



Group Policy Management



File Action View Window Help



Group Policy Management

- Forest: forest.local
 - Domains
 - forest.local
 - Default Domain Controllers Policy**
 - Default Domain Policy
 - Enforce_Strong_Passwords
 - Domain Controllers
 - FRANCE
 - GROUPS
 - INDIA
 - INTERNS
 - SOUTH_KOREA
 - Group Policy Objects
 - WMI Filters
 - Starter GPOs
 - Sites
 - Group Policy Modeling
 - Group Policy Results

Default Domain Controllers Policy

Scope Details Settings Delegation

Links

Display links in this location: forest.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link En
Domain Controllers	No	Yes
forest.local	No	Yes

Security Filtering

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

Name
Authenticated Users

Add... Remove Properties

WMI Filtering

This GPO is linked to the following WMI filter:

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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-ADUser -Identity ravi -Properties MemberOf, Enabled, LastLogonDate | Select-Object Name, Enabled, LastLogonDate, @{Name="Groups";Expression={$_.MemberOf | % { (Get-ADGroup $_).Name }} -join ", "}}

Name Enabled LastLogonDate Groups
-----
Ravi True 6/19/2025 1:27:50 PM Workstation_Users, INTERN_LEADS, MFA_required, IT_Admins, Remote Management Users

PS C:\Users\Administrator> Get-ADUser -Identity adrien -Properties MemberOf, Enabled, LastLogonDate | Select-Object Name, Enabled, LastLogonDate, @{Name="Groups";Expression={$_.MemberOf | % { (Get-ADGroup $_).Name }} -join ", "}}

Name Enabled LastLogonDate Groups
-----
Adrien True 6/19/2025 10:48:09 AM Workstation_Users, MFA_required, Design_Team, Remote Management Users

PS C:\Users\Administrator> Get-ADUser -Identity yoojung -Properties MemberOf, Enabled, LastLogonDate | Select-Object Name, Enabled, LastLogonDate, @{Name="Groups";Expression={$_.MemberOf | % { (Get-ADGroup $_).Name }} -join ", "}}

Name Enabled LastLogonDate Groups
-----
Kim Yoo Jung True Workstation_Users, IT_Admins, Remote Management Users

PS C:\Users\Administrator> Get-ADUser -Identity hari -Properties MemberOf, Enabled, LastLogonDate | Select-Object Name, Enabled, LastLogonDate, @{Name="Groups";Expression={$_.MemberOf | % { (Get-ADGroup $_).Name }} -join ", "}}

Name Enabled LastLogonDate Groups
-----
Hari True Workstation_Users, HR_Junior, Finance_Team, Remote Management Users

PS C:\Users\Administrator>
```

Active Directory Users and Computers

File Action View Help



- Active Directory Users and Com
- > Saved Queries
- > forest.local
 - > BuiltIn
 - > Computers
 - > Domain Controllers
 - > ForeignSecurityPrincipal:
 - > FRANCE
 - > PARIS
 - DESIGN
 - GROUPS
 - > INDIA
 - > INTERNS
 - > Keys
 - LostAndFound
 - Managed Service Accou
 - > Program Data
 - Microsoft
 - > SOUTH_KOREA
 - SEOUL
 - > System
 - > Users
 - > NTDS Quotas
 - > TPM Devices

Name	Type	Description
Azure	Security Group...	
Design_Team	Security Group...	
Engineering	Security Group...	
Finance_Team	Security Group...	Accounting access
Helpdesk	Security Group...	
HR_Junior	Security Group...	Junior HR staff with password reset rights
Hybrid_Wor...	Security Group...	
INTERN_LEA...	Security Group...	Intern Leads manage Intern OUs
IT_Admins	Security Group...	Admin rights
Laptop_Users	Security Group...	
Marketing_...	Security Group...	
MFA_required	Security Group...	MFA-enabled users
No_PW_Expiry	Security Group...	
Printer_Acco...	Security Group...	
Project_Ash...	Security Group...	
SharePoint_...	Security Group...	
WFH_Emplo...	Security Group...	
Workstation...	Security Group...	Users allowed to log on to workstations

Finance_Team Properties



Object

Security

Attribute Editor

General

Members

Member Of

Managed By

Members:

Name

Active Directory Domain Services Folder



Hari

forest.local/INDIA/CHENNAI/HR

Add...

Remove

OK

Cancel

Apply

Help

HR_Junior Properties



Object

Security

Attribute Editor


General

Members

Member Of

Managed By

Members:

Name	Active Directory Domain Services Folder
 Hari	forest.local/INDIA/CHENNAI/HR



Hari

forest.local/INDIA/CHENNAI/HR

Add...

Remove

OK

Cancel

Apply

Help

INTERN_LEADS Properties



Object

Security

Attribute Editor

General

Members

Member Of

Managed By

Members:

Name

Active Directory Domain Services Folder



Ravi

forest.local/INDIA/PUNE/MARKETING



Add...

Remove

OK

Cancel

Apply

Help

IT_Admis Properties



Object

Security

Attribute Editor



General

Members

Member Of

Managed By

Members:

Name	
	Active Directory Domain Services Folder
 Kim Yoo Jung	forest.local/SOUTH_KOREA/SEOUL/MARKETI...
 Ravi	forest.local/INDIA/PUNE/MARKETING

Add...

Remove

OK

Cancel

Apply

Help

MFA_required Properties



Object

Security

Attribute Editor



General

Members

Member Of

Managed By

Members:

Name	Active Directory Domain Services Folder
 Adrien	forest.local/FRANCE/PARIS/DESIGN
 Ravi	forest.local/INDIA/PUNE/MARKETING

Add...

Remove

OK

Cancel

Apply

Help

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Users\yoojung> New-ADUser -Name "TestUser3" -Path "OU=SEOUL, OU=SOUTH_KOREA, DC=forest, DC=local" -AccountPassword (ConvertTo-SecureString "Pass123!" -AsPlainText -Force) -Enabled $true -Credential (Get-Credential "forest\yoojung")
```

New-ADUser : Access is denied

At line:1 char:1

+ New-ADUser -Name "TestUser3" -Path "OU=SEOUL, OU=SOUTH_KOREA, DC=fore ...

+ ~~~~~

+ CategoryInfo : PermissionDenied: (CN=TestUser3,OU...orest, DC=local:String) [New-ADUser], UnauthorizedAccess
Exception
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:System.UnauthorizedAccessException,Microsoft.ActiveDirectory.Manag
ement.Commands.NewADUser

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

IT_Admins Properties



General

Members

Member Of

Managed By

Object

Security

Attribute Editor

Group or user names:

- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- IT_Admins (FOREST\IT_Admins)**
- Domain Admins (FOREST\Domain Admins)

Add...

Remove

Permissions for IT_Admins

Allow

Deny

Full control



Read



Write



Create all child objects



Delete all child objects



For special permissions or advanced settings, click Advanced.

Advanced

OK

Cancel

Apply

Help

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Windows\system32> New-ADUser -Name "TestUser" -Path "OU=SEOUL, OU=SOUTH_KOREA, DC=forest,DC=local" -AccountPassword (ConvertTo-SecureString "Pass123!" -AsPlainText -Force) -Enabled $true -Credential (Get-Credential "forest\yoojung")
```

Windows PowerShell credential request



Enter your credentials.

User name:

forest\yoojung

Password:

••••••••

OK

Cancel

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Windows\system32> New-ADUser -Name "TestUser" -Path "OU=SEOUL, OU=SOUTH_KOREA, DC=forest,DC=local" -AccountPassword (ConvertTo-SecureString "Pass123!" -AsPlainText -Force) -Enabled $true -Credential (Get-Credential "forest\yoojung")
```

New-ADUser : Either the target name is incorrect or the server has rejected the client credentials.

At line:1 char:1

```
+ New-ADUser -Name "TestUser" -Path "OU=SEOUL, OU=SOUTH_KOREA, DC=fores ...
```

```
+ ~~~~~
```

```
+ CategoryInfo          : SecurityError: (:) [New-ADUser], AuthenticationException
```

```
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:System.Security.Authentication.AuthenticationException,Microsoft.ActiveDirectory.Management.Commands.NewADUser
```

```
PS C:\Windows\system32> New-ADUser -Name "TestUser" -Path "OU=SEOUL, OU=SOUTH_KOREA, DC=forest,DC=local" -AccountPassword (ConvertTo-SecureString "Pass123!" -AsPlainText -Force) -Enabled $true -Credential (Get-Credential "forest\yoojung")
```

New-ADUser : Access is denied

At line:1 char:1

```
+ New-ADUser -Name "TestUser" -Path "OU=SEOUL, OU=SOUTH_KOREA, DC=fores ...
```

```
+ ~~~~~
```

```
+ CategoryInfo          : PermissionDenied: (CN=TestUser,OU=...forest,DC=local:String) [New-ADUser], UnauthorizedAccessException
```

```
+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:System.UnauthorizedAccessException,Microsoft.ActiveDirectory.Management.Commands.NewADUser
```

```
PS C:\Windows\system32> _
```

```
PS C:\Users\yoojung> NEW-ADUSER -Name "TestUser" -Path $OU ` -AccountPassword (CONVERTTO-SECURESTRING "Pass123!" -ASPLAINTEXT -Force) ` -Enabled $true -Credential (Get-Credential "forest\yoojung")
```

```
New-ADUser : Cannot validate argument on parameter 'Path'. The argument is null or empty. Provide an argument that is not null or empty, and then try the command again.
```

```
At line:1 char:35
```

```
+ NEW-ADUSER -Name "TestUser" -Path $OU ` -AccountPassword (CONVERTTO-S ...
```

```
+  
+ ~~~~
```

```
+ CategoryInfo          : InvalidData: (:) [New-ADUser], ParameterBindingValidationException
```

```
+ FullyQualifiedErrorId : ParameterArgumentValidationError,Microsoft.ActiveDirectory.Management.Commands.NewADUser
```

The command completed successfully

```
PS C:\Users\yoojung> NEW-ADUSER -Name "TestUser" -Path $OU ` -AccountPassword (CONVERTTO-SECURESTRING "Pass123!" -ASPLAINTEXT -Force) ` -Enabled $true -Credential (Get-Credential "forest\yoojung")
```

New-ADUser : Cannot validate argument on parameter 'Path'. The argument is null or empty. Provide an argument that is not null or empty, and then try the command again.

At line:1 char:35

```
+ NEW-ADUSER -Name "TestUser" -Path $OU ` -AccountPassword (CONVERTTO-S ...
```

+ ~~~~

+ CategoryInfo : InvalidData: (:) [New-ADUser], ParameterBindingValidationException

+ FullyQualifiedErrorId : ParameterArgumentValidationError,Microsoft.ActiveDirectory.Management.Commands.NewADUser

```
PS C:\Users\yoojung> $OU = "OU=SEOUL,OU=SOUTH_KOREA,DC=forest,DC=local"
```

```
PS C:\Users\yoojung> NEW-ADUSER -Name "TestUser" -Path $OU ` -AccountPassword (CONVERTTO-SECURESTRING "Pass123!" -ASPLAINTEXT -Force) -Enabled $true -Credential (Get-Credential "forest\yoojung")
```

NEW-ADUSER : Access is denied

At line:1 char:1

```
+ NEW-ADUSER -Name "TestUser" -Path $OU ` -AccountPassword (CONVERTTO-S ...
```

+ ~~~~~

+ CategoryInfo : PermissionDenied: (CN=TestUser,OU=...forest,DC=local:String) [New-ADUser], UnauthorizedAccessException

+ FullyQualifiedErrorId : ActiveDirectoryCmdlet:System.UnauthorizedAccessException,Microsoft.ActiveDirectory.Management.Commands.NewADUser

```
PS C:\Users\yoojung> dscls $OU /G "IT_Admins:CC;user" /I:S
```

Parameter /G was unexpected.

Displays or modifies permissions (ACLs) of an Active Directory Domain Services (AD DS) Object

```
DSACLs object [/I:TSP] [/N] [/P:YN] [/G <group/user>:<perms> [...]]  
            [/R <group/user> [...]] [/D <group/user>:<perms> [...]]  
            [/S] [/T] [/A] [/resetDefaultDACL] [/resetDefaultSACL]  
            [/takeOwnership] [/user:<userName>] [/passwd:<passwd> | *]  
            [/simple]
```

object Path to the AD DS object for which to display or
 manipulate the ACLs

Path is the RFC 1779 format of the name, as in

```
CN=John Doe,OU=Software,OU=Engineering,DC=Widget,DC=com
```

A specific AD DS can be denoted by prepending \\server[:port]\
to the object, as in

```
\\ADSERVER\CN=John Doe,OU=Software,OU=Engineering,DC=Widget,DC=US
```

no options displays the security on the object.

/I Inheritance flags:
 T: This object and sub objects
 S: Sub objects only
 P: Propagate inheritable permissions one level only.

/N Replaces the current access on the object, instead of
 editing it.

/P Mark the object as protected
 Y:Yes
 N:No

maintained.

/G <group/user>:<perms>

Grant specified group (or user) specified permissions.

See below for format of <group/user> and <perms>

/D <group/user>:<perms>

Deny specified group (or user) specified permissions.

See below for format of <group/user> and <perms>

/R <group/user> Remove all permissions for the specified group (or user).

See below for format of <group/user>

/S

Restore the security on the object to the default for that object class as defined in AD DS Schema. This option works when dscls is bound to NTDS. To restore default ACL of an object in AD LDS use /resetDefaultDACL and /resetDefaultSACL options.

/T

Restore the security on the tree of objects to the default for the object class.

This switch is valid only with the /S option.

/A

When displaying the security on an AD DS object, display the auditing information as well as the permissions and ownership information.

/resetDefaultDACL Restore the DACL on the object to the default for that object class as defined in AD DS Schema.

/resetDefaultSACL Restore the SACL on the object to the default for that object class as defined in AD DS Schema.

/takeOwnership Take ownership of the object.

/domain:<domainName> Connect to ldap server using this domain account of the user.

option is not used dsacIs will bind as the currently logged on user, using SSPI.

/passwd:<passwd> | * Passwd for the user account.

/simple Bind to server using ldap simple bind. Note that the clear text password will be sent over the wire.

<user/group> should be in the following forms:

- group@domain or domain\group
- user@domain or domain\user
- FQDN of the user or group
- A string SID

<perms> should be in the following form:

[Permission bits];[Object/Property];[Inherited Object Type]

Permission bits can have the following values concatenated together:

Generic Permissions

GR	Generic Read
GE	Generic Execute
GW	Generic Write
GA	Generic All

Specific Permissions

SD	Delete
DT	Delete an object and all of it's children
RC	Read security information
WD	Change security information
WO	Change owner information
LC	List the children of an object

CC	Create child object
----	---------------------

DC	Delete a child object
----	-----------------------

For these two permissions, if [Object/Property] is not specified to define a specific child object type,

CC Create child object
DC Delete a child object
For these two permissions, if [Object/Property] is not specified to define a specific child object type, they apply all types of child objects otherwise they apply to that specific child object type.

WS Write To Self (also known as Validated Write). There are 3 kinds of validated writes:
Self-Membership (bf9679c0-0de6-11d0-a285-00aa003049e2) applied to Group object. It allows updating membership of a group in terms of adding/removing to its own account.
Example: (WS; bf9679c0-0de6-11d0-a285-00aa003049e2; AU) applied to group X, allows an Authenticated User to add/remove oneself to/from group X, but not anybody else.
Validated-DNS-Host-Name (72e39547-7b18-11d1-adeb-00c04fd8d5cd) applied to computer object. It allows updating the DNS host name attribute that is compliant with the computer name & domain name.
Validated-SPN (f3a64788-5306-11d1-a9c5-0000f80367c1) applied to computer object: It allows updating the SPN attribute that is compliant to the DNS host name of the computer.

WP Write property
RP Read property
For these two permissions, if [Object/Property] is not specified to define a specific property, they apply to all properties of the object otherwise they apply to that specific property of the object.

CA Control access right
For this permission, if [Object/Property] is not specified to define the specific "extended right" for control access, it applies to all control accesses meaningful on the object, otherwise it applies to the specific extended right for that object.

this permission.

[Object/Property]

must be the display name of the object type or the property.

for example "user" is the display name for user objects and

"telephone number" is the display name for telephone number property.

[Inherited Object Type]

must be the display name of the object type that the permissions

are expected to be inherited to. The permissions MUST be Inherit Only.

NOTE: This must only be used when defining object specific permissions that override the default permissions defined in the AD DS schema for that object type. USE THIS WITH CAUTION and ONLY IF YOU UNDERSTAND object specific permissions.

Examples of a valid <perms> would be:

SDRCWDWO;;user

means:

Delete, Read security information, Change security information and Change ownership permissions on objects of type "user".

CCDC;group;

means:

Create child and Delete child permissions to create/delete objects of type group.

RPWP;telephonenumber;

means:

read property and write property permissions on telephone number property

You can specify more than one user in a command.

The command completed successfully

PS C:\Users\yoojung> NEW-ADUSER -Name "TestUser" -Path \$OU ` -AccountPassword (CONVERTTO-SECURESTRING "Pass123!" -ASPLAINTEXT)

— □ ×

- > Custom Views
- Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
- > Applications and Services Logs
- Subscriptions

[illegible]

- Security
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this...
- View
- Refresh
- Help
- Event 5379, Microsoft W...
- Event Properties
- Attach Task To This ...
- Copy