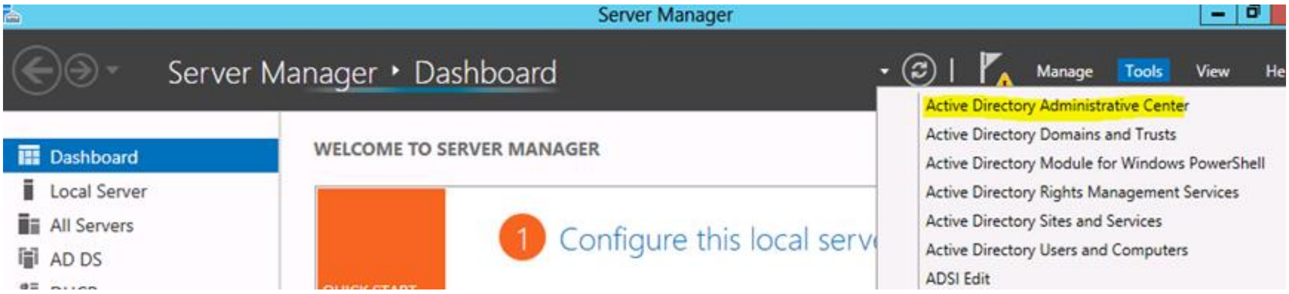
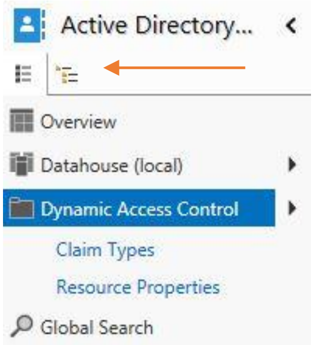
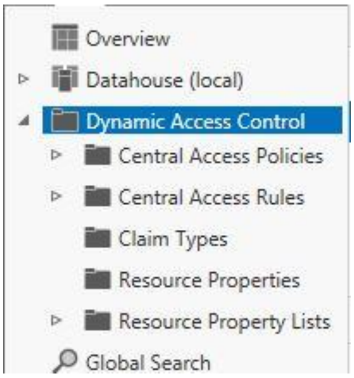
LAB: DYNAMIC ACCESS CONTROL

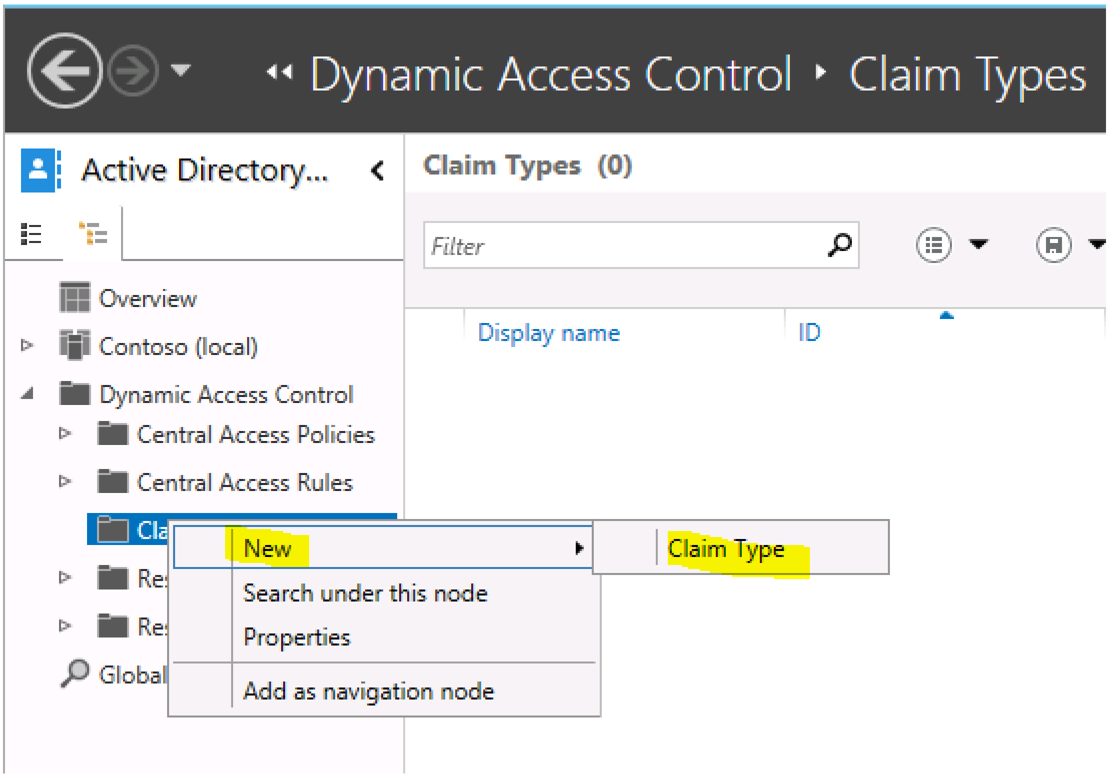
BUR-DC1 üzerinde Active Directory Administrative Center Aracını çalıştırın.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Dashboard
Local Server
All Servers
AD DS
WELCOME TO SERVER MANAGER
1 Configure this local serv
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Rights Management Services
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit

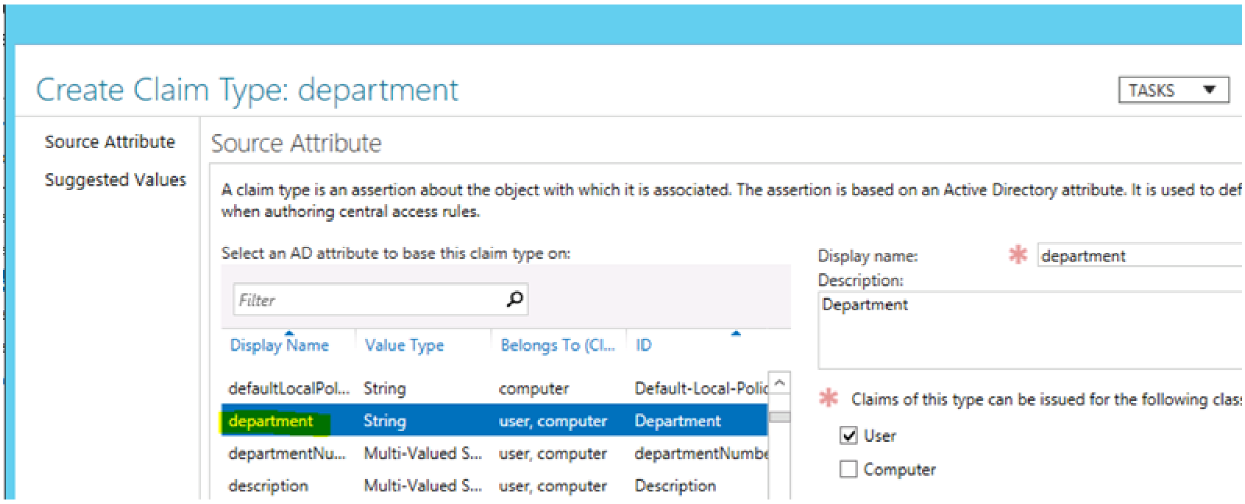




Dynamic Access Control altında **Claim Types** üzerinde sağ tıklayın.



Department ve Country alanlarını Filter bölümüne yazıp ekleyin



Create Claim Type: department

Source Attribute

A claim type is an assertion about the object with which it is associated. The assertion is based on an Active Directory attribute. It is used to def when authoring central access rules.

Select an AD attribute to base this claim type on:

Display Name	Value Type	Belongs To (Cl...	ID
defaultLocalPol...	String	computer	Default-Local-Polic
department	String	user, computer	Department
departmentNu...	Multi-Valued S...	user, computer	departmentNumbe
description	Multi-Valued S...	user, computer	Description

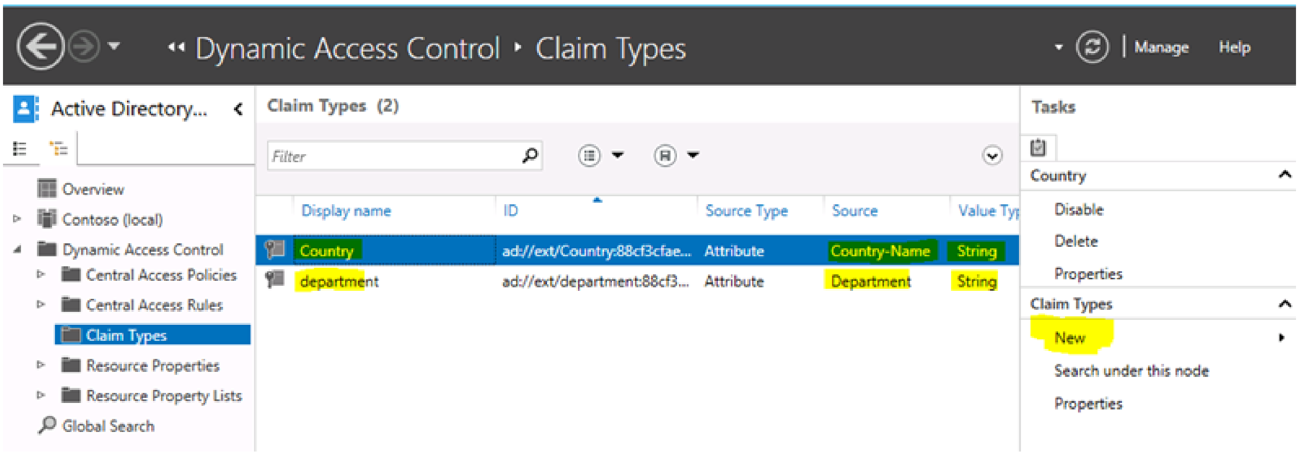
Display name: * department

Description: Department

* Claims of this type can be issued for the following clas

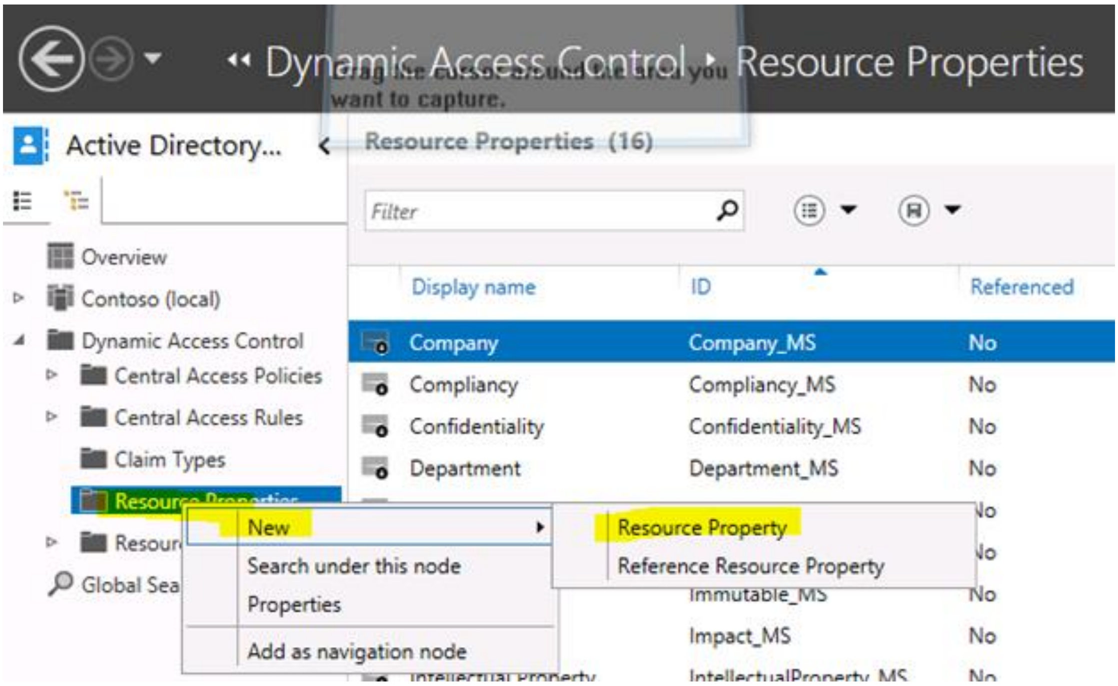
☑ User

☐ Computer



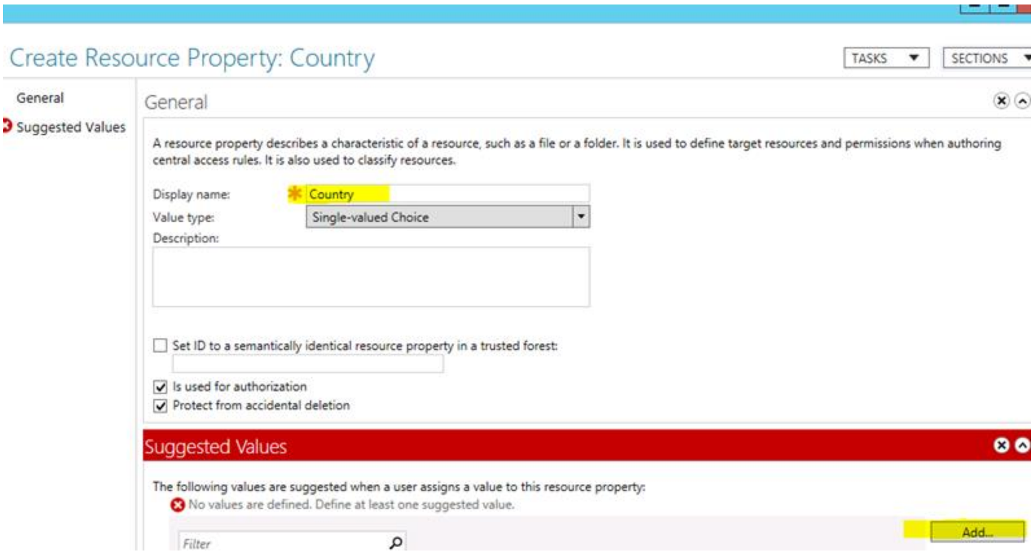
Claim Types (2)

Display name	ID	Source Type	Source	Value Typ
Country	ad://ext/Country:88cf3cfae...	Attribute	Country-Name	String
department	ad://ext/department:88cf3...	Attribute	Department	String



Resource Properties (16)

Display name	ID	Referenced
Company	Company_MS	No
Compliancy	Compliancy_MS	No
Confidentiality	Confidentiality_MS	No
Department	Department_MS	No
		No
		No
	Immutable_MS	No
	Impact_MS	No
Intellectual Property	IntellectualProperty_MS	No



Create Resource Property: Country

General

A resource property describes a characteristic of a resource, such as a file or a folder. It is used to define target resources and permissions when authoring central access rules. It is also used to classify resources.

Display name: Country

Value type: Single-valued Choice

Description:

☐ Set ID to a semantically identical resource property in a trusted forest:

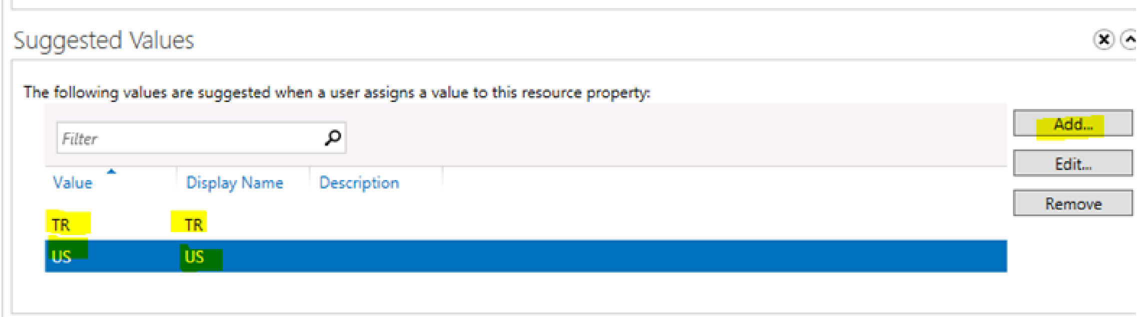
☑ Is used for authorization

☑ Protect from accidental deletion

Suggested Values

The following values are suggested when a user assigns a value to this resource property:

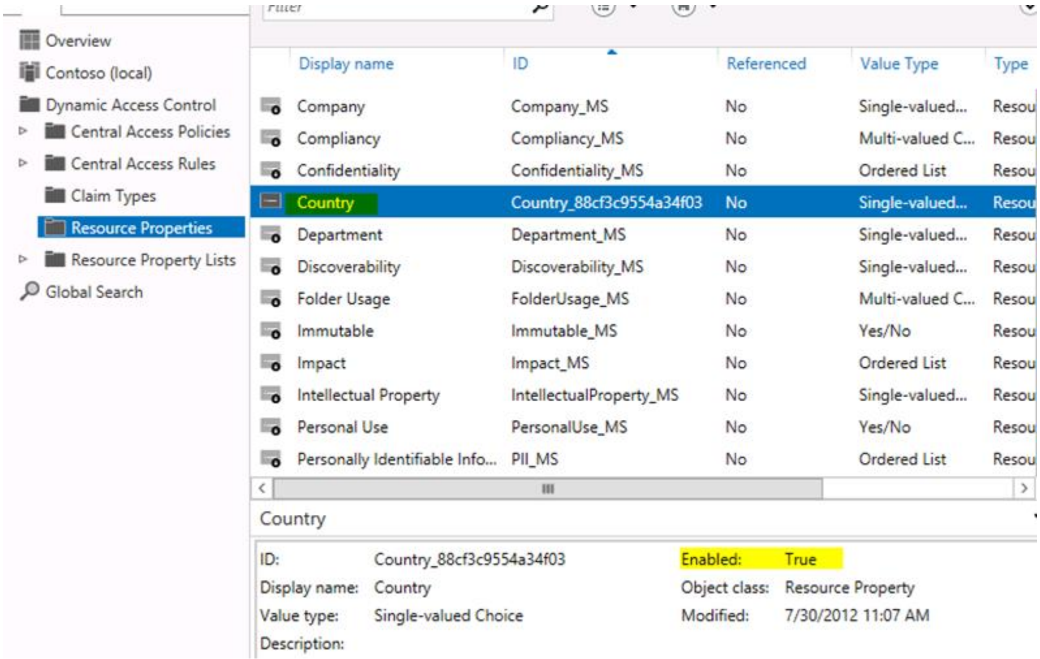
No values are defined. Define at least one suggested value.



Suggested Values

The following values are suggested when a user assigns a value to this resource property:

Value	Display Name	Description
TR	TR	
US	US	



Display name	ID	Referenced	Value Type	Type
Company	Company_MS	No	Single-valued...	Resou
Compliancy	Compliancy_MS	No	Multi-valued C...	Resou
Confidentiality	Confidentiality_MS	No	Ordered List	Resou
Country	Country_88cf3c9554a34f03	No	Single-valued...	Resou
Department	Department_MS	No	Single-valued...	Resou
Discoverability	Discoverability_MS	No	Single-valued...	Resou
Folder Usage	FolderUsage_MS	No	Multi-valued C...	Resou
Immutable	Immutable_MS	No	Yes/No	Resou
Impact	Impact_MS	No	Ordered List	Resou
Intellectual Property	IntellectualProperty_MS	No	Single-valued...	Resou
Personal Use	PersonalUse_MS	No	Yes/No	Resou
Personally Identifiable Info...	PII_MS	No	Ordered List	Resou

Country

ID: Country_88cf3c9554a34f03

Enabled: True

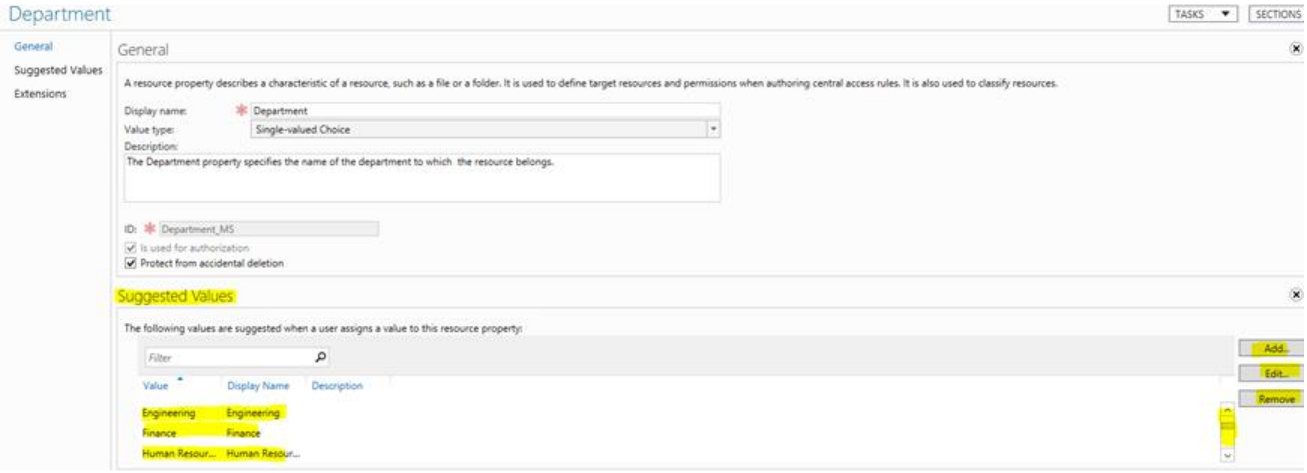
Display name: Country

Object class: Resource Property

Value type: Single-valued Choice

Modified: 7/30/2012 11:07 AM

Description:



Department

General

A resource property describes a characteristic of a resource, such as a file or a folder. It is used to define target resources and permissions when authoring central access rules. It is also used to classify resources.

Display name: Department

Value type: Single-valued Choice

Description:

The Department property specifies the name of the department to which the resource belongs.

ID: Department_MS

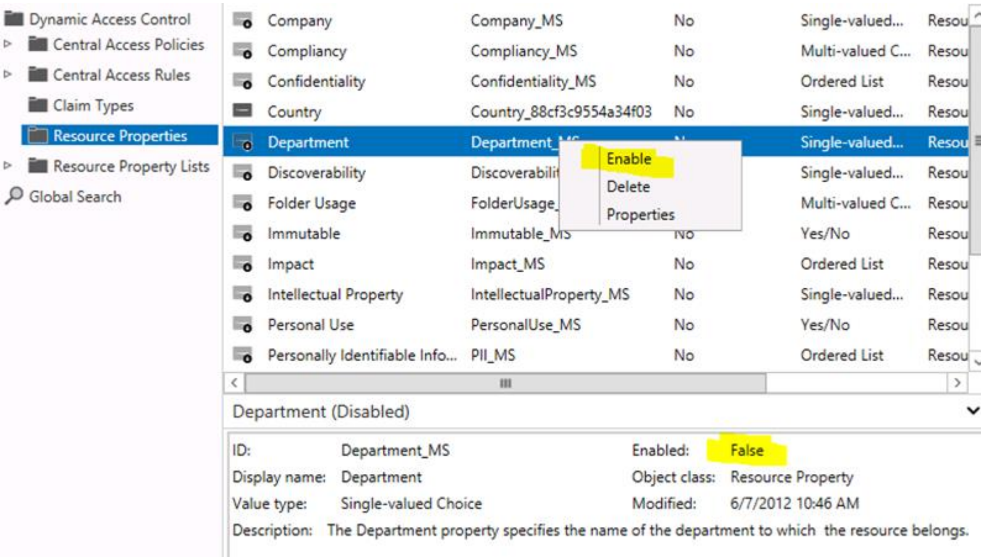
☑ Is used for authorization

☑ Protect from accidental deletion

Suggested Values

The following values are suggested when a user assigns a value to this resource property:

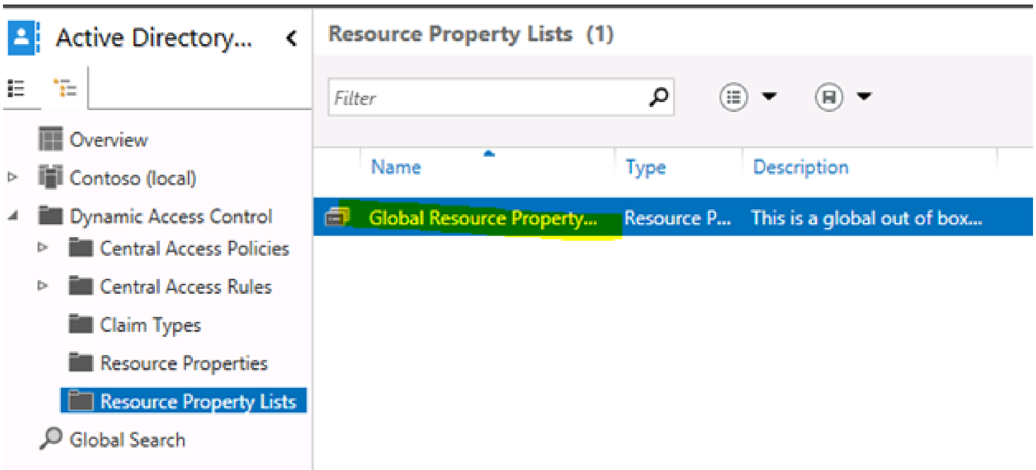
Value	Display Name	Description
Engineering	Engineering	
Finance	Finance	
Human Resour...	Human Resour...	



Company	Company_MS	No	Single-valued...	Resou
Compliancy	Compliancy_MS	No	Multi-valued C...	Resou
Confidentiality	Confidentiality_MS	No	Ordered List	Resou
Country	Country_88cf3c9554a34f03	No	Single-valued...	Resou
Department	Department_MS	N	Single-valued...	Resou
Discoverability	Discoverabilit		Single-valued...	Resou
Folder Usage	FolderUsage_		Multi-valued C...	Resou
Immutable	Immutable_MS	No	Yes/No	Resou
Impact	Impact_MS	No	Ordered List	Resou
Intellectual Property	IntellectualProperty_MS	No	Single-valued...	Resou
Personal Use	PersonalUse_MS	No	Yes/No	Resou
Personally Identifiable Info...	PII_MS	No	Ordered List	Resou

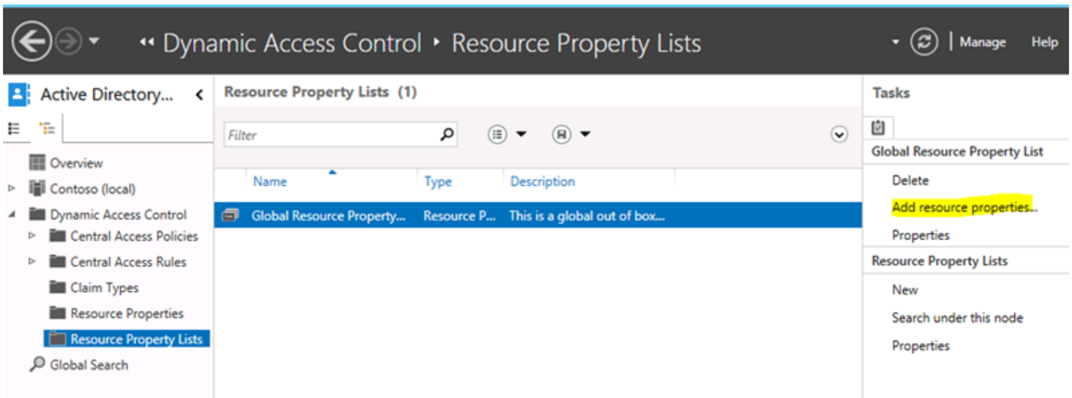
Department (Disabled)

ID: Department_MS
Enabled: False
Display name: Department
Object class: Resource Property
Value type: Single-valued Choice
Modified: 6/7/2012 10:46 AM
Description: The Department property specifies the name of the department to which the resource belongs.



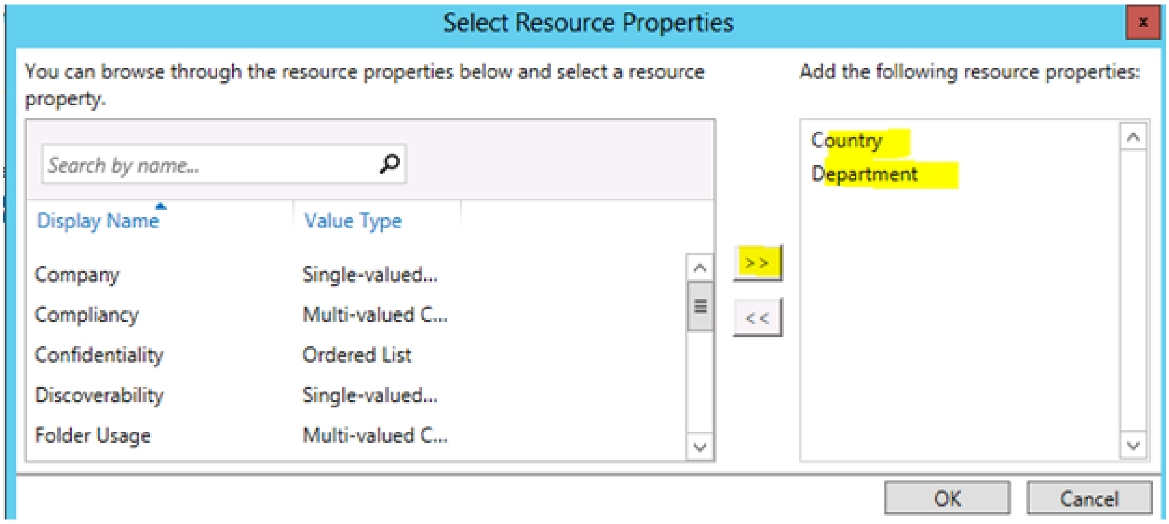
Resource Property Lists (1)

Name	Type	Description
Global Resource Property...	Resource P...	This is a global out of box...



Resource Property Lists (1)

Name	Type	Description
Global Resource Property...	Resource P...	This is a global out of box...

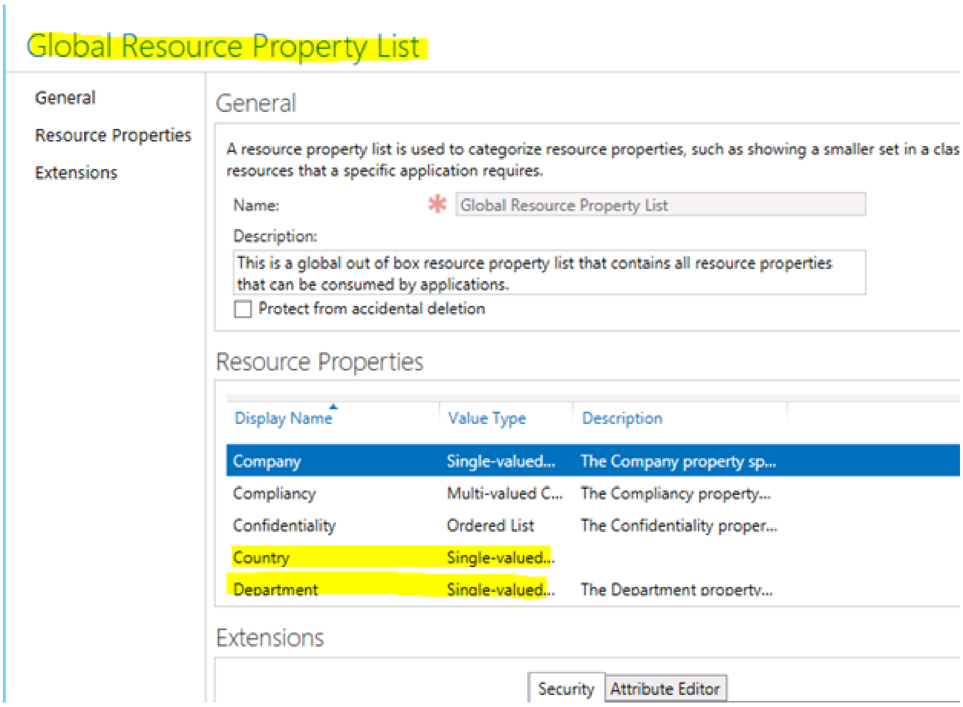

Select Resource Properties

You can browse through the resource properties below and select a resource property.

Add the following resource properties:

Display Name	Value Type
Company	Single-valued...
Compliancy	Multi-valued C...
Confidentiality	Ordered List
Discoverability	Single-valued...
Folder Usage	Multi-valued C...

Country
Department



Global Resource Property List

General

A resource property list is used to categorize resource properties, such as showing a smaller set in a clas resources that a specific application requires.

Name: * Global Resource Property List

Description:

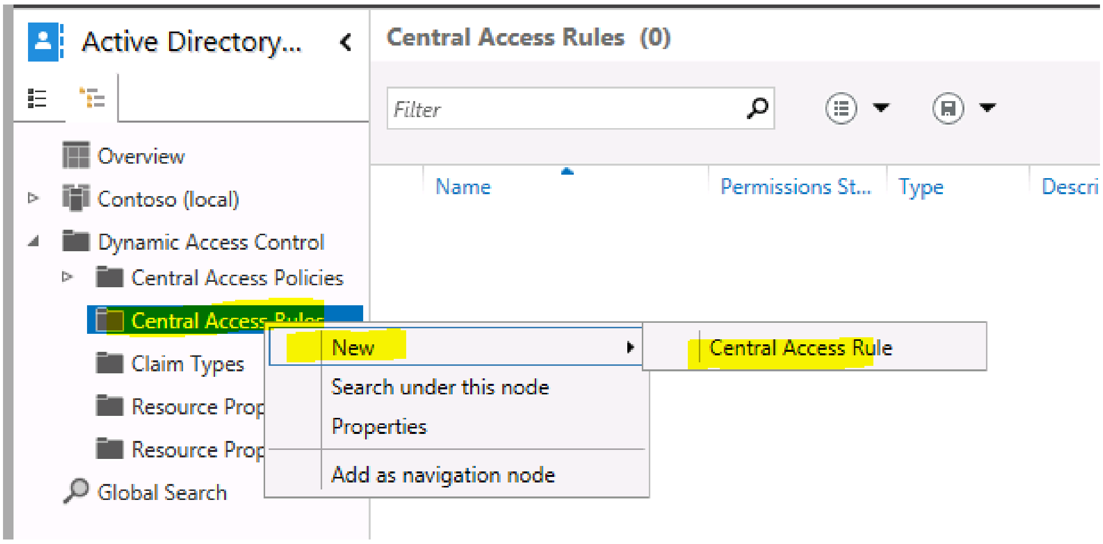
This is a global out of box resource property list that contains all resource properties that can be consumed by applications.

□ Protect from accidental deletion

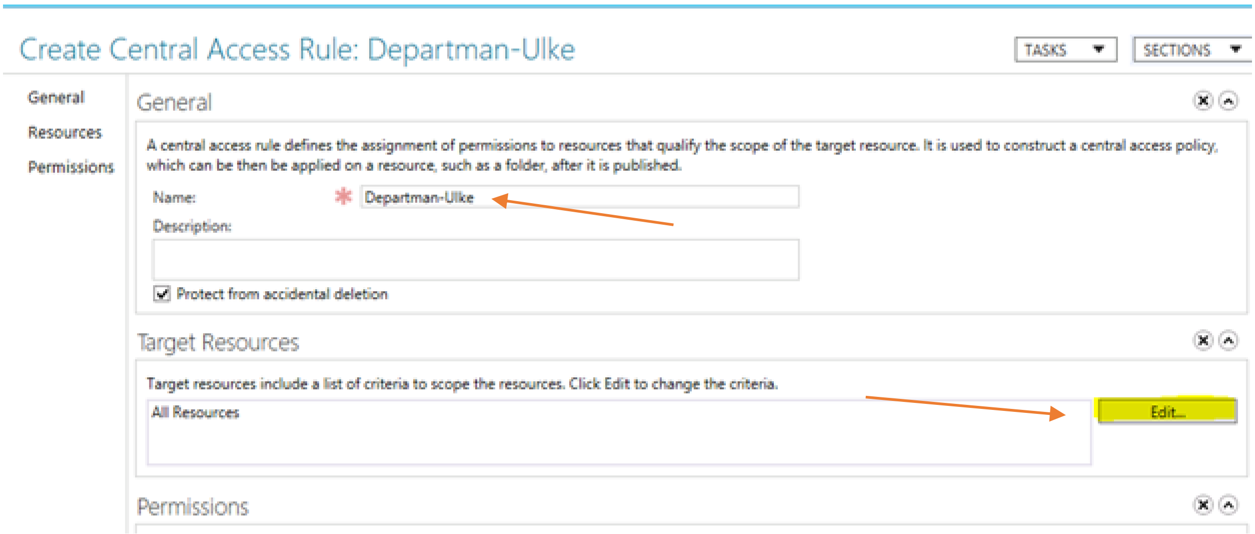
Resource Properties

Display Name	Value Type	Description
Company	Single-valued...	The Company property sp...
Compliancy	Multi-valued C...	The Compliancy property...
Confidentiality	Ordered List	The Confidentiality proper...
Country	Single-valued...	
Department	Single-valued...	The Department property...

Extensions



Central Access Rules (0)



Create Central Access Rule: Departman-Ulke

General

A central access rule defines the assignment of permissions to resources that qualify the scope of the target resource. It is used to construct a central access policy, which can be then be applied on a resource, such as a folder, after it is published.

Name: * Departman-Ulke

Description:

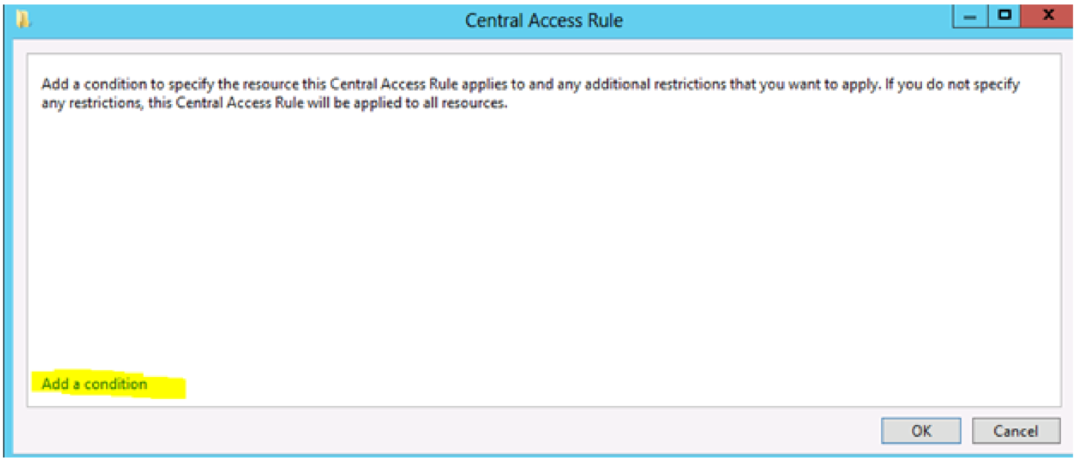
☑ Protect from accidental deletion

Target Resources

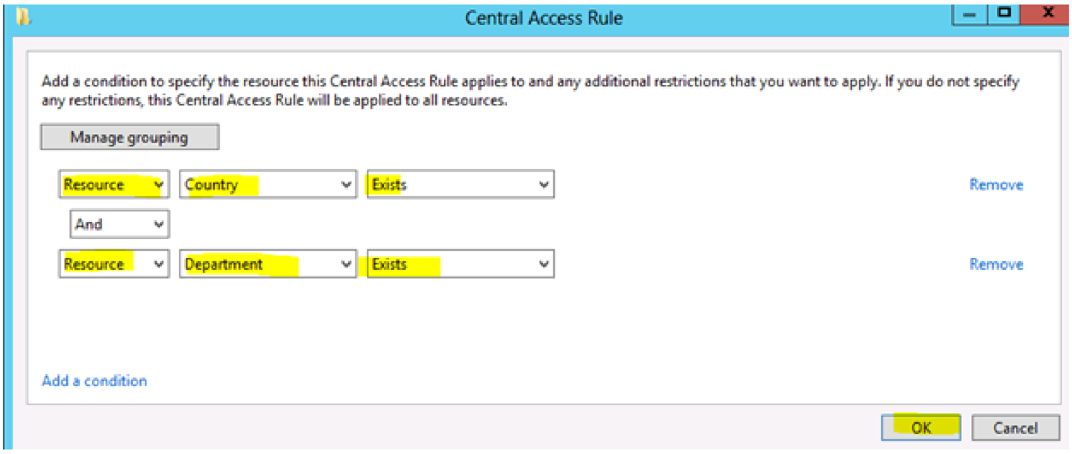
Target resources include a list of criteria to scope the resources. Click Edit to change the criteria.

All Resources

Permissions



Add a condition to specify the resource this Central Access Rule applies to and any additional restrictions that you want to apply. If you do not specify any restrictions, this Central Access Rule will be applied to all resources.

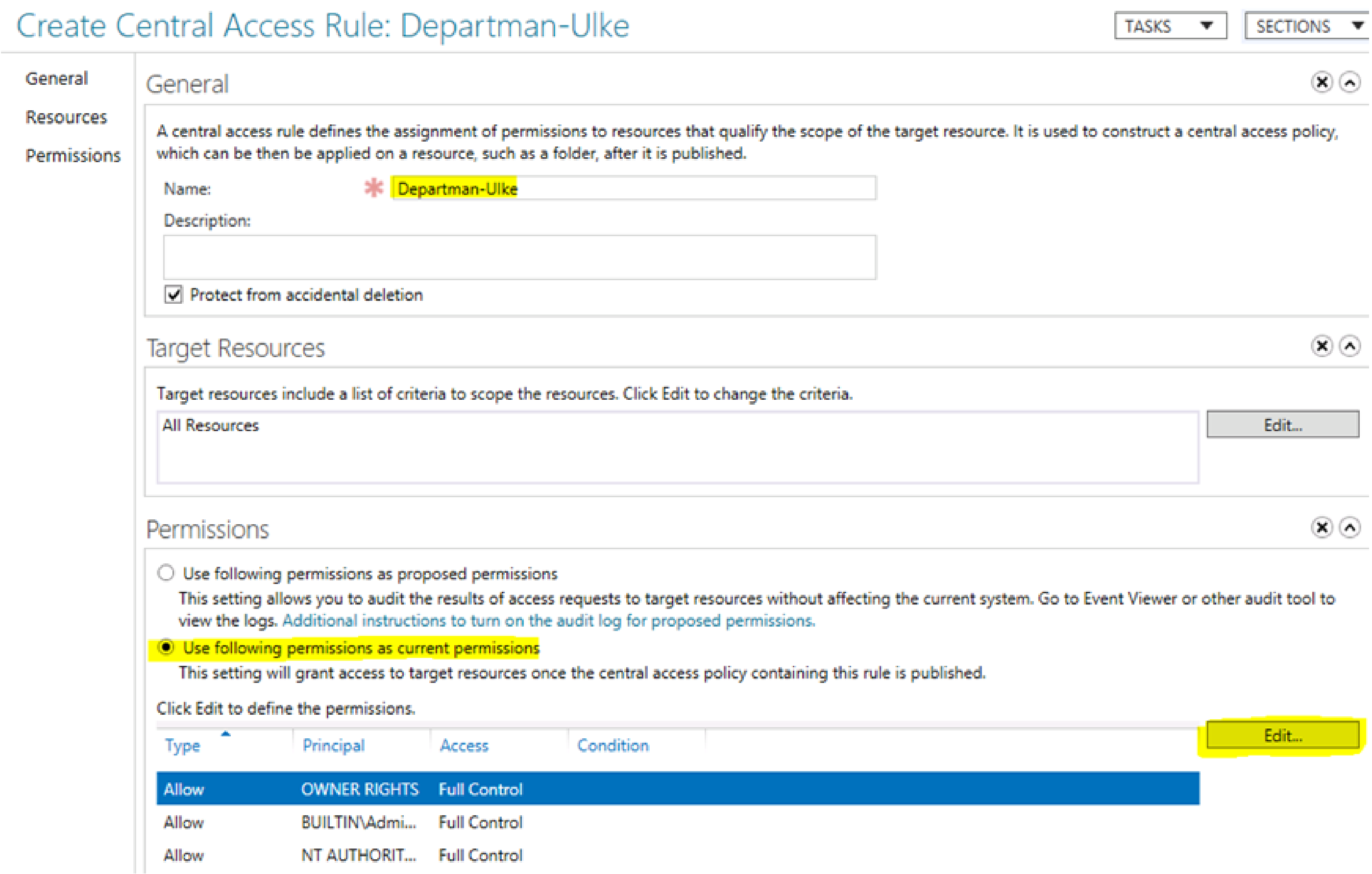


Add a condition to specify the resource this Central Access Rule applies to and any additional restrictions that you want to apply. If you do not specify any restrictions, this Central Access Rule will be applied to all resources.

Resource | Country | Exists

And

Resource | Department | Exists



General

A central access rule defines the assignment of permissions to resources that qualify the scope of the target resource. It is used to construct a central access policy, which can be then be applied on a resource, such as a folder, after it is published.

Name: * Departman-Ulke

Description:

☑ Protect from accidental deletion

Target Resources

Target resources include a list of criteria to scope the resources. Click Edit to change the criteria.

All Resources

Permissions

○ Use following permissions as proposed permissions

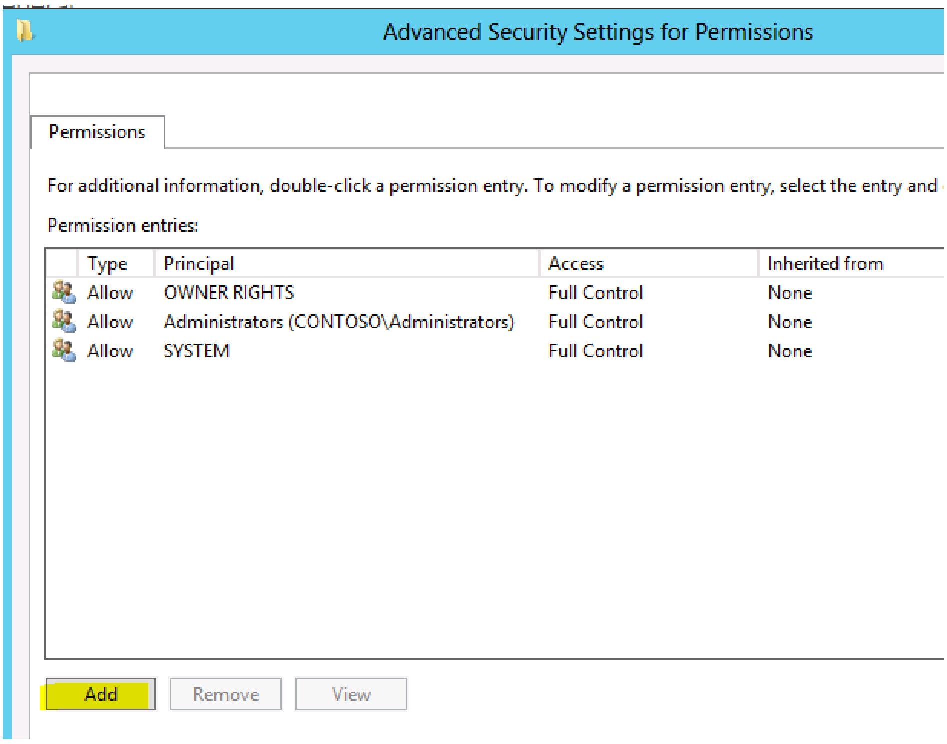
This setting allows you to audit the results of access requests to target resources without affecting the current system. Go to Event Viewer or other audit tool to view the logs. Additional instructions to turn on the audit log for proposed permissions.

● Use following permissions as current permissions

This setting will grant access to target resources once the central access policy containing this rule is published.

Click Edit to define the permissions.

Type	Principal	Access	Condition
Allow	OWNER RIGHTS	Full Control	
Allow	BUILTIN\Admi...	Full Control	
Allow	NT AUTHORIT...	Full Control	



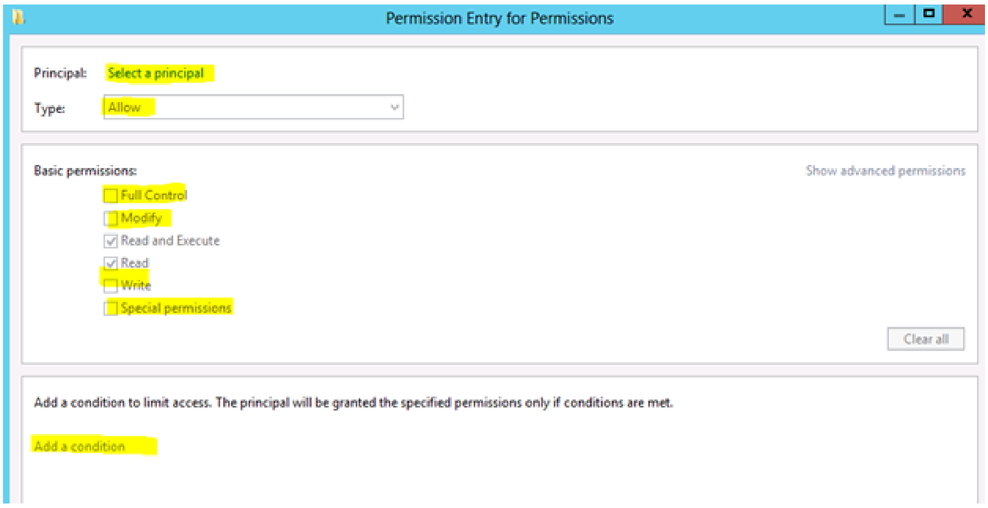
Advanced Security Settings for Permissions

Permissions

For additional information, double-click a permission entry. To modify a permission entry, select the entry and

Permission entries:

Type	Principal	Access	Inherited from
Allow	OWNER RIGHTS	Full Control	None
Allow	Administrators (CONTOSO\Administrators)	Full Control	None
Allow	SYSTEM	Full Control	None



Permission Entry for Permissions

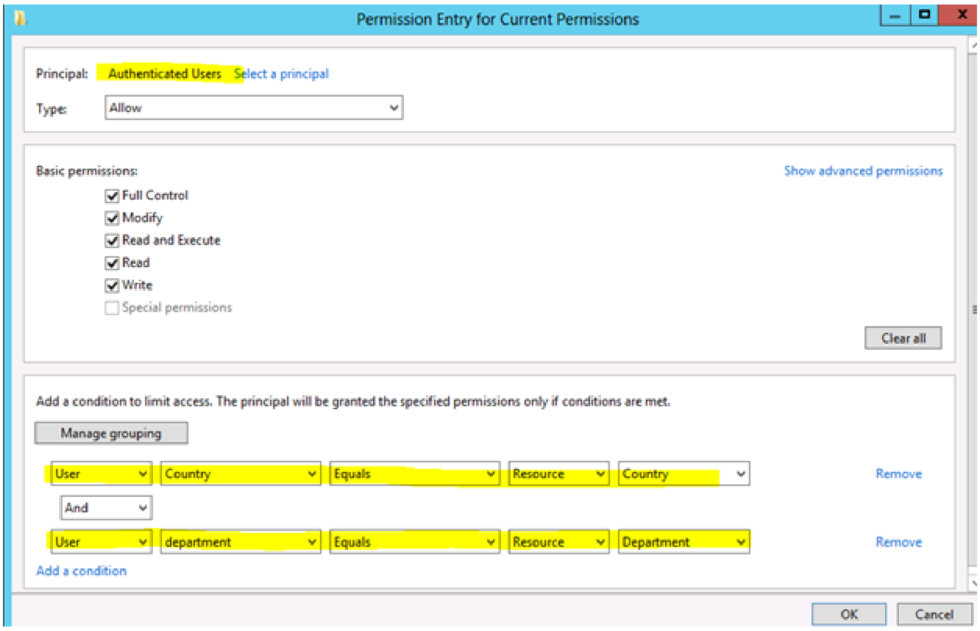
Principal: Select a principal

Type: Allow

Basic permissions:

- □ Full Control
- □ Modify
- ☑ Read and Execute
- ☑ Read
- □ Write
- □ Special permissions

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.



Permission Entry for Current Permissions

Principal: Authenticated Users Select a principal

Type: Allow

Basic permissions:

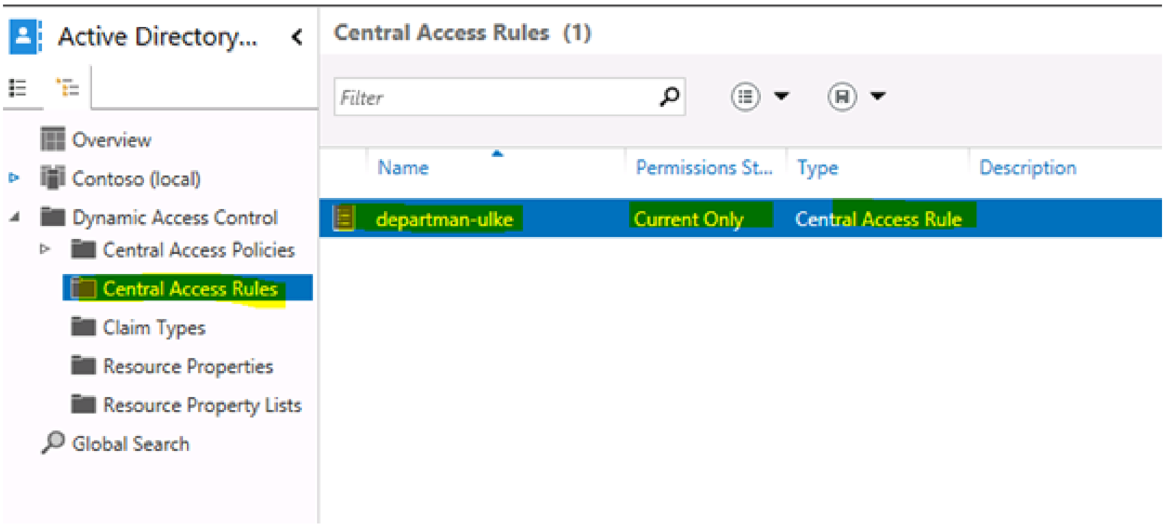
- ☑ Full Control
- ☑ Modify
- ☑ Read and Execute
- ☑ Read
- ☑ Write
- □ Special permissions

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

User | Country | Equals | Resource | Country | Remove

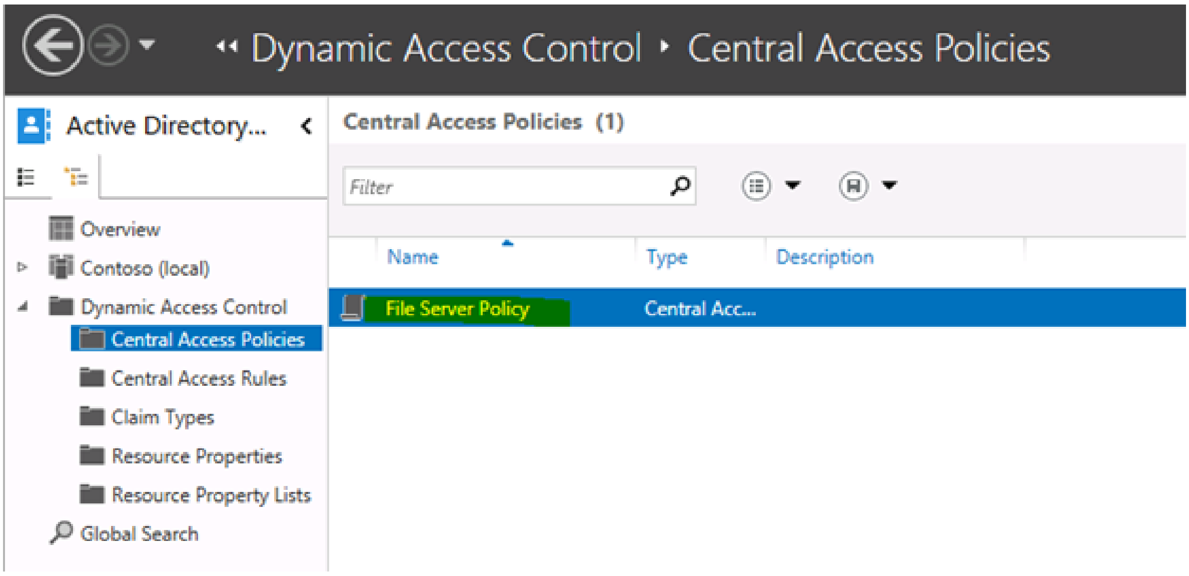
And

User | department | Equals | Resource | Department | Remove



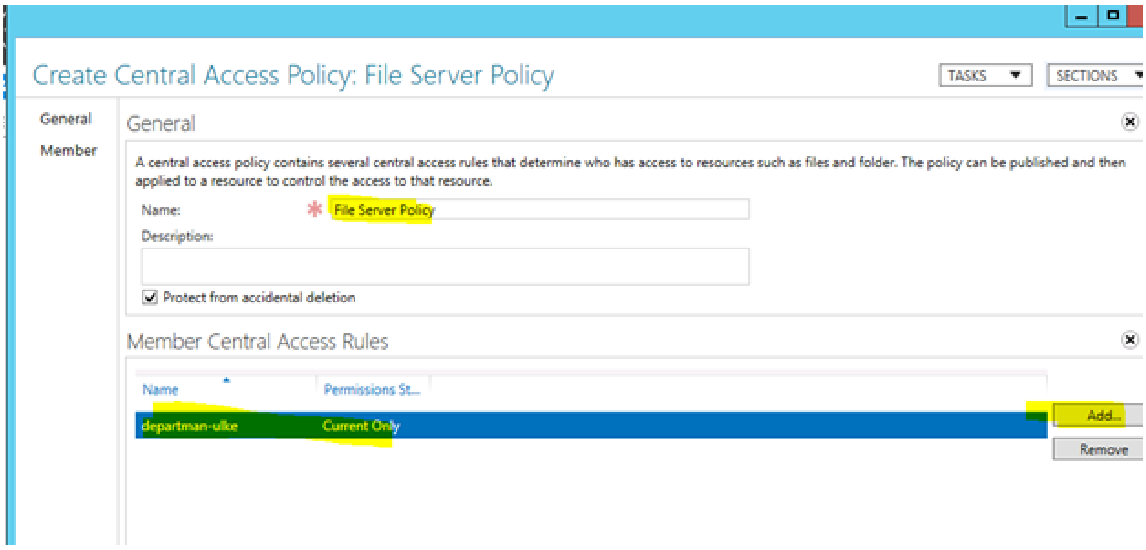
Central Access Rules (1)

Name	Permissions St...	Type	Description
departman-ulke	Current Only	Central Access Rule	



Central Access Policies (1)

Name	Type	Description
File Server Policy	Central Acc...	



Create Central Access Policy: File Server Policy

General

A central access policy contains several central access rules that determine who has access to resources such as files and folder. The policy can be published and then applied to a resource to control the access to that resource.

Name: * File Server Policy

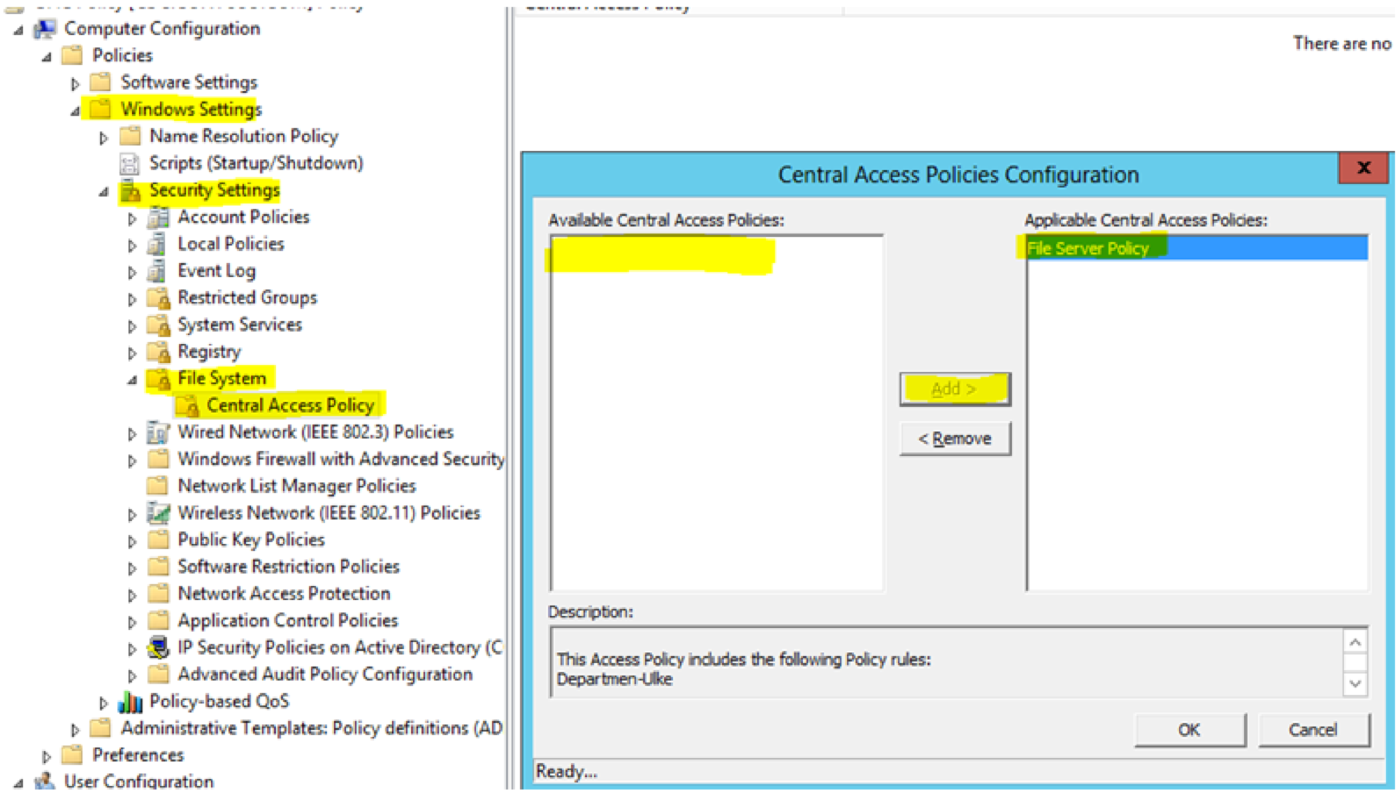
Description:

☑ Protect from accidental deletion

Member Central Access Rules

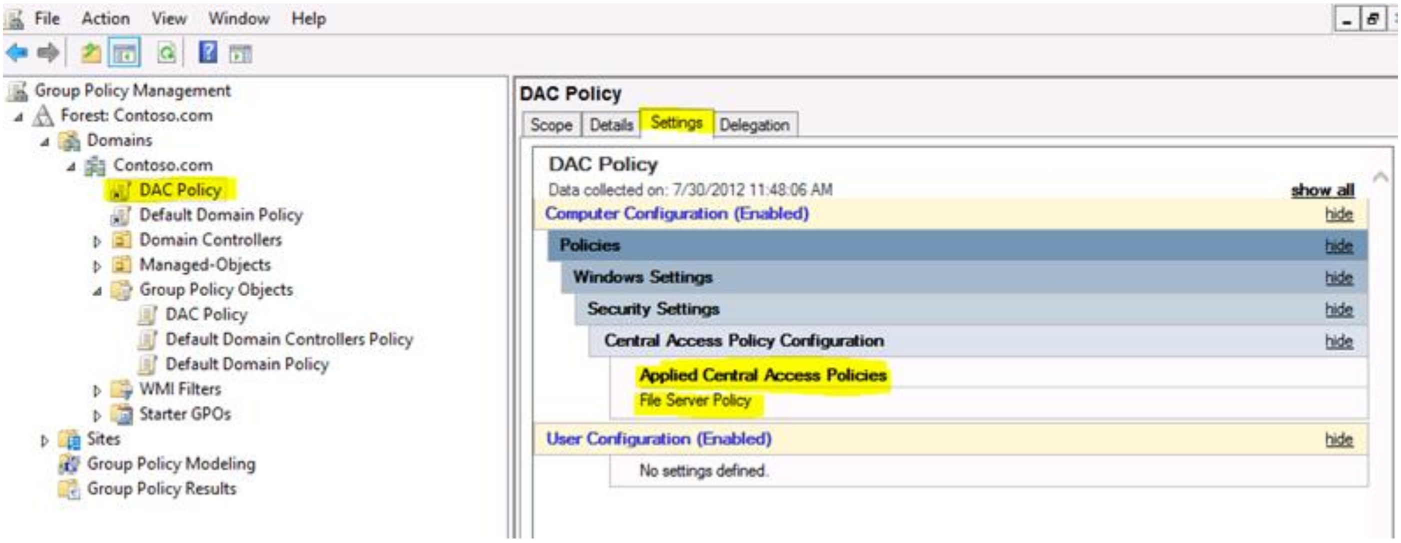
Name	Permissions St...
departman-ulke	Current Only

BUR-DC1 üzerinde Group Policy Management'ı açın


Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Central Access Policy
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (C
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (AD
Preferences
User Configuration
There are no
Central Access Policies Configuration
Available Central Access Policies:
Applicable Central Access Policies:
Add >
< Remove
Description:
OK
Cancel
Ready...

Applicable Central Access Policies: File Server Policy

Description: This Access Policy includes the following Policy rules:
Departmen-Ulke



DAC Policy

Data collected on: 7/30/2012 11:48:06 AM

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Central Access Policy Configuration

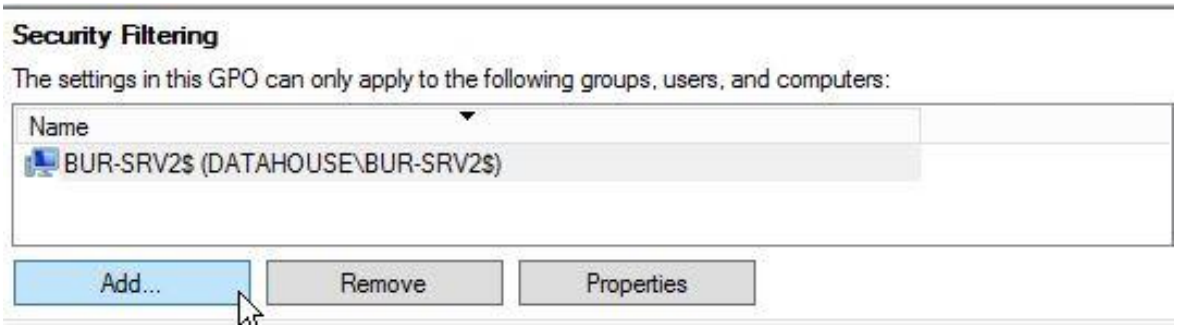
Applied Central Access Policies

File Server Policy

User Configuration (Enabled)

No settings defined.

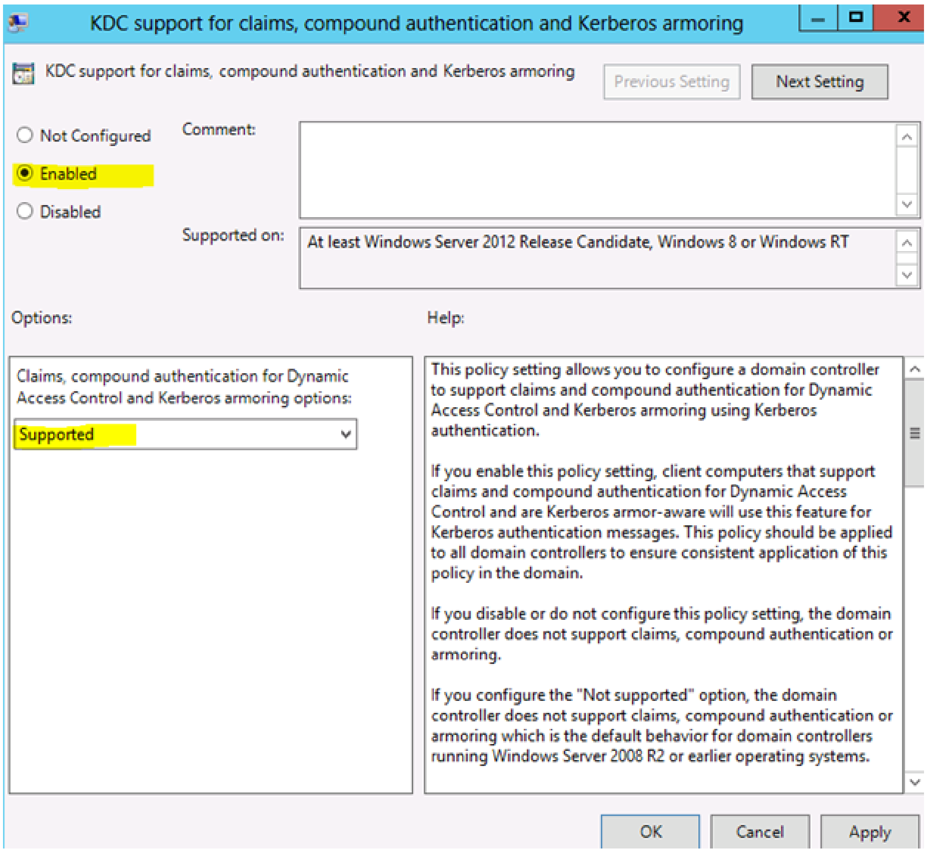
Security Filtering alanında sadece File server olarak kullanacağınız sunucu adını yazın



The settings in this GPO can only apply to the following groups, users, and computers:

BUR-SRV2$ (DATAHOUSE\BUR-SRV2$)

Group Policy üzerinde “**DEFAULT DOMAIN CONTROLLERS POLICY”** GPOSU üzerinde aşağıdaki policyleri ekleyin



KDC support for claims, compound authentication and Kerberos armoring

KDC support for claims, compound authentication and Kerberos armoring

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2012 Release Candidate, Windows 8 or Windows RT

Options:

Claims, compound authentication for Dynamic Access Control and Kerberos armoring options:

Supported

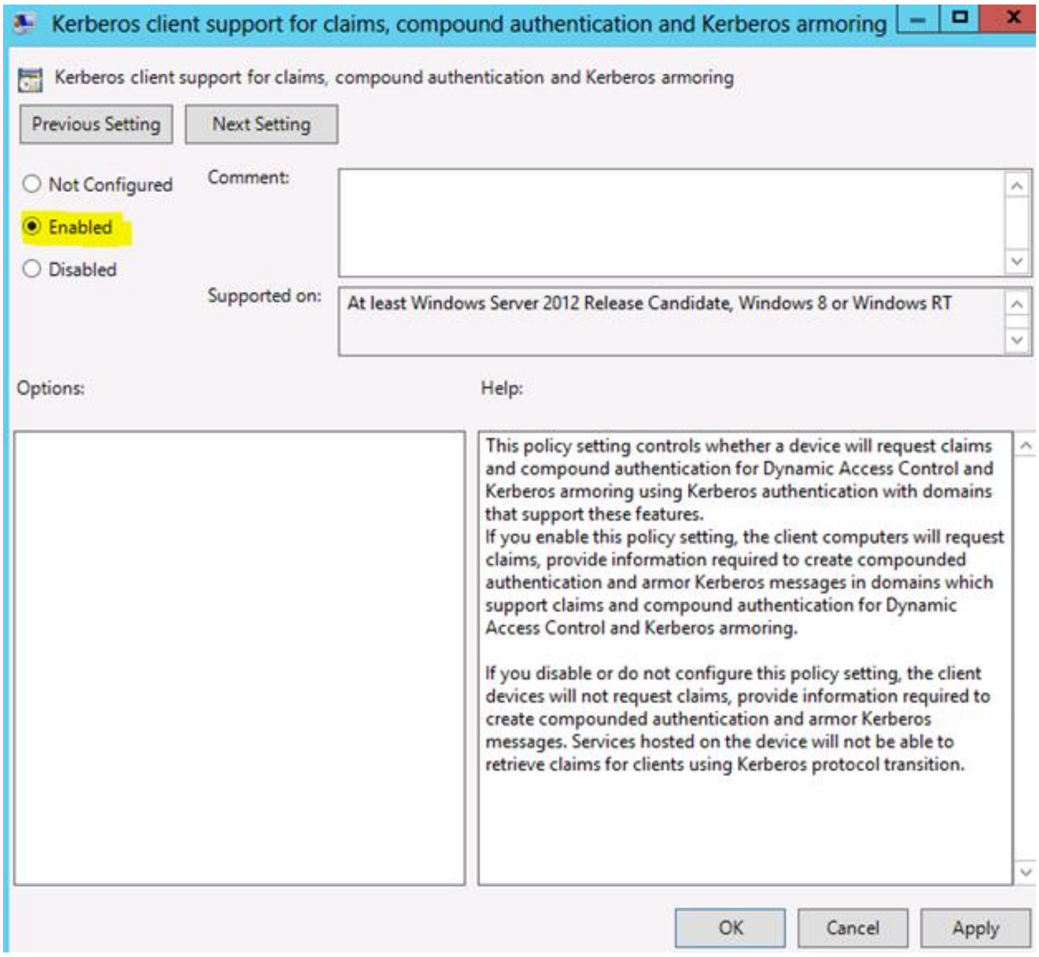
Help:

This policy setting allows you to configure a domain controller to support claims and compound authentication for Dynamic Access Control and Kerberos armoring using Kerberos authentication.

If you enable this policy setting, client computers that support claims and compound authentication for Dynamic Access Control and are Kerberos armor-aware will use this feature for Kerberos authentication messages. This policy should be applied to all domain controllers to ensure consistent application of this policy in the domain.

If you disable or do not configure this policy setting, the domain controller does not support claims, compound authentication or armoring.

If you configure the "Not supported" option, the domain controller does not support claims, compound authentication or armoring which is the default behavior for domain controllers running Windows Server 2008 R2 or earlier operating systems.



Kerberos client support for claims, compound authentication and Kerberos armoring

Kerberos client support for claims, compound authentication and Kerberos armoring

○ Not Configured
● Enabled
○ Disabled

Comment:

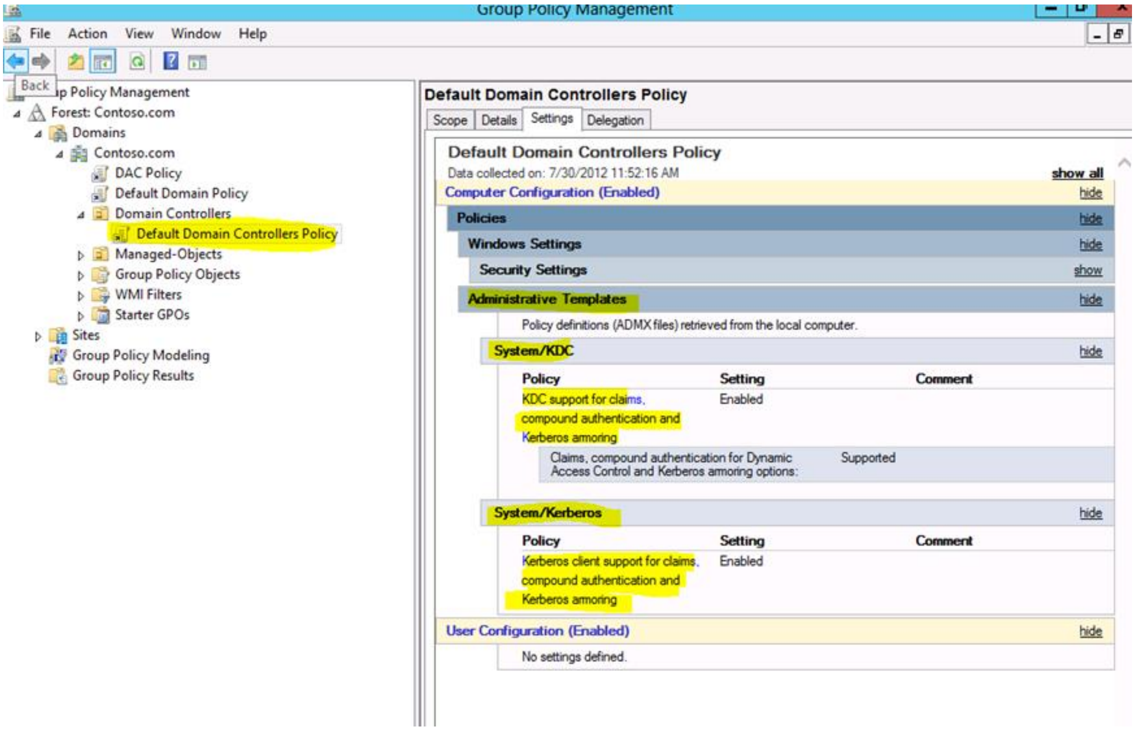
Supported on: At least Windows Server 2012 Release Candidate, Windows 8 or Windows RT

Options:

Help:

This policy setting controls whether a device will request claims and compound authentication for Dynamic Access Control and Kerberos armoring using Kerberos authentication with domains that support these features.
If you enable this policy setting, the client computers will request claims, provide information required to create compounded authentication and armor Kerberos messages in domains which support claims and compound authentication for Dynamic Access Control and Kerberos armoring.

If you disable or do not configure this policy setting, the client devices will not request claims, provide information required to create compounded authentication and armor Kerberos messages. Services hosted on the device will not be able to retrieve claims for clients using Kerberos protocol transition.



Default Domain Controllers Policy

Default Domain Controllers Policy

Data collected on: 7/30/2012 11:52:16 AM

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

System/KDC

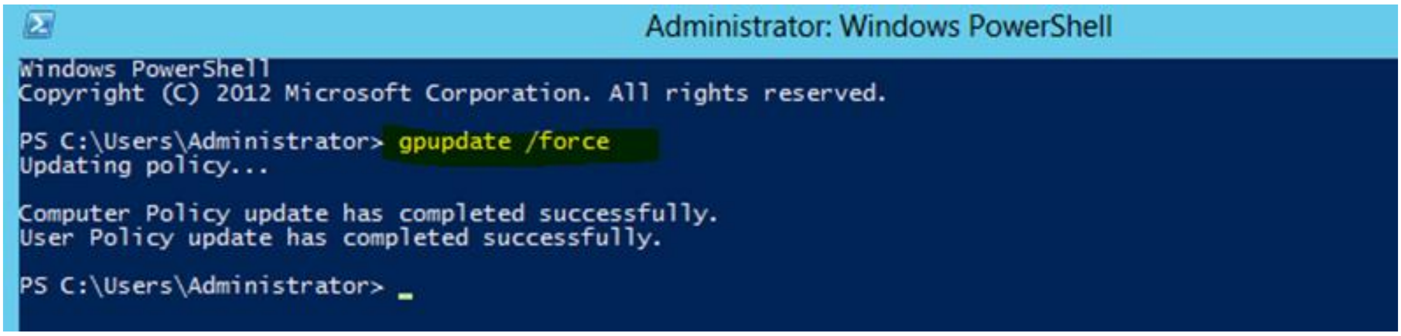
Policy	Setting	Comment
KDC support for claims, compound authentication and Kerberos armoring	Enabled	
Claims, compound authentication for Dynamic Access Control and Kerberos armoring options:	Supported	

System/Kerberos

Policy	Setting	Comment
Kerberos client support for claims, compound authentication and Kerberos armoring	Enabled	

User Configuration (Enabled)

No settings defined.



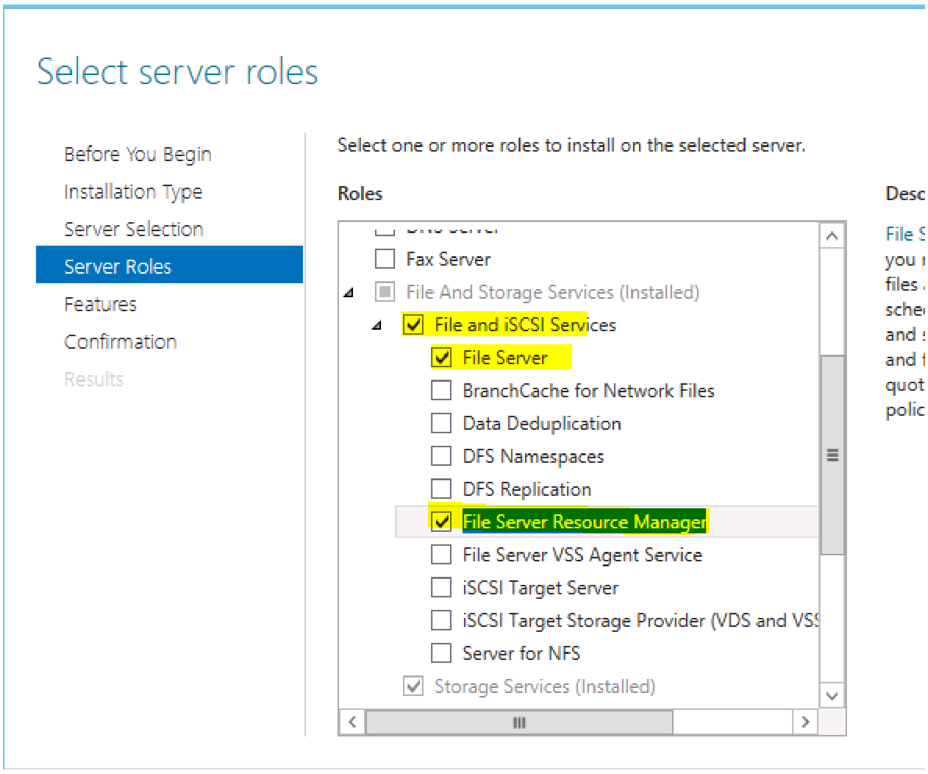
```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator> _
```

BUR-SRV2 Üzerinde **File server Resource Manager** Rolünü kurun.



Select server roles

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

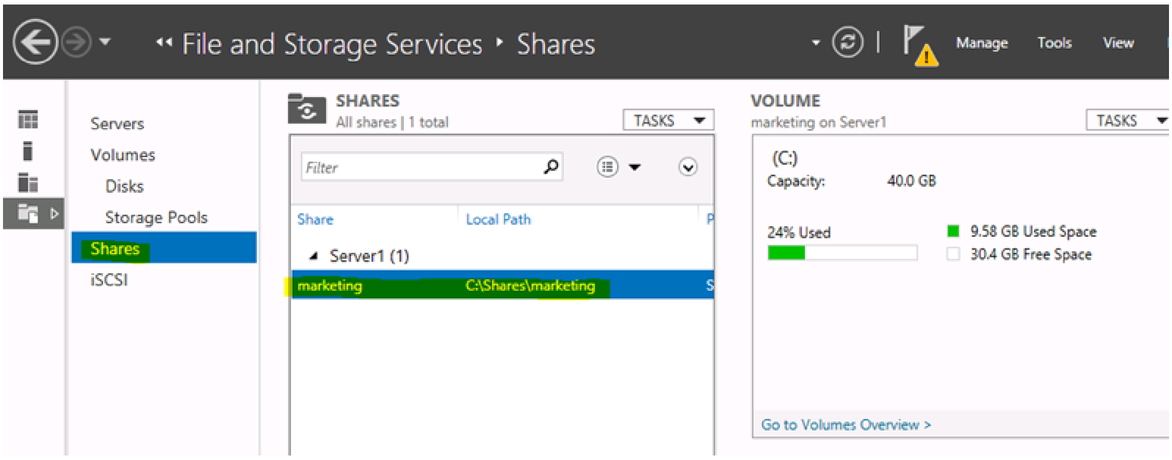
Roles

- □ Fax Server
- ▣ File And Storage Services (Installed)
  - ☑ File and iSCSI Services
    - ☑ File Server
    - □ BranchCache for Network Files
    - □ Data Deduplication
    - □ DFS Namespaces
    - □ DFS Replication
    - ☑ File Server Resource Manager
    - □ File Server VSS Agent Service
    - □ iSCSI Target Server
    - □ iSCSI Target Storage Provider (VDS and VSS
    - □ Server for NFS
  - ☑ Storage Services (Installed)

Desc

File S you i files sche and s and t quot polic

BUR-SRV2 üzerinde **“C:\shares\marketing”** klasörlerini ekleyin.



SHARES
All shares | 1 total

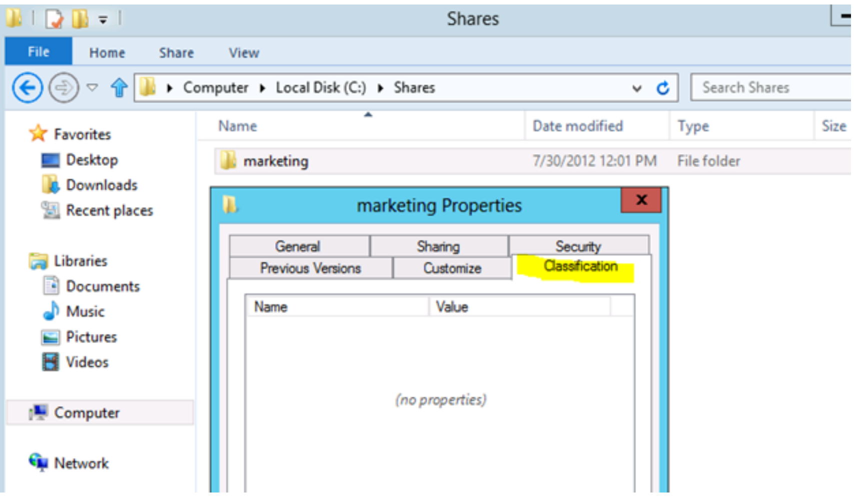
Share	Local Path
Server1 (1)	
marketing	C:\Shares\marketing

VOLUME
marketing on Server1

(C:)
Capacity: 40.0 GB

24% Used
9.58 GB Used Space
30.4 GB Free Space

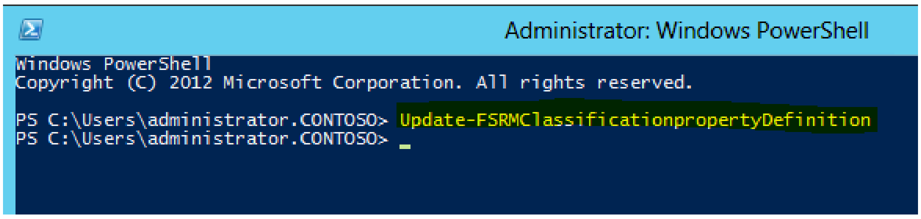
Go to Volumes Overview >



Name	Date modified	Type	Size
marketing	7/30/2012 12:01 PM	File folder	

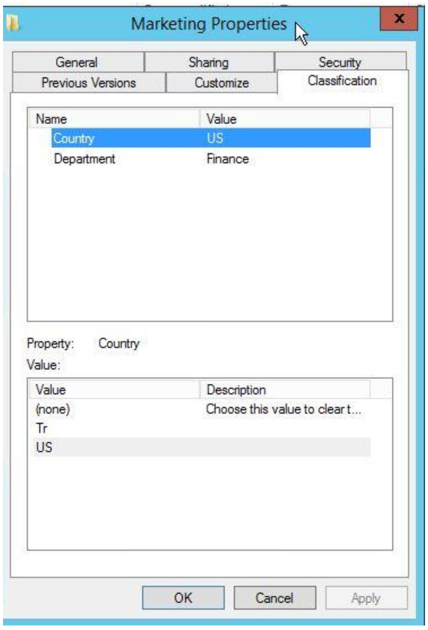
marketing Properties

Name	Value
(no properties)	



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.CONTOSO> Update-FSRMClassificationpropertyDefinition
PS C:\Users\administrator.CONTOSO> _
```

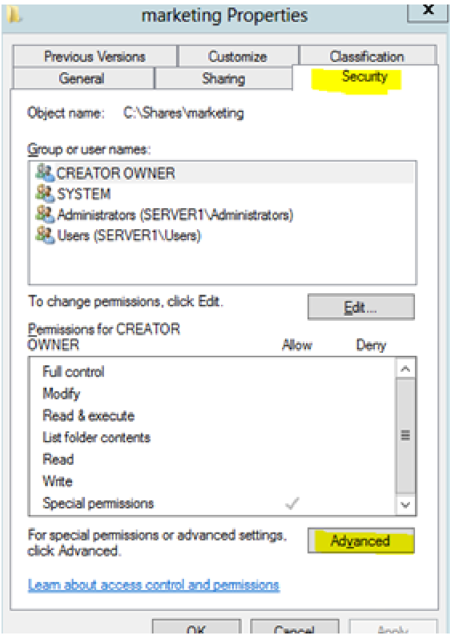


Name	Value
Country	US
Department	Finance

Property: Country

Value:

Value	Description
(none)	Choose this value to clear t...
Tr	
US	



Object name: C:\Shares\marketing

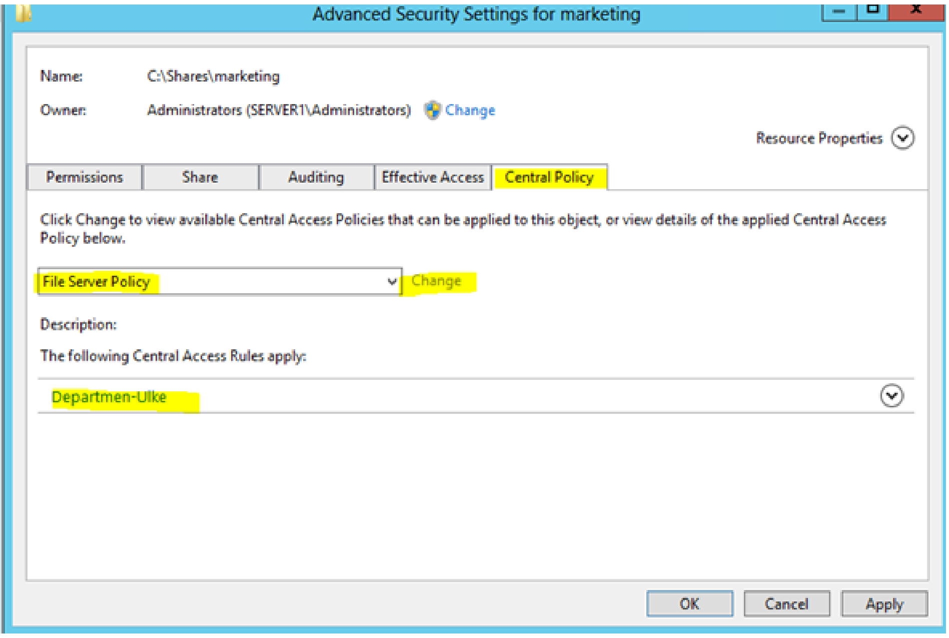
Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (SERVER1\Administrators)
- Users (SERVER1\Users)

To change permissions, click Edit.

Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		
Special permissions	✓	

For special permissions or advanced settings, click Advanced.



Name: C:\Shares\marketing

Owner: Administrators (SERVER1\Administrators) Change

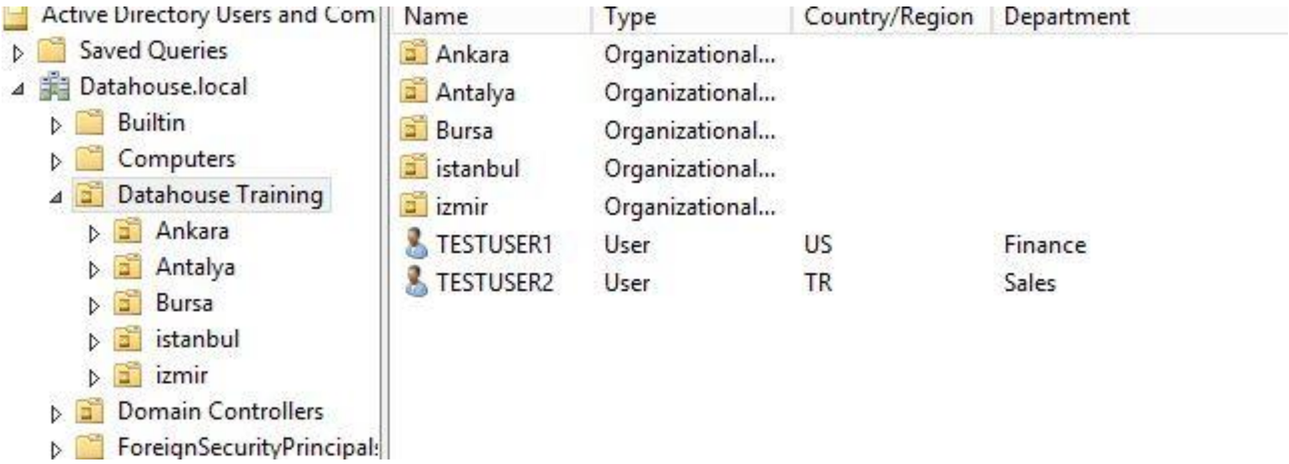
Click Change to view available Central Access Policies that can be applied to this object, or view details of the applied Central Access Policy below.

File Server Policy Change

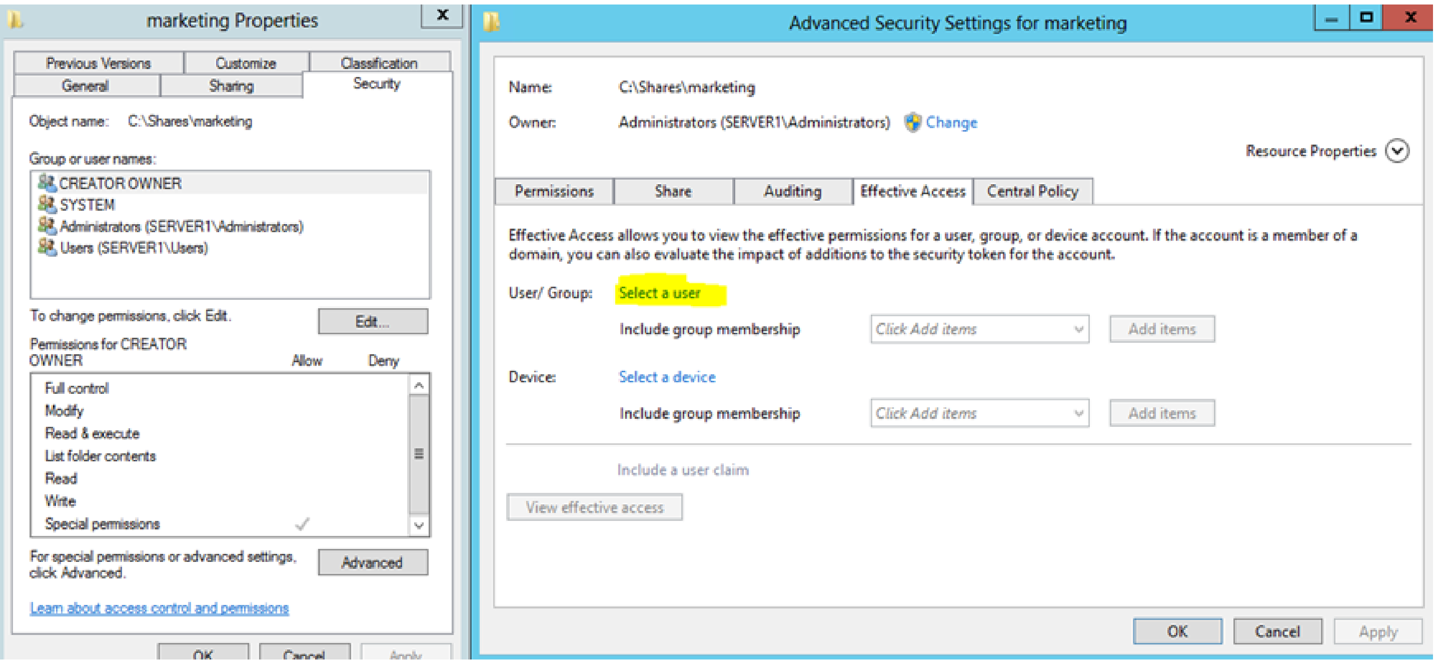
Description:

The following Central Access Rules apply:

Departmen-Ulke



Name	Type	Country/Region	Department
Ankara	Organizational...		
Antalya	Organizational...		
Bursa	Organizational...		
istanbul	Organizational...		
izmir	Organizational...		
TESTUSER1	User	US	Finance
TESTUSER2	User	TR	Sales



Object name: C:\Shares\marketing

Group or user names:

CREATOR OWNER
SYSTEM
Administrators (SERVER1\Administrators)
Users (SERVER1\Users)

To change permissions, click Edit.

Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		
Special permissions	✓	

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Name: C:\Shares\marketing

Owner: Administrators (SERVER1\Administrators)

Effective Access allows you to view the effective permissions for a user, group, or device account. If the account is a member of a domain, you can also evaluate the impact of additions to the security token for the account.

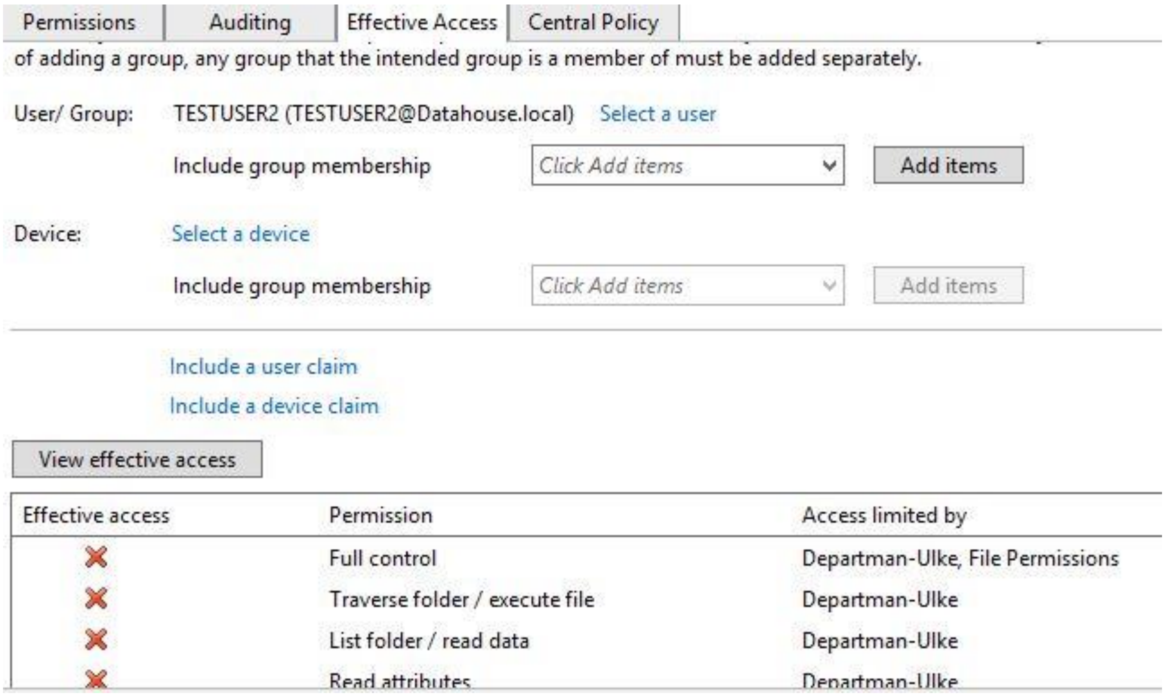
User/ Group: Select a user

Include group membership: Click Add items

Device: Select a device

Include group membership: Click Add items

Include a user claim



of adding a group, any group that the intended group is a member of must be added separately.

User/ Group: TESTUSER2 (TESTUSER2@Datahouse.local) Select a user

Include group membership: Click Add items

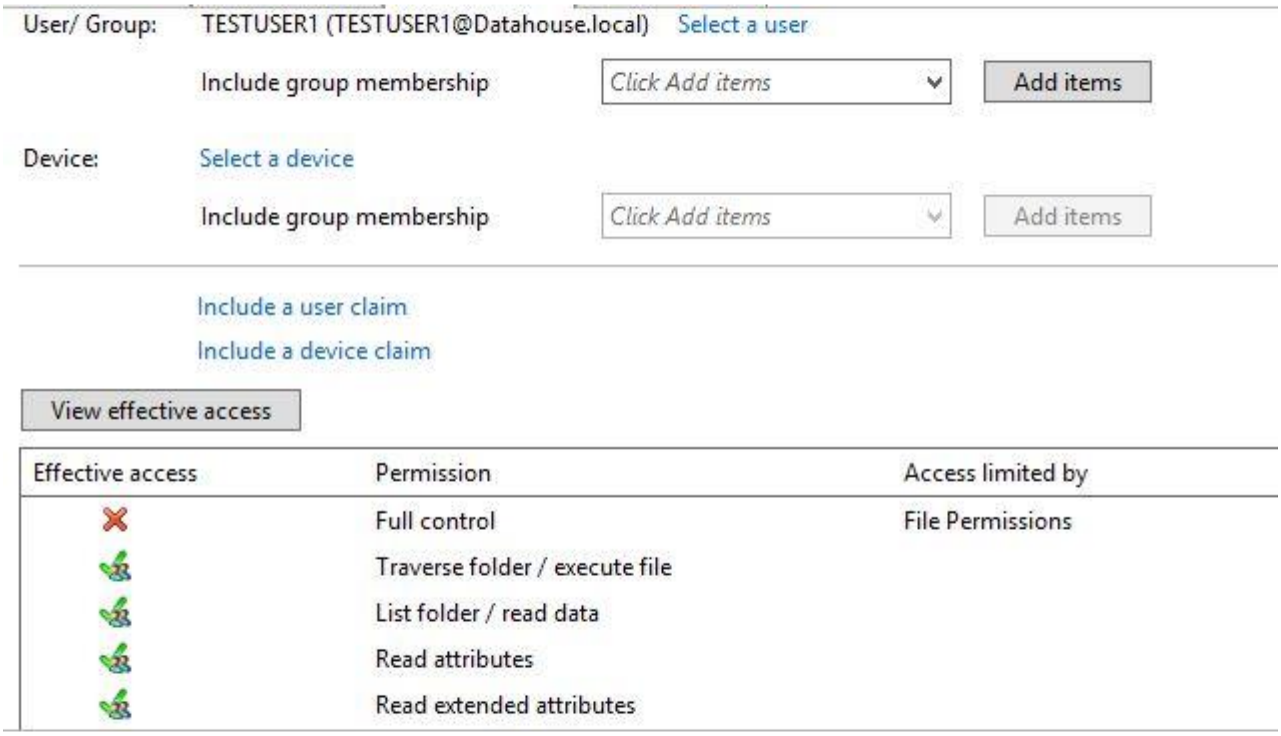
Device: Select a device

Include group membership: Click Add items

Include a user claim

Include a device claim

Effective access	Permission	Access limited by
✗	Full control	Departman-Ulke, File Permissions
✗	Traverse folder / execute file	Departman-Ulke
✗	List folder / read data	Departman-Ulke
✗	Read attributes	Departman-Ulke



User/ Group: TESTUSER1 (TESTUSER1@Datahouse.local) Select a user

Include group membership Click Add items

Device: Select a device

Include group membership Click Add items

Effective access	Permission	Access limited by
✗	Full control	File Permissions
✓	Traverse folder / execute file	
✓	List folder / read data	
✓	Read attributes	
✓	Read extended attributes	