Active Directory Hardening

# Securing Authentication Methods:

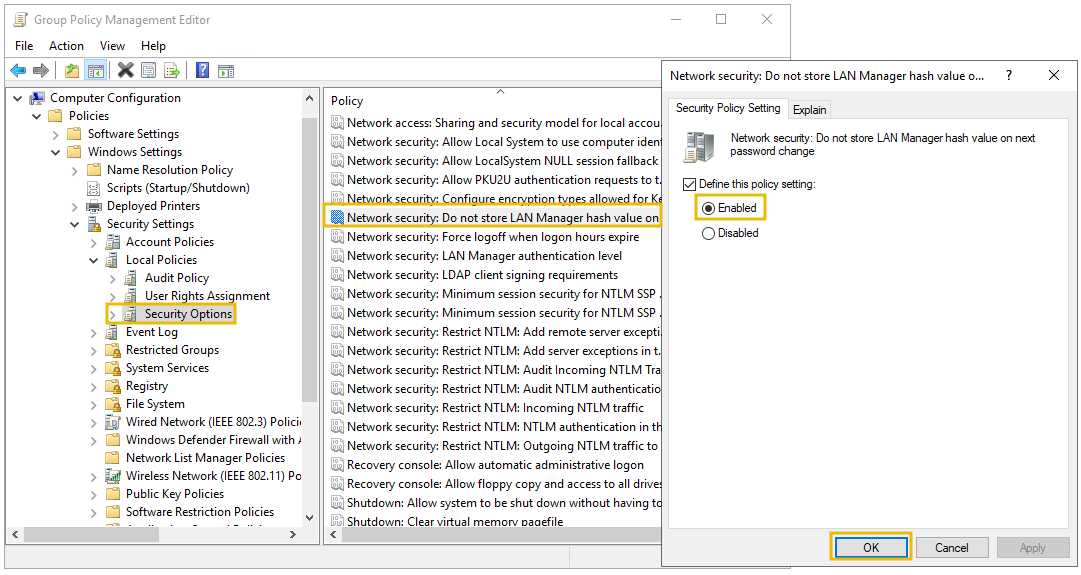
## LAN Manager Hash:

User Password Hashes, LAN Manager hash (LAM) and Windows NT hash are stored in AD. The LM hash is relatively weaker than the NT hash and prone to Brute force attack.

Recommendation: Prevent Windows from storing the password’s LM hash.

### Action:

|  |
| --- |
| Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Network security - Do not store LM hash value on next password change policy > select "Define policy setting" |



* Check!

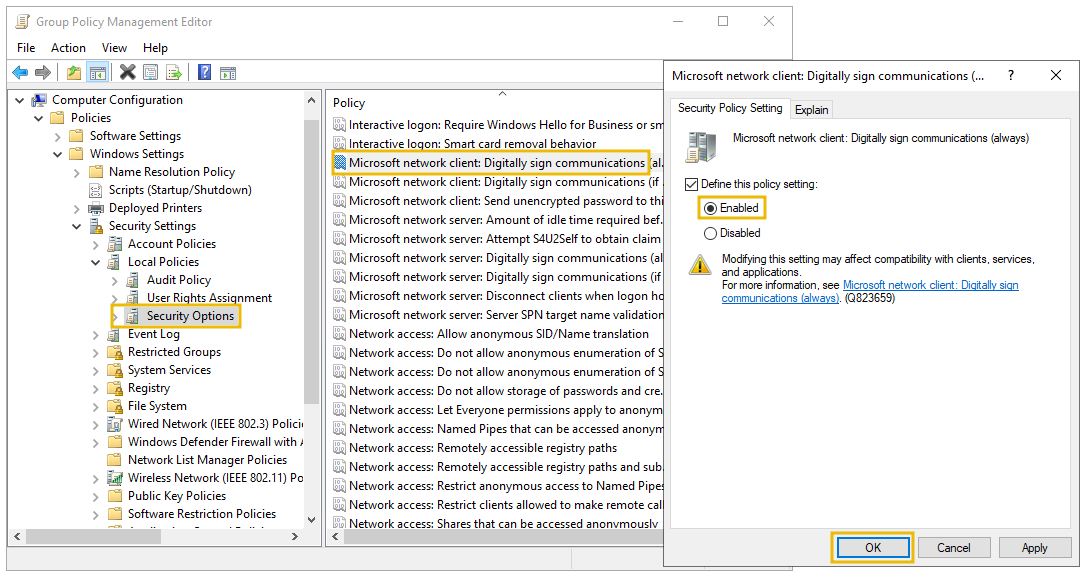
## SMB Signing:

SMB is a Microsoft-based file and printer communication protocol. It is prone to MiTM attack, that may result in modification of SMB traffic in transit, if not the signing is enabled. SMB packet signing ensures the integrity of data for both client and server.

Recommendation: Enable SMB packet signing.

Action:

|  |
| --- |
| Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Microsoft network server: Digitally sign communication (always) > select Enable Digitally Sign Communications |



* Check!

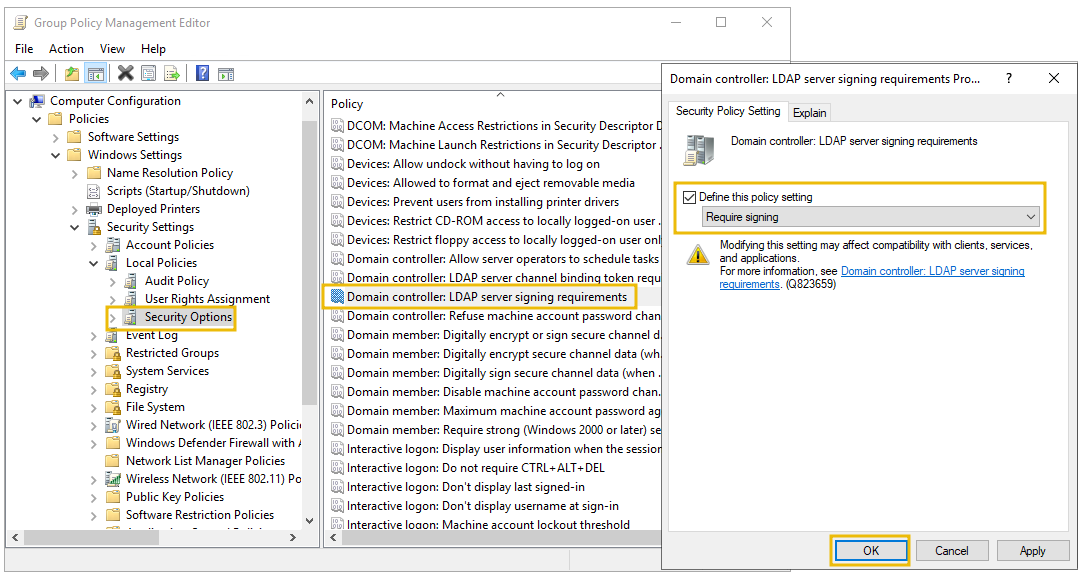
## LDAP Signing:

LDAP is used to locate and authenticate resources on the Network. LDAP is targeted with MiTM and replay attack using custom LDAP request. LDAP Signing is a Simple Authentication and Security Layer (SASL) property that allows only signed LDAP requests and reject plain text or non SASL requests.

Recommendation: Enable LDAP Signing

Action:

|  |
| --- |
| Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Domain controller: LDAP server signing requirements > select Require signing from the dropdown |



* Check!

## Password Rotation:

Active Directory password security is critical to address because of security breaches and password reuse. Password rotation may be applied through implementing password rotation tool or PS script. In general, it should be done in every 3 months.

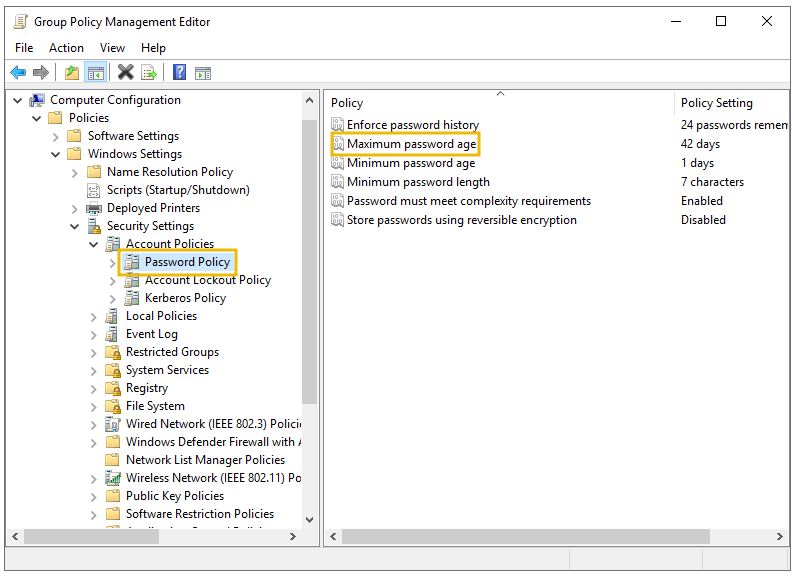
Alternative option can be implementing MFA, so that password should not be rotated so often.

## Password Policies:

Attackers use various corporate password-compromise techniques, including brute force, dictionary, password spraying, credential attacks etc. All organisations must have a strict password policy to defend against all such attacks. Password policies mean different rules for creating passwords, including length, complexity, and changing frequency. For viewing and configuring the password policy, you can use the following:

### Action:

Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy



### Understanding Password Policy Settings:

**Enforce password history:** Prevent at least 10 to 15 old passwords from being set as new ones.

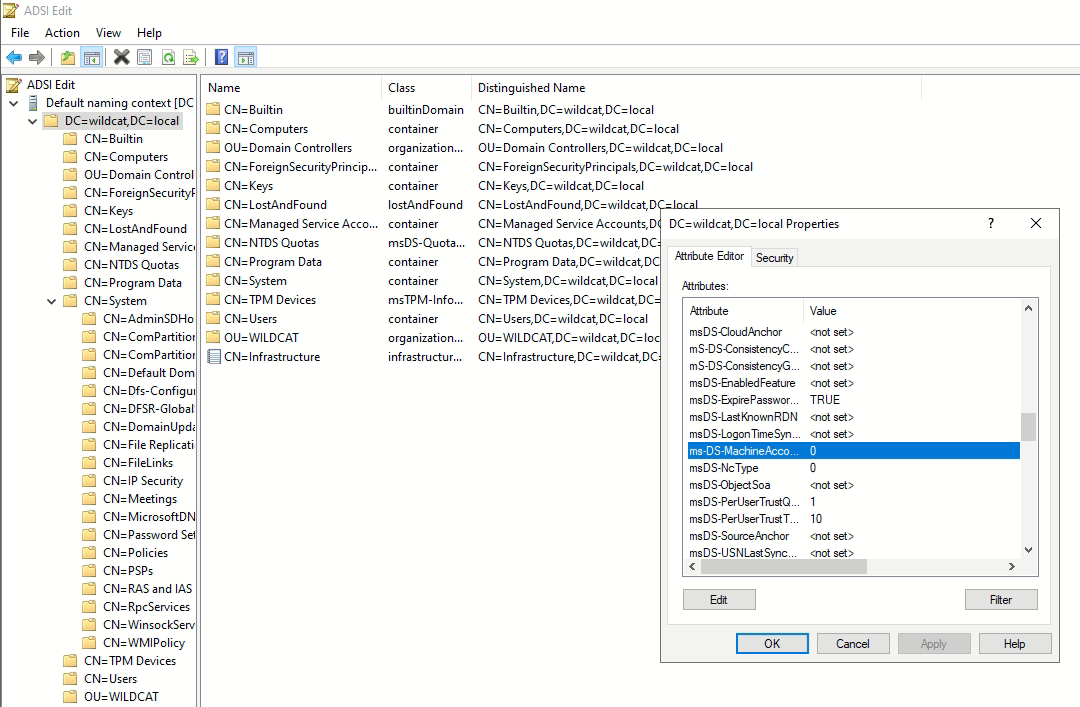
**Minimum password length:** The minimum password length should be set between 10 to 14.

**Complexity requirements:** Must not contain the name of the user account and ensure the password has uppercase letters, lowercase letters, digits, or special characters.

Implementing Least Privilege Model (AD Tiering):

## Unprivileged users can add computer accounts to the domain:

Disable “ms-DS-Machine-Account Quota” accesing the ADSI Edit tool. First connect to the Domain from the ADSI tool > right click on the “DC=…, DC=local” and find the attribute and set it to 0.



REF:

https://tryhackme.com/room/activedirectoryhardening

https://book.hacktricks.xyz/windows-hardening/active-directory-methodology