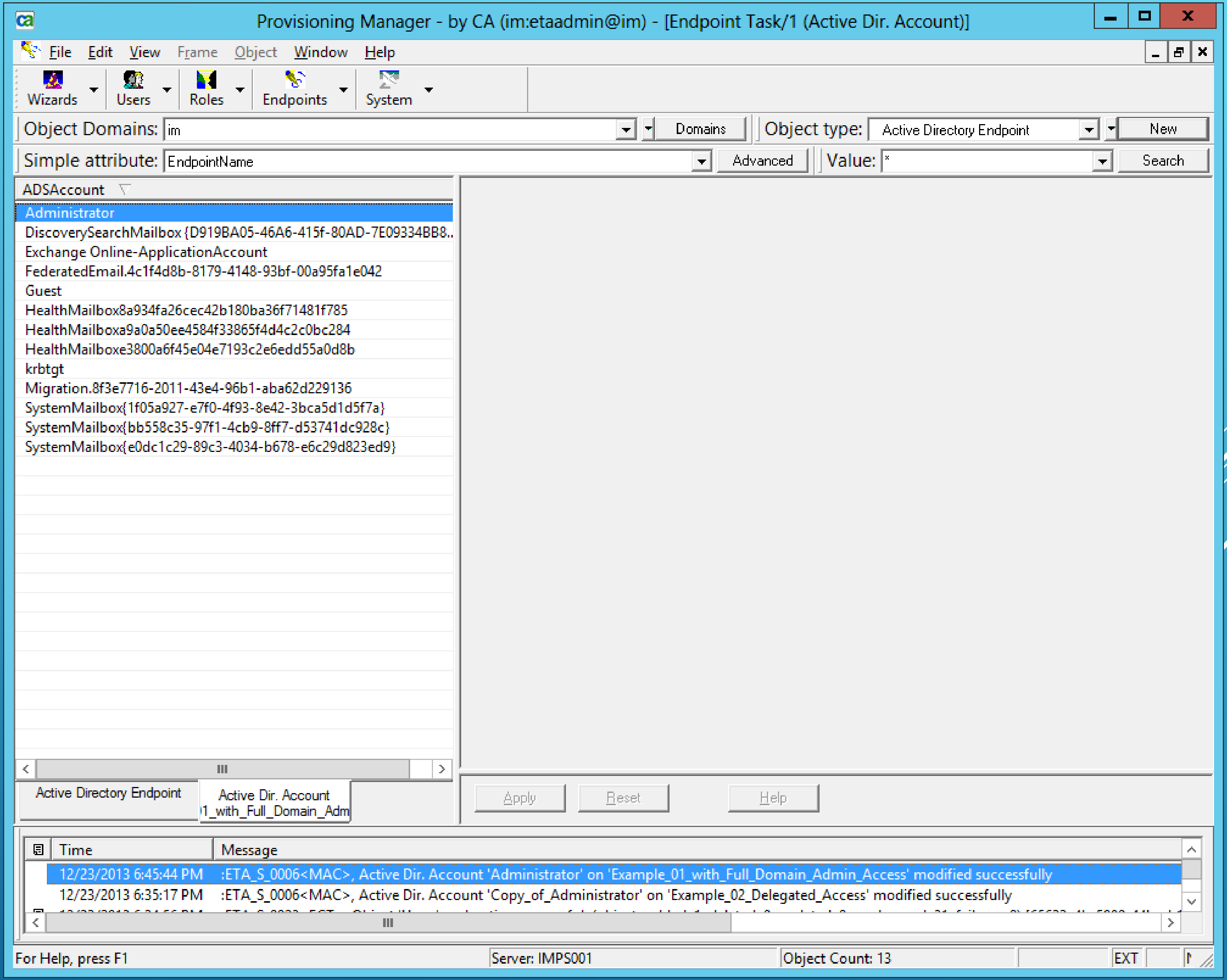
:ETA_E_0008<MAC>, Active Dir. Account 'Administrator' on 'Example_02_Delegated_Access' modification failed: Connector Server Modify failed: Insufficient Rights (ldaps://imps001.exchange.dom:20403)

| Time | |
|---|---|
| 12/23/2013 7:04:11 PM | modification failed: Connector Server Modify failed: Insuf |
| 12/23/2013 6:58:24 PM | reated successfully |

For Help, press F1 — Server: IMPS001 — Object Count: 14

# VALIDATE THAT FULL ADMINISTRATOR HAS NO ISSUE WITH CHANGING PASSWORD (SAME PROCESS ON PRIOR SLIDE)

# SUCCESS MESSAGE AT BOTTOM OF GUI


Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Dir. Account)]
File Edit View Frame Object Window Help
Wizards
Users
Roles
Endpoints
System
Domains
New
Advanced
Search
ADSAccount
Active Directory Endpoint
Active Dir. Account
1_with_Full_Domain_Adm
Apply
Reset
Help

Object Domains: im

Object type: Active Directory Endpoint

Simple attribute: EndpointName

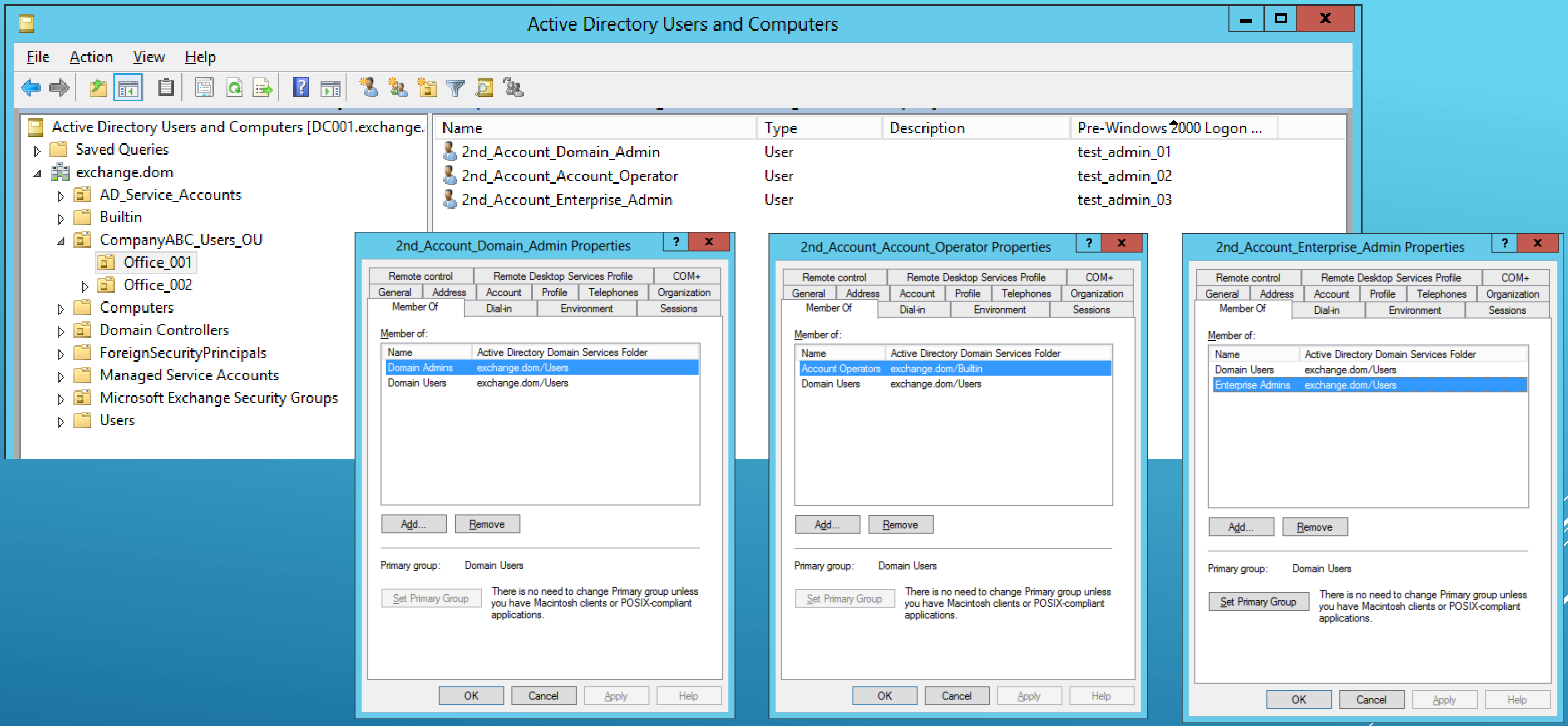
Value: *

ADSAccount:

- Administrator
- DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB8..
- Exchange Online-ApplicationAccount
- FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042
- Guest
- HealthMailbox8a934fa26cec42b180ba36f71481f785
- HealthMailboxa9a0a50ee4584f33865f4d4c2c0bc284
- HealthMailboxe3800a6f45e04e7193c2e6edd55a0d8b
- krbtgt
- Migration.8f3e7716-2011-43e4-96b1-aba62d229136
- SystemMailbox{1f05a927-e7f0-4f93-8e42-3bca5d1d5f7a}
- SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}
- SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}

```
Time                    Message
12/23/2013 6:45:44 PM   :ETA_S_0006<MAC>, Active Dir. Account 'Administrator' on 'Example_01_with_Full_Domain_Admin_Access' modified successfully
12/23/2013 6:35:17 PM   :ETA_S_0006<MAC>, Active Dir. Account 'Copy_of_Administrator' on 'Example_02_Delegated_Access' modified successfully
```

For Help, press F1 | Server: IMPS001 | Object Count: 13 | EXT



| Name | Type | Description | Pre-Windows 2000 Logon ... |
|---|---|---|---|
| 2nd_Account_Domain_Admin | User | | test_admin_01 |
| 2nd_Account_Account_Operator | User | | test_admin_02 |
| 2nd_Account_Enterprise_Admin | User | | test_admin_03 |

2nd_Account_Domain_Admin Properties

Member of:

| Name | Active Directory Domain Services Folder |
|---|---|
| Domain Admins | exchange.dom/Users |
| Domain Users | exchange.dom/Users |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

2nd_Account_Account_Operator Properties

Member of:

| Name | Active Directory Domain Services Folder |
|---|---|
| Account Operators | exchange.dom/Builtin |
| Domain Users | exchange.dom/Users |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

2nd_Account_Enterprise_Admin Properties

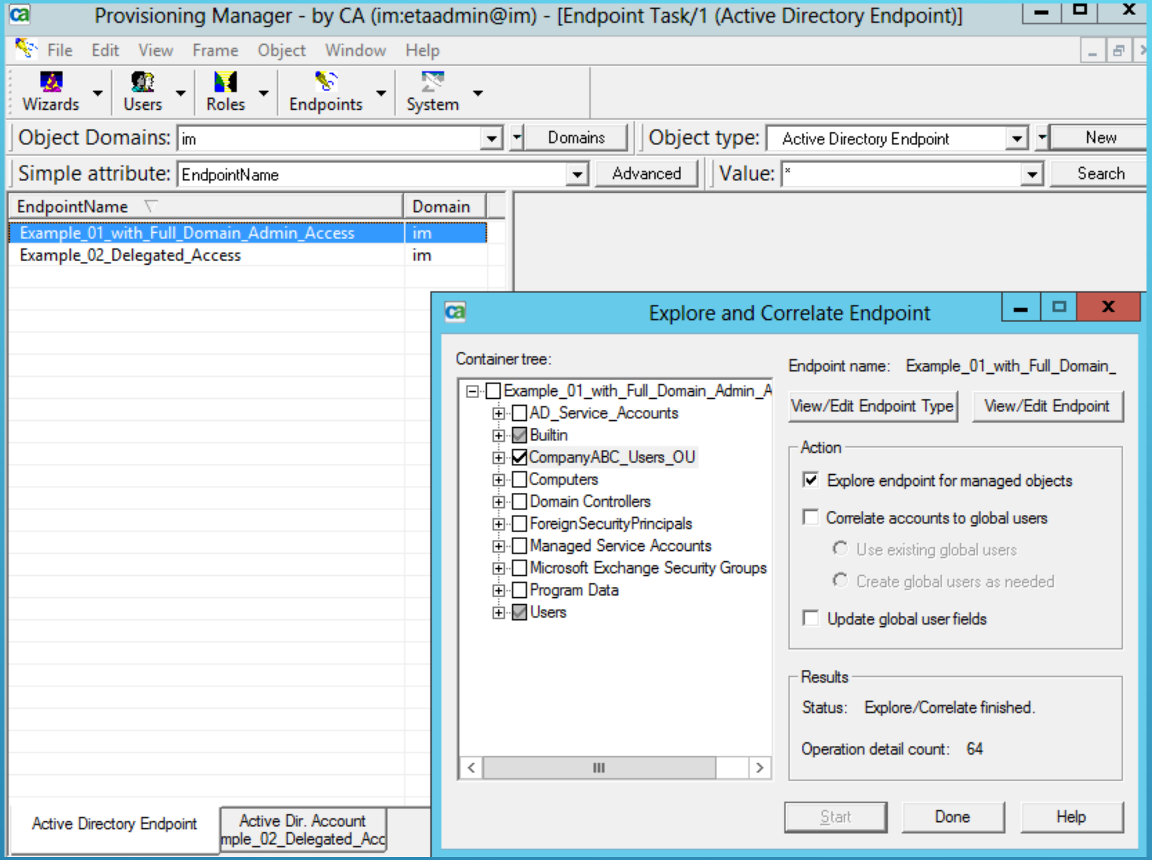
Member of:

| Name | Active Directory Domain Services Folder |
|---|---|
| Domain Users | exchange.dom/Users |
| Enterprise Admins | exchange.dom/Users |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

# CREATE THREE TEST ADMIN ACCOUNTS TO CHECK DEFAULT AD GROUP /DOMAIN POLICIES



Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Directory Endpoint)]

Object Domains: im
Object type: Active Directory Endpoint
Simple attribute: EndpointName
Value: *

| EndpointName | Domain |
|---|---|
| Example_01_with_Full_Domain_Admin_Access | im |
| Example_02_Delegated_Access | im |

Active Directory Endpoint | Active Dir. Account mple_02_Delegated_Acc

Explore and Correlate Endpoint

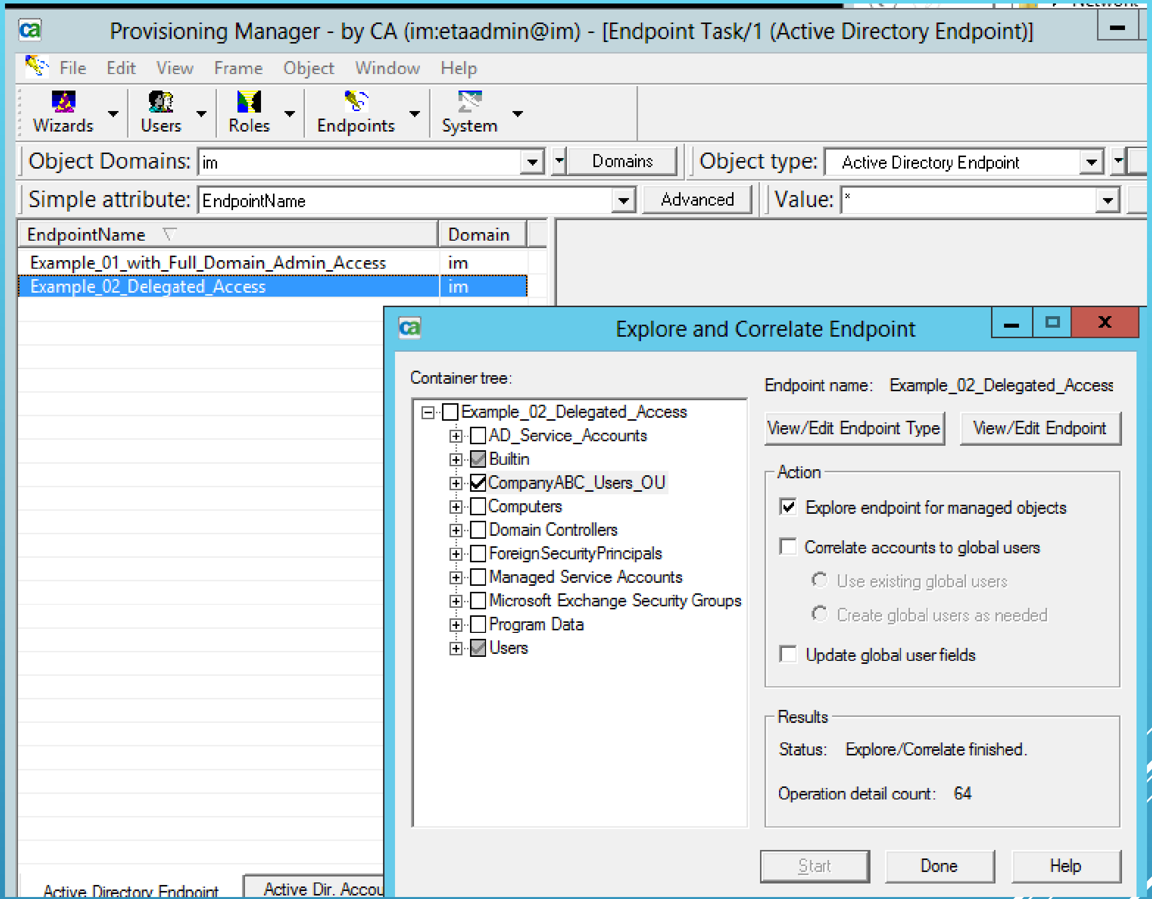
Container tree:

- □ Example_01_with_Full_Domain_Admin_A
  - □ AD_Service_Accounts
  - ☑ Builtin
  - ☑ CompanyABC_Users_OU
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Managed Service Accounts
  - □ Microsoft Exchange Security Groups
  - □ Program Data
  - ☑ Users

Endpoint name: Example_01_with_Full_Domain_

Action
- ☑ Explore endpoint for managed objects
- □ Correlate accounts to global users
  - ○ Use existing global users
  - ○ Create global users as needed
- □ Update global user fields

Results
Status: Explore/Correlate finished.
Operation detail count: 64



Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Directory Endpoint)]

Object Domains: im
Object type: Active Directory Endpoint
Simple attribute: EndpointName
Value: *

| EndpointName | Domain |
|---|---|
| Example_01_with_Full_Domain_Admin_Access | im |
| Example_02_Delegated_Access | im |

Active Directory Endpoint | Active Dir. Accou

Explore and Correlate Endpoint

Container tree:

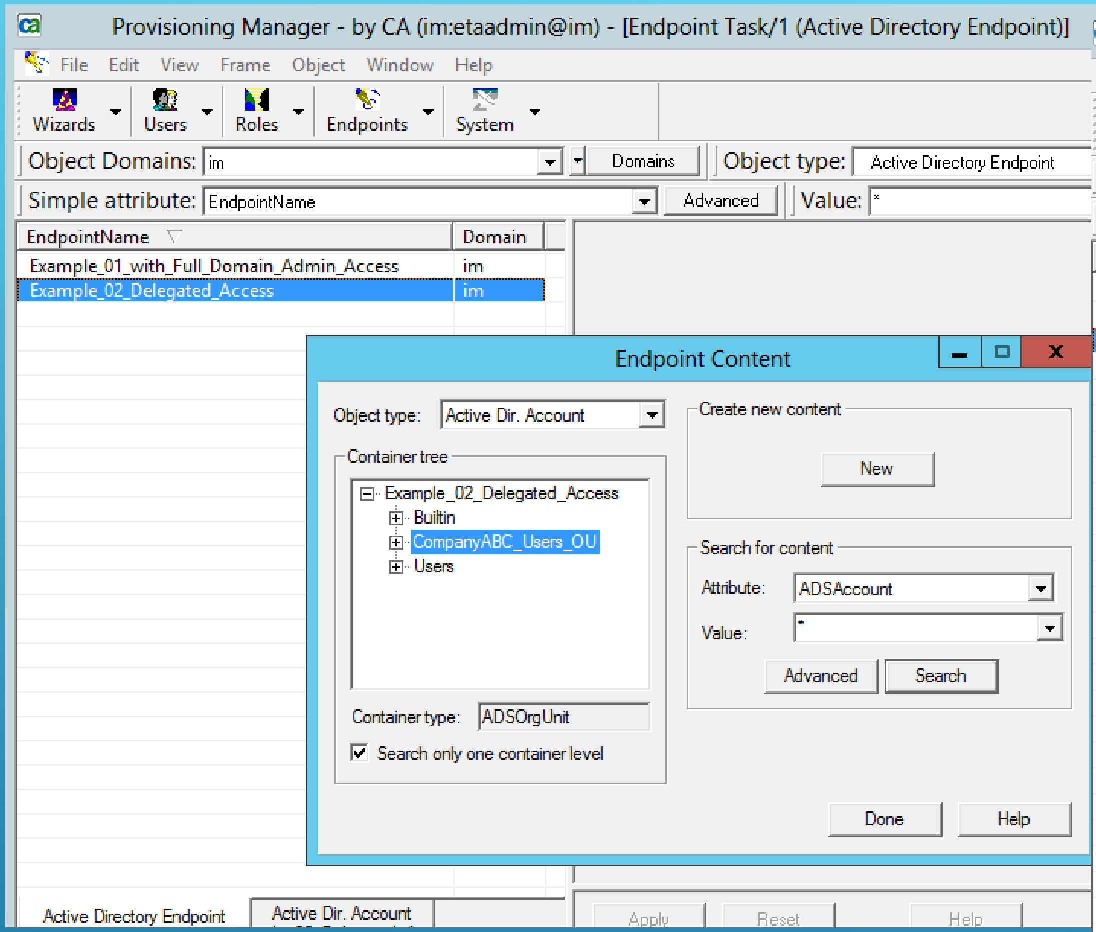
- □ Example_02_Delegated_Access
  - □ AD_Service_Accounts
  - ☑ Builtin
  - ☑ CompanyABC_Users_OU
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Managed Service Accounts
  - □ Microsoft Exchange Security Groups
  - □ Program Data
  - ☑ Users

Endpoint name: Example_02_Delegated_Access

Action
- ☑ Explore endpoint for managed objects
- □ Correlate accounts to global users
  - ○ Use existing global users
  - ○ Create global users as needed
- □ Update global user fields

Results
Status: Explore/Correlate finished.
Operation detail count: 64

# PERFORM EXPLORE OF OU FOR TEST ACCOUNTS


Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Directory Endpoint)]

Object Domains: im

Object type: Active Directory Endpoint

Simple attribute: EndpointName

Value: *

| EndpointName | Domain |
|---|---|
| Example_01_with_Full_Domain_Admin_Access | im |
| Example_02_Delegated_Access | im |

Endpoint Content

Object type: Active Dir. Account

Container tree

- Example_02_Delegated_Access
  - Builtin
  - CompanyABC_Users_OU
  - Users

Container type: ADSOrgUnit

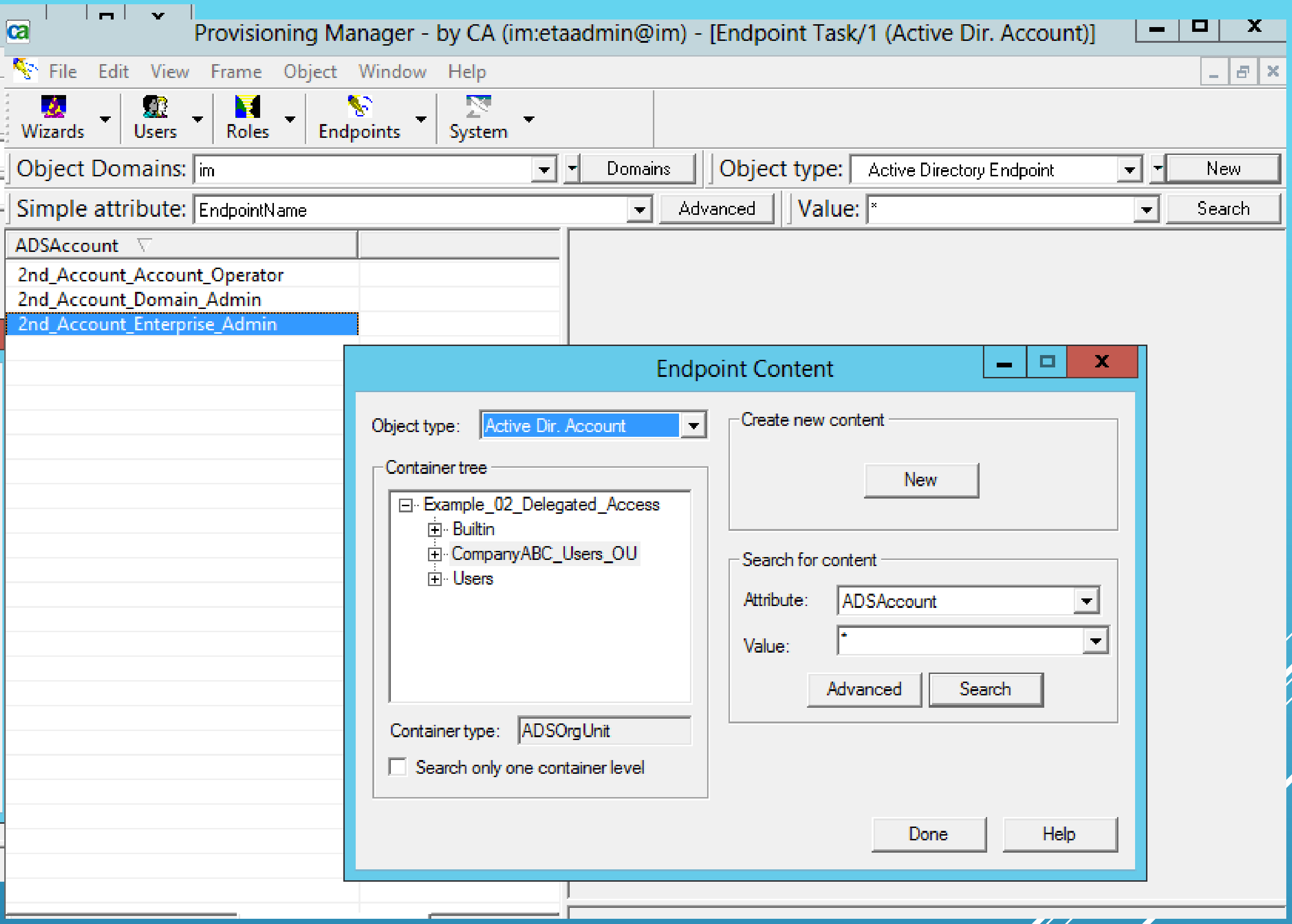
☑ Search only one container level

Create new content

Search for content

Attribute: ADSAccount

Value: *


Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Dir. Account)]

Object Domains: im

Object type: Active Directory Endpoint

Simple attribute: EndpointName

Value: *

| ADSAccount |
|---|
| 2nd_Account_Account_Operator |
| 2nd_Account_Domain_Admin |
| 2nd_Account_Enterprise_Admin |

Endpoint Content

Object type: Active Dir. Account

Container tree

- Example_02_Delegated_Access
  - Builtin
  - CompanyABC_Users_OU
  - Users

Container type: ADSOrgUnit

□ Search only one container level

Create new content

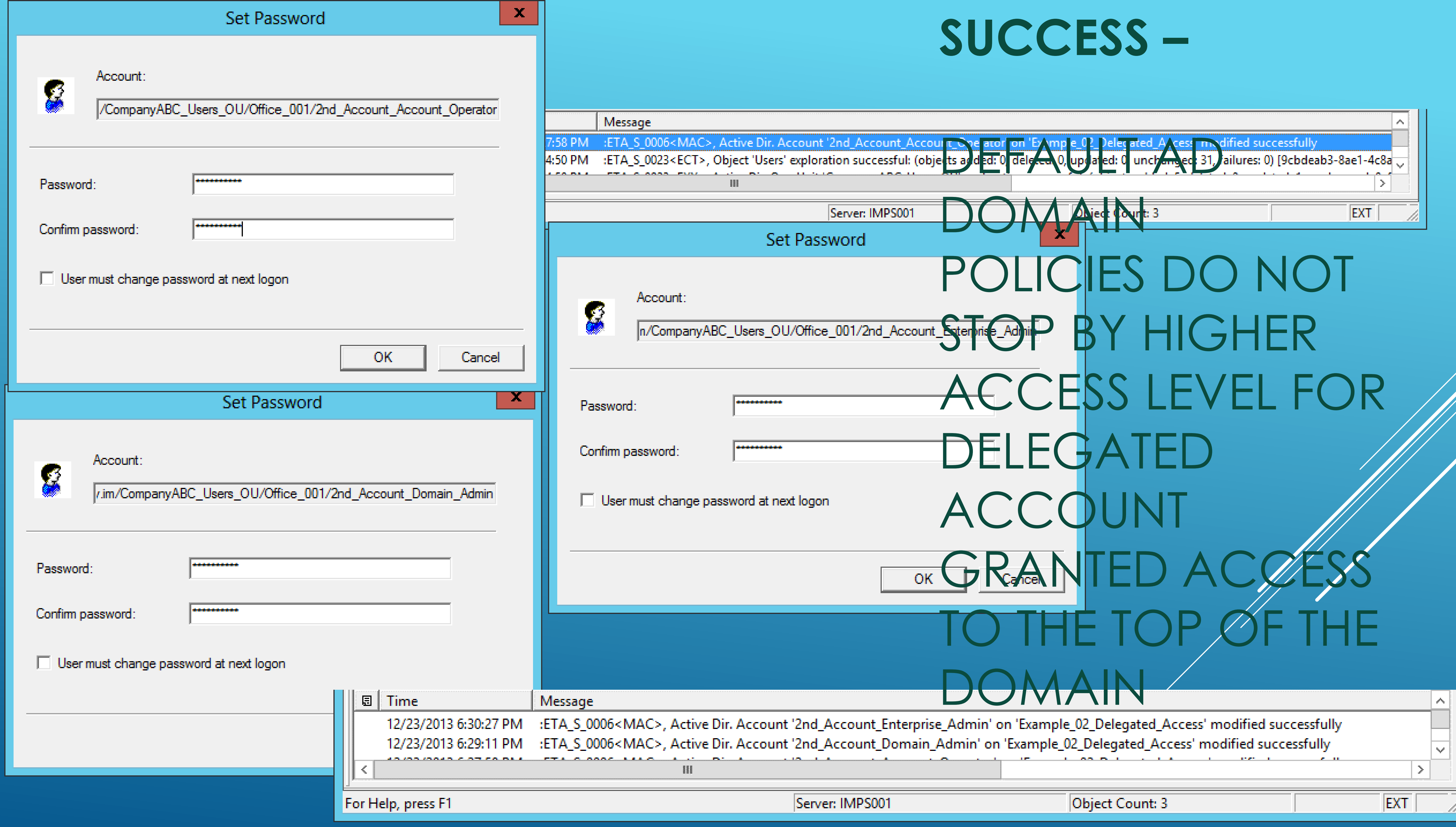
Search for content

Attribute: ADSAccount

Value: *

# SELECT THE OU AND TEST ACCOUNTS TO CHECK WITH THE DELEGATED ADMIN ACCOUNT

# SUCCESS – DEFAULT AD DOMAIN POLICIES DO NOT STOP BY HIGHER ACCESS LEVEL FOR DELEGATED ACCOUNT GRANTED ACCESS TO THE TOP OF THE DOMAIN



Set Password

Account: /CompanyABC_Users_OU/Office_001/2nd_Account_Account_Operator

Password: ***********

Confirm password: ***********

☐ User must change password at next logon

OK Cancel

Set Password

Account: /.im/CompanyABC_Users_OU/Office_001/2nd_Account_Domain_Admin

Password: ***********

Confirm password: ***********

☐ User must change password at next logon

Set Password

Account: n/CompanyABC_Users_OU/Office_001/2nd_Account_Enterprise_Admin

Password: ***********

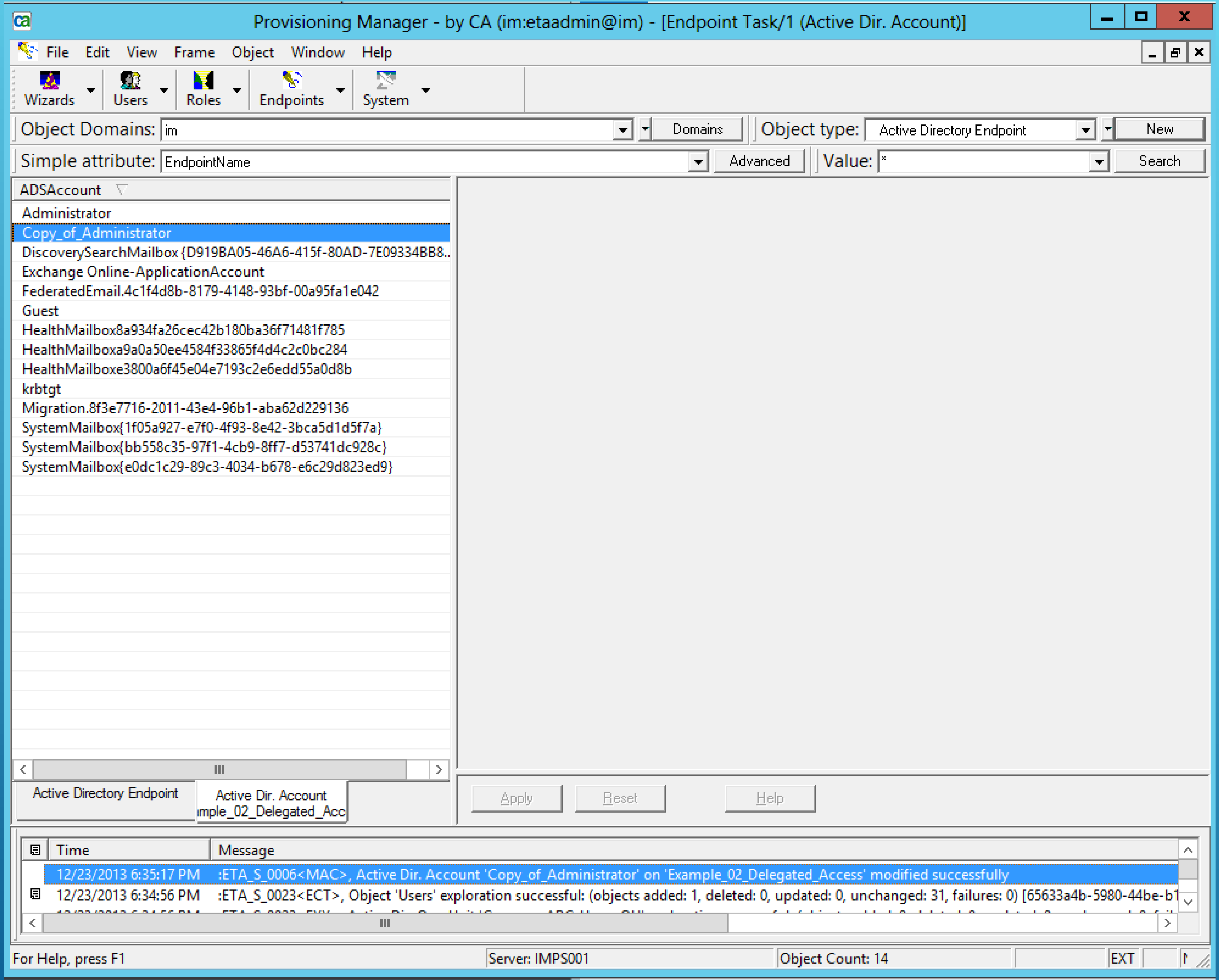
Confirm password: ***********

☐ User must change password at next logon

OK Cancel

```
Message
7:58 PM   :ETA_S_0006<MAC>, Active Dir. Account '2nd_Account_Account_Operator' on 'Example_02_Delegated_Access' modified successfully
4:50 PM   :ETA_S_0023<ECT>, Object 'Users' exploration successful: (objects added: 0, deleted: 0, updated: 0, unchanged: 31, failures: 0) [9cbdeab3-8ae1-4c8a
Server: IMPS001   Object Count: 3   EXT
```

```
Time                   Message
12/23/2013 6:30:27 PM  :ETA_S_0006<MAC>, Active Dir. Account '2nd_Account_Enterprise_Admin' on 'Example_02_Delegated_Access' modified successfully
12/23/2013 6:29:11 PM  :ETA_S_0006<MAC>, Active Dir. Account '2nd_Account_Domain_Admin' on 'Example_02_Delegated_Access' modified successfully
For Help, press F1   Server: IMPS001   Object Count: 3   EXT
```


Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Dir. Account)]
File Edit View Frame Object Window Help
Wizards
Users
Roles
Endpoints
System
Domains
New
Advanced
Search
Apply
Reset
Help

Object Domains: im

Object type: Active Directory Endpoint

Simple attribute: EndpointName

Value: *

ADSAccount

- Administrator
- Copy_of_Administrator
- DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB8..
- Exchange Online-ApplicationAccount
- FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042
- Guest
- HealthMailbox8a934fa26cec42b180ba36f71481f785
- HealthMailboxa9a0a50ee4584f33865f4d4c2c0bc284
- HealthMailboxe3800a6f45e04e7193c2e6edd55a0d8b
- krbtgt
- Migration.8f3e7716-2011-43e4-96b1-aba62d229136
- SystemMailbox{1f05a927-e7f0-4f93-8e42-3bca5d1d5f7a}
- SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}
- SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}

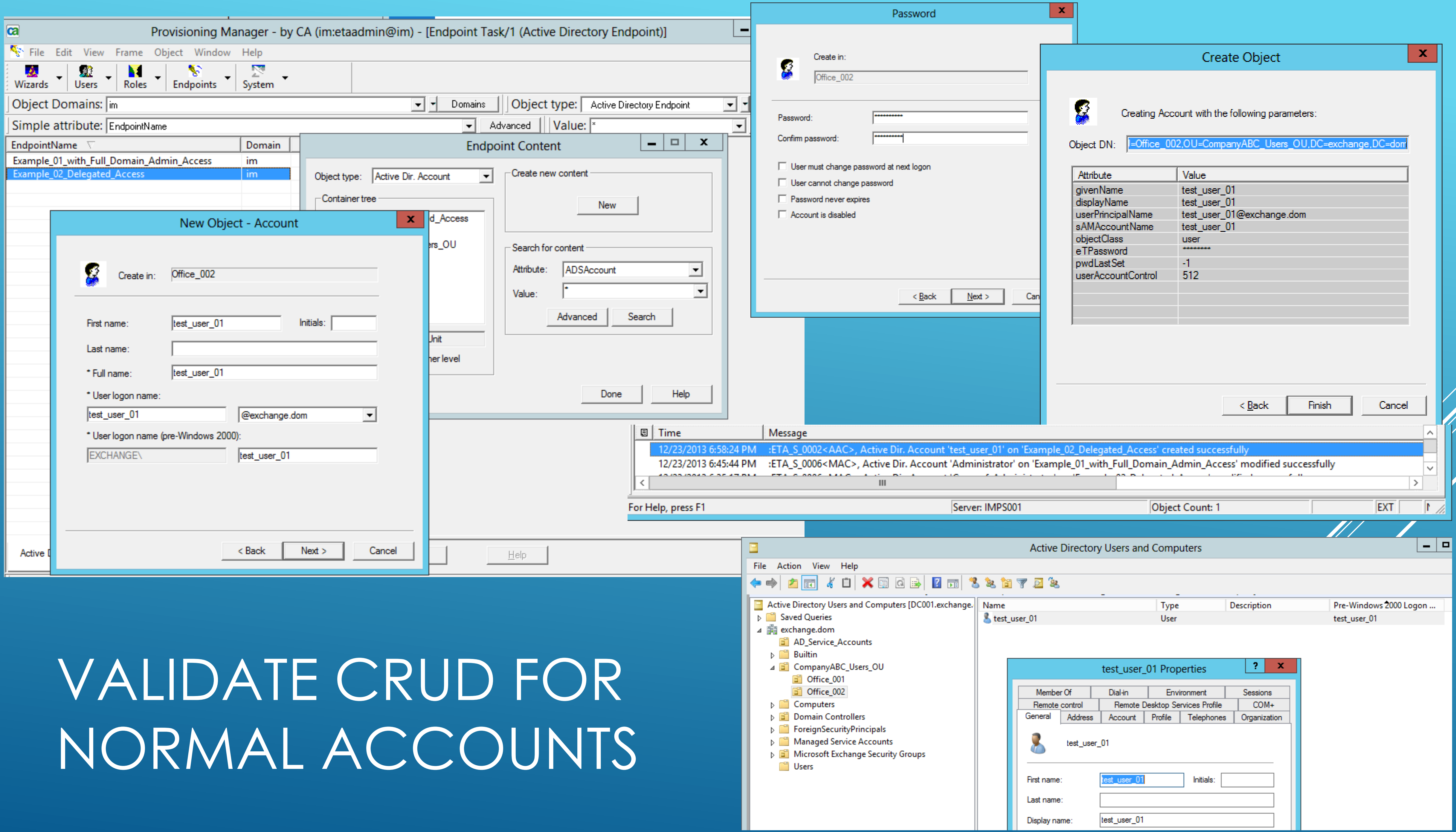
Active Directory Endpoint | Active Dir. Account mple_02_Delegated_Acc

```
Time                     Message
12/23/2013 6:35:17 PM    :ETA_S_0006<MAC>, Active Dir. Account 'Copy_of_Administrator' on 'Example_02_Delegated_Access' modified successfully
12/23/2013 6:34:56 PM    :ETA_S_0023<ECT>, Object 'Users' exploration successful: (objects added: 1, deleted: 0, updated: 0, unchanged: 31, failures: 0) [65633a4b-5980-44be-b1
```

For Help, press F1 | Server: IMPS001 | Object Count: 14 | EXT

# CHECK IF COPY OF DEFAULT ADMINISTRATOR IS PROTECTED AS WELL.

# NO. DELEGATED ADMIN IS ABLE TO CHANGE THIS ACCOUNT'S PASSWORD.



Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Directory Endpoint)]

Object Domains: im

Object type: Active Directory Endpoint

Simple attribute: EndpointName

Value: *

| EndpointName | Domain |
|---|---|
| Example_01_with_Full_Domain_Admin_Access | im |
| Example_02_Delegated_Access | im |

Endpoint Content

Object type: Active Dir. Account

Container tree

Create new content: New

Search for content

Attribute: ADSAccount

Value: *

Advanced Search

New Object - Account

Create in: Office_002

First name: test_user_01

Initials:

Last name:

* Full name: test_user_01

* User logon name: test_user_01 @exchange.dom

* User logon name (pre-Windows 2000): EXCHANGE\ test_user_01

Password

Create in: Office_002

Password: ***********

Confirm password: ***********

□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

Create Object

Creating Account with the following parameters:

Object DN: =Office_002,OU=CompanyABC_Users_OU,DC=exchange,DC=dom

| Attribute | Value |
|---|---|
| givenName | test_user_01 |
| displayName | test_user_01 |
| userPrincipalName | test_user_01@exchange.dom |
| sAMAccountName | test_user_01 |
| objectClass | user |
| eTPassword | ******** |
| pwdLastSet | -1 |
| userAccountControl | 512 |

```
Time                     Message
12/23/2013 6:58:24 PM    :ETA_S_0002<AAC>, Active Dir. Account 'test_user_01' on 'Example_02_Delegated_Access' created successfully
12/23/2013 6:45:44 PM    :ETA_S_0006<MAC>, Active Dir. Account 'Administrator' on 'Example_01_with_Full_Domain_Admin_Access' modified successfully
```

For Help, press F1 | Server: IMPS001 | Object Count: 1 | EXT

Active Directory Users and Computers

- Active Directory Users and Computers [DC001.exchange.
  - Saved Queries
  - exchange.dom
    - AD_Service_Accounts
    - Builtin
    - CompanyABC_Users_OU
      - Office_001
      - Office_002
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Microsoft Exchange Security Groups
    - Users

| Name | Type | Description | Pre-Windows 2000 Logon ... |
|---|---|---|---|
| test_user_01 | User | | test_user_01 |

test_user_01 Properties

Member Of | Dial-in | Environment | Sessions | Remote control | Remote Desktop Services Profile | COM+ | General | Address | Account | Profile | Telephones | Organization

test_user_01

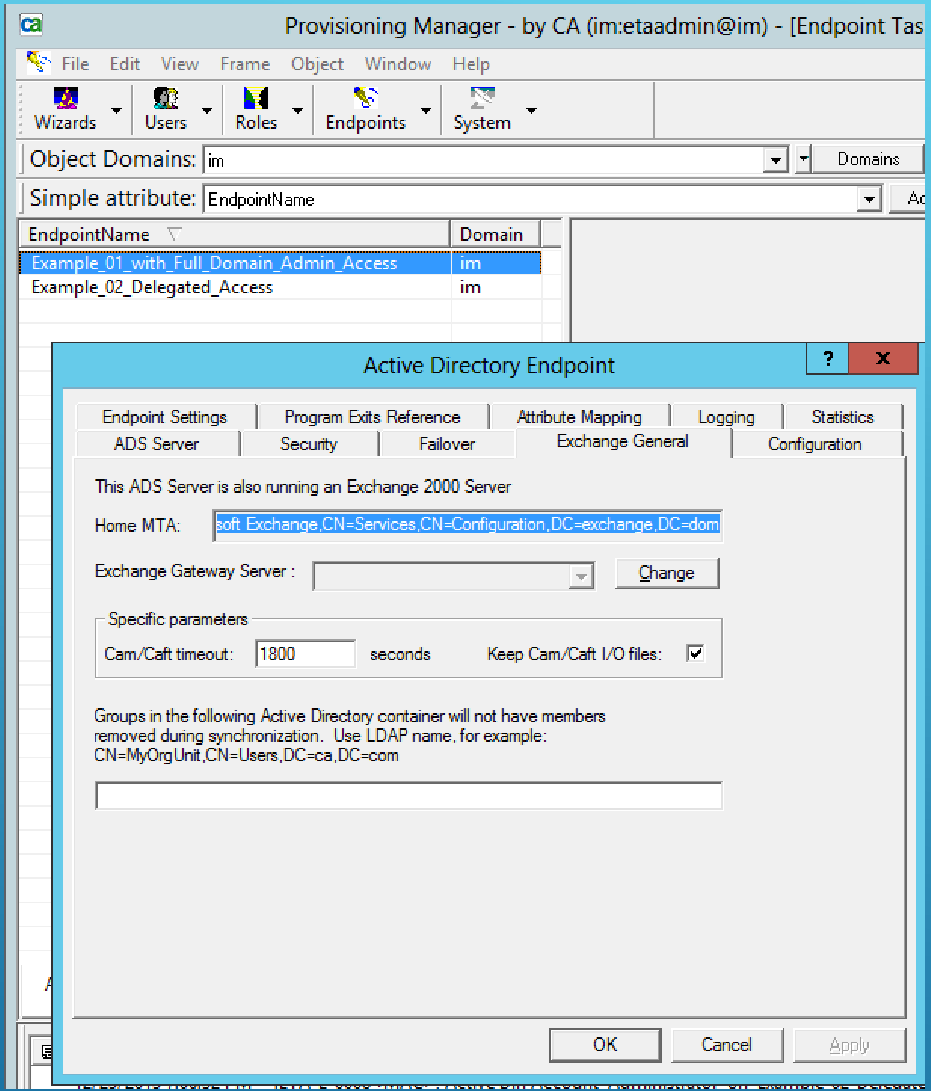
First name: test_user_01

Initials:

Last name:

Display name: test_user_01

# VALIDATE CRUD FOR NORMAL ACCOUNTS



Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Tas

Object Domains: im

Simple attribute: EndpointName

| EndpointName | Domain |
|---|---|
| Example_01_with_Full_Domain_Admin_Access | im |
| Example_02_Delegated_Access | im |

Active Directory Endpoint

This ADS Server is also running an Exchange 2000 Server

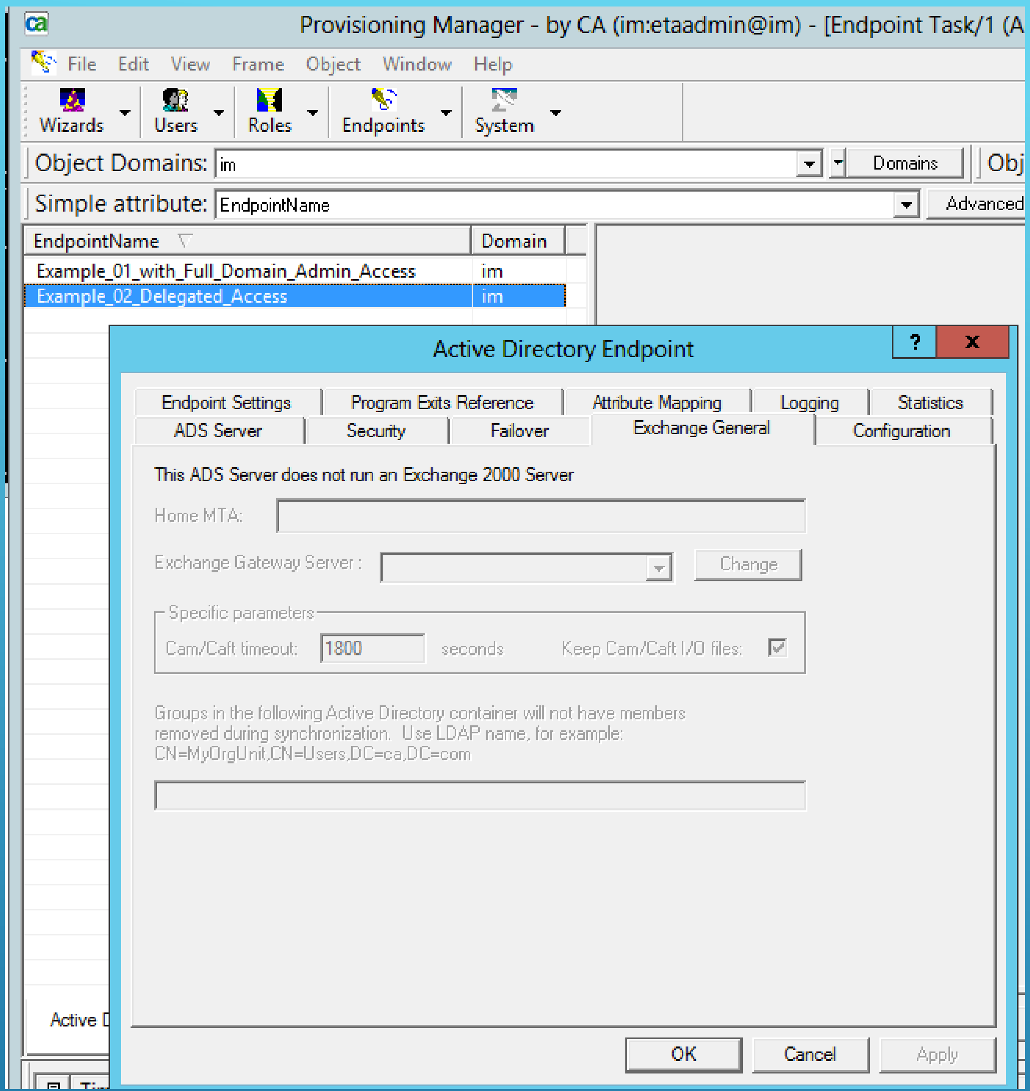
Home MTA: soft Exchange,CN=Services,CN=Configuration,DC=exchange,DC=dom

Exchange Gateway Server :

Specific parameters

Cam/Caft timeout: 1800 seconds  Keep Cam/Caft I/O files: ☑

Groups in the following Active Directory container will not have members removed during synchronization. Use LDAP name, for example: CN=MyOrgUnit,CN=Users,DC=ca,DC=com



Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (A

Object Domains: im

Simple attribute: EndpointName

| EndpointName | Domain |
|---|---|
| Example_01_with_Full_Domain_Admin_Access | im |
| Example_02_Delegated_Access | im |

Active Directory Endpoint

This ADS Server does not run an Exchange 2000 Server

Home MTA:

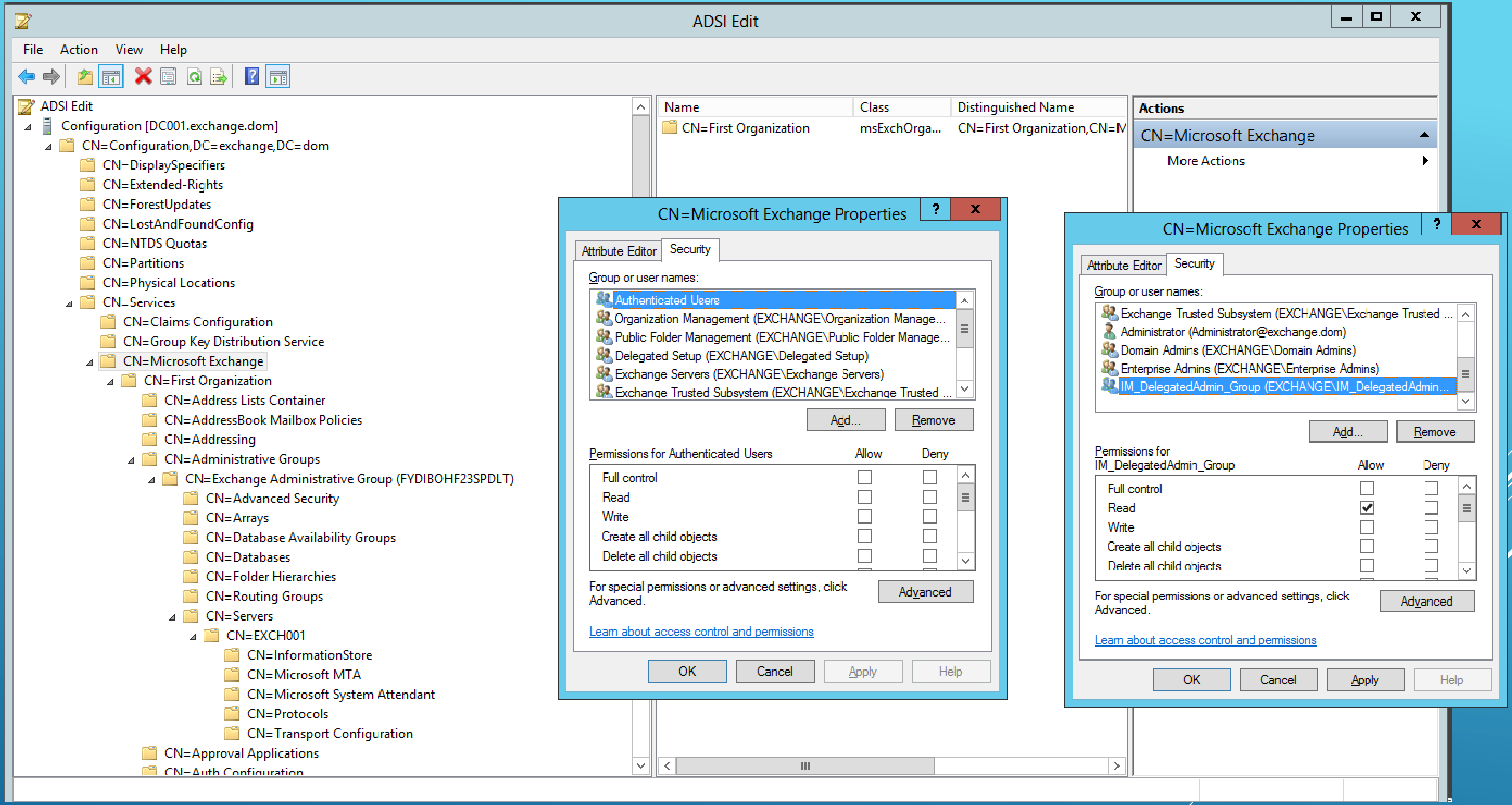
Exchange Gateway Server :

Specific parameters

Cam/Caft timeout: 1800 seconds  Keep Cam/Caft I/O files: ☑

Groups in the following Active Directory container will not have members removed during synchronization. Use LDAP name, for example: CN=MyOrgUnit,CN=Users,DC=ca,DC=com

# EXCHANGE ACCESS CHECK - NO EXCHANGE SERVER SEEN WITH DELEGATED ACCOUNT WITH CRUD ACCESS - FAIL



ADSI Edit

File Action View Help

- ADSI Edit
  - Configuration [DC001.exchange.dom]
    - CN=Configuration,DC=exchange,DC=dom
      - CN=DisplaySpecifiers
      - CN=Extended-Rights
      - CN=ForestUpdates
      - CN=LostAndFoundConfig
      - CN=NTDS Quotas
      - CN=Partitions
      - CN=Physical Locations
      - CN=Services
        - CN=Claims Configuration
        - CN=Group Key Distribution Service
        - CN=Microsoft Exchange
          - CN=First Organization
            - CN=Address Lists Container
            - CN=AddressBook Mailbox Policies
            - CN=Addressing
            - CN=Administrative Groups
              - CN=Exchange Administrative Group (FYDIBOHF23SPDLT)
                - CN=Advanced Security
                - CN=Arrays
                - CN=Database Availability Groups
                - CN=Databases
                - CN=Folder Hierarchies
                - CN=Routing Groups
                - CN=Servers
                  - CN=EXCH001
                    - CN=InformationStore
                    - CN=Microsoft MTA
                    - CN=Microsoft System Attendant
                    - CN=Protocols
                    - CN=Transport Configuration
            - CN=Approval Applications
            - CN=Auth Configuration

| Name | Class | Distinguished Name |
|---|---|---|
| CN=First Organization | msExchOrga... | CN=First Organization,CN=M |

Actions

CN=Microsoft Exchange

More Actions

CN=Microsoft Exchange Properties

Attribute Editor | Security

Group or user names:

- Authenticated Users
- Organization Management (EXCHANGE\Organization Manage...
- Public Folder Management (EXCHANGE\Public Folder Manage...
- Delegated Setup (EXCHANGE\Delegated Setup)
- Exchange Servers (EXCHANGE\Exchange Servers)
- Exchange Trusted Subsystem (EXCHANGE\Exchange Trusted ...

Add... Remove

| Permissions for Authenticated Users | Allow | Deny |
|---|---|---|
| Full control | □ | □ |
| Read | □ | □ |
| Write | □ | □ |
| Create all child objects | □ | □ |
| Delete all child objects | □ | □ |

For special permissions or advanced settings, click Advanced. Advanced

Learn about access control and permissions

OK Cancel Apply Help

CN=Microsoft Exchange Properties

Attribute Editor | Security

Group or user names:

- Exchange Trusted Subsystem (EXCHANGE\Exchange Trusted ...
- Administrator (Administrator@exchange.dom)
- Domain Admins (EXCHANGE\Domain Admins)
- Enterprise Admins (EXCHANGE\Enterprise Admins)
- IM_DelegatedAdmin_Group (EXCHANGE\IM_DelegatedAdmin...

Add... Remove

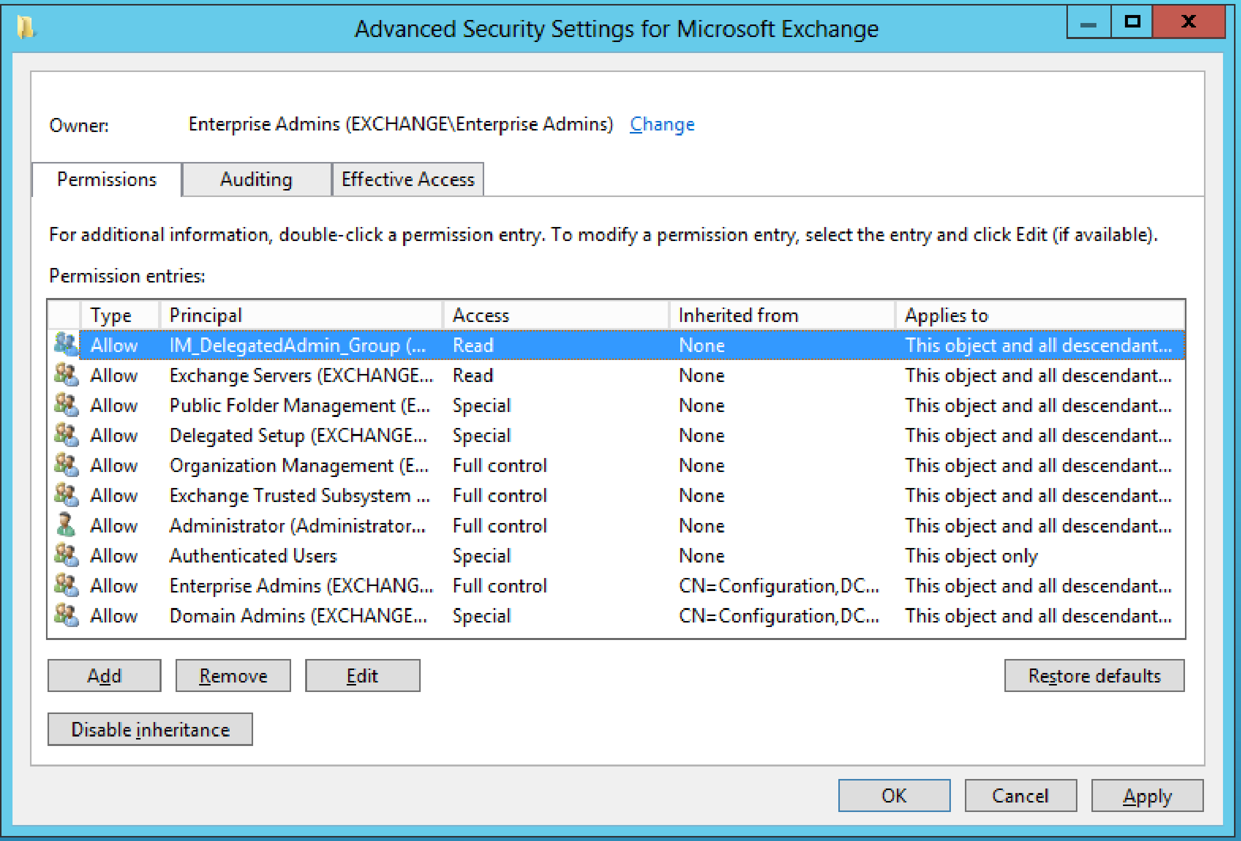
| Permissions for IM_DelegatedAdmin_Group | Allow | Deny |
|---|---|---|
| Full control | □ | □ |
| Read | ☑ | □ |
| Write | □ | □ |
| Create all child objects | □ | □ |
| Delete all child objects | □ | □ |

For special permissions or advanced settings, click Advanced. Advanced

Learn about access control and permissions

OK Cancel Apply Help

USE MS TOOL, ADSIEDIT, AS AN EXISTING AD ADMIN, TO UPDATE/VIEW SECURITY OF EXCHANGE CONFIGURATION IN THE ACTIVE DIRECTORY DOMAIN
& ADD NEW SECURITY GROUP WITH READ ACCESS



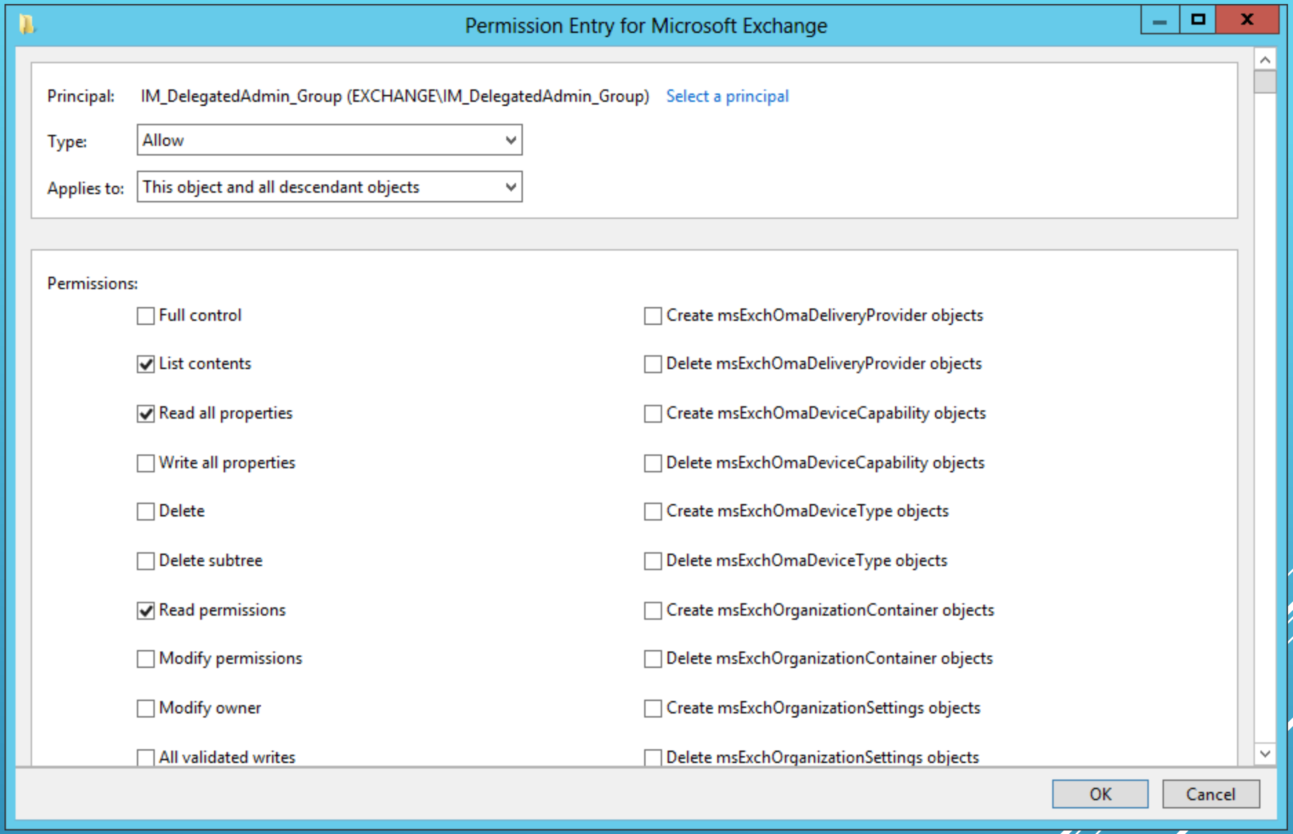
Advanced Security Settings for Microsoft Exchange

Owner: Enterprise Admins (EXCHANGE\Enterprise Admins) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

| Type | Principal | Access | Inherited from | Applies to |
|---|---|---|---|---|
| Allow | IM_DelegatedAdmin_Group (... | Read | None | This object and all descendant... |
| Allow | Exchange Servers (EXCHANGE... | Read | None | This object and all descendant... |
| Allow | Public Folder Management (E... | Special | None | This object and all descendant... |
| Allow | Delegated Setup (EXCHANGE... | Special | None | This object and all descendant... |
| Allow | Organization Management (E... | Full control | None | This object and all descendant... |
| Allow | Exchange Trusted Subsystem ... | Full control | None | This object and all descendant... |
| Allow | Administrator (Administrator... | Full control | None | This object and all descendant... |
| Allow | Authenticated Users | Special | None | This object only |
| Allow | Enterprise Admins (EXCHANG... | Full control | CN=Configuration,DC... | This object and all descendant... |
| Allow | Domain Admins (EXCHANGE... | Special | CN=Configuration,DC... | This object and all descendant... |



Permission Entry for Microsoft Exchange

Principal: IM_DelegatedAdmin_Group (EXCHANGE\IM_DelegatedAdmin_Group) Select a principal

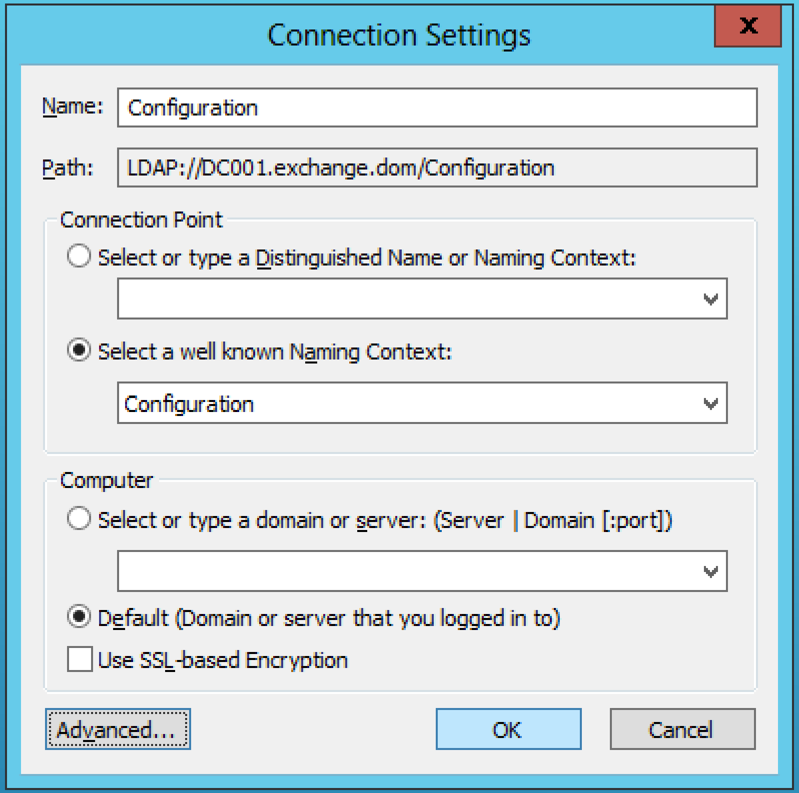
Type: Allow

Applies to: This object and all descendant objects

Permissions:

- □ Full control
- ☑ List contents
- ☑ Read all properties
- □ Write all properties
- □ Delete
- □ Delete subtree
- ☑ Read permissions
- □ Modify permissions
- □ Modify owner
- □ All validated writes
- □ Create msExchOmaDeliveryProvider objects
- □ Delete msExchOmaDeliveryProvider objects
- □ Create msExchOmaDeviceCapability objects
- □ Delete msExchOmaDeviceCapability objects
- □ Create msExchOmaDeviceType objects
- □ Delete msExchOmaDeviceType objects
- □ Create msExchOrganizationContainer objects
- □ Delete msExchOrganizationContainer objects
- □ Create msExchOrganizationSettings objects
- □ Delete msExchOrganizationSettings objects

# SELECT ADVANCED / EDIT TO GRANT READ ACCESS TO "APPLIES TO: THIS OBJECT AND ALL DESCENDANT OBJECTS"



Connection Settings

Name: Configuration

Path: LDAP://DC001.exchange.dom/Configuration

Connection Point

○ Select or type a Distinguished Name or Naming Context:

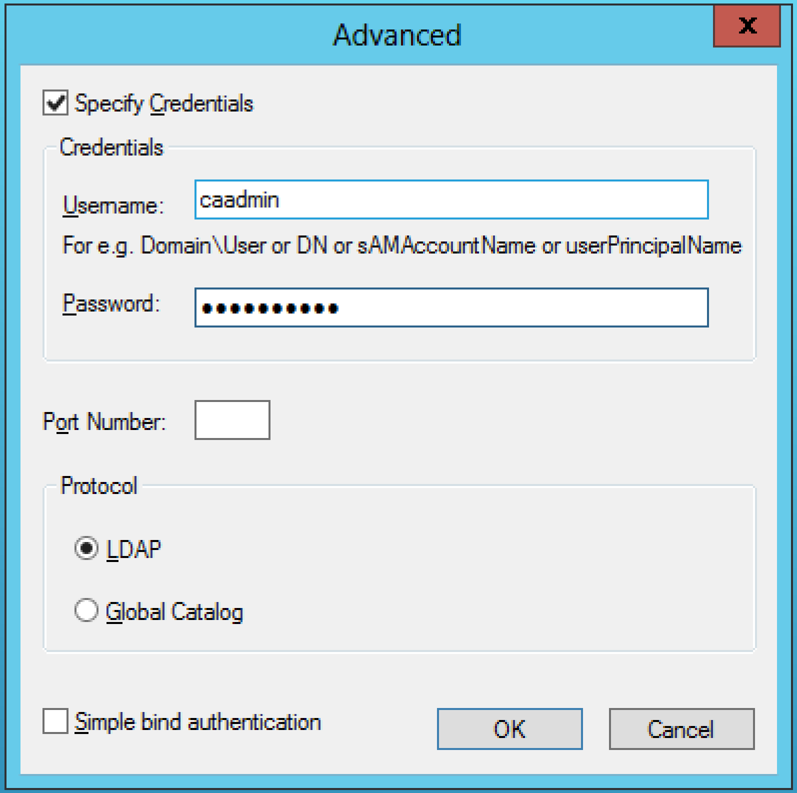
● Select a well known Naming Context: Configuration

Computer

○ Select or type a domain or server: (Server | Domain [:port])

● Default (Domain or server that you logged in to)

□ Use SSL-based Encryption



Advanced

☑ Specify Credentials

Credentials

Username: caadmin

For e.g. Domain\User or DN or sAMAccountName or userPrincipalName

Password: ●●●●●●●●●●●

Port Number:

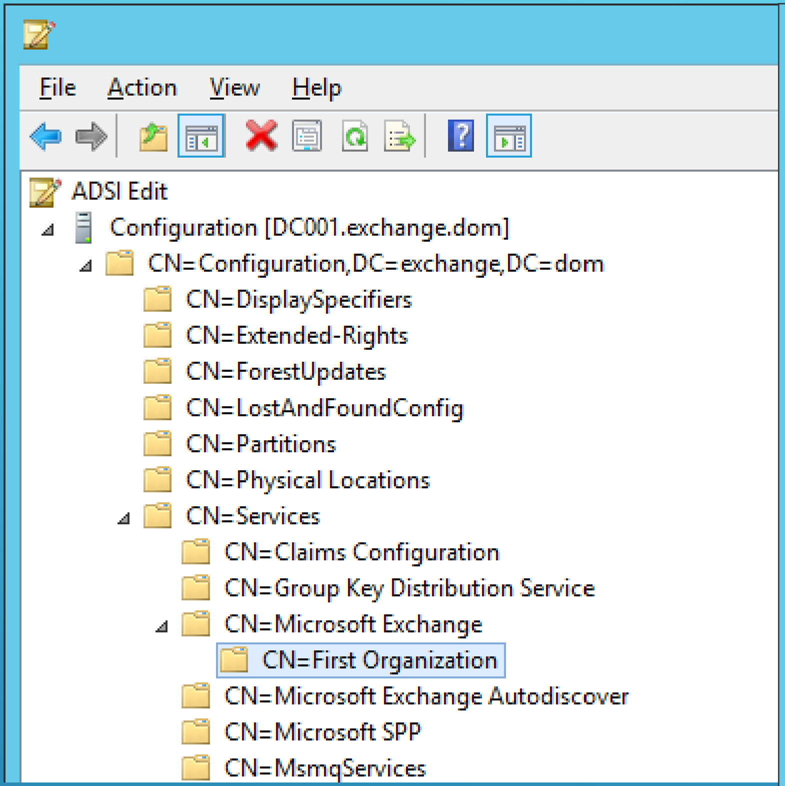
Protocol

● LDAP

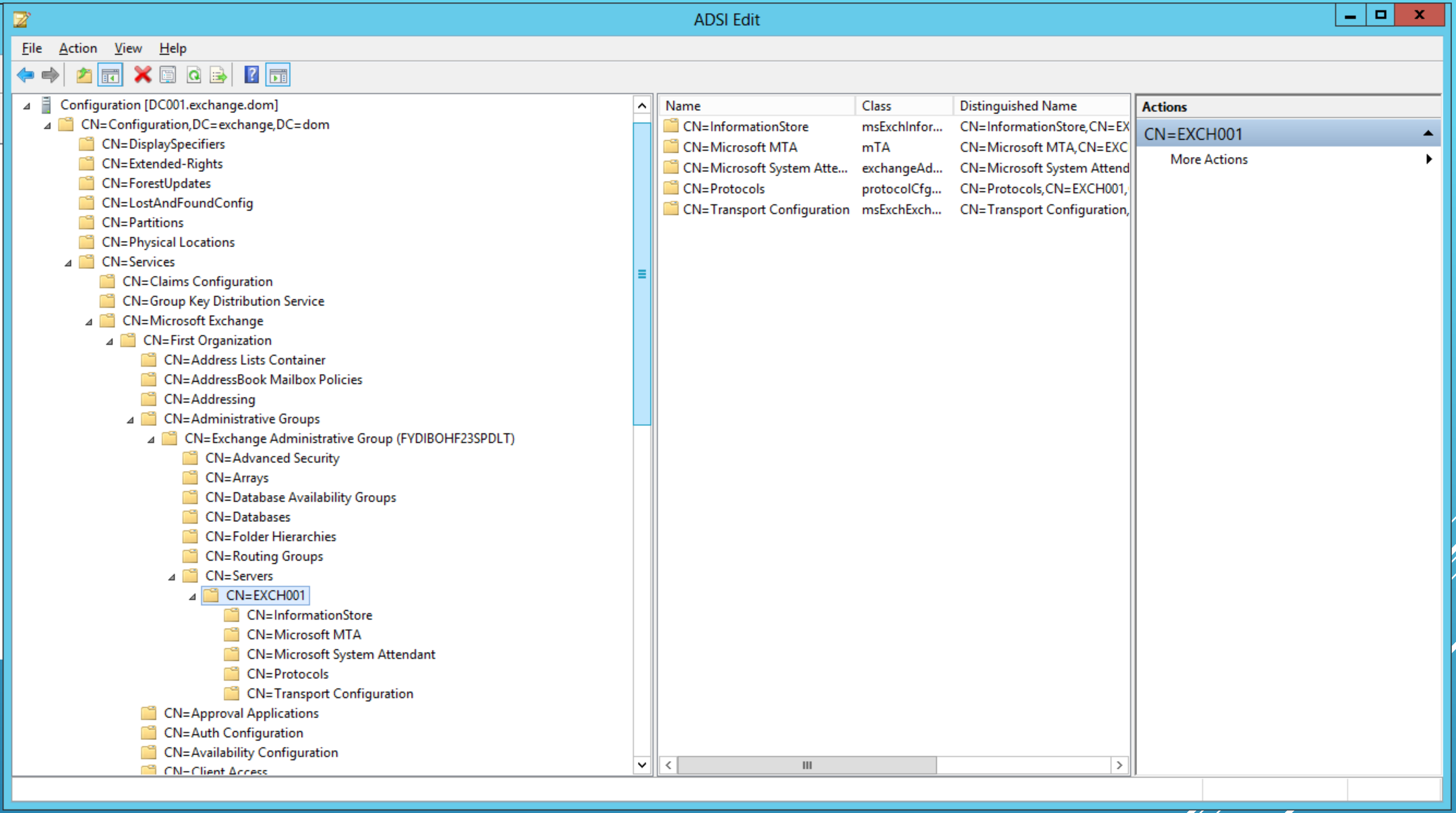
○ Global Catalog

□ Simple bind authentication

# CHECK ACCESS IS CORRECT. CLICK ADVANCE AND USE NEW SERVICE ACCOUNT & PASSWORD



- ADSI Edit
  - Configuration [DC001.exchange.dom]
    - CN=Configuration,DC=exchange,DC=dom
      - CN=DisplaySpecifiers
      - CN=Extended-Rights
      - CN=ForestUpdates
      - CN=LostAndFoundConfig
      - CN=Partitions
      - CN=Physical Locations
      - CN=Services
        - CN=Claims Configuration
        - CN=Group Key Distribution Service
        - CN=Microsoft Exchange
          - CN=First Organization
        - CN=Microsoft Exchange Autodiscover
        - CN=Microsoft SPP
        - CN=MsmqServices



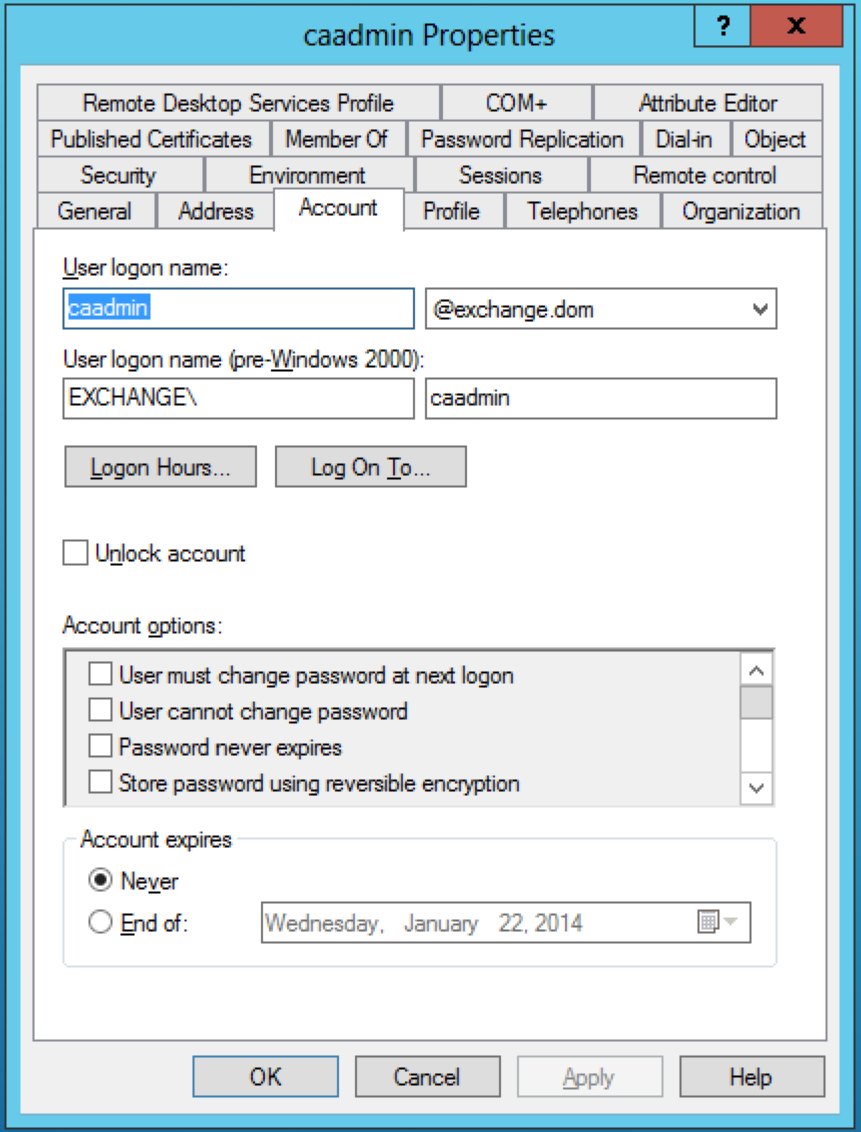
- Configuration [DC001.exchange.dom]
  - CN=Configuration,DC=exchange,DC=dom
    - CN=DisplaySpecifiers
    - CN=Extended-Rights
    - CN=ForestUpdates
    - CN=LostAndFoundConfig
    - CN=Partitions
    - CN=Physical Locations
    - CN=Services
      - CN=Claims Configuration
      - CN=Group Key Distribution Service
      - CN=Microsoft Exchange
        - CN=First Organization
          - CN=Address Lists Container
          - CN=AddressBook Mailbox Policies
          - CN=Addressing
          - CN=Administrative Groups
            - CN=Exchange Administrative Group (FYDIBOHF23SPDLT)
              - CN=Advanced Security
              - CN=Arrays
              - CN=Database Availability Groups
              - CN=Databases
              - CN=Folder Hierarchies
              - CN=Routing Groups
              - CN=Servers
                - CN=EXCH001
                  - CN=InformationStore
                  - CN=Microsoft MTA
                  - CN=Microsoft System Attendant
                  - CN=Protocols
                  - CN=Transport Configuration
          - CN=Approval Applications
          - CN=Auth Configuration
          - CN=Availability Configuration
          - CN=Client Access

| Name | Class | Distinguished Name |
|---|---|---|
| CN=InformationStore | msExchInfor... | CN=InformationStore,CN=EX |
| CN=Microsoft MTA | mTA | CN=Microsoft MTA,CN=EXC |
| CN=Microsoft System Atte... | exchangeAd... | CN=Microsoft System Attend |
| CN=Protocols | protocolCfg... | CN=Protocols,CN=EXCH001, |
| CN=Transport Configuration | msExchExch... | CN=Transport Configuration, |

CN=EXCH001

IF ACESS IS INCORRECT, ACCOUNT WILL NOT BE ABLE TO ACCESS BEYOND CN=MICROSOFT EXCHANGE.

IF ACCESS IS CORRECT, ACCOUNT WILL BE ABLE TO VIEW ALL EXCHANGE SERVERS IN THE ACTIVE DIRECTORY DOMAIN



User logon name: caadmin @exchange.dom

User logon name (pre-Windows 2000): EXCHANGE\ caadmin

□ Unlock account

Account options:

- □ User must change password at next logon
- □ User cannot change password
- □ Password never expires
- □ Store password using reversible encryption

Account expires

● Never

○ End of: Wednesday, January 22, 2014

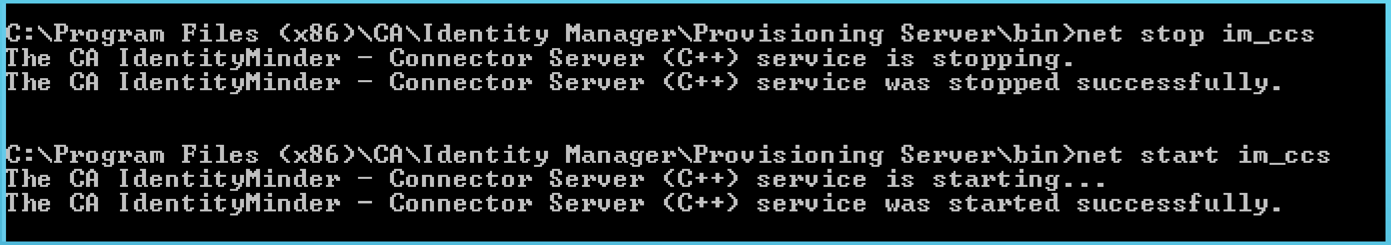
# ENSURE SERVICE'S AD ACCOUNT TAB IS POPULATED FOR BOTH USER LOGIN NAME FIELDS

# OTHERWISE THIS ERROR WILL APPEAR IN THE IMPS ADS LOGS

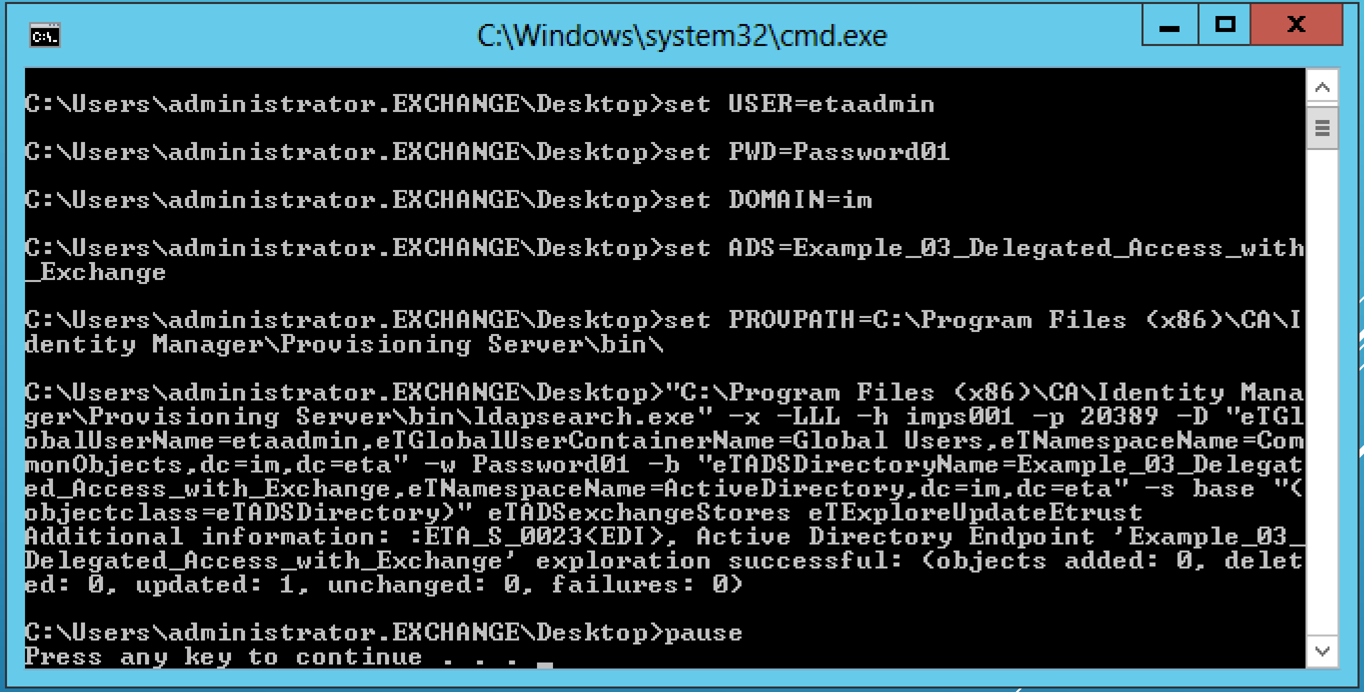
# "UNABLE TO RESOLVE OBJECTSID"

# BOUNCE IM_CCS SERVICE AND FORCE A "REFRESH" OF THE AD DOMAIN

# (OR CREATE A NEW ONE)

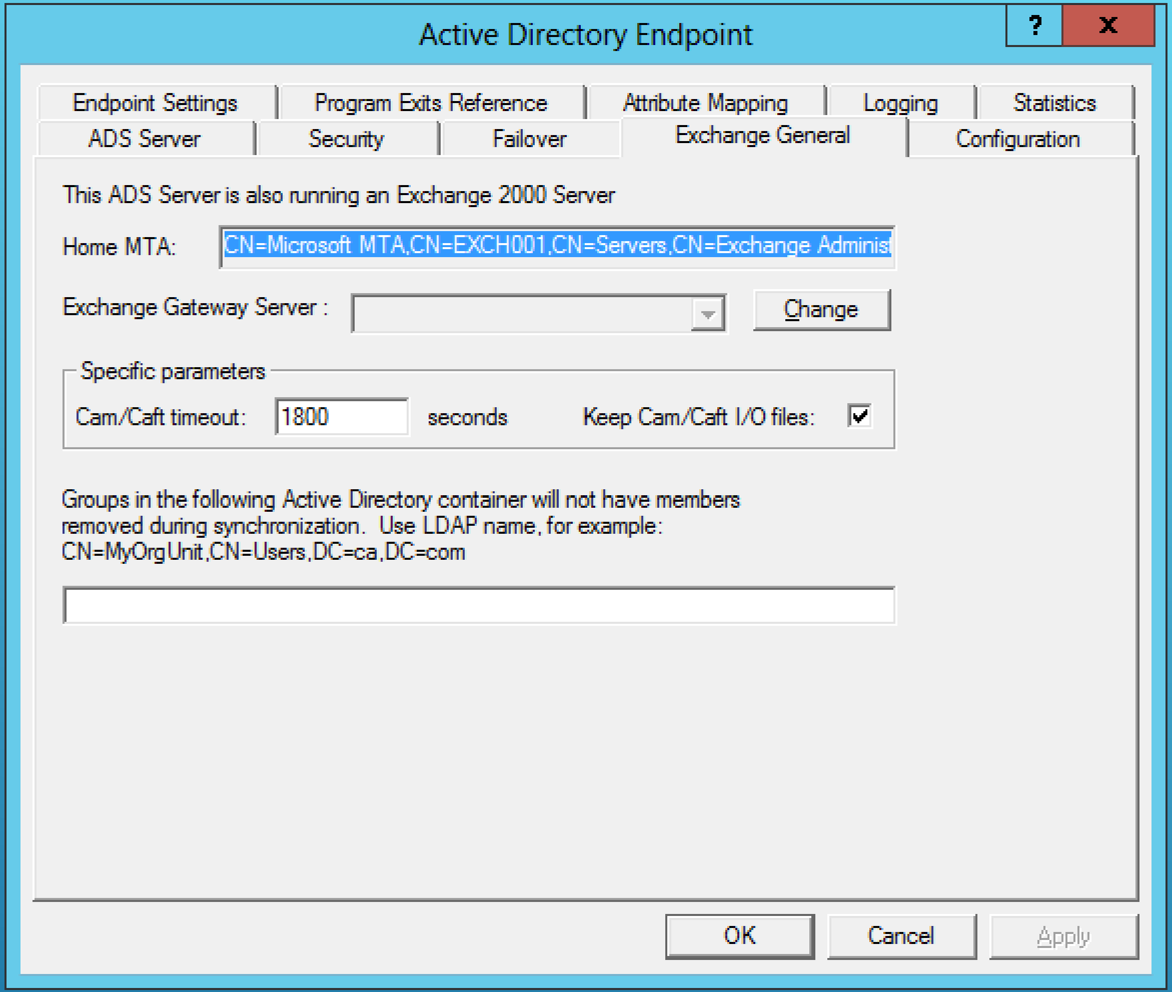


```
C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\bin>net stop im_ccs
The CA IdentityMinder - Connector Server (C++) service is stopping.
The CA IdentityMinder - Connector Server (C++) service was stopped successfully.

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\bin>net start im_ccs
The CA IdentityMinder - Connector Server (C++) service is starting...
The CA IdentityMinder - Connector Server (C++) service was started successfully.
```



```
C:\Users\administrator.EXCHANGE\Desktop>set USER=etaadmin

C:\Users\administrator.EXCHANGE\Desktop>set PWD=Password01

C:\Users\administrator.EXCHANGE\Desktop>set DOMAIN=im

C:\Users\administrator.EXCHANGE\Desktop>set ADS=Example_03_Delegated_Access_with
_Exchange

C:\Users\administrator.EXCHANGE\Desktop>set PROVPATH=C:\Program Files (x86)\CA\I
dentity Manager\Provisioning Server\bin\

C:\Users\administrator.EXCHANGE\Desktop>"C:\Program Files (x86)\CA\Identity Mana
ger\Provisioning Server\bin\ldapsearch.exe" -x -LLL -h imps001 -p 20389 -D "eTGl
obalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamespaceName=Com
monObjects,dc=im,dc=eta" -w Password01 -b "eTADSDirectoryName=Example_03_Delegat
ed_Access_with_Exchange,eTNamespaceName=ActiveDirectory,dc=im,dc=eta" -s base "(
objectclass=eTADSDirectory)" eTADSexchangeStores eTExploreUpdateEtrust
Additional information: :ETA_S_0023<EDI>, Active Directory Endpoint 'Example_03_
Delegated_Access_with_Exchange' exploration successful: (objects added: 0, delet
ed: 0, updated: 1, unchanged: 0, failures: 0)

C:\Users\administrator.EXCHANGE\Desktop>pause
Press any key to continue . . .
```

```
set HOST=imps001
set USER=etaadmin
set PWD=Password01
set DOMAIN=im
set ADS=Example_03_Delegated_Access_with_Exchange
set PROVPATH=C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\bin\
"%PROVPATH%ldapsearch.exe" -x -LLL -h %HOST% -p 20389 -D "eTGlobalUserName=%USER%,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=%DOMAIN%,dc=eta" -w %PWD% -b
"eTADSDirectoryName=%ADS%,eTNamespaceName=ActiveDirectory,dc=%DOMAIN%,dc=eta" -s base "(objectclass=eTADSDirectory)" eTADSexchangeStores eTExploreUpdateEtrust
pause
```



This ADS Server is also running an Exchange 2000 Server

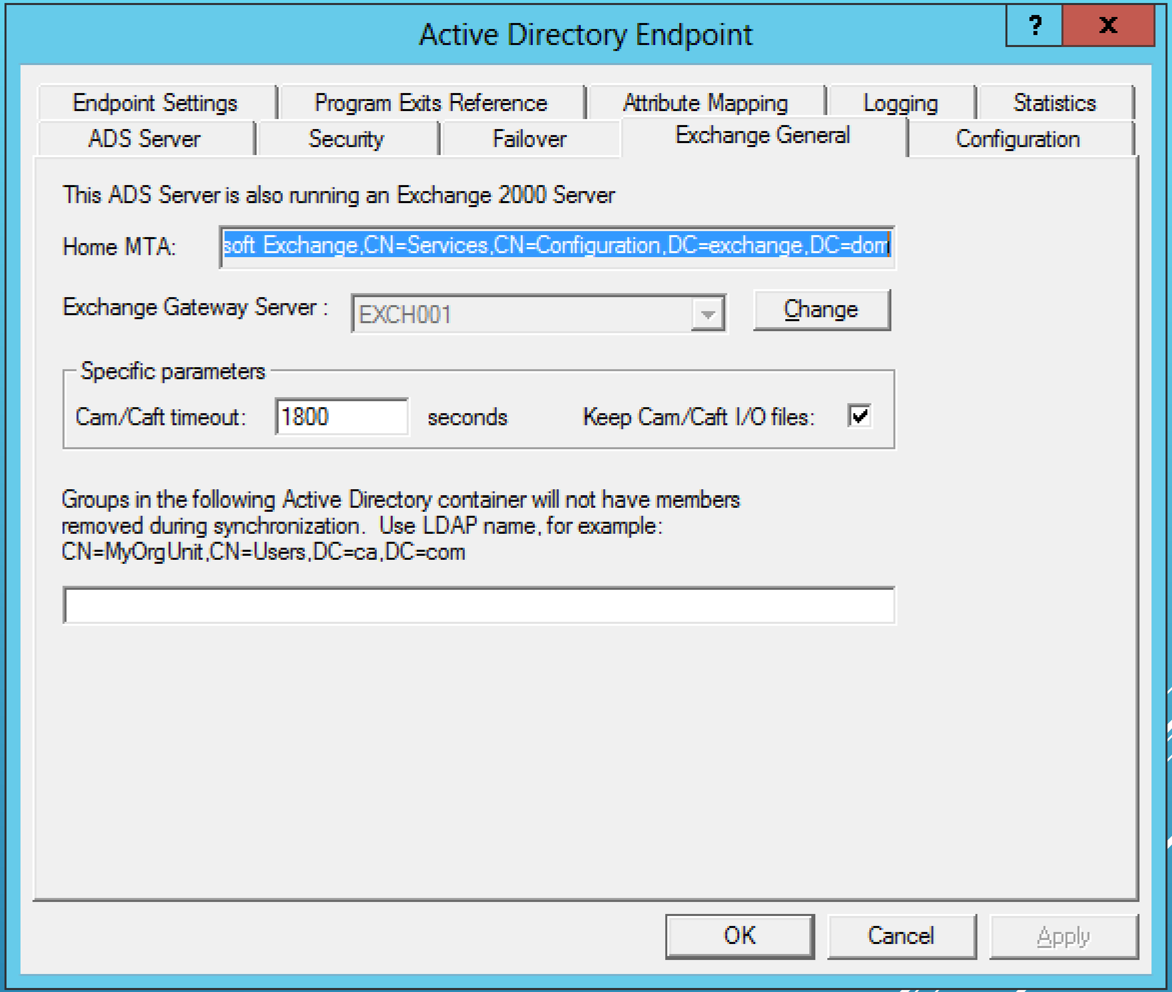
Home MTA: CN=Microsoft MTA,CN=EXCH001,CN=Servers,CN=Exchange Adminis

Exchange Gateway Server :

Specific parameters

Cam/Caft timeout: 1800 seconds Keep Cam/Caft I/O files: ☑

Groups in the following Active Directory container will not have members removed during synchronization. Use LDAP name, for example: CN=MyOrgUnit,CN=Users,DC=ca,DC=com



This ADS Server is also running an Exchange 2000 Server

Home MTA: soft Exchange,CN=Services,CN=Configuration,DC=exchange,DC=dom

Exchange Gateway Server : EXCH001

Specific parameters

Cam/Caft timeout: 1800 seconds Keep Cam/Caft I/O files: ☑

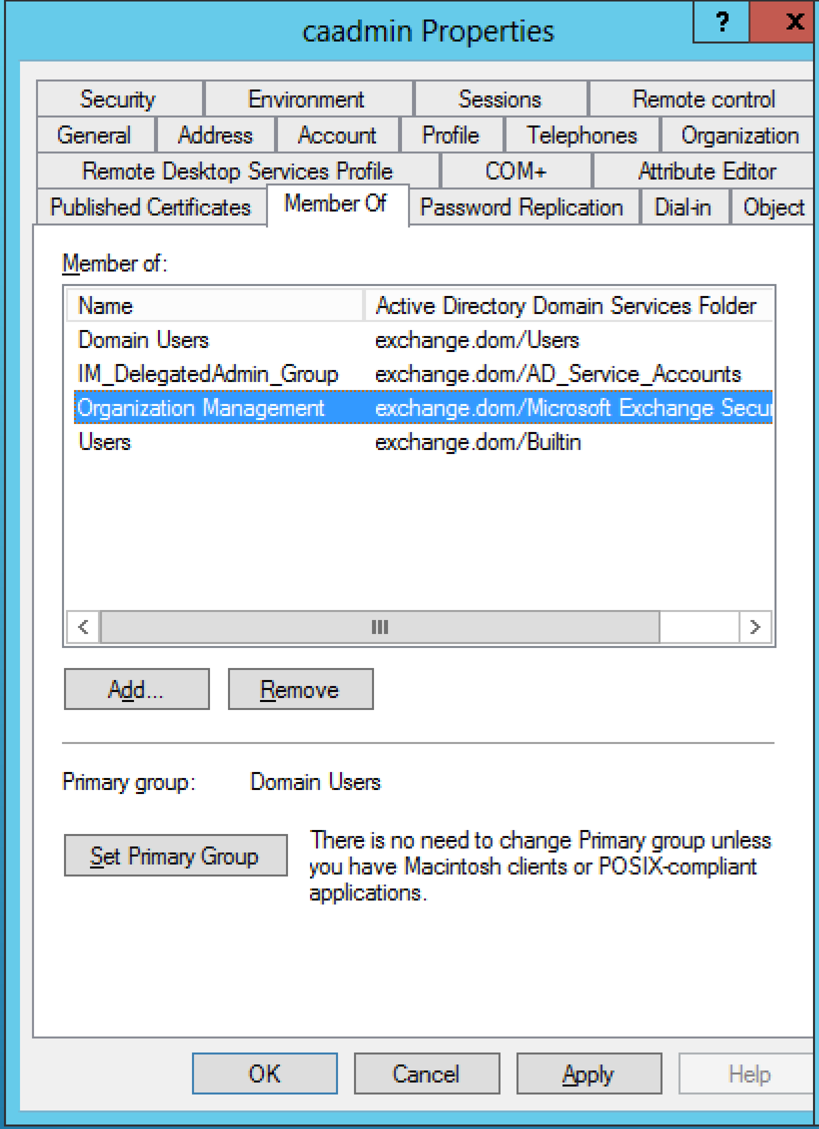
Groups in the following Active Directory container will not have members removed during synchronization. Use LDAP name, for example: CN=MyOrgUnit,CN=Users,DC=ca,DC=com

OPEN IMPS MANAGER AND THE AD ENDPOINT PROPERTIES TAB TO CHECK EXCHANGE GENERAL IS NOW POPULATED. CHECK CHANGE AND SELECT THE “GATEWAY SERVER” EXCHANGE SERVER ENTRY

# ADDED THE CORRECT EXCHANGE SERVICE GROUP LEVEL OF ACCESS TO ALLOW CREATION & MANAGEMENT OF MAILBOXES (& RIGHTS)

FULL ACCESS – ORGANIZATION MANAGEMENT

MINIMAL ACCESS – DISCOVERY MANAGEMENT



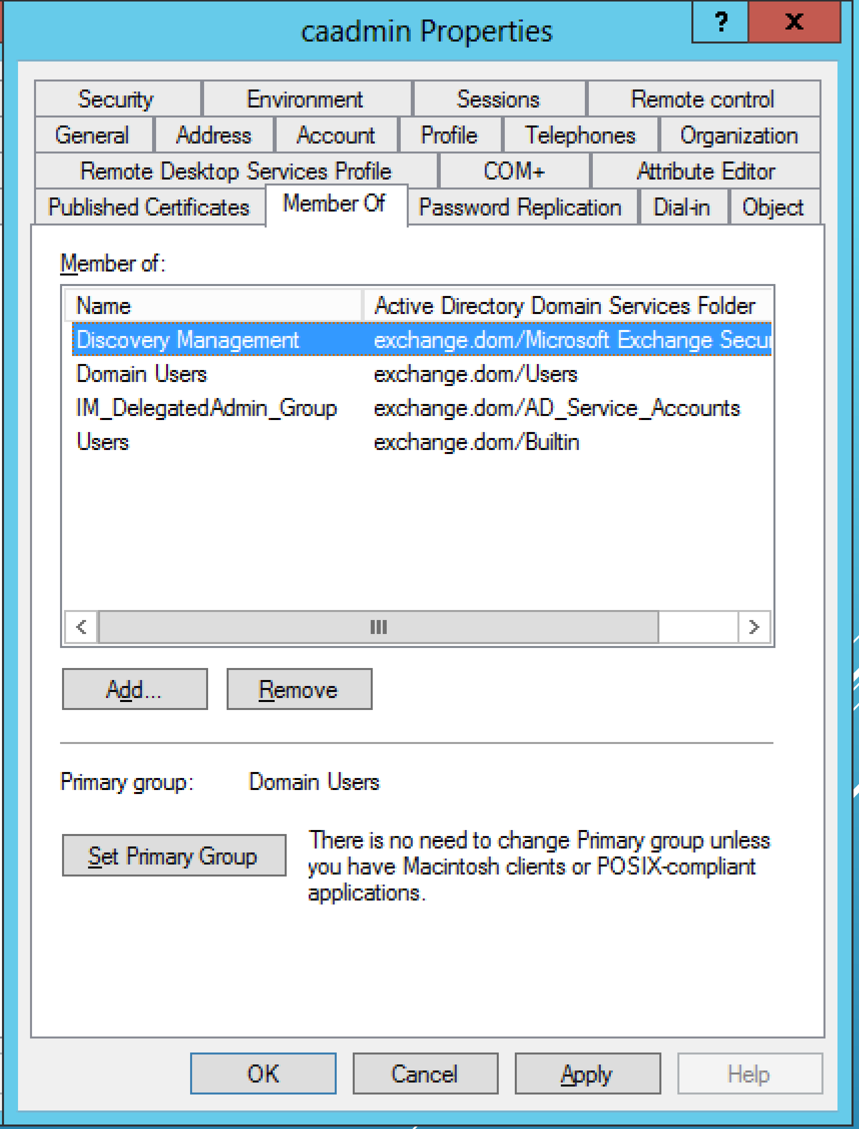
caadmin Properties

Member of:

| Name | Active Directory Domain Services Folder |
|---|---|
| Domain Users | exchange.dom/Users |
| IM_DelegatedAdmin_Group | exchange.dom/AD_Service_Accounts |
| Organization Management | exchange.dom/Microsoft Exchange Secu |
| Users | exchange.dom/Builtin |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.



caadmin Properties

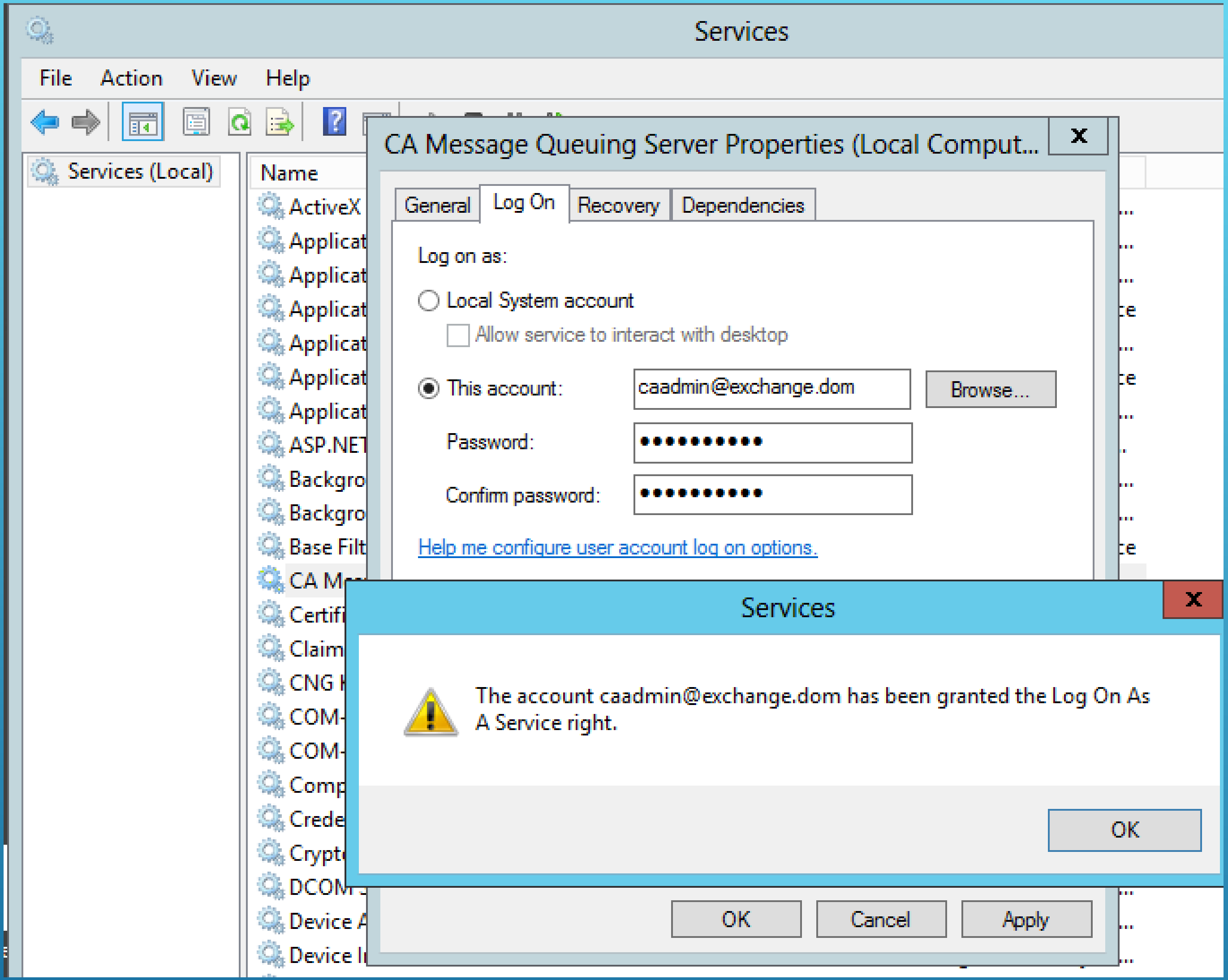
Member of:

| Name | Active Directory Domain Services Folder |
|---|---|
| Discovery Management | exchange.dom/Microsoft Exchange Secu |
| Domain Users | exchange.dom/Users |
| IM_DelegatedAdmin_Group | exchange.dom/AD_Service_Accounts |
| Users | exchange.dom/Builtin |

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

https://supportcontent.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1569112.html



CA Message Queuing Server Properties (Local Comput...

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: caadmin@exchange.dom

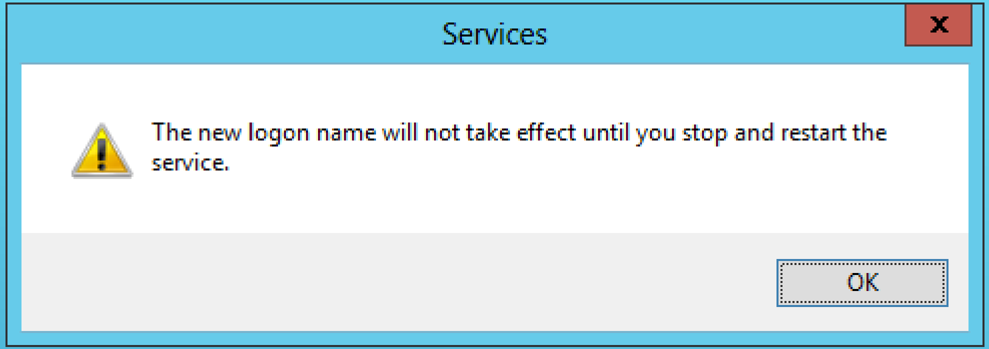
Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

Help me configure user account log on options.

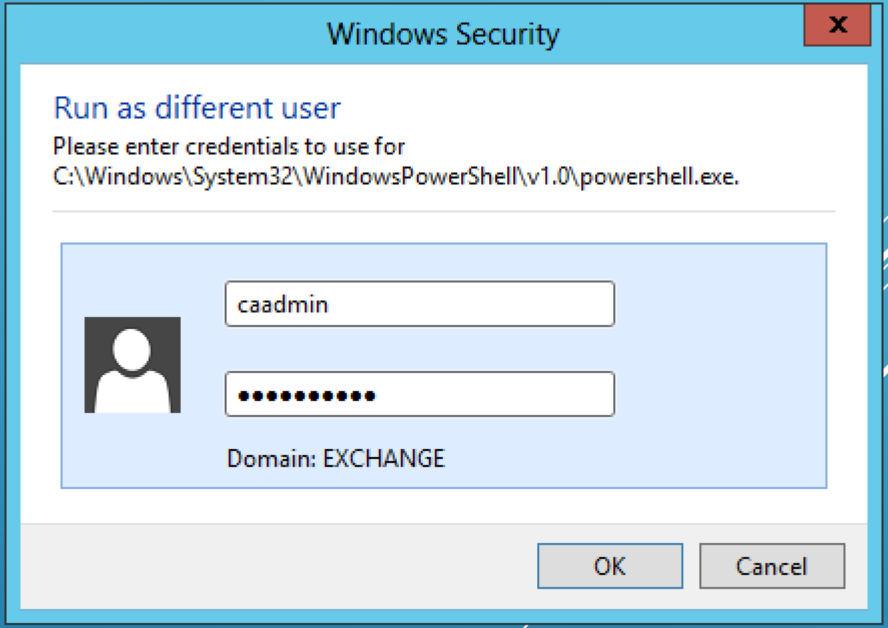
Services

The account caadmin@exchange.dom has been granted the Log On As A Service right.



Services

The new logon name will not take effect until you stop and restart the service.



Windows Security

Run as different user

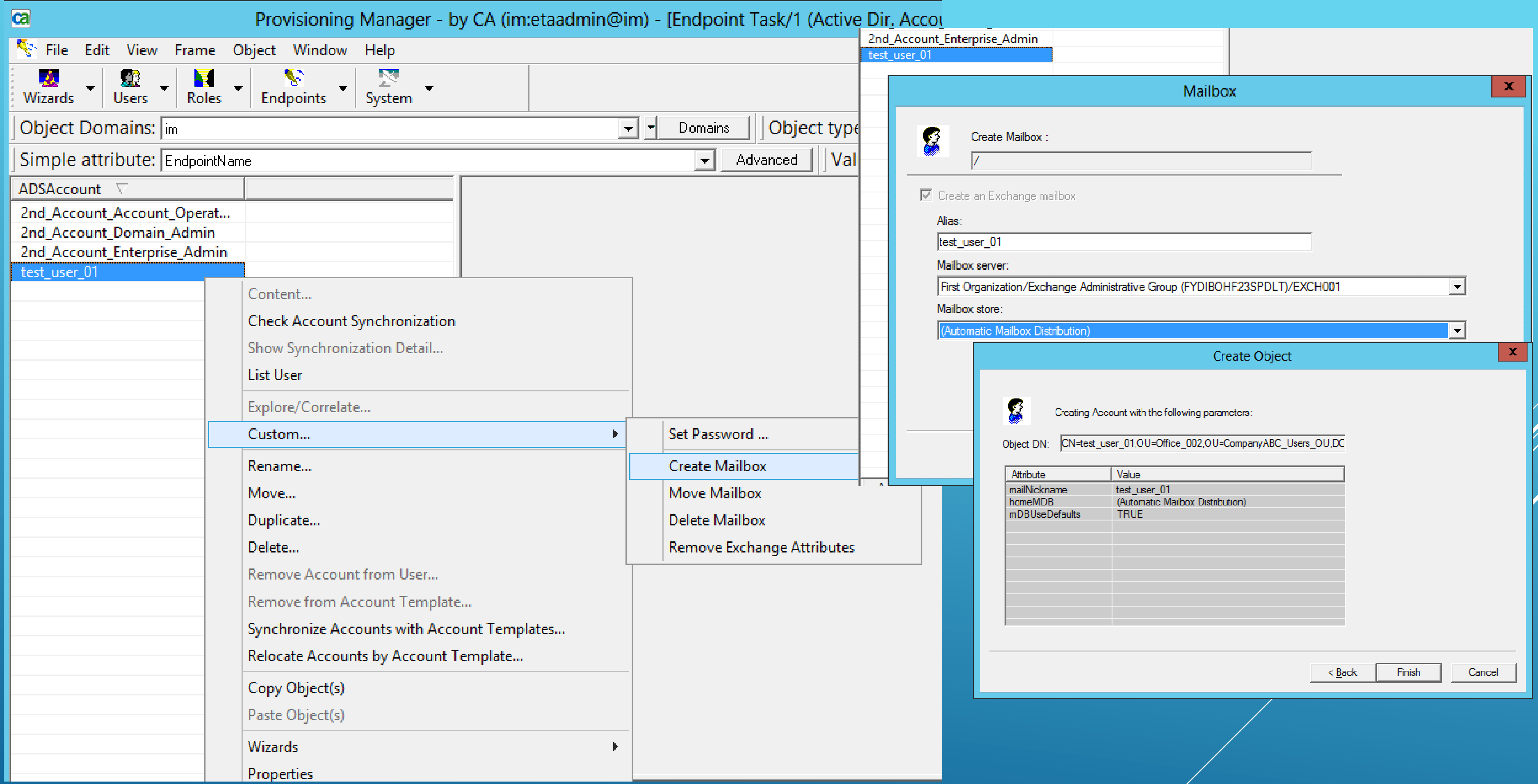
Please enter credentials to use for C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.

caadmin

●●●●●●●●●●●

Domain: EXCHANGE

# UPDATE SERVICE ACCOUNT ON EXCHANGE SERVER


Provisioning Manager - by CA (im:etaadmin@im) - [Endpoint Task/1 (Active Dir. Accou
File
Edit
View
Frame
Object
Window
Help
Wizards
Users
Roles
Endpoints
System
Domains
Advanced
Object type
Val
ADSAccount
2nd_Account_Account_Operat...
2nd_Account_Domain_Admin
2nd_Account_Enterprise_Admin
test_user_01
Content...
Check Account Synchronization
Show Synchronization Detail...
List User
Explore/Correlate...
Custom...
Rename...
Move...
Duplicate...
Delete...
Remove Account from User...
Remove from Account Template...
Synchronize Accounts with Account Templates...
Relocate Accounts by Account Template...
Copy Object(s)
Paste Object(s)
Wizards
Properties
Set Password ...
Create Mailbox
Move Mailbox
Delete Mailbox
Remove Exchange Attributes
2nd_Account_Enterprise_Admin
test_user_01
Mailbox
Create Object
&lt; Back
Finish
Cancel

Object Domains: im

Simple attribute: EndpointName

Mailbox

Create Mailbox : /

☑ Create an Exchange mailbox

Alias: test_user_01

Mailbox server: First Organization/Exchange Administrative Group (FYDIBOHF23SPDLT)/EXCH001

Mailbox store: (Automatic Mailbox Distribution)

Create Object

Creating Account with the following parameters:

Object DN: CN=test_user_01,OU=Office_002,OU=CompanyABC_Users_OU,DC

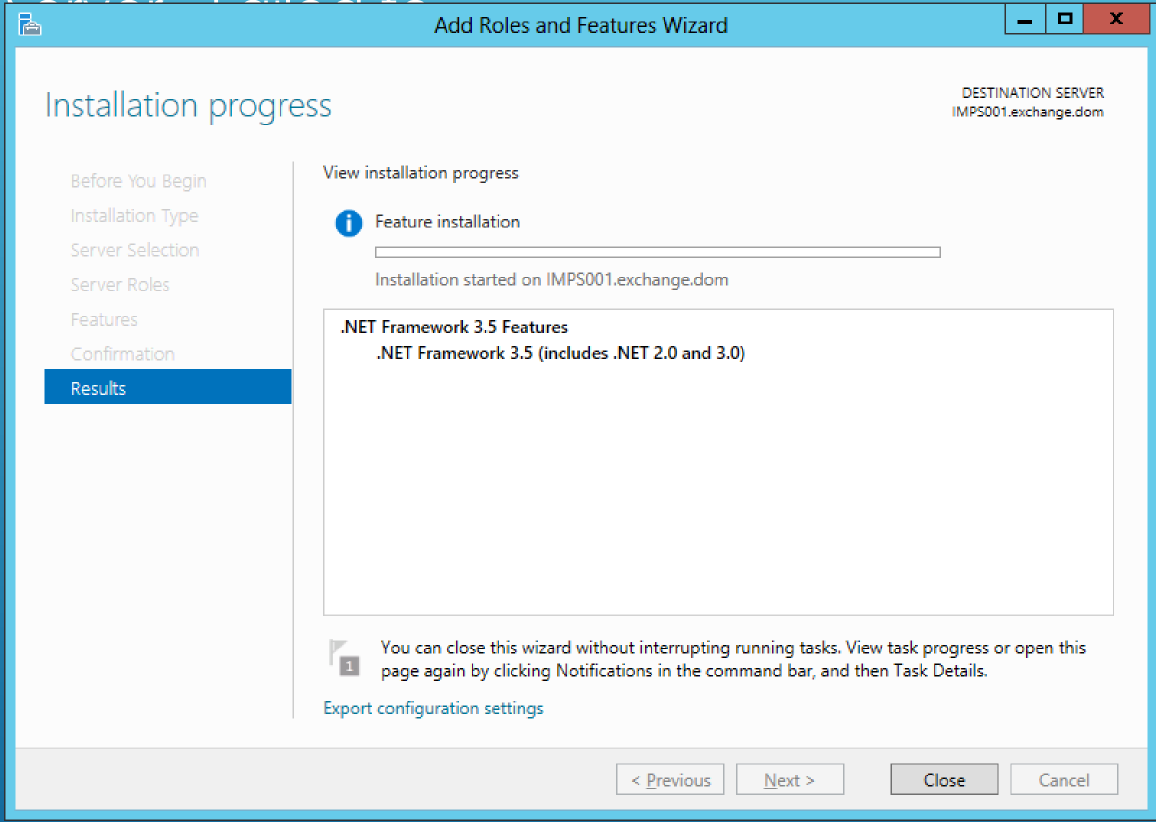
| Attribute | Value |
|---|---|
| mailNickname | test_user_01 |
| homeMDB | (Automatic Mailbox Distribution) |
| mDBUseDefaults | TRUE |

# TEST CRUD WITH ADDING EXCHANGE MAILBOX

# ADDITIONAL NOTES – IMPS ON WINDOWS 2012 SERVER

```
2013.12.23.17:23:55.746    INFO C++ Connector Server - TID=0x8a8: create DMODirectoryEntry 0x27d8eb0
2013.12.23.17:23:55.746    INFO C++ Connector Server - TID=0x8a8: create DMODirectoryEntry 0x27d9030
2013.12.23.17:27:07.302   FATAL C++ Connector Server - Failed to load module W2KNamespace.dll
2013.12.23.17:27:07.317   FATAL C++ Connector
load module W2KNamespace.dll
2013.12.23.17:28:54.679   FATAL C++ Connector
load module W2KNamespace.dll
```

# ADD .NET 3.5 FRAMEWORK FOR WINDOWS 2012 TO AVOID LOAD MODULE ERROR MESSAGE



Installation progress

DESTINATION SERVER
IMPS001.exchange.dom

View installation progress

Feature installation

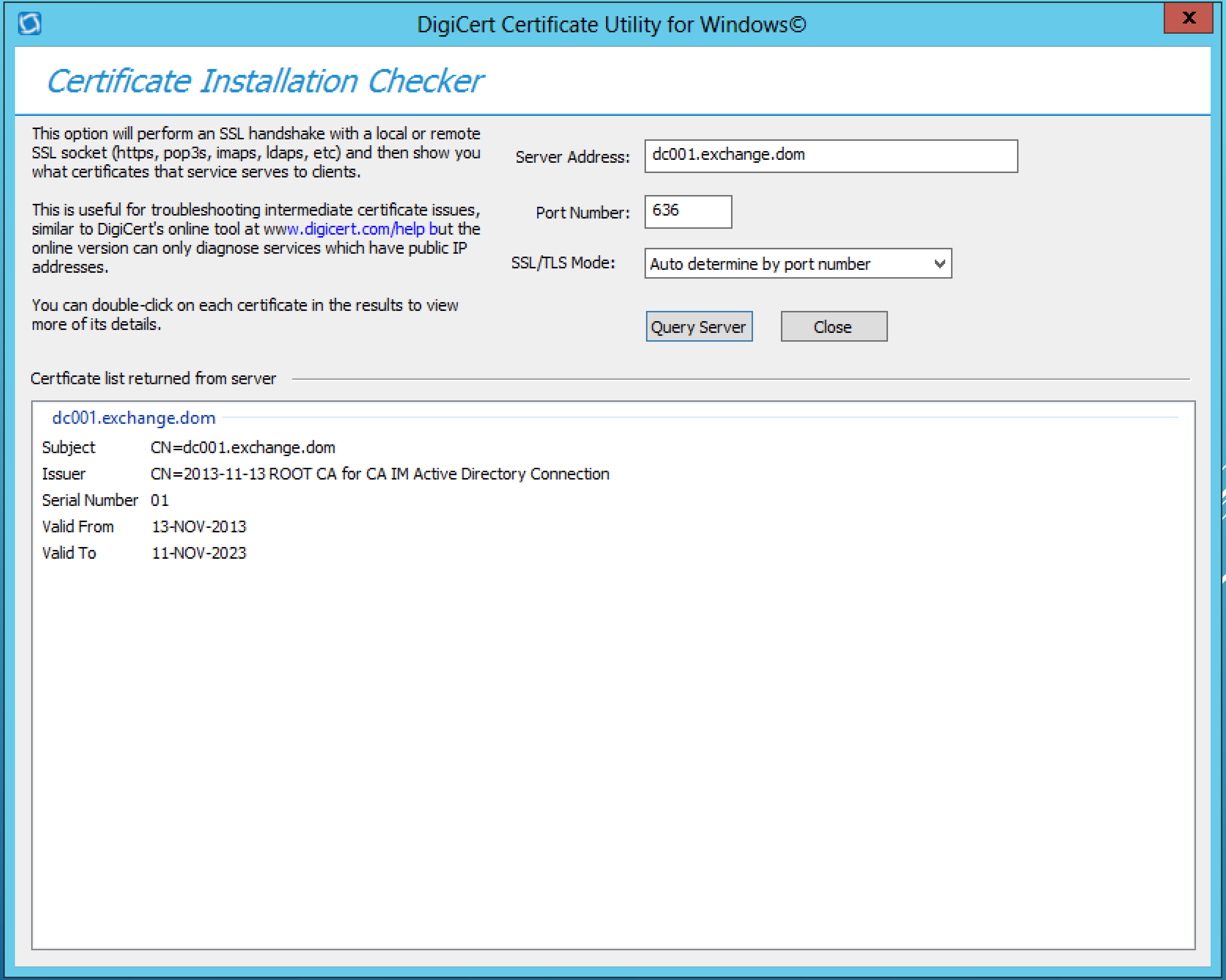
Installation started on IMPS001.exchange.dom

.NET Framework 3.5 Features
    .NET Framework 3.5 (includes .NET 2.0 and 3.0)

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

# USE THIS ALTERNATIVE TOOL TO VIEW IF AD DOMAIN OR SERVER CA CERT IS DEPLOYED & AVAILABLE FOR IMPS USE



DigiCert Certificate Utility for Windows©
Certificate Installation Checker

This option will perform an SSL handshake with a local or remote SSL socket (https, pop3s, imaps, ldaps, etc) and then show you what certificates that service serves to clients.

This is useful for troubleshooting intermediate certificate issues, similar to DigiCert's online tool at www.digicert.com/help but the online version can only diagnose services which have public IP addresses.

You can double-click on each certificate in the results to view more of its details.

Server Address: dc001.exchange.dom

Port Number: 636

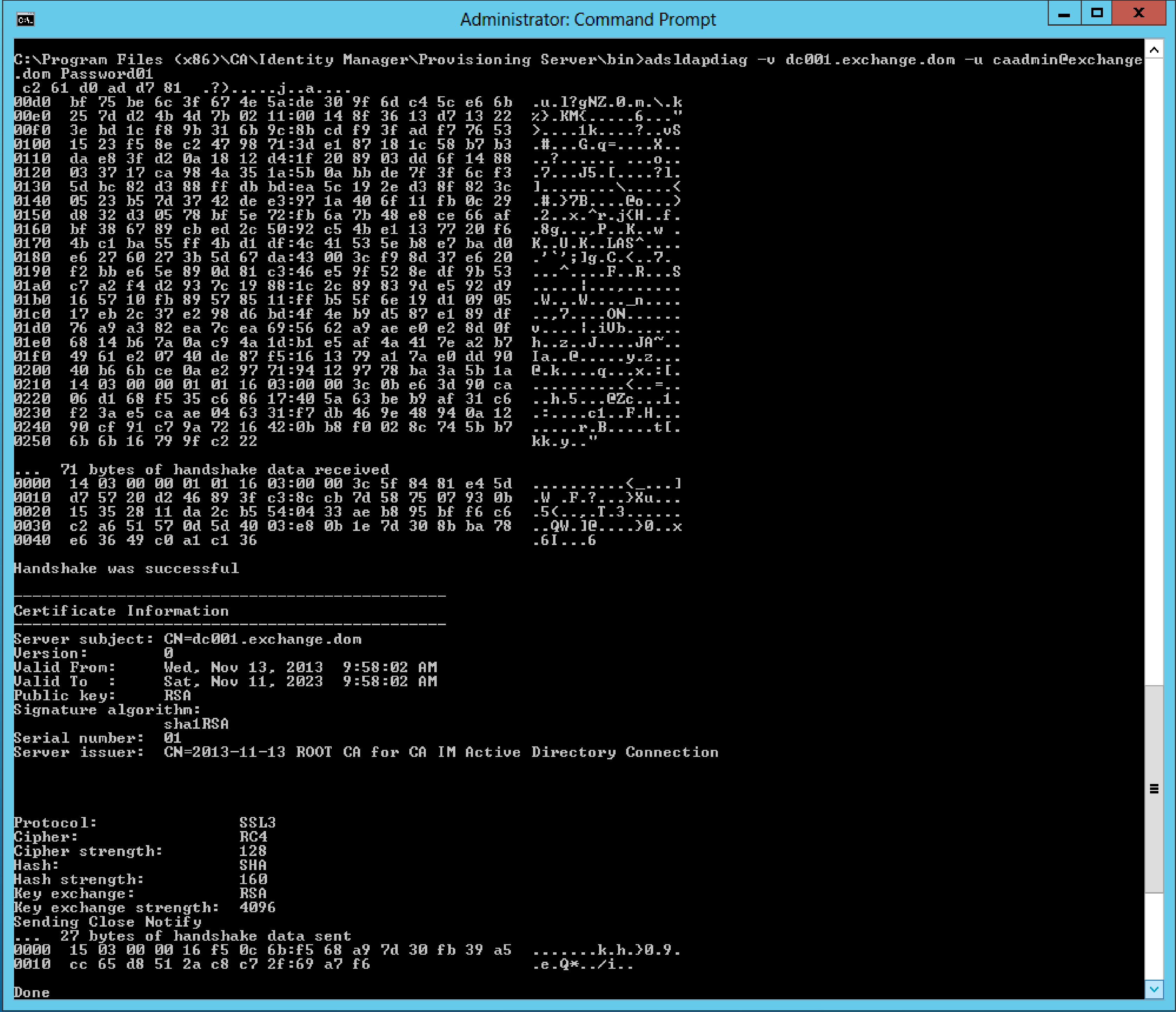
SSL/TLS Mode: Auto determine by port number

Certficate list returned from server

dc001.exchange.dom

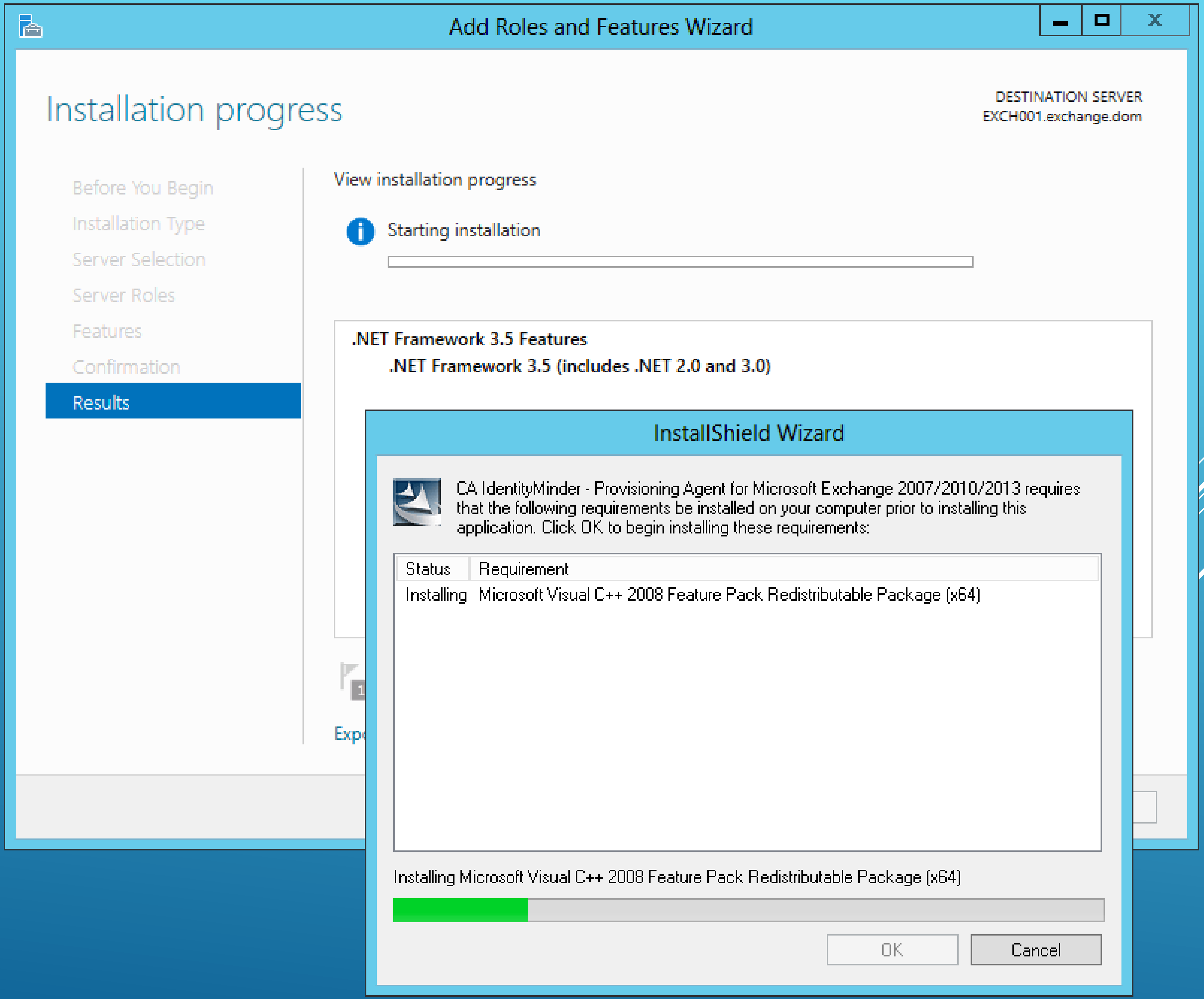
| | |
|---|---|
| Subject | CN=dc001.exchange.dom |
| Issuer | CN=2013-11-13 ROOT CA for CA IM Active Directory Connection |
| Serial Number | 01 |
| Valid From | 13-NOV-2013 |
| Valid To | 11-NOV-2023 |

# USE THE BINARY IN THE IMPS FOLDER TO CHECK SSL CERT FOR AD DOMAIN



```
C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\bin>adsldapdiag -v dc001.exchange.dom -u caadmin@exchange
.dom Password01
 c2 61 d0 ad d7 81  .?)....j..a....
00d0  bf 75 be 6c 3f 67 4e 5a:de 30 9f 6d c4 5c e6 6b  .u.l?gNZ.0.m.\.k
00e0  25 7d d2 4b 4d 7b 02 11:00 14 8f 36 13 d7 13 22  %}.KM{.....6..."
00f0  3e bd 1c f8 9b 31 6b 9c:8b cd f9 3f ad f7 76 53  >....1k....?..vS
0100  15 23 f5 8e c2 47 98 71:3d e1 87 18 1c 58 b7 b3  .#...G.q=....X..
0110  da e8 3f d2 0a 18 12 d4:1f 20 89 03 dd 6f 14 88  ..?...... ...o..
0120  03 37 17 ca 98 4a 35 1a:5b 0a bb de 7f 3f 6c f3  .7...J5.[....?l.
0130  5d bc 82 d3 88 ff db bd:ea 5c 19 2e d3 8f 82 3c  ]........\.....<
0140  05 23 b5 7d 37 42 de e3:97 1a 40 6f 11 fb 0c 29  .#.}7B....@o...)
0150  d8 32 d3 05 78 bf 5e 72:fb 6a 7b 48 e8 ce 66 af  .2..x.^r.j{H..f.
0160  bf 38 67 89 cb ed 2c 50:92 c5 4b e1 13 77 20 f6  .8g...,P..K..w .
0170  4b c1 ba 55 ff 4b d1 df:4c 41 53 5e b8 e7 ba d0  K..U.K..LAS^....
0180  e6 27 60 27 3b 5d 67 da:43 00 3c f9 8d 37 e6 20  .'`';]g.C.<..7.
0190  f2 bb e6 5e 89 0d 81 c3:46 e5 9f 52 8e df 9b 53  ...^....F..R...S
01a0  c7 a2 f4 d2 93 7c 19 88:1c 2c 89 83 9d e5 92 d9  .....|..,.......
01b0  16 57 10 fb 89 57 85 11:ff b5 5f 6e 19 d1 09 05  .W...W...._n....
01c0  17 eb 2c 37 e2 98 d6 bd:4f 4e b9 d5 87 e1 89 df  ..,7....ON......
01d0  76 a9 a3 82 ea 7c ea 69:56 62 a9 ae e0 e2 8d 0f  v....|.iVb......
01e0  68 14 b6 7a 0a c9 4a 1d:b1 e5 af 4a 41 7e a2 b7  h..z..J....JA~..
01f0  49 61 e2 07 40 de 87 f5:16 13 79 a1 7a e0 dd 90  Ia..@.....y.z...
0200  40 b6 6b ce 0a e2 97 71:94 12 97 78 ba 3a 5b 1a  @.k....q...x.:[.
0210  14 03 00 00 01 01 16 03:00 00 3c 0b e6 3d 90 ca  ..........<..=..
0220  06 d1 68 f5 35 c6 86 17:40 5a 63 be b9 af 31 c6  ..h.5...@Zc...1.
0230  f2 3a e5 ca ae 04 63 31:f7 db 46 9e 48 94 0a 12  .:....c1..F.H...
0240  90 cf 91 c7 9a 72 16 42:0b b8 f0 02 8c 74 5b b7  .....r.B.....t[.
0250  6b 6b 16 79 9f c2 22                             kk.y.."

...  71 bytes of handshake data received
0000  14 03 00 00 01 01 16 03:00 00 3c 5f 84 81 e4 5d  ..........<_...]
0010  d7 57 20 d2 46 89 3f c3:8c cb 7d 58 75 07 93 0b  .W .F.?...}Xu...
0020  15 35 28 11 da 2c b5 54:04 33 ae b8 95 bf f6 c6  .5(..,.T.3......
0030  c2 a6 51 57 0d 5d 40 03:e8 0b 1e 7d 30 8b ba 78  ..QW.]@....}0..x
0040  e6 36 49 c0 a1 c1 36                             .6I...6

Handshake was successful

----------------------------------------------
Certificate Information
----------------------------------------------
Server subject: CN=dc001.exchange.dom
Version:        0
Valid From:     Wed, Nov 13, 2013  9:58:02 AM
Valid To  :     Sat, Nov 11, 2023  9:58:02 AM
Public key:     RSA
Signature algorithm:
                sha1RSA
Serial number:  01
Server issuer:  CN=2013-11-13 ROOT CA for CA IM Active Directory Connection



Protocol:               SSL3
Cipher:                 RC4
Cipher strength:        128
Hash:                   SHA
Hash strength:          160
Key exchange:           RSA
Key exchange strength:  4096
Sending Close Notify
...  27 bytes of handshake data sent
0000  15 03 00 00 16 f5 0c 6b:f5 68 a9 7d 30 fb 39 a5  .......k.h.}0.9.
0010  cc 65 d8 51 2a c8 c7 2f:69 a7 f6                 .e.Q*../i..

Done
```

# ENSURE EXCHANGE SERVER HAS .NET 3.5 INSTALLED; OTHERWISE IT WILL REQUIRE A REBOOT OF THE EXCHANGE SERVER + ANOTHER REBOOT FOR MS VC++ 2008



Installation progress

DESTINATION SERVER
EXCH001.exchange.dom

View installation progress

Starting installation

.NET Framework 3.5 Features
.NET Framework 3.5 (includes .NET 2.0 and 3.0)

CA IdentityMinder - Provisioning Agent for Microsoft Exchange 2007/2010/2013 requires that the following requirements be installed on your computer prior to installing this application. Click OK to begin installing these requirements:

| Status | Requirement |
|---|---|
| Installing | Microsoft Visual C++ 2008 Feature Pack Redistributable Package (x64) |

Installing Microsoft Visual C++ 2008 Feature Pack Redistributable Package (x64)