EX NO:5	SECURITY GROUP POLICIES MANAGEMENT
DATE:31/08/2023	

AIM: To do the security group policy management in our system.

PROCEDURE:

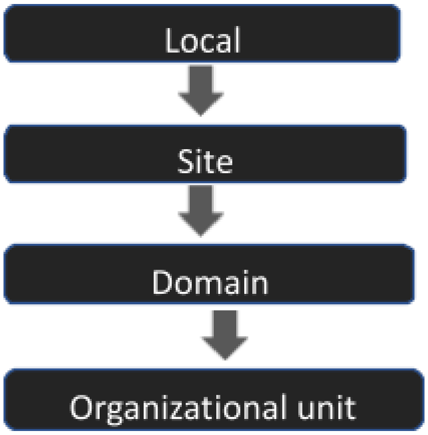
Implementing Group Policy Objects

Group policies are typically linked to multiple objects in the Active Directory, including sites, domains, or organizational units. However, they cannot be directly linked to individual users or security groups.

When multiple GPOs (Group Policy Objects) are linked to organizational units, they are processed following a hierarchy. The GPO linked to the highest-level OU is processed first, followed by its child OUs, and so on, until it reaches the specific computer or user object. The GPO associated with the last processed OU takes precedence and overrides any previous settings.

In terms of processing order, the GPOs are processed based on the hierarchy and object type, with sites being processed first, then domains, and finally organizational units. This means that the GPOs linked to sites have the lowest precedence, followed by domain-linked GPOs, and finally, organizational unit-linked GPOs, which have the highest precedence in the processing order. This order is essential to understand as it determines which GPO settings apply and which ones take precedence when there are conflicting policies.

The order of processing for Group Policy Objects is from the broadest level, such as the site, down to the most specific level, like the organizational unit, with the last processed GPO having the highest priority and overriding any conflicting settings.



Group Policy is processed in order

NOTE: To view the precedence of Group Policies on any site, domain, or Organizational Unit (OU), go to the "Group Policy inheritance" tab. The first object that applies last takes precedence over all others.

Implementing Group Policy on an Organizational Unit

First, ensure that you have the Group Policy Management Console (GPMC) installed in the administrative tools. If not, follow these steps:

1. Go to Administrative Tools > Group Policy Management.

2. Right-click on Group Policy Objects and select "New."

3. Name your policy.

4. Click "Link an Existing GPO" to link a GPO to an Organizational Unit.

5. Select the Group Policy Object you want to link.

Note: You can edit the GPO by right-clicking and selecting "Edit."

Configuring Group Policy Settings

A Group Policy Object (GPO) is a collection of Group Policy settings. Normally, a user can edit GPOs that are locally installed on each computer, yet an administrator can create non-local GPOs. **To disable Windows Messenger from running, follow these steps:**

1. Create a GPO as mentioned above.
2. Right-click and edit the Group Policy settings.
3. Your new GPO will appear to the right. Right-click on the GPO and select "Edit."
4. Navigate to User Configuration > Administrative Templates > Windows Components > Windows Messenger.
5. Two Group Policy settings will appear. Double-click on "Do not allow Windows Messenger to be run."
6. There are three options: Not configured, enabled, and disabled. Not configured means that the GPO takes precedence and allows users to use Windows Messenger. Enabled means that you are not allowing Windows Messenger to run, and disabled allows users to run Windows Messenger. (In case you forget what each means, you can press the "Explain" tab, and a clear description will show.)

Note: After configuring the GPO, you can still link it to an OU, Domain, or site by right-clicking on one of the objects and choosing "Link an existing GPO."

Determining Applied GPOs

To determine what effective Group Policies are applied to a user or computer, use the Group Policy Results Wizard. Open the Group Policy Management, then:

1. Right-click on "Group Policy Results" and select "Group Policy Results Wizard."
2. Select a user or computer.
3. A report will be displayed under "Group Policy Results."
4. Click "Show the report" to identify the section of interest.

Security Policies

Some of the other popular security options you can set in Group Policy are:

1. **Password Policy**

Go to Group Policy Object Editor > Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy. There are six options:

a. Enforce password history (keep a history of all passwords assigned and don't allow repetition).
b. Maximum password age (Allows a maximum amount of time a password can be kept before changed. After it expires, the user has to assign a new password).
c. Minimum password age (Determines the minimum amount of time a user can keep his/her password).
d. Password must meet complex requirements (lower case, upper case, numbers, and special characters).
e. Store passwords using reversible encryption (stores passwords in the equivalent of plaintext).

2.**Account Lockout Policy**

Go to Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy.

a. Account lockout duration (A defined number of times in which the user is allowed to enter the correct password).
b. Account lockout threshold (A defined number of times in which the user can enter an incorrect password).
c. Reset account lockout counter after (resets the counter for lockouts after a predetermined time).

3.**User Rights Assignment**

Go to Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment. You can choose either to deny or grant a right for users.

4.**Security Options**

Go to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options. You can choose to grant or deny a number of security options to certain users or groups.

RESULT: The implementation of security group management policy