10/3/2022

Indian Institute of Technology, Patna

Spring 2022

CS547 (Foundation of Computer Security)

Assignment - 3

(Answer File)

Submitted To:

Dr Somanath Tripathy
Dept. Of Computer Sci & Engg
IIT Patna

Submitted by:

Vikul Kumar *(2011CS24)*
Mangesh *(1801CS16)*
Priyadrasta Raut *(2111CS10)*
Shamsher *(2111CS22)*

Assignment - 3

Access Control Methods in *Windows 10*

Contents:

I. Brief Introduction to Windows 10 User Security

Windows 10 is the most recent version of the Microsoft Operating System that was released on July 29, 2015, as a successor to Windows 8. It is probably the most secure version of Windows ever. Windows 10 is the closest Microsoft has come to a virus-proof operating system so far. When compared to other versions of Windows, Microsoft has included many in-built defence mechanisms in Windows 10 which will ensure the Confidentiality, Integrity, and Availability of the system and these features will be discussed in detail.

Security Capabilities	Description
Securing user identity with Windows Hello	sign into your device using a passcode (PIN) or another biometric based authentication
Windows Defender Credential Guard	protects your systems from credential theft attack techniques (pass-the-hash or pass-the-ticket) as well as helping prevent malware from accessing system secrets even if the process is running with admin privileges
FIDO Alliance	Fast Identity Online (FIDO) defined protocols are becoming the open standard for providing strong authentication that helps prevent phishing and are user-friendly and privacy-respecting
Microsoft Authenticator	allows easy, secure sign-ins for all your online accounts using multi-factor authentication, password less phone sign-in, or password autofill
Smart Cards	tamper-resistant portable storage devices that can enhance the security of tasks in Windows, such as authenticating clients, signing code, securing e-mail, and signing in with Windows domain accounts
Access Control	Access control is the process of authorizing users, groups, and computers to access objects and assets on a network or computer. Computers can control the use of system and network resources through the interrelated mechanisms of authentication and authorization

II. Access Control Overview

In the access control model, users and groups (also referred to as security principals) are represented by unique security identifiers (SIDs). They are assigned rights and permissions that inform the operating system what each user and group can do. Each resource has an owner who grants permissions to security principals. During the access control check, these permissions are examined to determine which security principals can access the resource and how they can access it.

Security principals perform actions (which include Read, Write, Modify, or Full control) on objects. Objects include files, folders, printers, registry keys, and Active Directory Domain Services (ADDS) objects. Shared resources use access control lists (ACLs) to assign permissions

Object owners generally grant permissions to security groups rather than to individual users. Users and computers that are added to existing groups assume the permissions of that group. If an object (such as a folder) can hold other objects (such as subfolders and files), it is called a container. In a hierarchy of objects, the relationship between a container and its content is expressed by referring to the container as the parent. An object in the container is referred to as the child, and the child inherits the access control settings of the parent. Object owners often define permissions for container objects, rather than individual child objects, to ease access control management.

Permissions

For any object permissions can be given to:
1) Groups, users and other objects with security identifiers in the domain
2) Groups and users in that domain and any trusted domains
3) Local groups and users on the computer where the object resides

Common permissions are read, write, change owner, delete and share. Inheritance allows administrators to easily assign and manage permissions. This feature automatically causes objects within a container to inherit all the inheritable permissions of that container.

When you need to change the permissions on a file, you can run Windows Explorer, right-click the file name, and click Properties. On the Security tab, you can change permissions on the file.

User rights

User rights grant specific privileges and sign-in rights to users and groups in your computing environment. Administrators can assign specific rights to group accounts or to individual user accounts. These rights authorize users to perform specific actions, such as signing in to a system interactively or backing up files and directories.

Object Auditing

With administrator's rights, you can audit users' successful or failed access to objects. You can select which object access to audit by using the access control user interface, but first you must enable the audit policy by selecting Audit object access under Local Policies in Local Security Settings. You can then view these security-related events in the Security log in Event Viewer.

III. Security Identifiers

A SID, short for security identifier, is a number used to identify user, group, and computer accounts in Windows. They're created when the account is first made in Windows and no two SIDs on a computer are ever the same. The term security ID is sometimes used in place of SID or security identifier.

Why Does Windows Use SIDs?

Users refer to accounts by the account's name, like "username1" or "username2", but Windows uses the SID when dealing with accounts internally. If Windows referred to a common name like we do, instead of a SID, then everything associated with that name would become void or inaccessible if the name were changed in any way. So instead of making it impossible to change the name of your account, the user account is instead tied to an unchangeable string (the SID), which allows the username to change without affecting any of the user's settings. While a username can be changed as many times you like, you're unable to change the SID that's associated with an account without having to manually update all the security settings that were associated with that user to rebuild its identity.

Finding SID in WIN 10 of all Users ?

```
PS C:\Users\mange> wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-3191258257-1768706679-2935636463-500
ciscoacvpnmcuser    S-1-5-21-3191258257-1768706679-2935636463-1002
DefaultAccount      S-1-5-21-3191258257-1768706679-2935636463-503
Guest               S-1-5-21-3191258257-1768706679-2935636463-501
mange               S-1-5-21-3191258257-1768706679-2935636463-1001
WDAGUtilityAccount  S-1-5-21-3191258257-1768706679-2935636463-504
```

Query based on SID/username can be done to find the other.

All SIDs start with S-1-5-21 but will otherwise be unique. If you need to, you can find a user's security identifier (SID) in Windows for matching users with their SIDs.

A few SIDs can be decoded without the instructions linked above. For example, the SID for the Administrator account in Windows always ends in 500. The SID for the Guest account always ends in 501.

You'll also find SIDs on every installation of Windows which correspond to certain built-in accounts. For example, the S-1-5-18 SID can be found in any copy of Windows you come across and corresponds to the Local System account, the system account that's loaded in Windows before a user logs on.

S	1	5	21-1180699209-877415012-3182924384	1004
Indicates that this is a SID	SID specification version number	Identifier authority	Domain or local computer identifier	Relative ID

The following are a few examples of the string values for groups and special users that are universal across all Windows installs:

- **S-1-0-0 (Null SID)**: the SID value is unknown, or for a group without any members
- **S-1-1-0 (World)**: This is a group of every user
- **S-1-2-0 (Local)**: This SID is assigned to users who log on to a local terminal

How do you change the SID in Windows?

Go to C:\Windows\System32\Sysprep and run sysprep.exe. Select the Generalize checkbox, then select OK. When Sysprep is done, restart the computer.

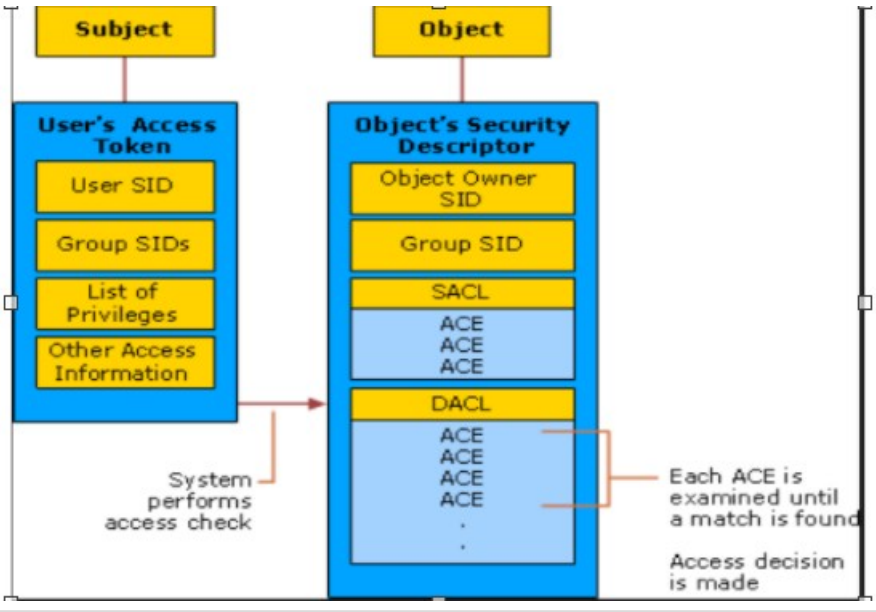
For more in-depth details, we can refer:

Security identifiers (Windows 10) - Windows security | Microsoft Docs

IV. Security Principals

Security principals are any entity that can be authenticated by the operating system, such as a user account, a computer account, or a thread or process that runs in the security context of a user or computer account, or the security groups for these accounts. Security principals have long been a foundation for controlling access to securable resources on Windows computers. Each security principal is represented in the operating system by a unique security identifier (SID).

The following diagram illustrates the Windows authorization and access control process. In this diagram, the subject (a process that is initiated by a user) attempts to access an object, such as a shared folder. The information in the user's access token is compared to the access control entries (ACEs) in the object's security descriptor, and the access decision is made. The SIDs of security principals are used in the user's access token and in the ACEs in the object's security descriptor.



V. Access Tokens

When a user logs on, Windows creates an access token for this user. It is used to store a user's identity and privileges.

Such an access token stores the following information:

- The user's SID (security identifier)
- The SIDs of the groups that the user belonged to when the user was authenticated
- A logon SID which identifies the current logon session
- The user's and groups' privileges
- An owner SID
- The SID for the primary group
- The default discretionary access control list (DACL) that is used when the user creates a securable object (without an explicit security descriptor)
- The source of the access token
- A flag that indicates if the token is a primary or an impersonation token
- A list of restricting SIDs (optional)
- Current impersonation levels
- Other statistics

An access token is a kernel object. There are two types of access tokens:

1. Primary access tokens

The primary access token is the access token that is created when a user logs on. It is created by the Local Security Authority (LSA). When the (logged-on) session starts a process or a thread, the primary access token is copied and the copy is attached to that process or thread.

2. Impersonation access tokens

Impersonation access tokens are typically used in client-server environments where a thread needs to run in a different security context than that of the process that started the thread.

Creating access tokens

Using the WinAPI, a new access token can be created with DuplicateTokenEx.

```
typedef struct _TOKEN_ACCESS_INFORMATION {
    PSID_AND_ATTRIBUTES_HASH SidHash;
    PSID_AND_ATTRIBUTES_HASH RestrictedSidHash;
    PTOKEN_PRIVILEGES Privileges;
    LUID AuthenticationId;
    TOKEN_TYPE TokenType;
    SECURITY_IMPERSONATION_LEVEL ImpersonationLevel;
    TOKEN_MANDATORY_POLICY MandatoryPolicy;
    DWORD Flags;
    DWORD AppContainerNumber;
    PSID PackageSid;
    PSID_AND_ATTRIBUTES_HASH CapabilitiesHash;
    PSID TrustLevelSid;
    PSECURITY_ATTRIBUTES_OPAQUE SecurityAttributes;
} TOKEN_ACCESS_INFORMATION, *PTOKEN_ACCESS_INFORMATION;
```

Fig: Definition of Access Token

VI. Security Descriptors and Access Control Lists

A security descriptor is a data structure that is associated with each securable object. All objects in Active Directory and all securable objects on a local computer or on the network have security descriptors to help control access to the objects. Security descriptors include information about who owns an object, who can access it and in what way, and what types of access are audited. Security descriptors contain the access control list (ACL) of an object, which includes all of the security permissions that apply to that object.

DACL

DACL is controlled by the owner of the object and specifies what level of access particular trustees have to the object. It can be NULL or non-existent (no restrictions, everyone full access), empty (no access at all), or a list, as the name implies. The DACL almost always contains one or more access control entries (ACEs).

SACL

SACL specifies which attempts to access the object are audited in the security event log. The ability to get or set (read or write) any object's SACL is controlled by the privilege `SeSecurityPrivilege`, which typically is only held by the local group `Administrators.`

VII. Accounts and Security Groups

Accounts and security groups that are created in an Active Directory domain are stored in the Active Directory database and managed by using Active Directory tools. These security principals are directory objects, and they can be used to manage access to domain resources.

Local user accounts and security groups are created on a local computer, and they can be used to manage access to resources on that computer. Local user accounts and security groups are stored in and managed by the Security Accounts Manager (SAM) on the local computer.

User Accounts, Local Accounts, Microsoft Accounts, etc. are some different types of accounts available in Windows 10 OS

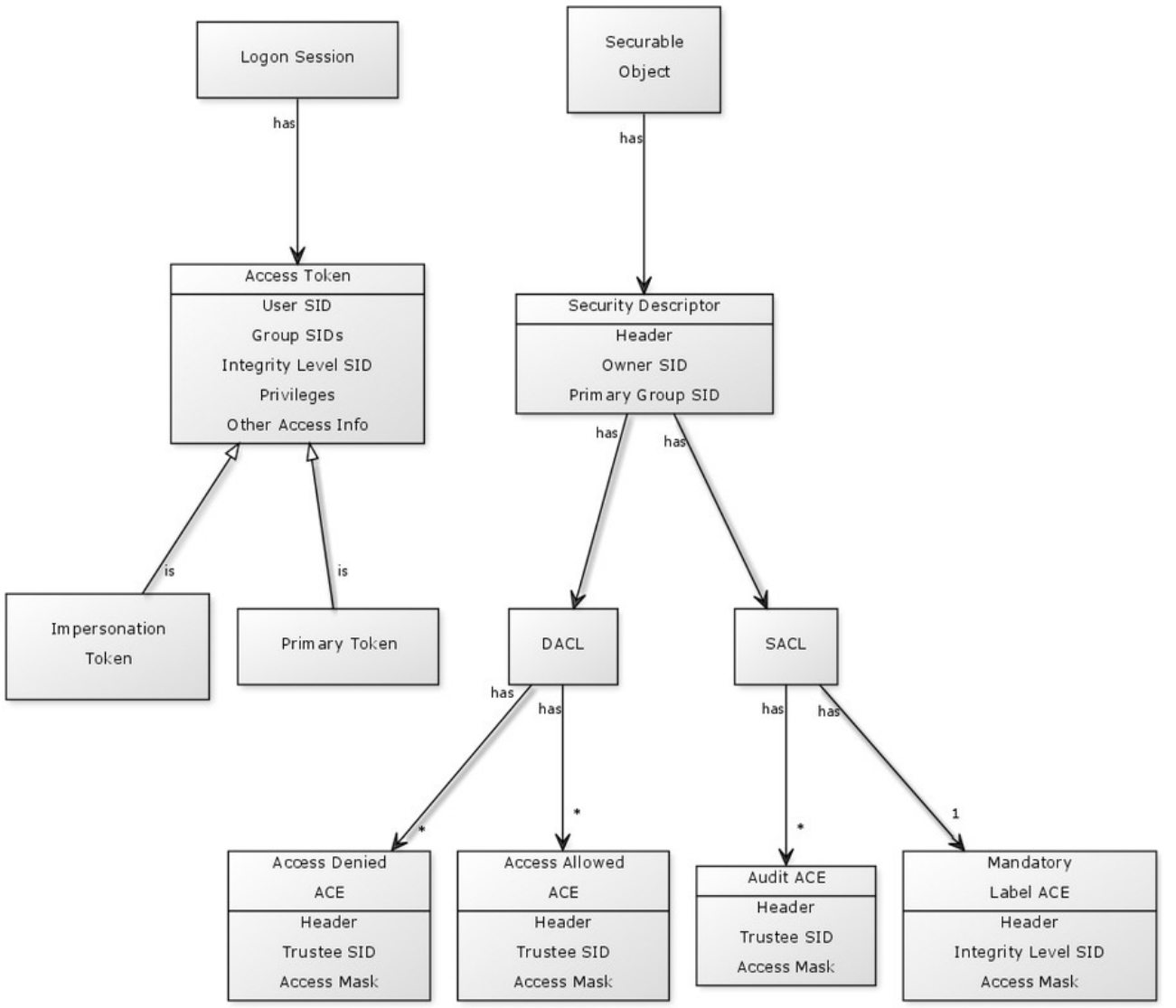


Fig. Access Control in Windows 10

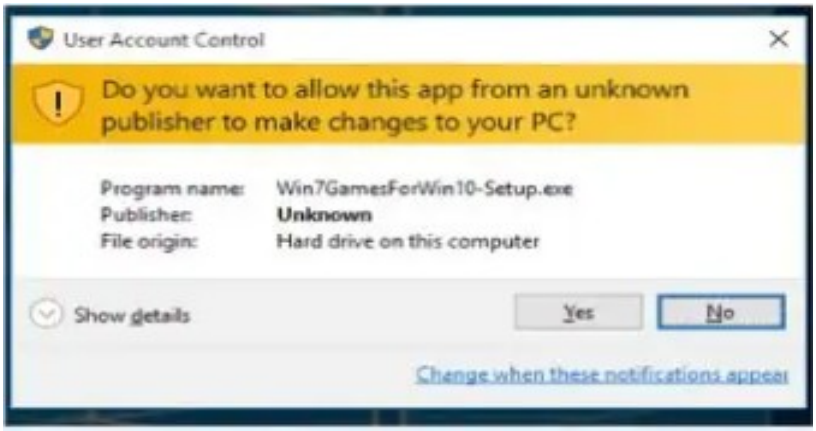
VIII. User Access Control (UAC)

UAC is a security feature in Windows 10 that prevents unauthorized or inadvertent changes to the operating system. The feature was first a part of the Windows Vista security system and has since been improved with each new version of Windows. UAC makes all the difference between standard user accounts and administrator accounts. With the feature, you have a basic level system security that helps save your system from malicious processes even with a security suite in place. User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

Among the changes that require administrative privileges include:

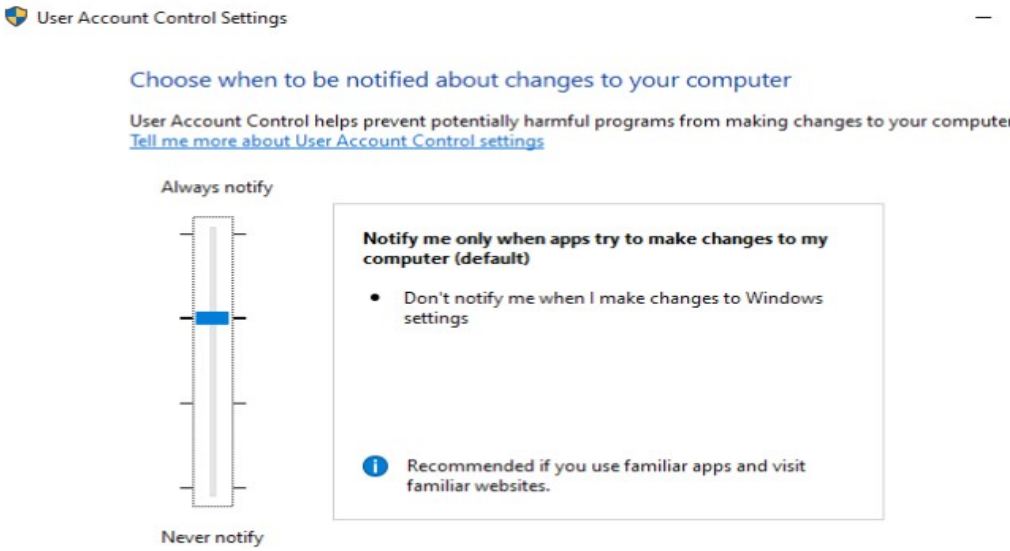
- Running Task Scheduler
- Making changes to UAC settings
- Windows Update configurations
- Adding or removing user accounts
- Changing system-wide files or settings in Program File or Windows folders
- Viewing or changing other users' files or folders
- Running apps as administrator
- Installing or uninstalling apps and drivers
- Changing Windows Firewall or system date and time settings
- Configuring Family Safety or Parental Controls
- Changing users' account type

Such changes can be initiated by users, viruses, malware, or applications. But if the administrator doesn't approve the changes, they won't be executed. Each time you run a desktop app that requires administrative permissions, the UAC pops up as shown below. You'll also see it when you want to change important system settings that require admin approval.



IX. UAC Slider Levels in Windows 10

In Windows Vista, there were only two UAC options: On or Off. In Windows 10 however, there are four UAC levels to choose from:



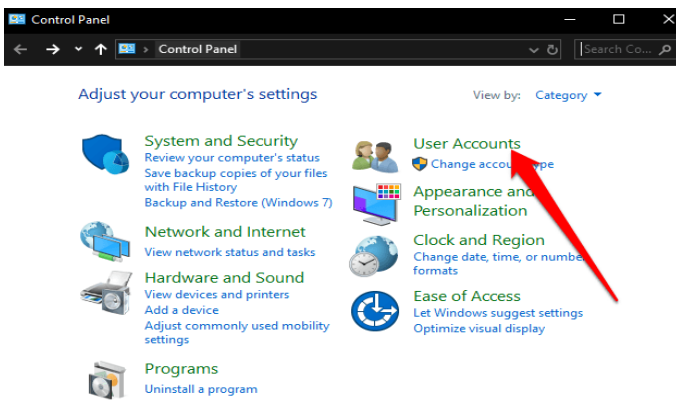
Disable UAC in Windows 10

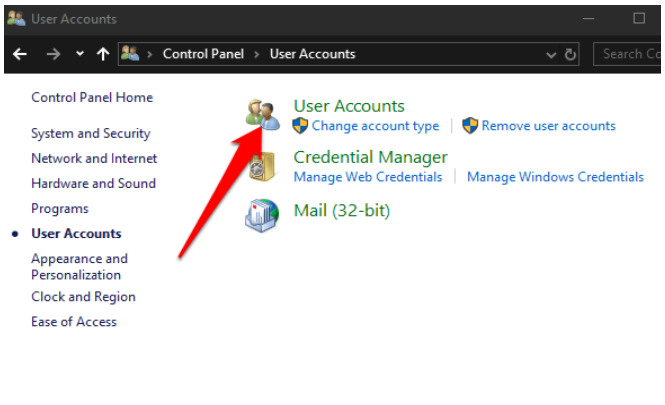
Disabling UAC on your computer is not recommended at all as doing this makes it easier for malicious programs to infect and manage your computer. If there are apps that keep triggering UAC, use Windows Task Scheduler to run those apps without admin rights and UAC prompts first, instead of disabling UAC altogether. We can do it via:

- Control Panel
- Group Policy
- Registry Editor
- Command Line

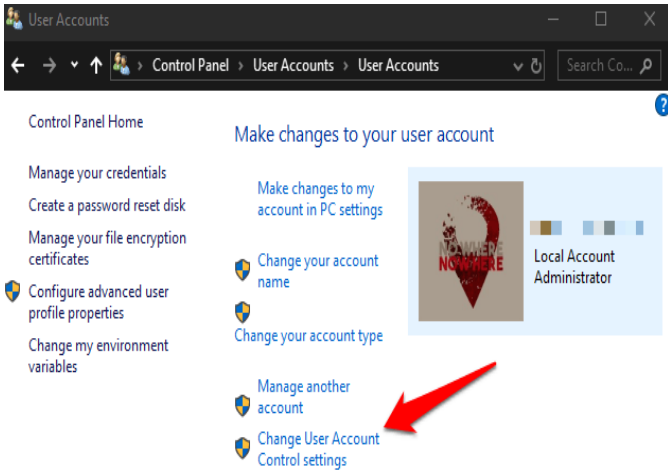
How to Disable UAC Using Control Panel

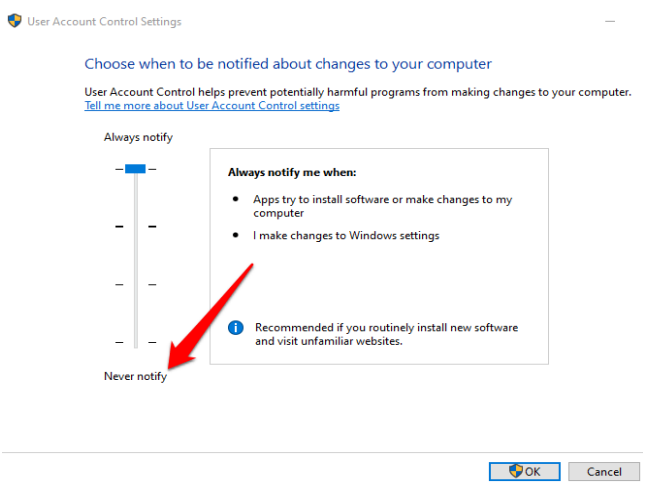
1. Open Control Panel and select **User Accounts**.Select **User Accounts** again.





3. Next, select **Change User Account Control settings**.
4. If you want to completely disable UAC, drag the slider to **Never notify** to turn UAC off and then click **OK**.





To turn UAC back on, drag the slider to the security level you want and then click **OK**. Confirm your selection or enter your admin password if prompted to, and then restart your computer to keep the changes

X. Dynamic Access Control (DAC)

Domain-based Dynamic Access Control enables administrators to apply access-control permissions and restrictions based on well-defined rules that can include the sensitivity of the resources, the job or role of the user, and the configuration of the device that is used to access these resources. Dynamic Access Control is not supported in Windows operating systems prior to Windows Server 2012 and Windows 8. When Dynamic Access Control is configured in environments with supported and non-supported versions of Windows, only the supported versions will implement the changes.

It allows to apply access control and restricted permission based conditional rules for accessing files and folders dynamically. For Example, if a new user joins a department or if an employee moves from one department to another department or his role changes, then the file and folder permissions changes are dynamically added and removed without the administrator's intervention. Some of the entities involved with Dynamic control to provide dynamic permissions are:

Claims types

It can be a user, device (computers etc.) or resources that have been published by a domain controller. To be more specific, it can be a user title, department, location, other property or a combination of these properties can be considered as a valid claim to provide access to the resources.

Resource properties

Creating classifications or tags that could be used to apply on the shared file resources. Classifications may be like tagging the folder with the department name. This value is compared with the user claim AD attribute for effective permission.

Resource property list (RPL)

Each of the resource properties are added to the resource property list and it is downloaded to the file server. Any number of RPLs can be deployed on the file server and global resource property list can be deployed on all the file servers in the organization.

Central Access Rule

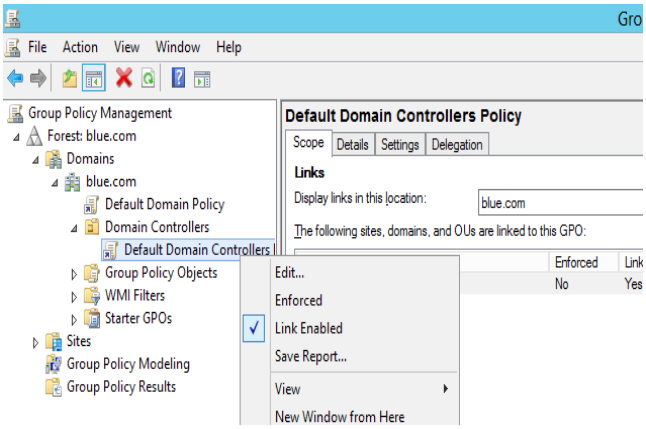
These rules are set of conditions involving claims which provide access or deny permissions.

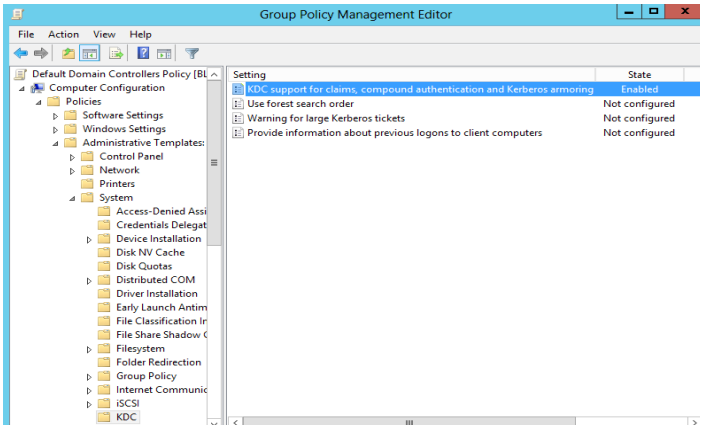
Central Access Policy

It can be one or more central access rules applied to provide the necessary permissions. These are in addition to the local NTFS permission provided on the files and folders.

Before we configure Dynamic Access Control in the environment, we need to configure the domain to support it. Below are the steps to perform the same:

1. Connect to the blue.com Domain control -> access Group policy management console -> Domain controllers -> Right click Default Domain Controllers Policy and select Edit.
2. In the group policy management editor, double-click computer configuration -> policies -> administrative template -> system -> KDC
3. Right-click “KDC support for claims, compound authentication, and Kerberos armouring” and enable it.



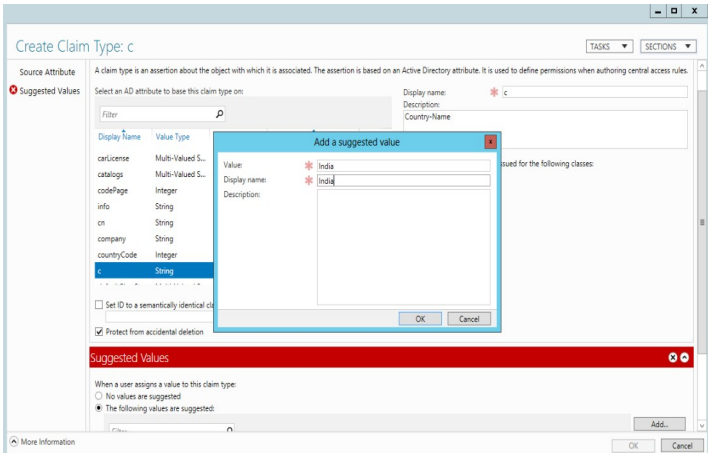


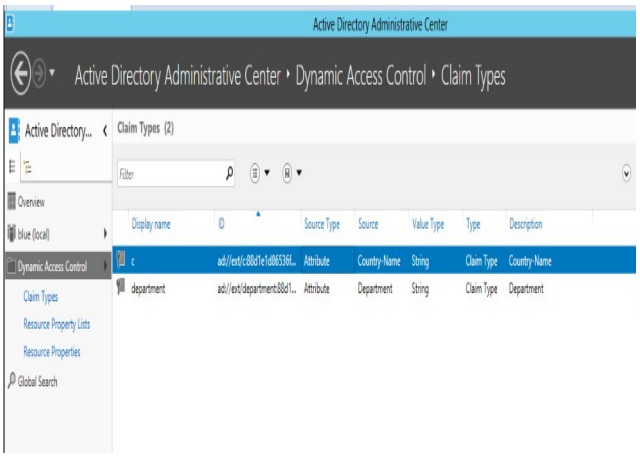
Configuring Claim Type

In this step, we will configure claim by defining the Active directory attribute which is used to provide access to the resource.

1. Login to Windows Server and click on Start -> Run and type “DSAC” to start ‘Active Directory Administrative Centre’.
2. On the left pane, click on ‘Dynamic Access Control’ -> select Claim Type -> Right-click select ‘New’ and select Claim Type.

3. Search for ‘C’ to create the claim type of country and scroll down to add the suggested value as ‘India’ and Display name as ‘India’
4. Repeat the same step by searching ‘Department’ in the claim type and add ‘IT’ and click ‘OK’.

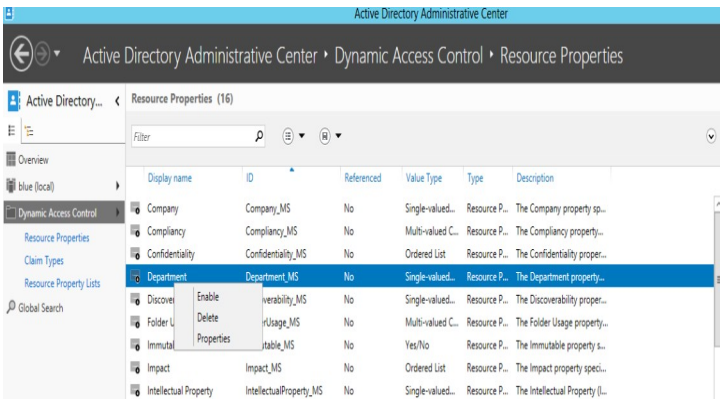


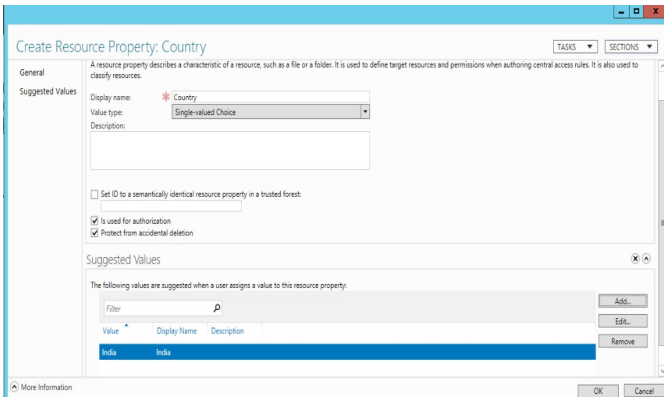


Resource Properties

Dynamic Access Control allows to create resources properties, which can be downloaded to the file server and tag them for classification purpose. Below are the steps to perform the same:

1. Connect to Active Directory Administrator Central -> select ‘Dynamic Access Control’
2. Double-click Resource properties -> right click ‘Department and select ‘Enable’.
3. From the bottom right section, select New -> Resource Property -> type display name as ‘Country’ -> click on ‘Add’ to add the suggested Values as “India” for display name.
4. Right-click on ‘Department’ from resource property and select ‘Enable’.



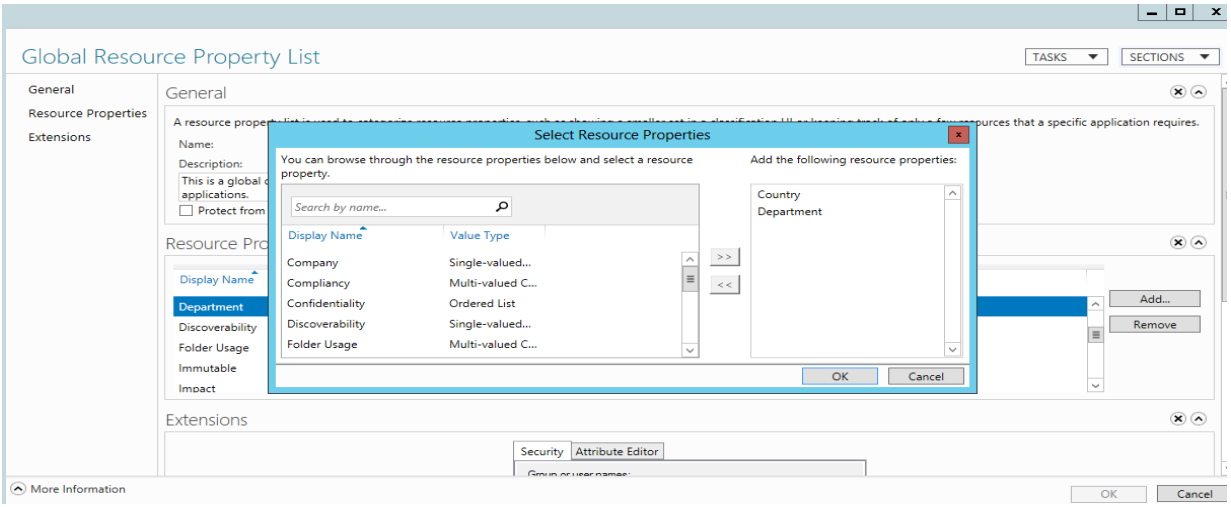


Resource Property Lists

The above created resource properties are added to the resource property list and this configuration list is downloaded to the fileserver.

1. Connect to Windows Server and access Active Directory Administrative Centre.
2. Double-click on Dynamic Access Control -> select Resource Property list from the left pane.
3. Double-click on Global Resource Property list from the centre pane.

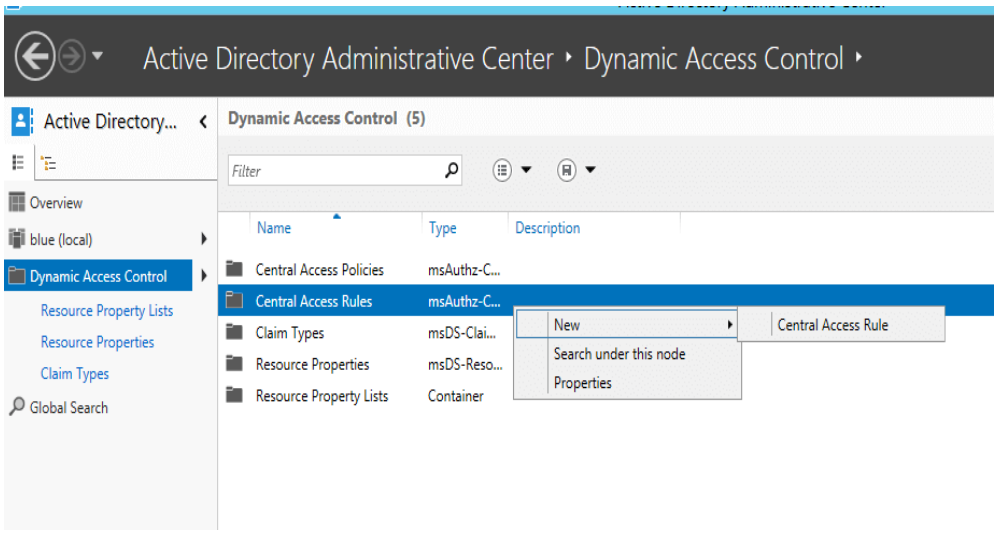
4. Click on ‘Add’ and select country and department into the ‘Global Resource property list’ and click ‘OK’.
5. Finally, close the Global Resource Property list window.



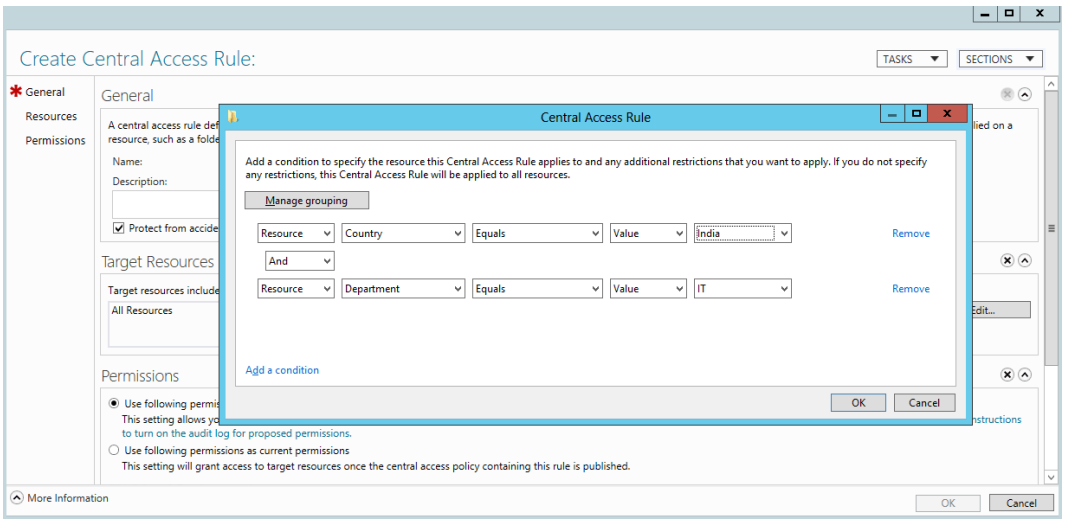
Central Access Rule:

These rules are set of conditions involving the above defined claims which provide access or deny permissions.

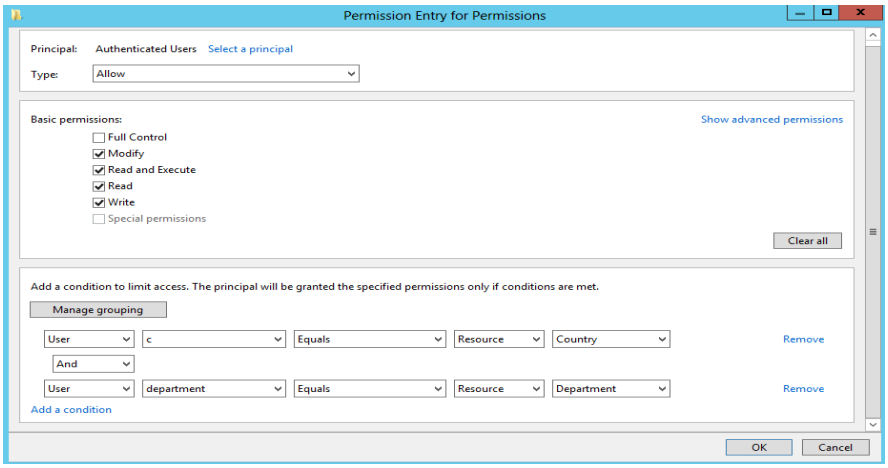
1. Connect to the Widows Server and connect to the Active Directory Administrative Center – > Dynamic Access Control
2. Right click on “Central Access Rules” -> new -> Central Access rule



3. Give the appropriate name on the “Create Access Rule” popup window -> Edit Target Resource -> Click on “Add condition”.
4. Select Target resource -> edit and update the resource condition as defined below.



5. Under Permissions in the Create Central Access Rule window, make sure that 'Use following permissions as current permissions' is checked and click 'Edit'.
6. At 'Permission Entry for Permission' window -> click on 'Select a principal' -> search for 'Authenticated Users' -> click 'OK'.
7. At Basic permission, Select Modify permission and keep other pre-existing default permission
8. Click two times on 'Add a condition' and modify the condition as defined below.

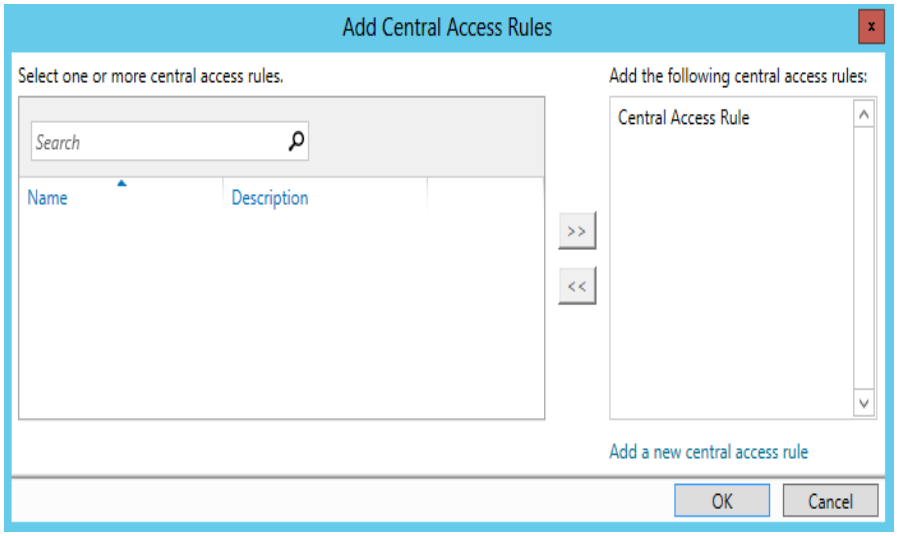


9. Click on 'OK' at Permission entry for permission, then click on 'OK' at Advanced security settings for permission and click 'OK' at Central Access Rule Window to create a new Central Access Rule

Central Access Policy:

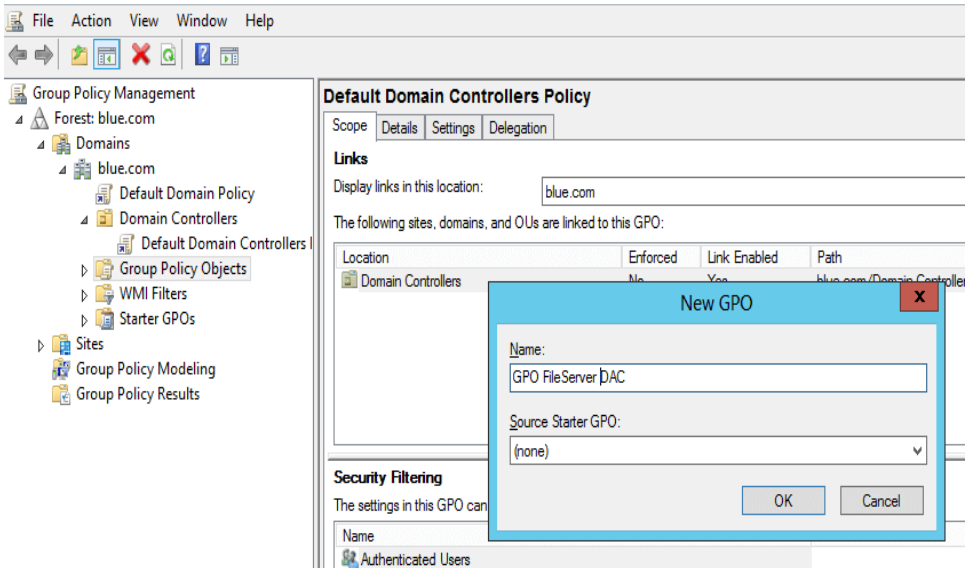
It can be one or more central access rules applied to provide the necessary permissions. We need to add central access rule, before it is distributed to the file server.

1. Connect to Active Directory Administrative Center and select Dynamic Access control.
2. Right-click on Center pane and select new-> Central Access policy.
3. Provide the appropriate name and click on the 'Add' button to add the Central Access Rule which was just created.

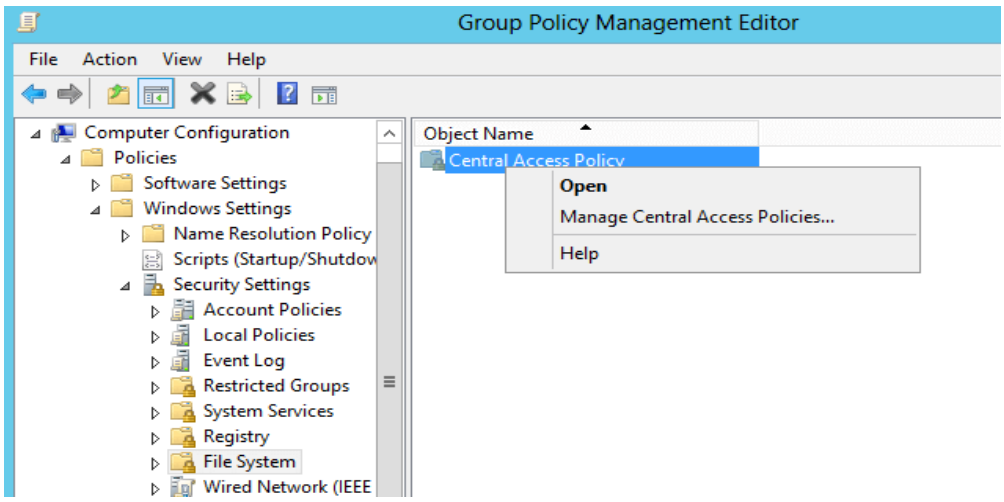


Configure group policy to publish Central Access Rule: Configure group policy to publish the Center Access rule to the file server.

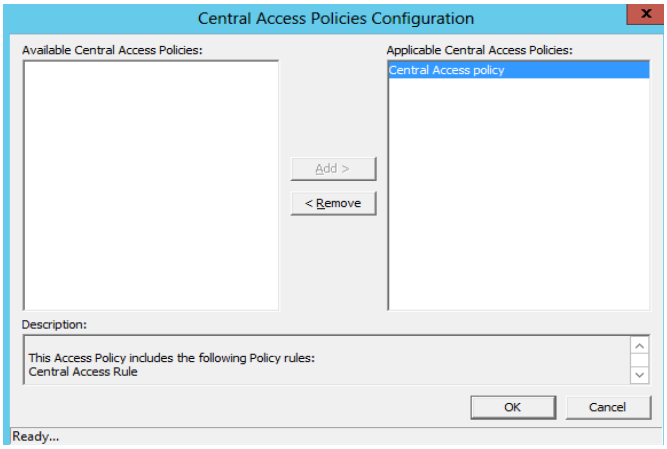
1. Connect to the Server Manager -> Start “Group policy management” console.
2. Expand the domain and right-click on “group policy objects” -> click new -> provide the name “GPO File Server DAC” and click OK.

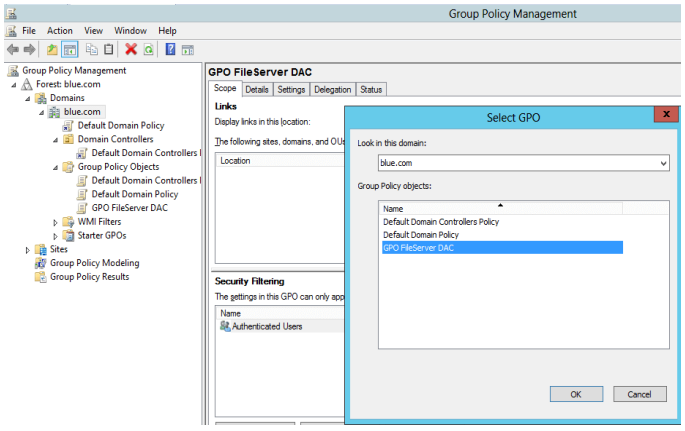


3. Edit the newly created GPO “GPO File Server DAC”
4. Expand Computer Configuration -> Policies ->Windows Settings -> Security Settings -> File System -> right-click on Central Access policy -> click on Manage Central Access policies to mage the same.



5. Select the Central Access Policy from the list and click on the ‘Add’ button.
6. Click ‘OK’ at Central Access Policy and Click on ‘OK’ at Group policy manager editor window.
7. Finally link the GPO to the domain. To do the same, right-click on the domain name ‘blue.com’ from the Group Policy Management console and select the newly created group policy object – “GPO Fileserver DAC”.
8. Click on ‘OK’ to apply the GPO and close the Group policy management console.





XI. Comparison for all Systems & Models

```
Discretionary Access Control

In discretionary access control (DAC), the owner of the object specifies which subjects
can access the object. This model is called discretionary because the control of access
is based on the discretion of the owner.

In these operating systems, when you create a file, you decide what access privileges
you want to give to other users; when they access your file, the operating system will
make the access control decision based on the access privileges you created.

Most operating systems such as all Windows, Linux, and Macintosh and most flavors of
Unix are based on DAC models.


Mandatory Access Control

In mandatory access control (MAC), the system (and not the users) specifies which subjects
can access specific data objects. The MAC model is based on security labels. Subjects are
given a security clearance (secret, top secret, confidential, etc.), and data objects are
given a security classification (secret, top secret, confidential, etc.). The clearance
and classification data are stored in the security labels, which are bound to the specific
subjects and objects.

When the system is making an access control decision, it tries to match the clearance of
the subject with the classification of the object. For example, if a user has a security
clearance of secret, and he requests a data object with a security classification of top
secret, then the user will be denied access because his clearance is lower than the
classification of the object. The MAC model is usually used in environments where
confidentiality is of utmost importance, such as a military institution.

Examples of the MAC-based commercial systems are SE Linux and Trusted Solaris.

Role-Based Access Control

Under this category of Access Control Management, access is granted based on the role &
responsibility of an individual. In this method, the admin can restrict access to privileged
information based on the duties, authority, and job competency of an individual.

Allows additional safety for sensitive & privileged information in an enterprise. Reduces
administrative work & IT Support In small companies, creating & maintaining track of roles
& requirements is a tedious job. The entire setup of role-based access control is labour
intensive
```

← The End →