Network Security Controls - Administrative Controls

Exercise 1: Implementing Password Policies using Windows Group Policy

The Group Policy Management Console (GPMC) is a scriptable Microsoft Management Console (MMC) snap-in, providing a single administrative tool for managing group policy across the enterprise. GPMC is the standard tool for managing group policy.

Lab Scenario

Network defenders can use the GPMC to manage group policy in the Active Directory (AD) across the enterprise. It can be used to protect user accounts and implement domain password policy to enable the use of complex and lengthy passwords. This prevents attackers from cracking the user account passwords through brute-force attacks. The network defender needs to configure group policy settings (group policy object, or GPO) in the AD domain to implement common password requirements.

Lab Objectives

This lab demonstrates how to create a GPO from the GPMC; this group policy will implement a common password policy to enable the use of complex and lengthy passwords in the AD domain.

Overview of the Group Policy

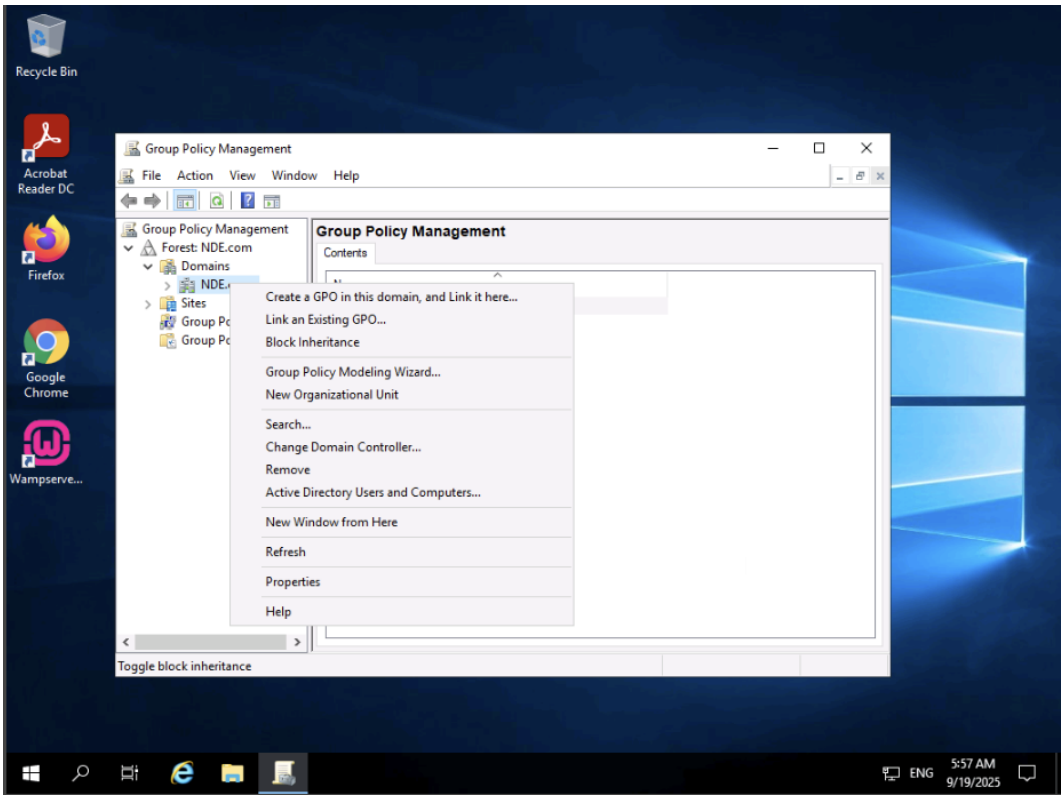
Group policy allows the network defender to manage drive mappings, registry settings, local users and groups, services, files, and folders without the need to learn a scripting language. GPO can help configure password history, password age, password length, and complexity as well as store passwords using reversible encryption policies for users' passwords. The AD domain contains two default GPOs:

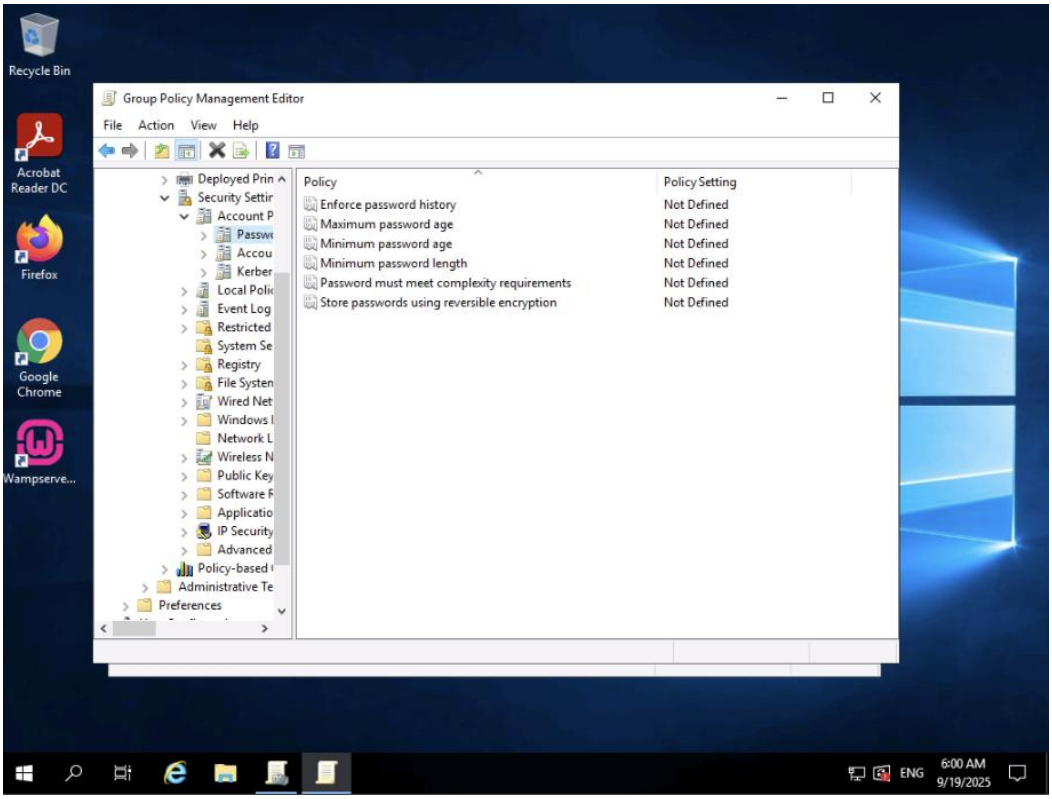
- Default domain policy, which is linked to the domain
- Default domain controllers policy, which is linked to the domain controller's organizational unit (OU).

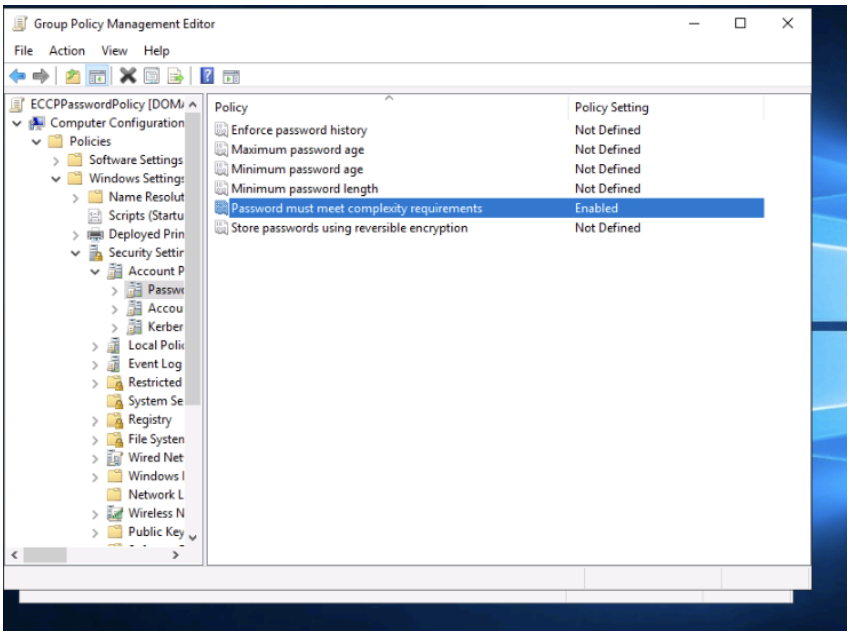
Order of Processing Group Policies:

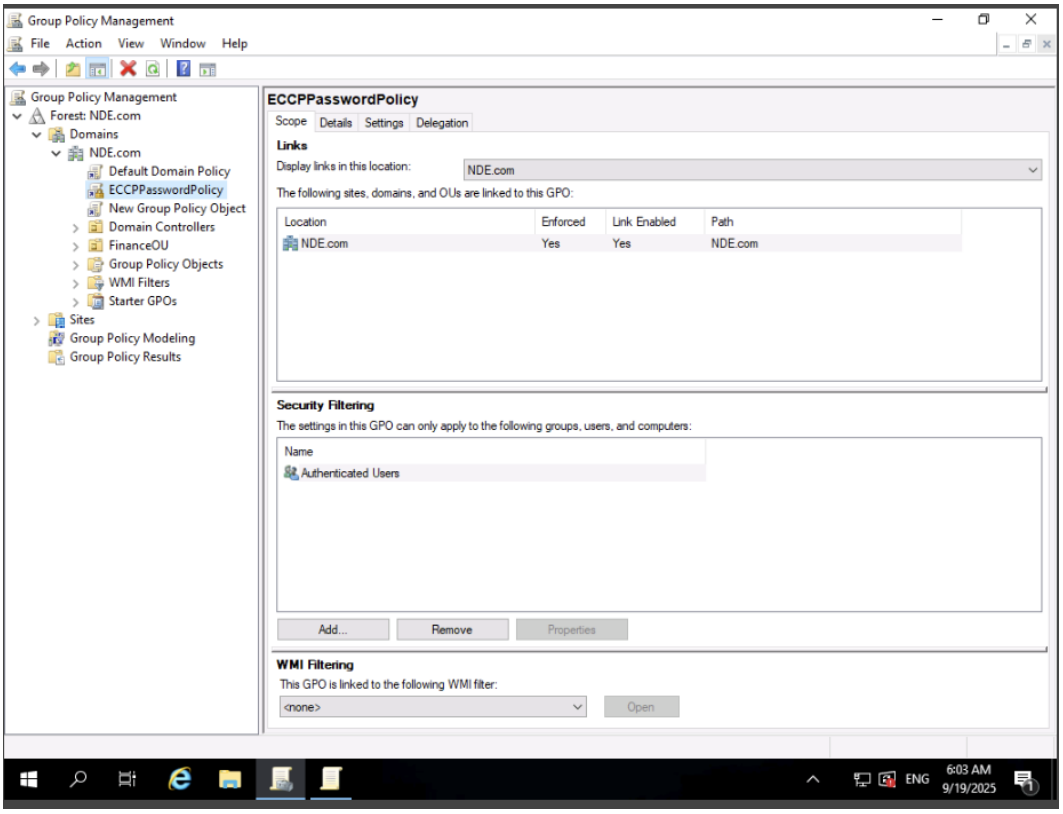
- Local computer policy (applied locally to the system and user)
- AD policies (site -> domain-> OU)
- Site: Applied to all members of a site; will override settings that are configured at the local level

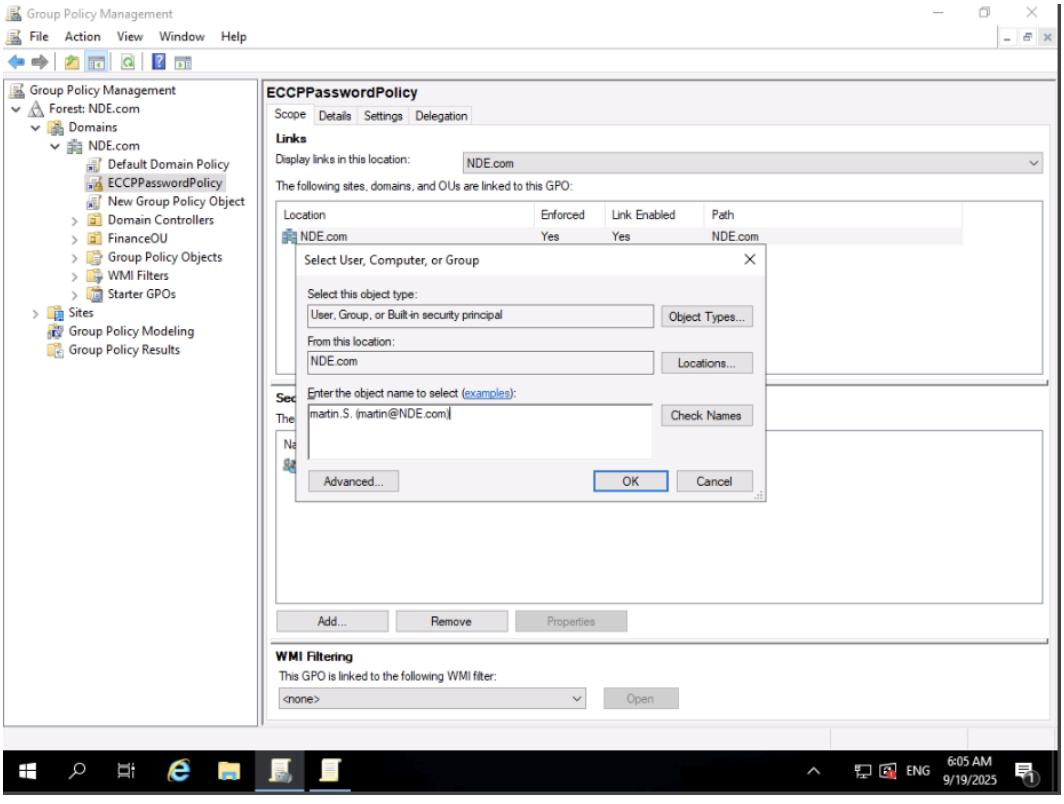
- Domain: GPOs linked to the domain; will override the GPO linked at the local and site level.
- Organizational unit: GPOs linked to OU will override any other GPOs, other than those linked to a sub-OU, or a GPO that is marked as "Enforced"
- Enforced: Will override all other GPOs, unless blocked by Block Inheritance.

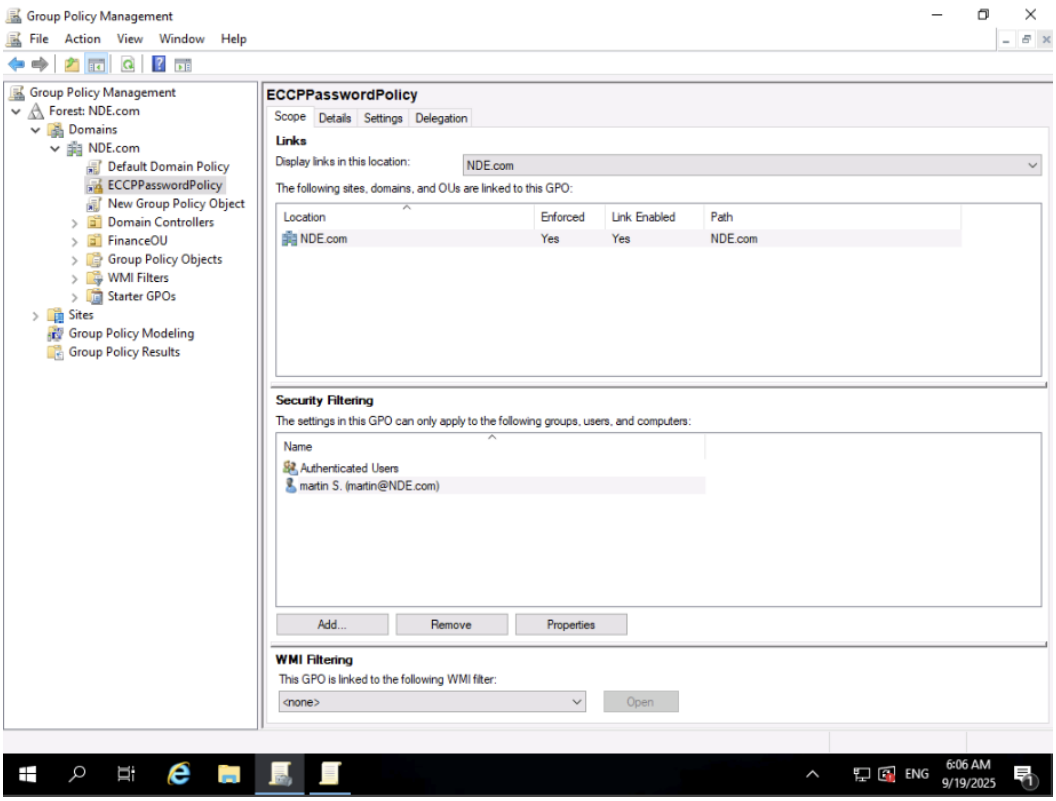


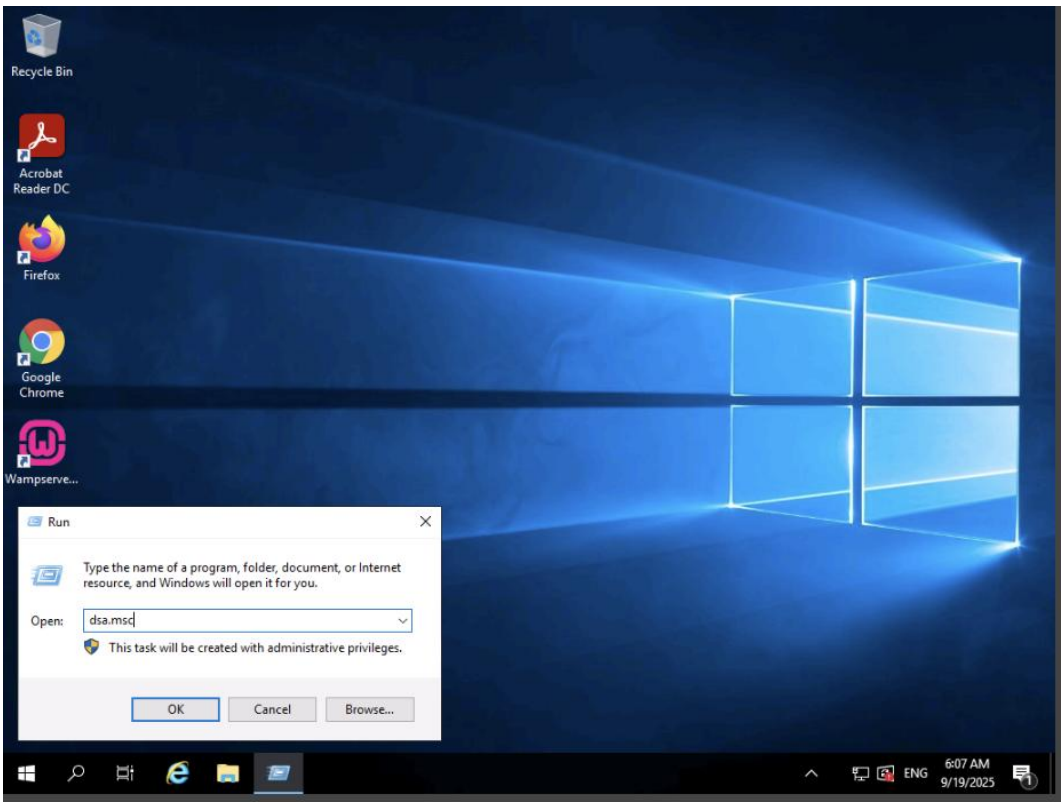

Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserve...
Group Policy Management Editor
File Action View Help
Policy
Policy Setting
Enforce password history
Not Defined
Maximum password age
Not Defined
Minimum password age
Not Defined
Minimum password length
Not Defined
Password must meet complexity requirements
Not Defined
Store passwords using reversible encryption
Not Defined
ENG
6:00 AM
9/19/2025

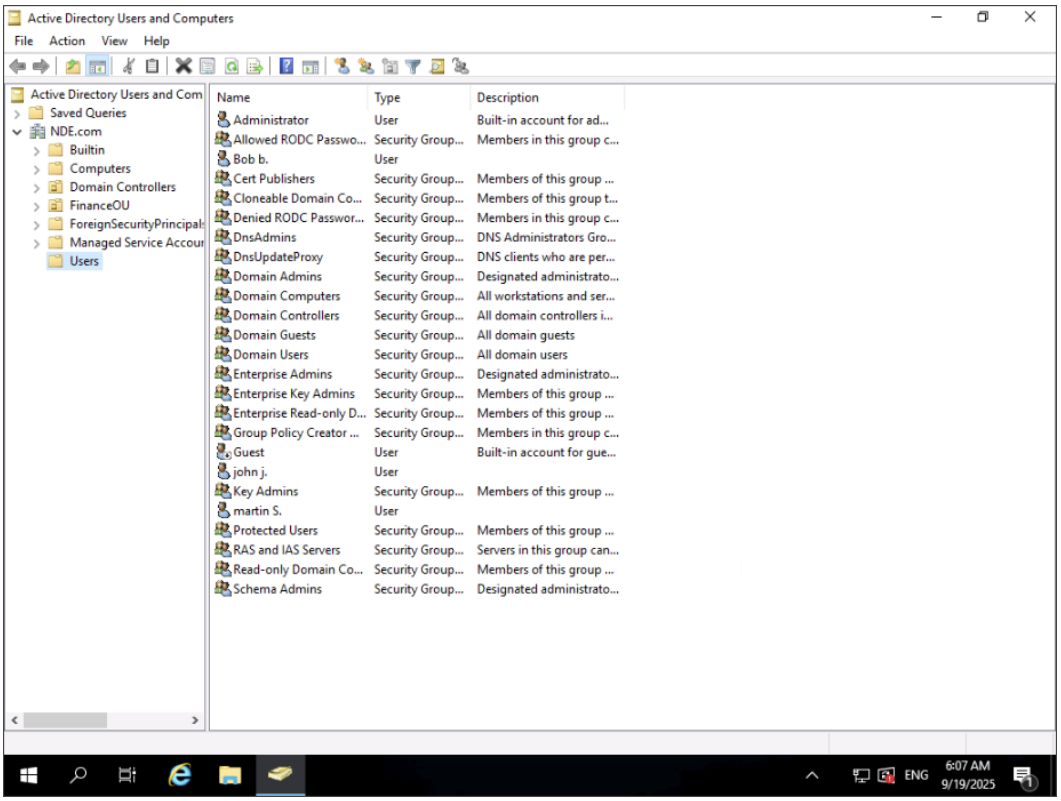

Group Policy Management Editor
File Action View Help
ECCPPasswordPolicy [DOMA
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolut
Scripts (Startu
Deployed Prin
Security Settir
Account P
Passwo
Accou
Kerber
Local Polic
Event Log
Restricted
System Se
Registry
File Systen
Wired Net
Windows I
Network L
Wireless N
Public Key
Policy
Policy Setting
Enforce password history
Not Defined
Maximum password age
Not Defined
Minimum password age
Not Defined
Minimum password length
Not Defined
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Not Defined

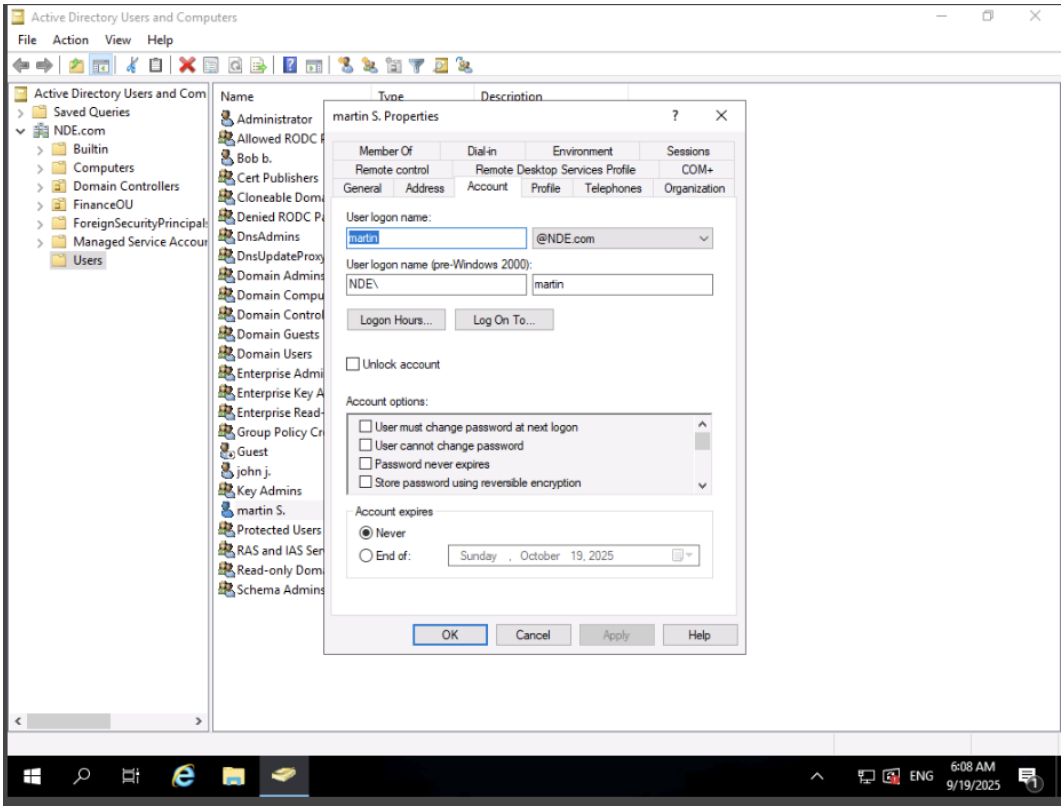

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: NDE.com
Domains
NDE.com
Default Domain Policy
ECCPPasswordPolicy
New Group Policy Object
Domain Controllers
FinanceOU
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
ECCPPasswordPolicy
Scope Details Settings Delegation
Links
Display links in this location: NDE.com
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
NDE.com Yes Yes NDE.com
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none> Open
ENG 6:03 AM 9/19/2025

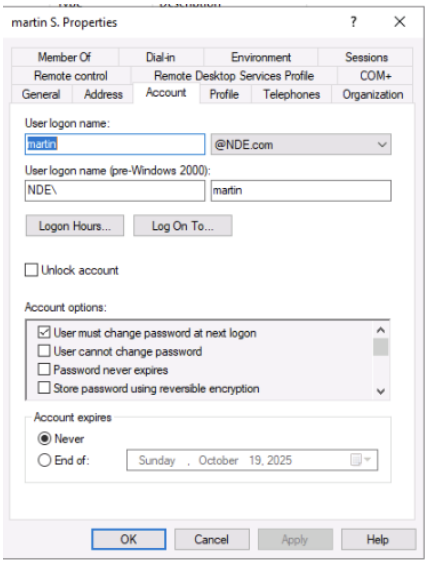

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: NDE.com
Domains
NDE.com
Default Domain Policy
ECCPPasswordPolicy
New Group Policy Object
Domain Controllers
FinanceOU
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
ECCPPasswordPolicy
Scope Details Settings Delegation
Links
Display links in this location: NDE.com
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
NDE.com Yes Yes NDE.com
Select User, Computer, or Group
Select this object type:
User, Group, or Built-in security principal
Object Types...
From this location:
NDE.com
Locations...
Enter the object name to select (examples):
martin.S. (martin@NDE.com)
Check Names
Advanced...
OK
Cancel
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none> Open
ENG 6:05 AM 9/19/2025

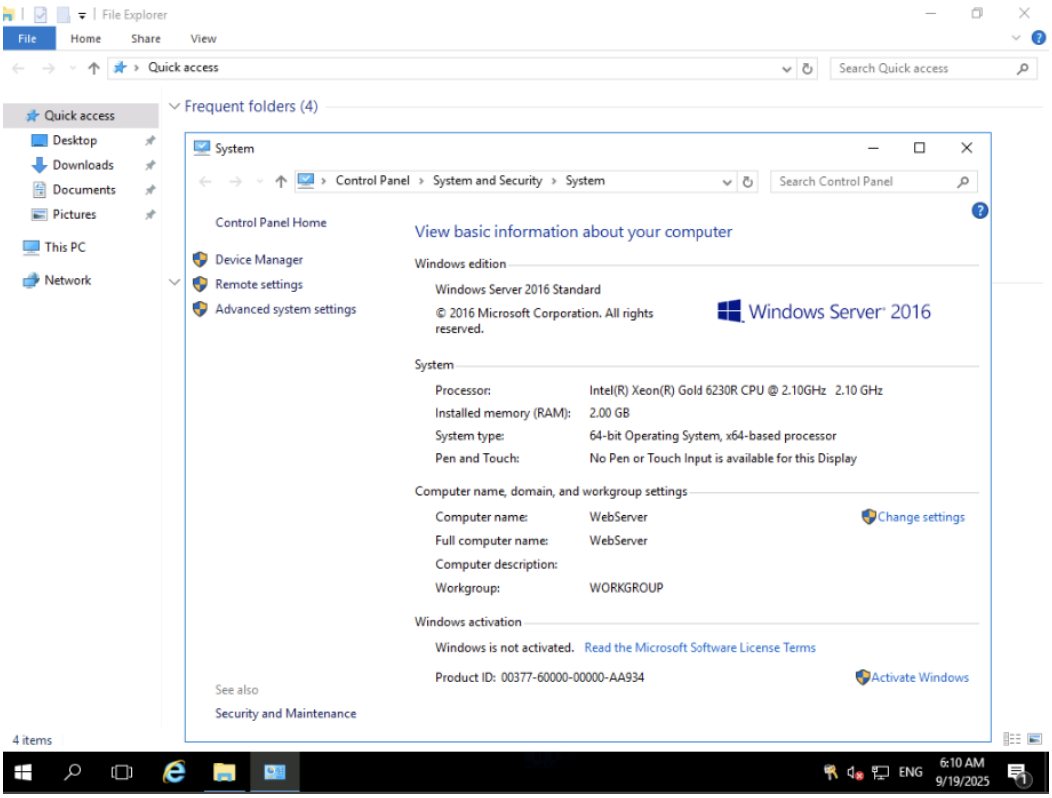

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: NDE.com
Domains
NDE.com
Default Domain Policy
ECCPPasswordPolicy
New Group Policy Object
Domain Controllers
FinanceOU
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
ECCPPasswordPolicy
Scope Details Settings Delegation
Links
Display links in this location: NDE.com
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
NDE.com Yes Yes NDE.com
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
martin S. (martin@NDE.com)
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none> Open
ENG 6:06 AM 9/19/2025

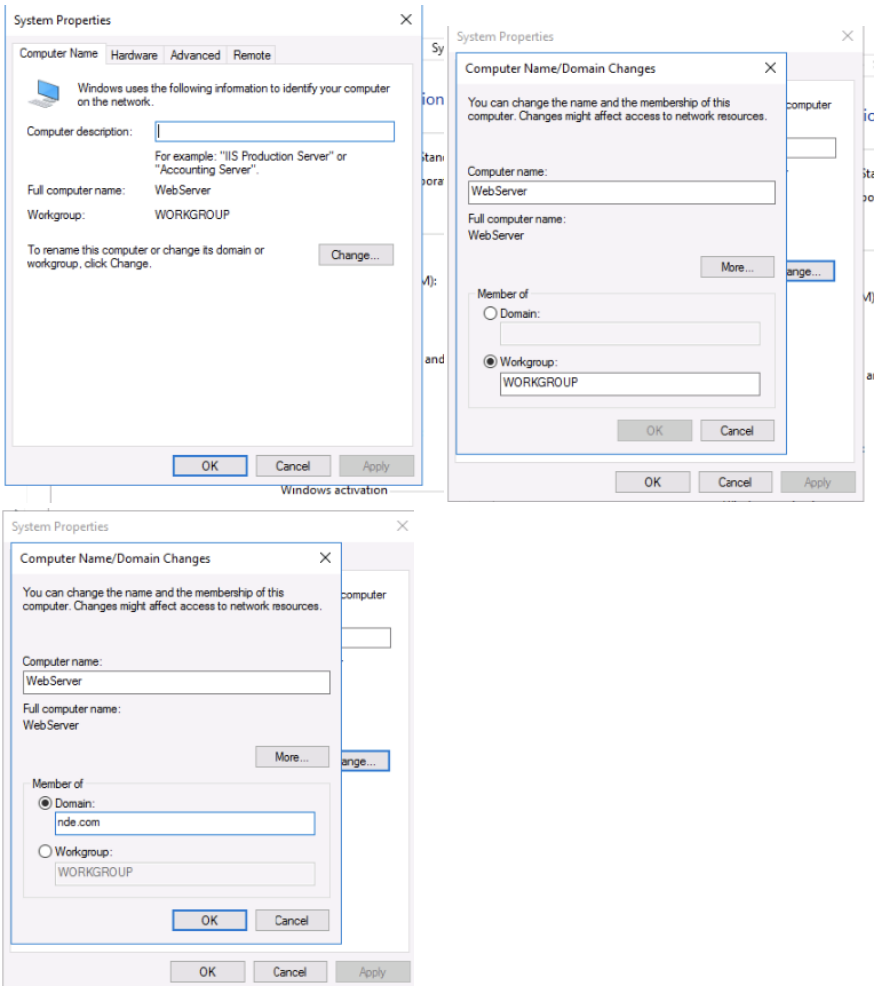

Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Wampserve...
Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open: dsa.msc
This task will be created with administrative privileges.
OK Cancel Browse...
ENG 6:07 AM 9/19/2025

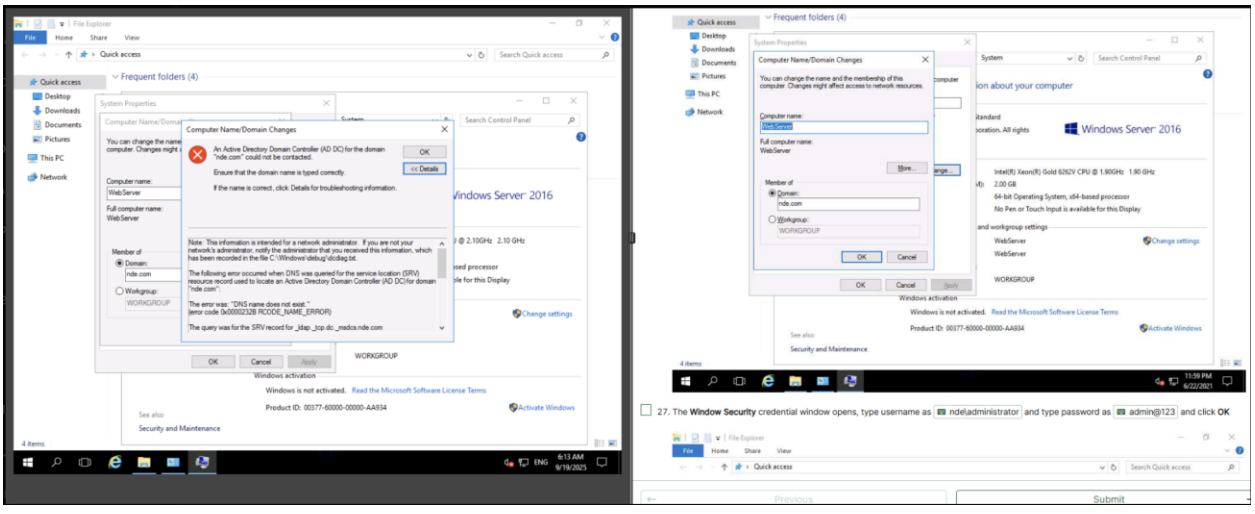

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
NDE.com
Builtin
Computers
Domain Controllers
FinanceOU
ForeignSecurityPrincipals
Managed Service Accour
Users
Name Type Description
Administrator User Built-in account for ad...
Allowed RODC Passwo... Security Group... Members in this group c...
Bob b. User
Cert Publishers Security Group... Members of this group ...
Cloneable Domain Co... Security Group... Members of this group t...
Denied RODC Passwor... Security Group... Members in this group c...
DnsAdmins Security Group... DNS Administrators Gro...
DnsUpdateProxy Security Group... DNS clients who are per...
Domain Admins Security Group... Designated administrato...
Domain Computers Security Group... All workstations and ser...
Domain Controllers Security Group... All domain controllers i...
Domain Guests Security Group... All domain guests
Domain Users Security Group... All domain users
Enterprise Admins Security Group... Designated administrato...
Enterprise Key Admins Security Group... Members of this group ...
Enterprise Read-only D... Security Group... Members of this group ...
Group Policy Creator ... Security Group... Members in this group c...
Guest User Built-in account for gue...
john j. User
Key Admins Security Group... Members of this group ...
martin S. User
Protected Users Security Group... Members of this group ...
RAS and IAS Servers Security Group... Servers in this group can...
Read-only Domain Co... Security Group... Members of this group ...
Schema Admins Security Group... Designated administrato...
ENG 6:07 AM 9/19/2025

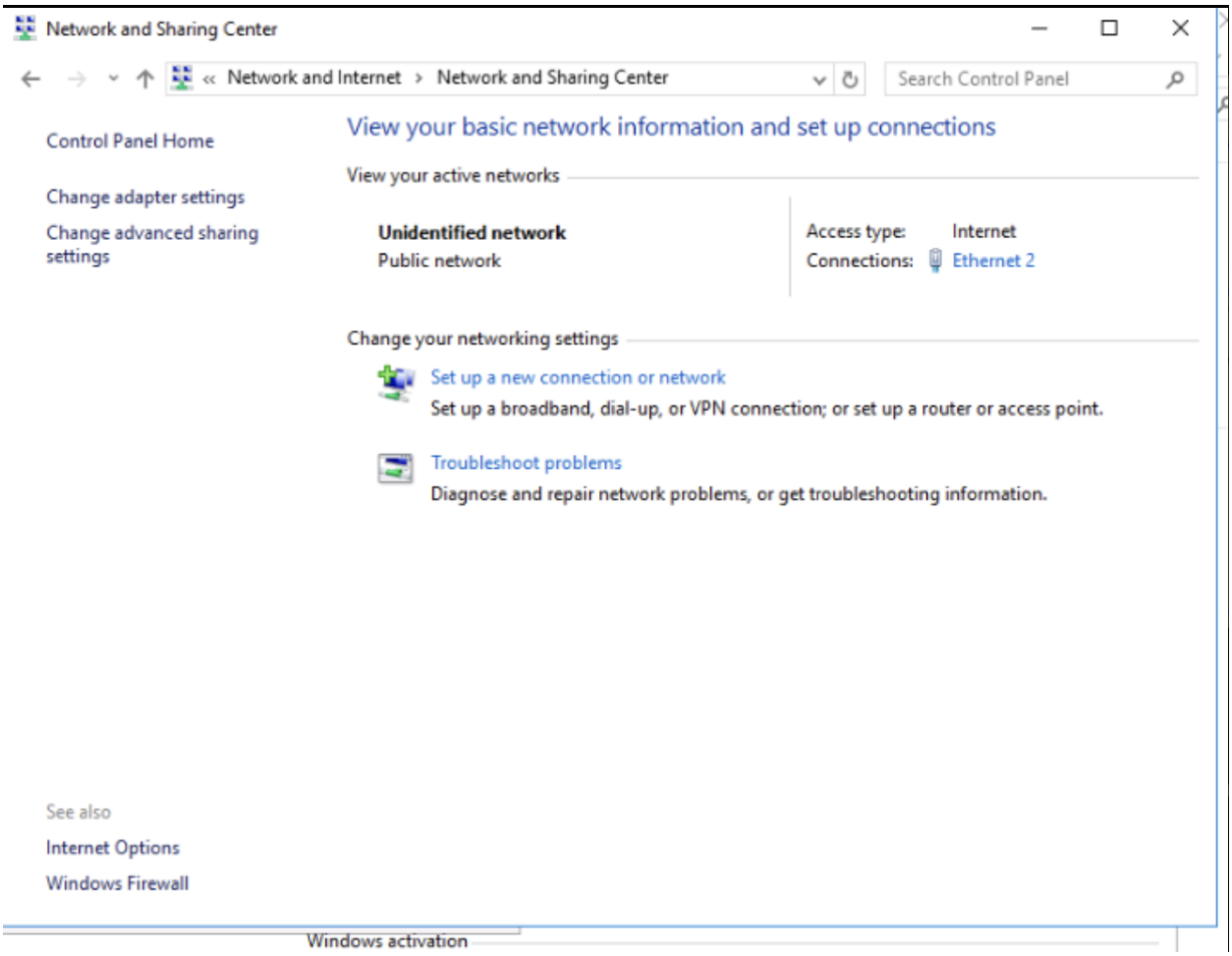

Active Directory Users and Computers
File Action View Help
martin S. Properties
Member Of Dial-in Environment Sessions
Remote control Remote Desktop Services Profile COM+
General Address Account Profile Telephones Organization
User logon name:
martin
@NDE.com
User logon name (pre-Windows 2000):
NDE\
martin
Logon Hours... Log On To...
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: Sunday , October 19, 2025
OK Cancel Apply Help
ENG 6:08 AM 9/19/2025

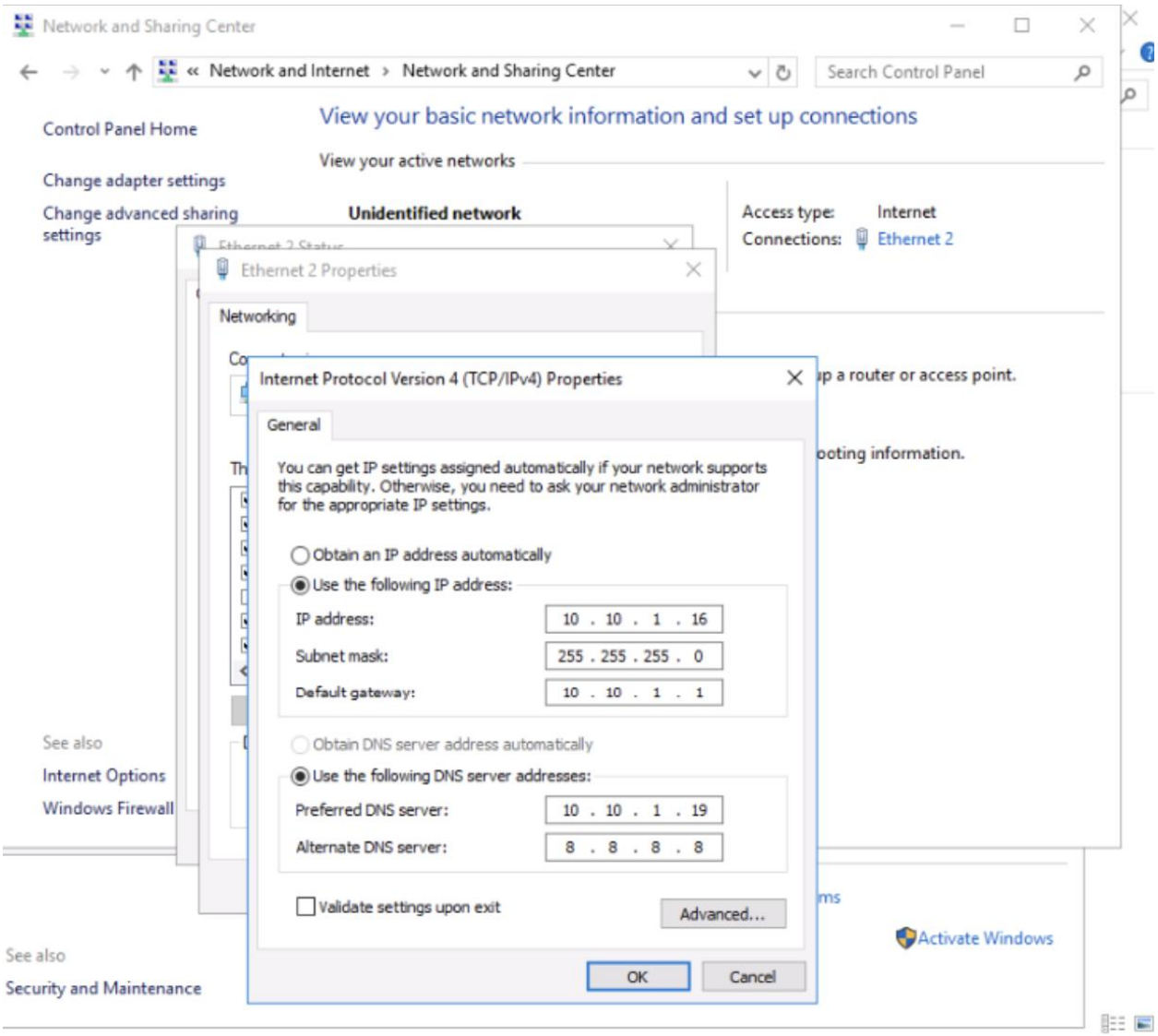

martin S. Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User logon name:
martin
@NDE.com
User logon name (pre-Windows 2000):
NDE\
martin
Logon Hours...
Log On To...
Unlock account
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account expires
Never
End of:
Sunday , October 19, 2025
OK
Cancel
Apply
Help

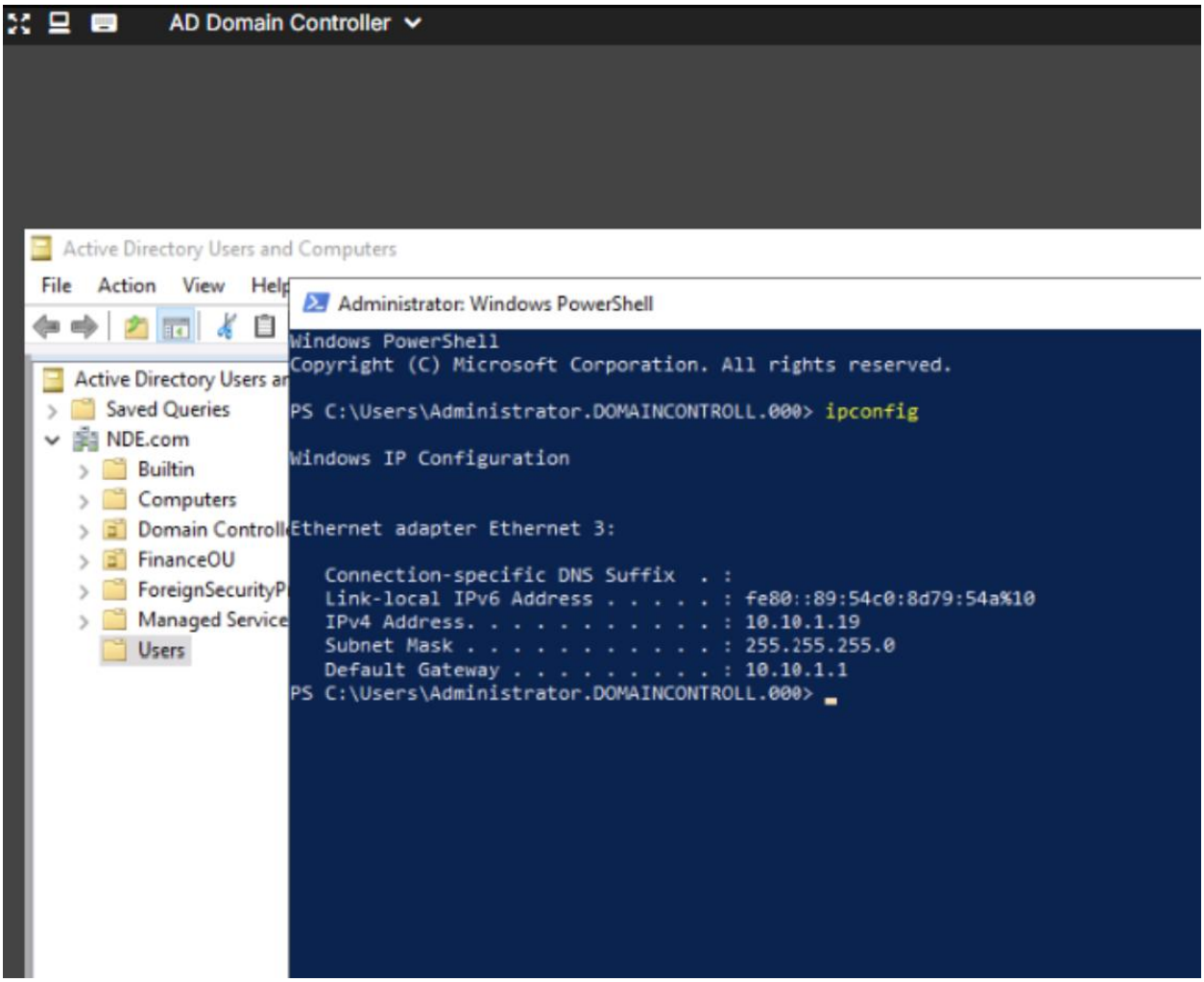

File Explorer
File
Home
Share
View
Quick access
Search Quick access
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Frequent folders (4)
System
Control Panel
System and Security
System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
Advanced system settings
View basic information about your computer
Windows edition
Windows Server 2016 Standard
© 2016 Microsoft Corporation. All rights reserved.
Windows Server 2016
System
Processor: Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz 2.10 GHz
Installed memory (RAM): 2.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings
Computer name: WebServer
Change settings
Full computer name: WebServer
Computer description:
Workgroup: WORKGROUP
Windows activation
Windows is not activated. Read the Microsoft Software License Terms
Product ID: 00377-60000-00000-AA934
Activate Windows
See also
Security and Maintenance
4 items
ENG
6:10 AM
9/19/2025


System Properties
Computer Name
Hardware
Advanced
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "IIS Production Server" or "Accounting Server".
Full computer name:
WebServer
Workgroup:
WORKGROUP
To rename this computer or change its domain or workgroup, click Change.
Change...
OK
Cancel
Apply
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
WebServer
Full computer name:
WebServer
More...
Member of
Domain:
Workgroup:
WORKGROUP
nde.com

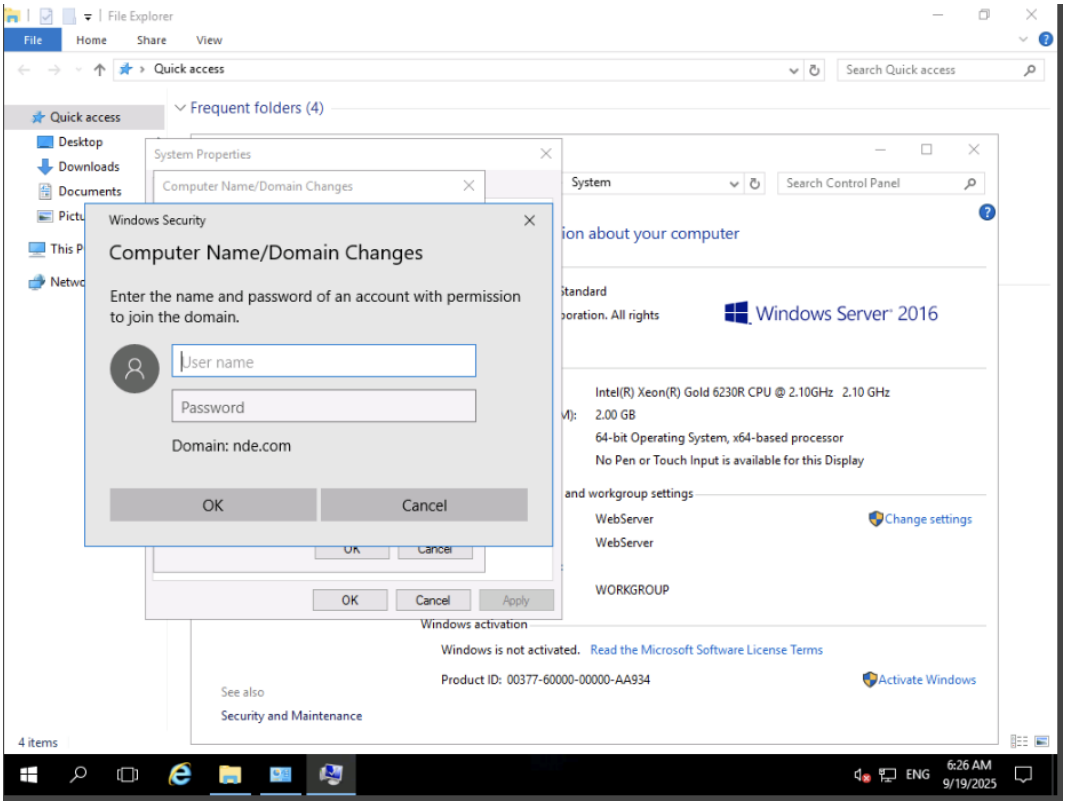

Frequent folders (4)
Computer Name/Domain Changes
Windows Server 2016
Windows activation
Windows is not activated. Read the Microsoft Software License Terms
Product ID: 00377-60000-00000-AA934
Activate Windows
Security and Maintenance
27. The Window Security credential window opens, type username as nde\administrator and type password as admin@123 and click OK
Previous
Submit

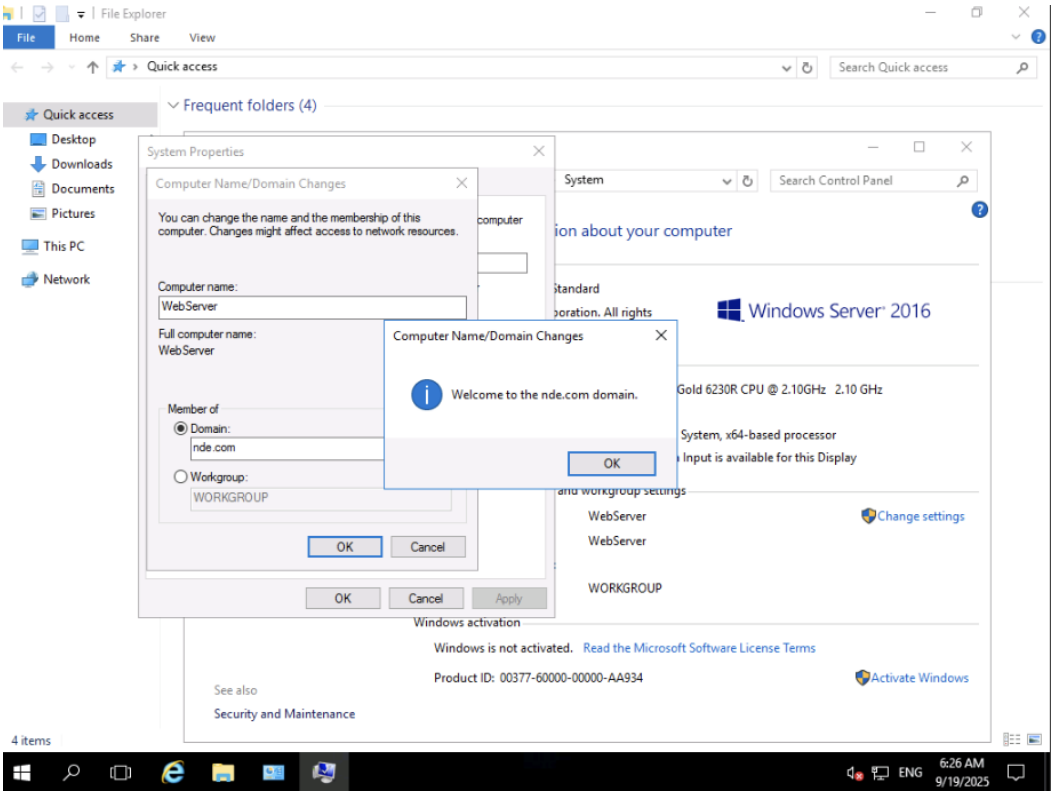

Network and Sharing Center
Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Unidentified network
Public network
Access type: Internet
Connections: Ethernet 2
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Internet Options
Windows Firewall
Windows activation

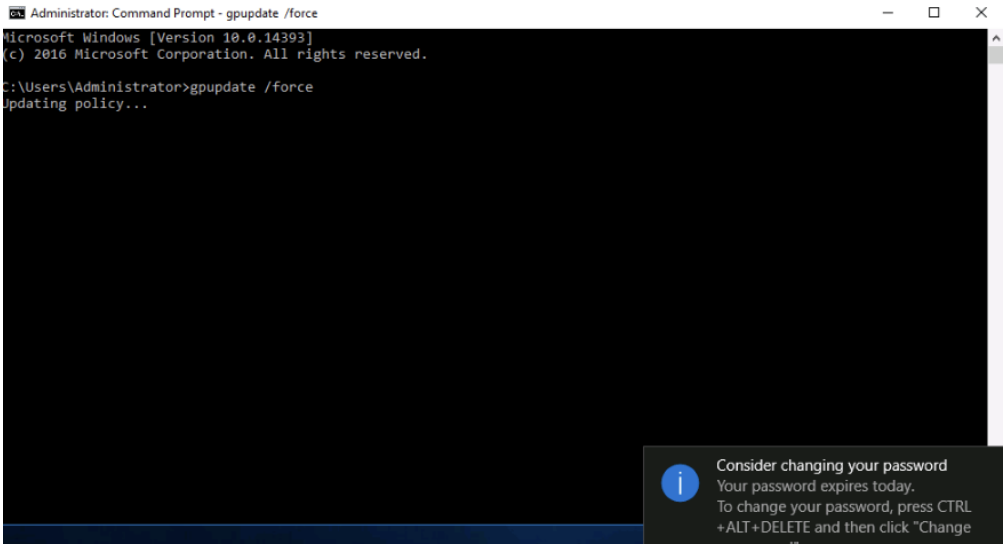

Network and Sharing Center
« Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
View your basic network information and set up connections
Change adapter settings
View your active networks
Change advanced sharing settings
Unidentified network
Access type: Internet
Connections: Ethernet 2
Ethernet 2 Properties
Networking
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 10 . 1 . 16
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 10 . 1 . 19
Alternate DNS server: 8 . 8 . 8 . 8
Validate settings upon exit
Advanced...
OK
Cancel
See also
Internet Options
Windows Firewall
See also
Security and Maintenance
Activate Windows

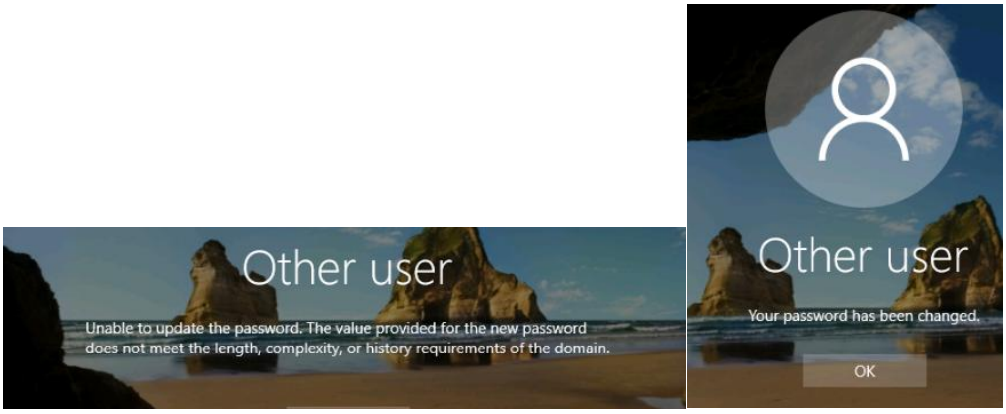


The WebServer machine failed to join the **NDE.com** domain because it was using Google DNS (8.8.8.8) as an alternate resolver. When domain lookups went to Google instead of the Domain Controller (10.10.1.19), the join attempt returned **“DNS name does not exist.”** After confirming that the Domain Controller’s IP was 10.10.1.19, the fix was to remove the external DNS entry and configure the WebServer to use only the Domain Controller for DNS. Flushing DNS and retrying the join should now allow the WebServer to successfully connect to the domain.


File Explorer
File
Home
Share
View
Quick access
Search Quick access
Frequent folders (4)
Desktop
Downloads
Documents
Pictures
This PC
Network
System Properties
Computer Name/Domain Changes
Windows Security
Computer Name/Domain Changes
Enter the name and password of an account with permission to join the domain.
User name
Password
Domain: nde.com
OK
Cancel
Apply
System
Search Control Panel
Windows Server 2016
Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz 2.10 GHz
2.00 GB
64-bit Operating System, x64-based processor
No Pen or Touch Input is available for this Display
WebServer
WebServer
Change settings
WORKGROUP
Windows activation
Windows is not activated. Read the Microsoft Software License Terms
Product ID: 00377-60000-00000-AA934
Activate Windows
See also
Security and Maintenance
4 items
ENG
6:26 AM
9/19/2025


File Explorer
File
Home
Share
View
Quick access
Search Quick access
Frequent folders (4)
Desktop
Downloads
Documents
Pictures
This PC
Network
System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
WebServer
Full computer name:
WebServer
Member of
Domain:
nde.com
Workgroup:
WORKGROUP
OK
Cancel
Apply
Computer Name/Domain Changes
Welcome to the nde.com domain.
OK
System
Search Control Panel
Windows Server 2016
Gold 6230R CPU @ 2.10GHz 2.10 GHz
System, x64-based processor
Input is available for this Display
WebServer
WebServer
Change settings
WORKGROUP
Windows activation
Windows is not activated. Read the Microsoft Software License Terms
Product ID: 00377-60000-00000-AA934
Activate Windows
See also
Security and Maintenance
4 items
ENG
6:26 AM
9/19/2025





Lab Summary: Implementing Password Policies using Windows Group Policy

Scenario

This lab demonstrated how to use the Group Policy Management Console (GPMC) in Active Directory to enforce strong password policies across a domain. Group policies are critical for protecting user accounts against brute-force attacks by requiring complex, unique, and regularly updated passwords.

Steps Completed

- Logged into the AD Domain Controller as Administrator.
- Opened **Group Policy Management** (gpmc.msc) and created a new GPO named **ECCPassword Policy** linked to the NDE.com domain.
- Configured password complexity requirements, including minimum length and mixed character sets.
- Enforced the GPO so it could not be overridden.
- Applied security filtering to target a specific user account (Martin).
- Updated the account properties to require a password change at the next logon.

Issues Encountered

- When attempting to join the **WebServer** client to the domain, the system returned an error: *"An Active Directory Domain Controller for the domain NDE.com could not be contacted."*
- Investigation showed that the WebServer was configured with **Google DNS (8.8.8.8)** as an alternate resolver. This caused domain lookups to fail since external DNS servers do not recognize private AD domains.

Resolution

- Reconfigured the WebServer's DNS to point only to the Domain Controller (10.10.1.19).
- Flushed DNS and re-registered the client records.
- Verified that nslookup nde.com and _ldap._tcp.dc._msdcs.nde.com resolved correctly to the Domain Controller.
- With DNS corrected, the WebServer could successfully join the domain and apply the password policy.

Reflection

This lab reinforced the importance of DNS in Active Directory operations. Even when group policies are configured correctly, domain clients will fail to join or apply policies if DNS points to external resolvers instead of the Domain Controller. Proper network configuration is essential for security controls like password policies to function as intended.