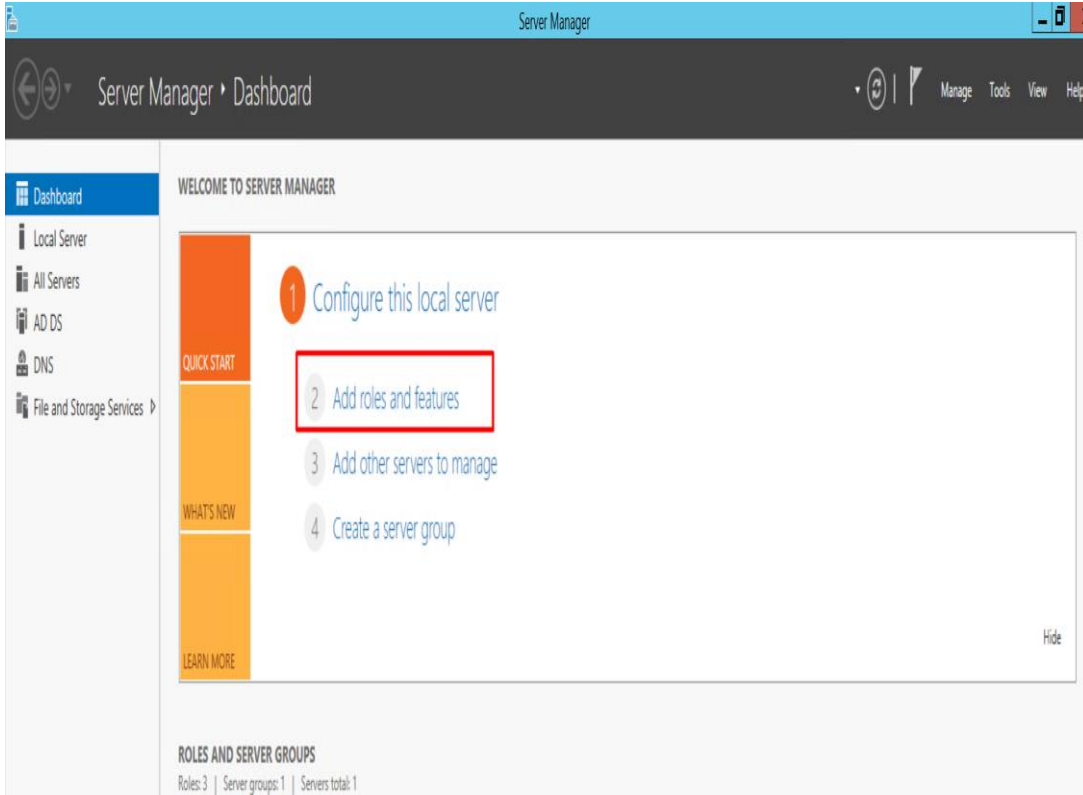
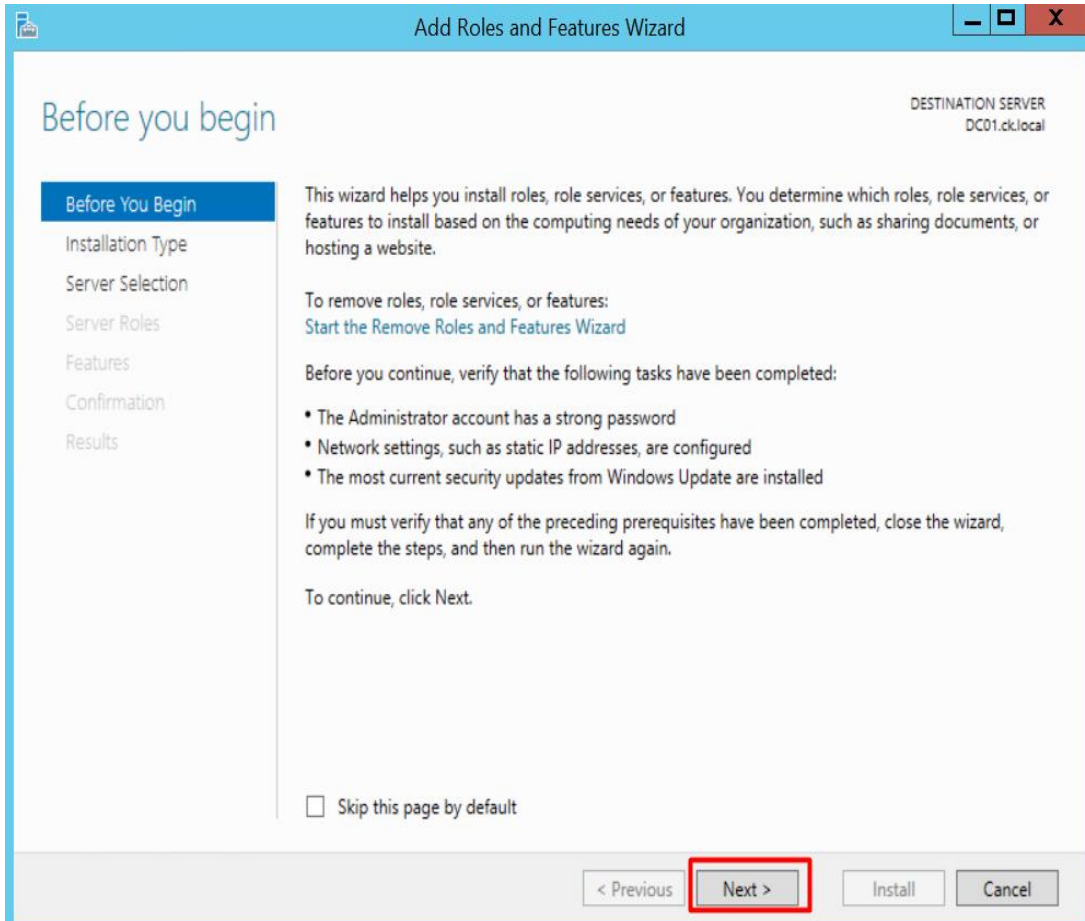


REMOTE ASSISTANCE KURULUMU VE KULLANIMI

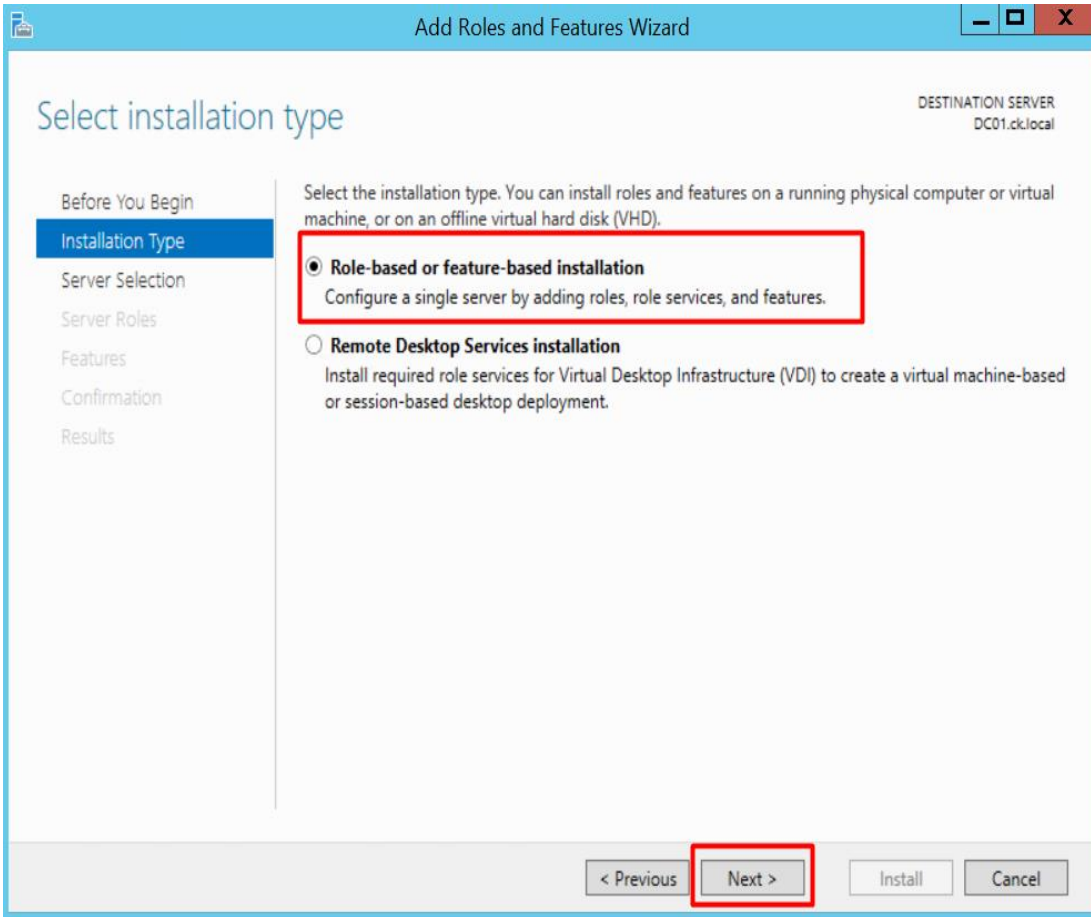
Remote Assistance microsoftun uzak masaüstü yardımı sağlamak adına geliştirmiş olduğu kullanışlı bir özelliğidir. Dağınık organizasyon yapılarınızda client cihazlarına uzaktan bağlantı sağlayıp işlemleri sağlamanız için kullanabileceğiniz faydalı ve güvenli bir tool.



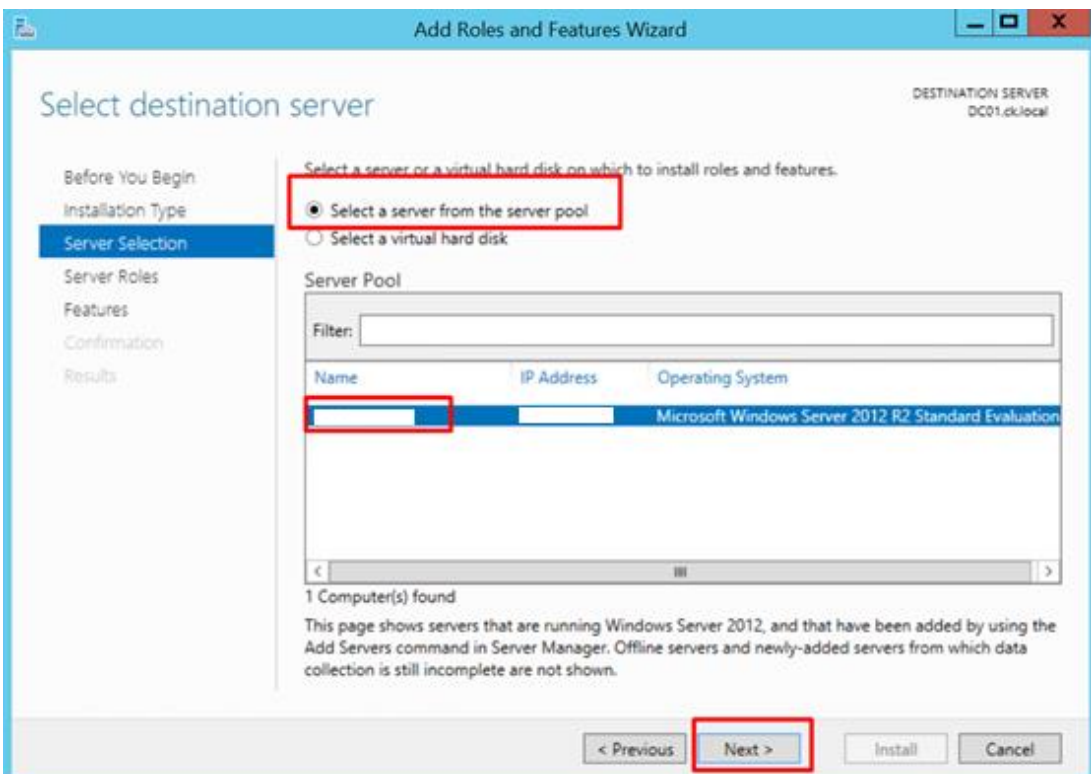
Kurulum için ilk olarak Server Manager Dashboardumuzda **Add roles and features** seçeneğini seçiyoruz



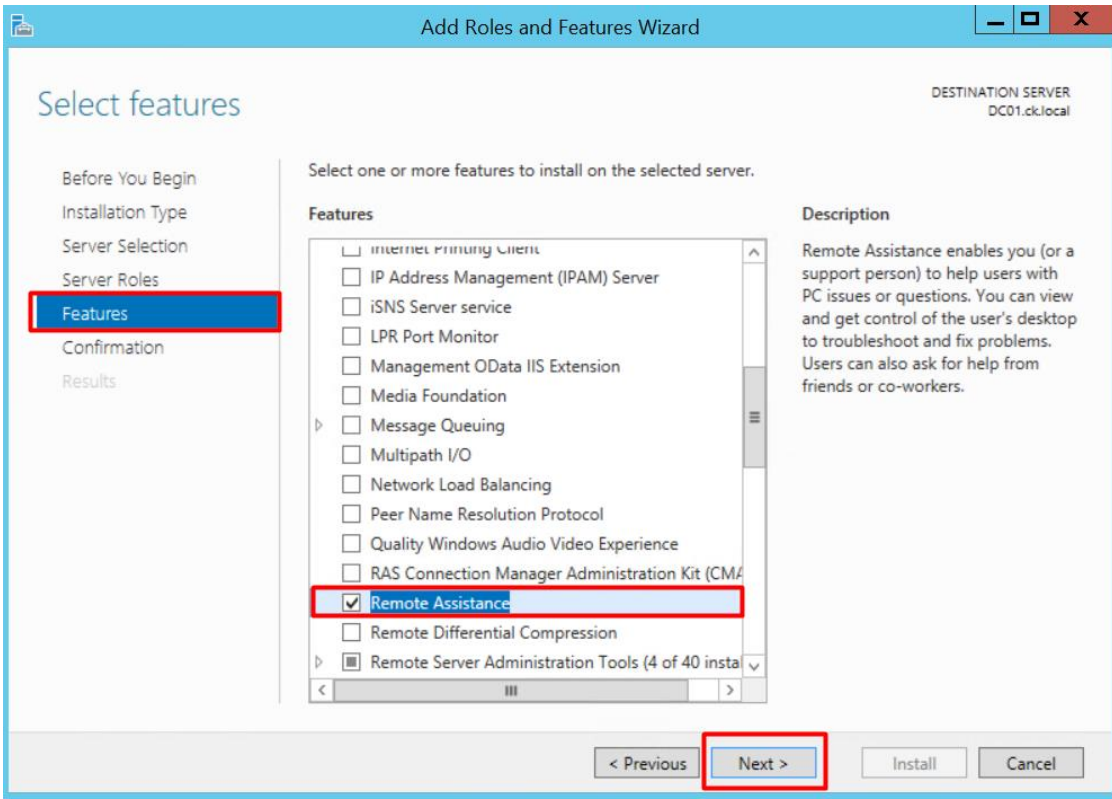
Açılan Before You Begin ekranını Next diyerek geçiyoruz



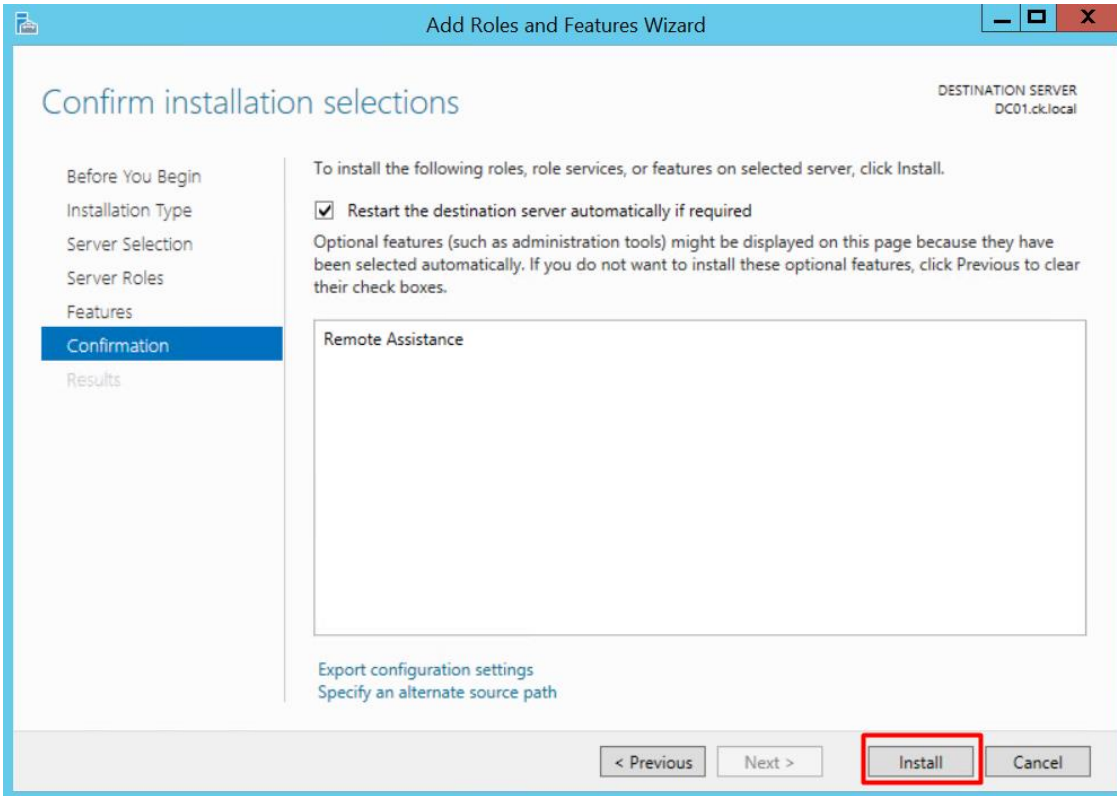
Installation Type bölümünde Rol yada özellik tabanlı kurulum yapacağımız için **Role-based or feature-based installation** seçeneğini seçiyoruz



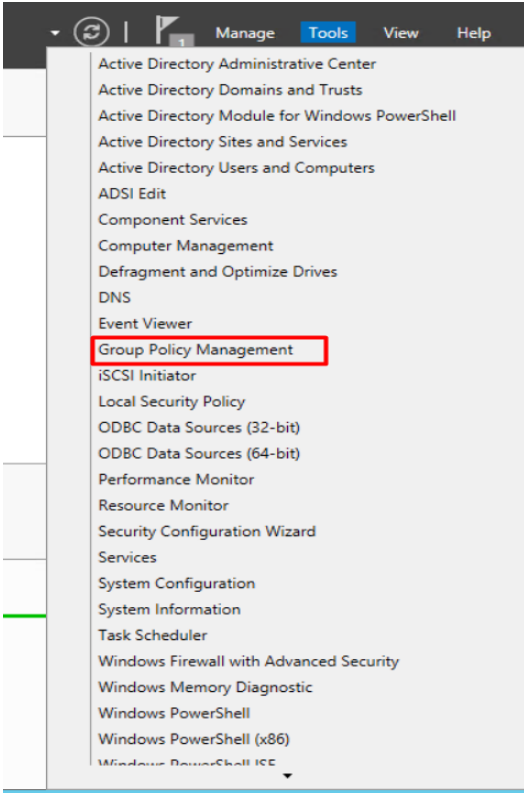
Server Selection bölümünde serverımızı seçerek ilerliyoruz



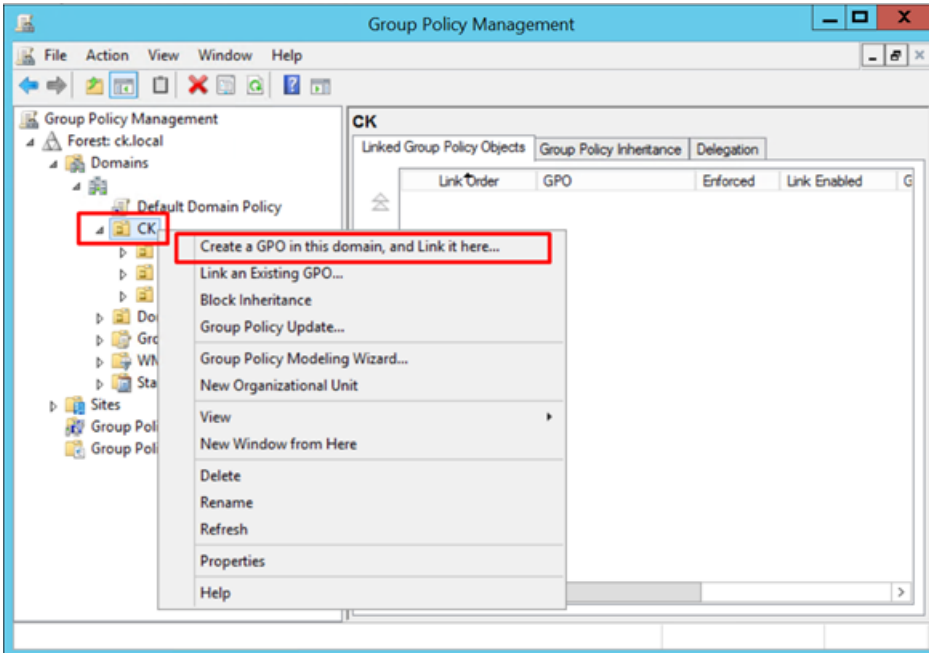
Bu tool bir özellik olarak sunulduğu için Server Roles bölümünü geçiyor ve Features Bölümüne geliyoruz. Burada Remote Assistance seçeneğini işaretliyoruz ve Next diyerek kurulumu devam ediyoruz.



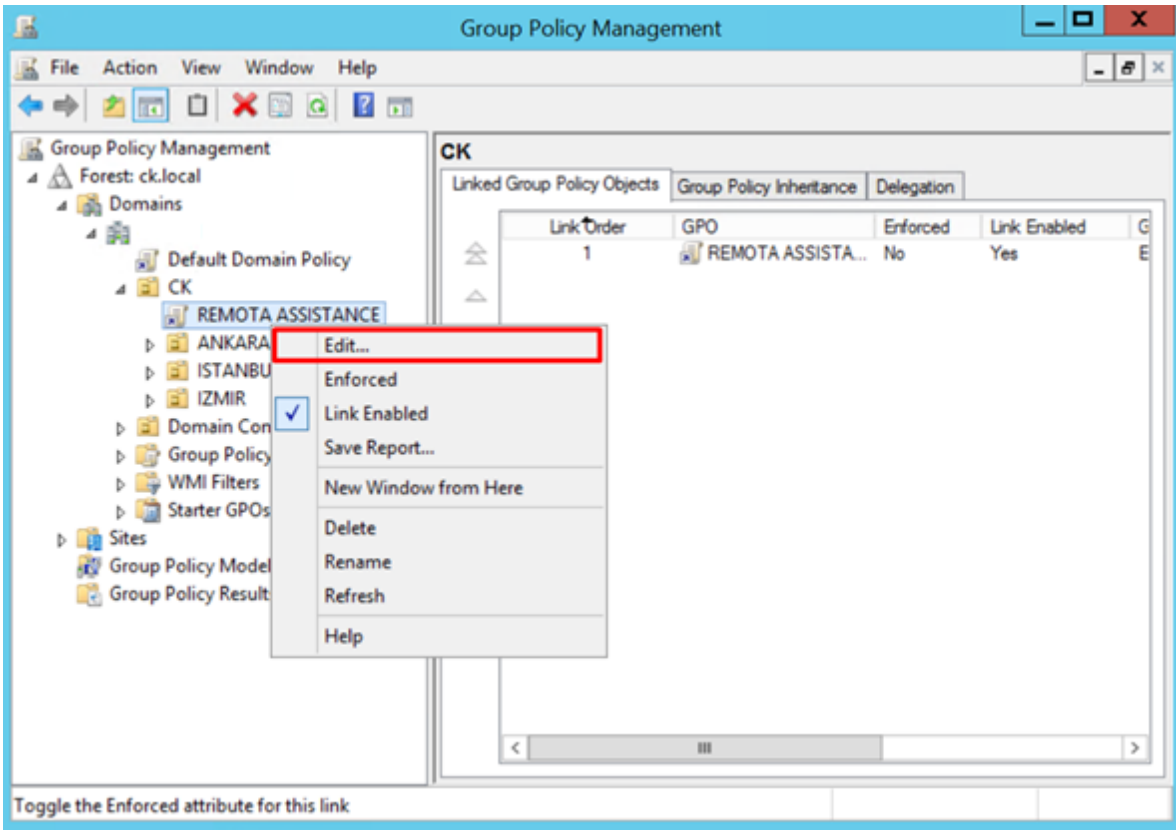
Next dedikten sonra açılan ekranda Install diyerek yükleme işleminin bitmesini bekliyoruz.



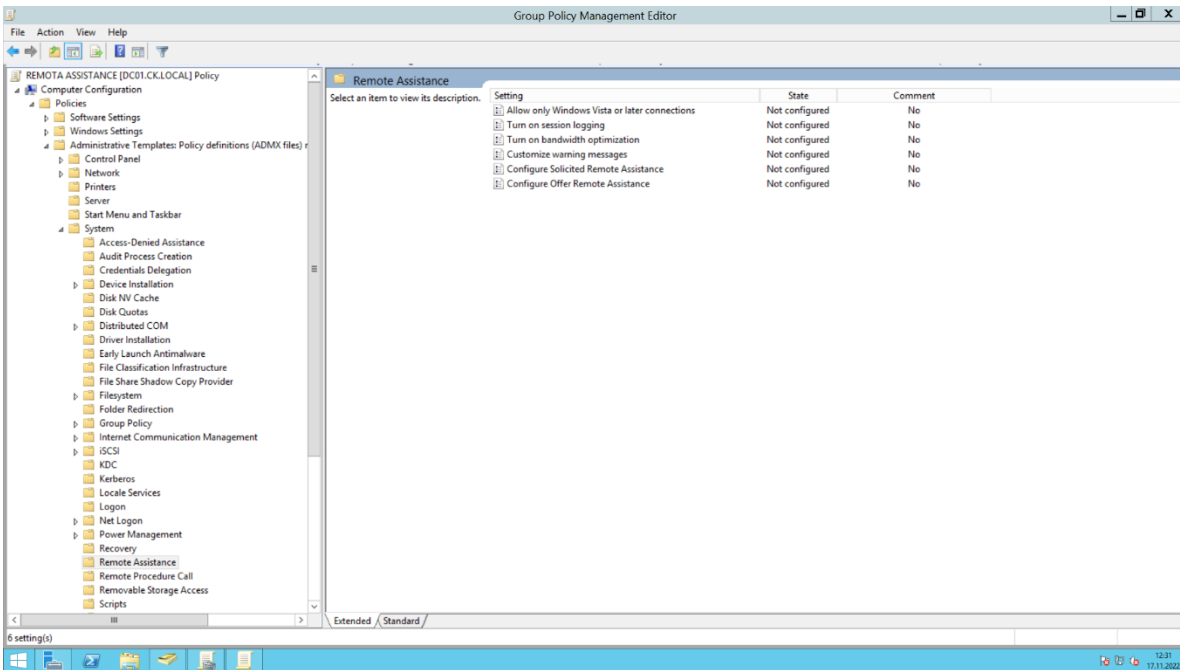
Domain ortamındaki bilgisayarlarda uzak bağlantı servisini aktif etmek için Tools bölümünü açıyor ve oradan Group Policy Managementı seçiyoruz



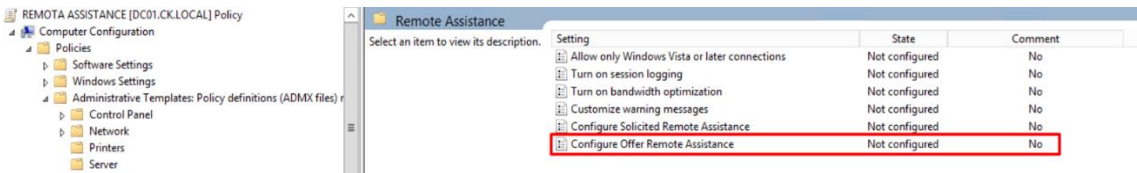
Ben bütün Computer objelerimi CK OU su altında topladığım için CK OU suna sağ tık yaparak yeni bir group policy oluşturuyor, adını belirliyor ve OU ya linkliyoruz.



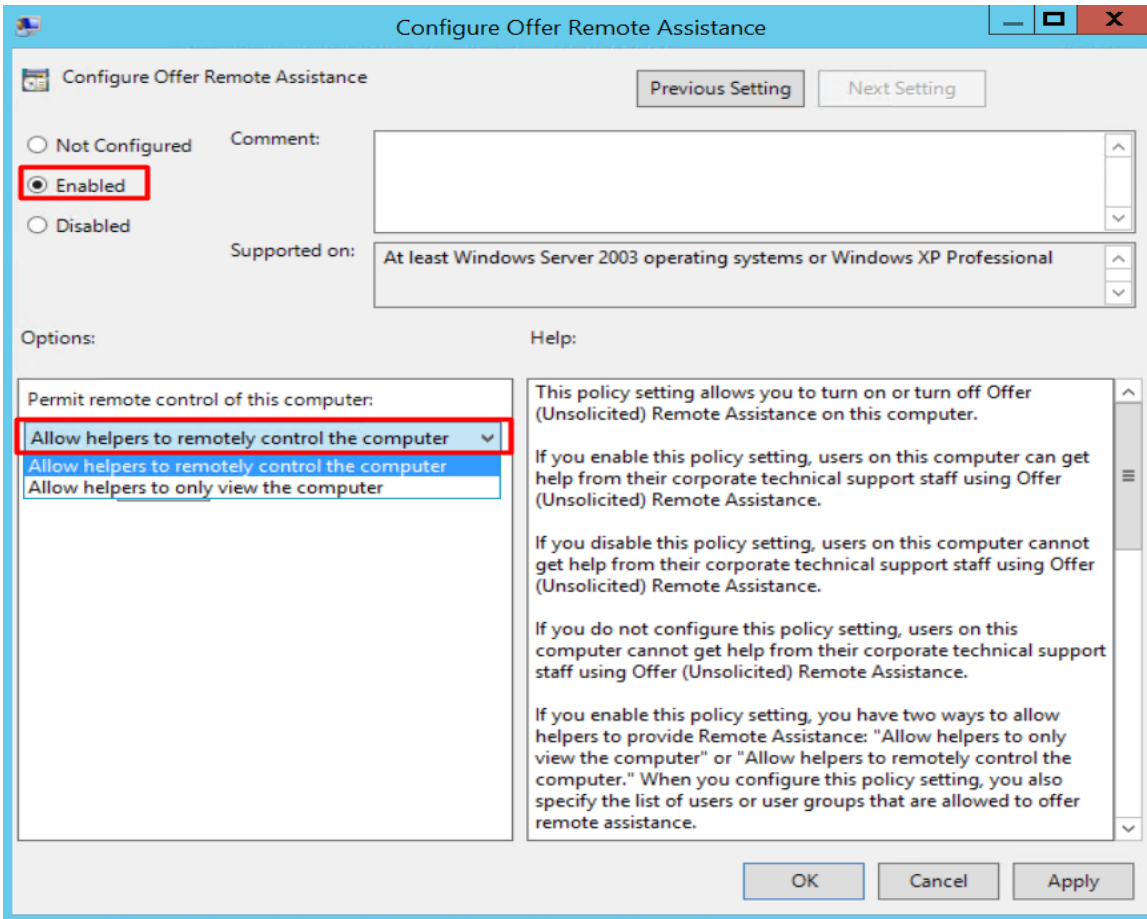
Linkleme işleminden sonra GPO'yu Editliyoruz.



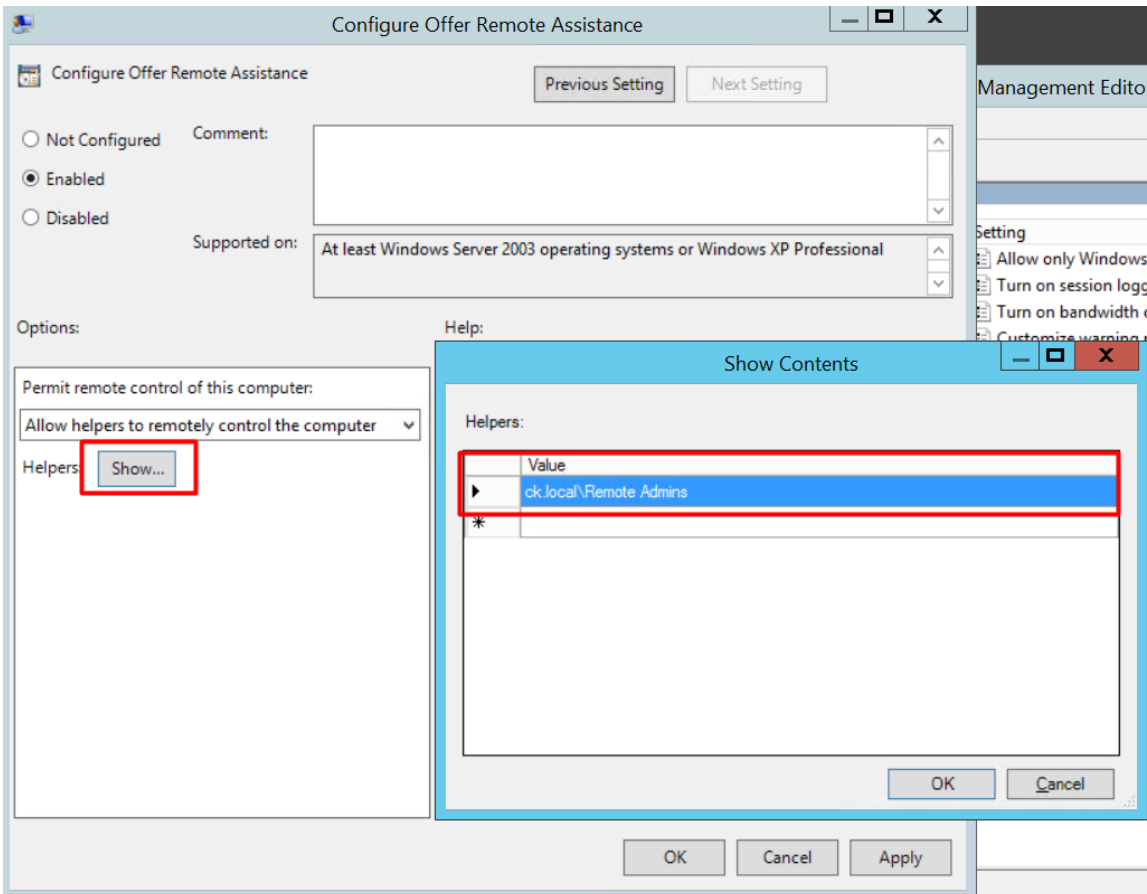
GPO'yu computer bazlı bir GPO olacağı için **Computer configuration > Policies > Administrative Templates > System** bölümünde yer alan **"Remote Assistance"** a geliyoruz.



Burada yer alan policylerden **Configure Offer Remote Assistance** i seçiyoruz



Açılan Policy ayarlarında Not Configured bölümünü Enabled ediyor ve Permit remote control of this computer Bölümünde Uzaktan destek verecek ekibimizin bilgisayarda işlem de yapabilmesini sağlayan Allow helpers to remotely control the computer seçeneğini seçiyor.



Aynı policyde Helpers Bölümünde Show seçeneğini tıklayarak uzak bağlantı yapacak grup veya kişileri ekliyoruz. Ben domain ortamımda Remote Admins grubu oluştururdum, sizler isterseniz domain admin grubunu ekleyebilirsiniz.

Setting	State	Comment
Allow only Windows Vista or later connections	Not configured	No
Turn on session logging	Not configured	No
Turn on bandwidth optimization	Not configured	No
Customize warning messages	Not configured	No
Configure Solicited Remote Assistance	Not configured	No
Configure Offer Remote Assistance	Enabled	No

Bu ayarı uyguladıktan sonra aynı bölümde bulunan Configure Solicited Remote Assistance bölümüne geliyor ve edit ediyoruz

Configure Solicited Remote Assistance

Previous Setting Next Setting

☐ Not Configured
☒ Enabled
☐ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Permit remote control of this computer:

Allow helpers to remotely control the computer

Maximum ticket time (value): 3

Maximum ticket time (units): Hours

Method for sending email invitations: Simple MAPI

Help:

This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer.

If you enable this policy setting, users on this computer can use email or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings.

If you disable this policy setting, users on this computer cannot use email or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.

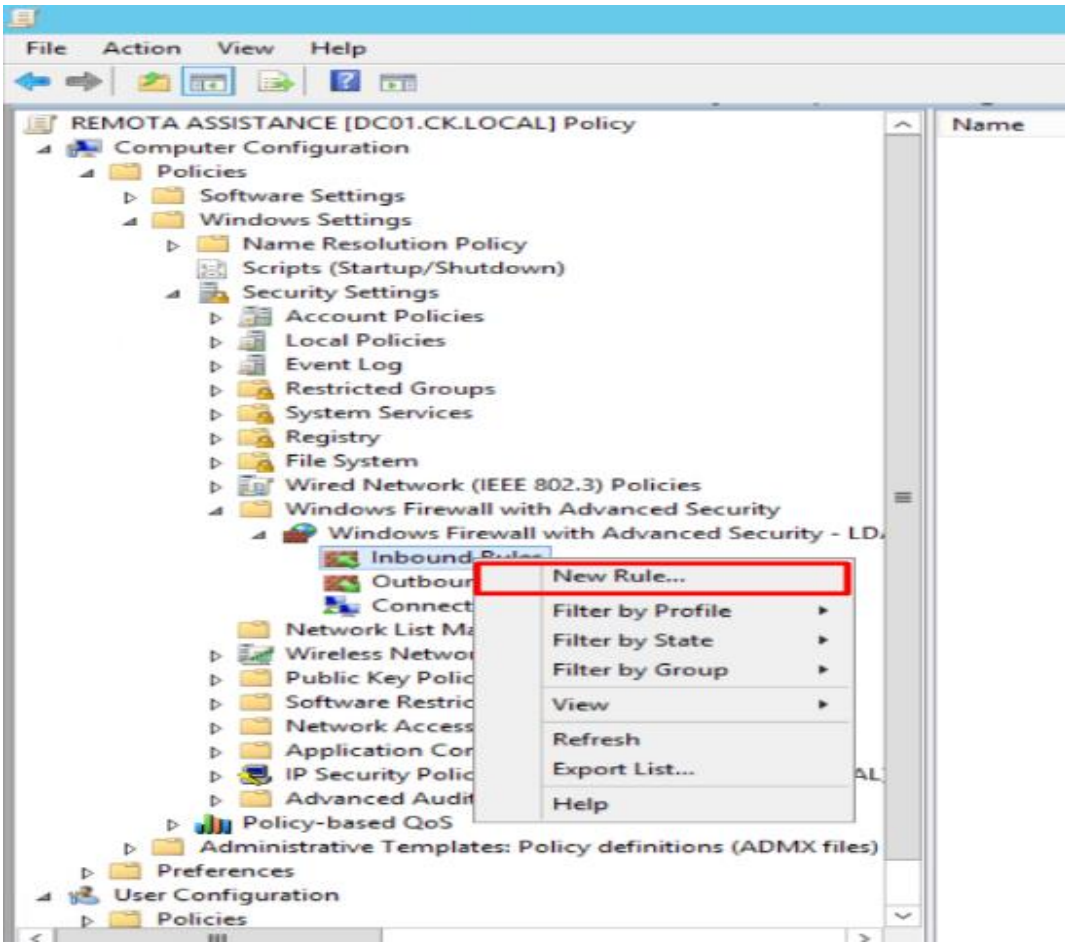
If you do not configure this policy setting, users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.

If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only

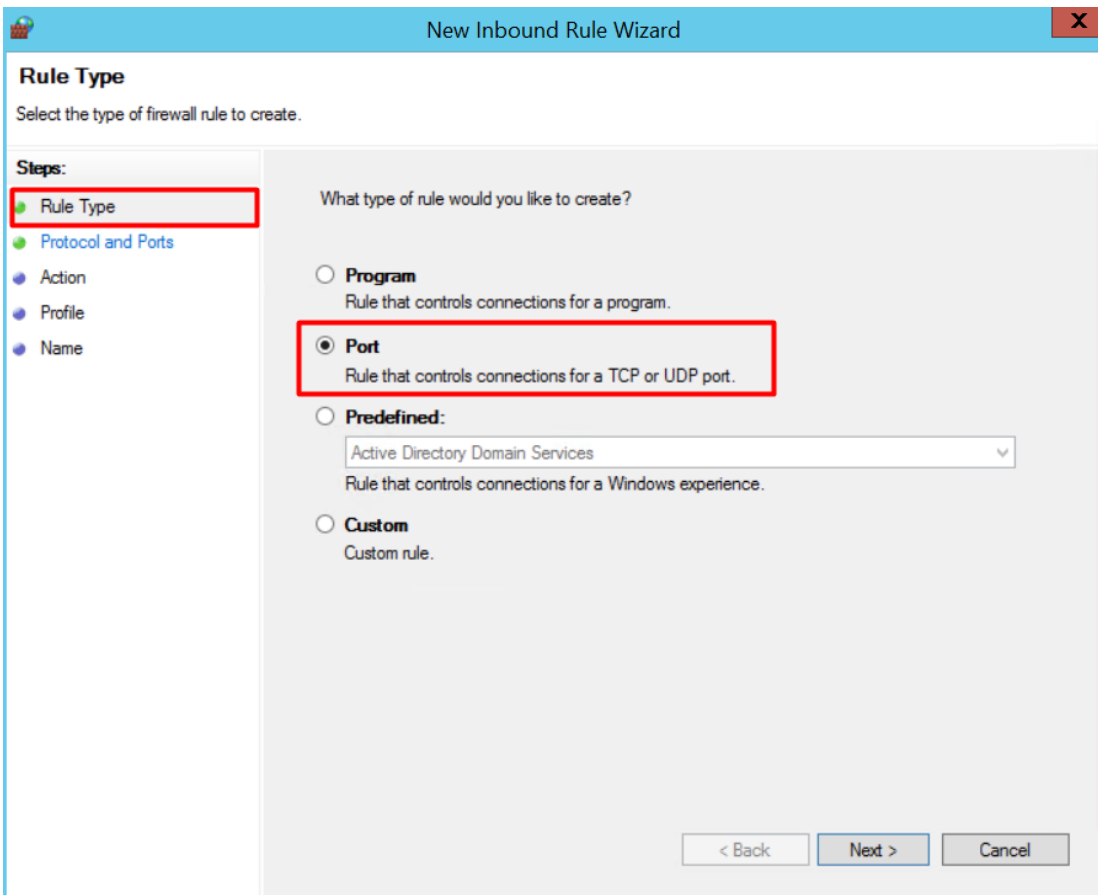
OK Cancel Apply

Düzenleme ekranında Not Configured bölümünü Enabled yapıyoruz ve bize 4 seçenek sunuyor, Allow helpers to remotely control the computer seçenği ile bilgisayarda işlem yapmamıza imkan veriyor, ticket time 3 olarak girdim ve altında da saat, gün ve dakika olarak seçilebilmektedir. Burada önemli olan Method for sending email invitationsbölümüdür, bu bölümde Simple MAPI chat ekranında anlık mesajlaşmaya olanak tanımaktadır.

Remote Assistance sekmesini yapılandırdıktan sonra kullanıcıların bilgisayarlarına bağlanabilmek adına aynı policyde firewall kuralları yazmamız gerekmektedir.



Computer Configuration
– Policies – Windows
Settings – Security
Settings – Windows
Firewall – Inbound Rules
bölümüne gelerek yeni
kural ekliyoruz



Kuralımız port bazlı
olacağı için Rule Type
olarak Portu
seçiyoruz.

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

☒ TCP

☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports

☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back Next > Cancel

Uzak Bağlantı **TCP** bir bağlantı tipi olduğu için ve 135 portunu kullanacağı için gerekli ayarları yapıyor ve Next diyoruz.

New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☐ **Block the connection**

< Back Next > Cancel

Allow the connection ile porttan gelen isteklere izin veriyoruz.

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**
Applies when a computer is connected to a public network location.

< Back Next > Cancel

Profile bölümünde firewall kuralının hangi ortamlarda geçerli olmasını istediğinizi soruyor, burada ben hepsini seçtim çünkü policyde ayarladığım üzere bilgisayara benim remote admins grubumun dışında herhangi bir kişi uzak bağlantı sağlayamayacaktır, isteyen arkadaşlar public i kaldırabilirler.

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

What type of rule would you like to create?

☒ **Program**
Rule that controls connections for a program.

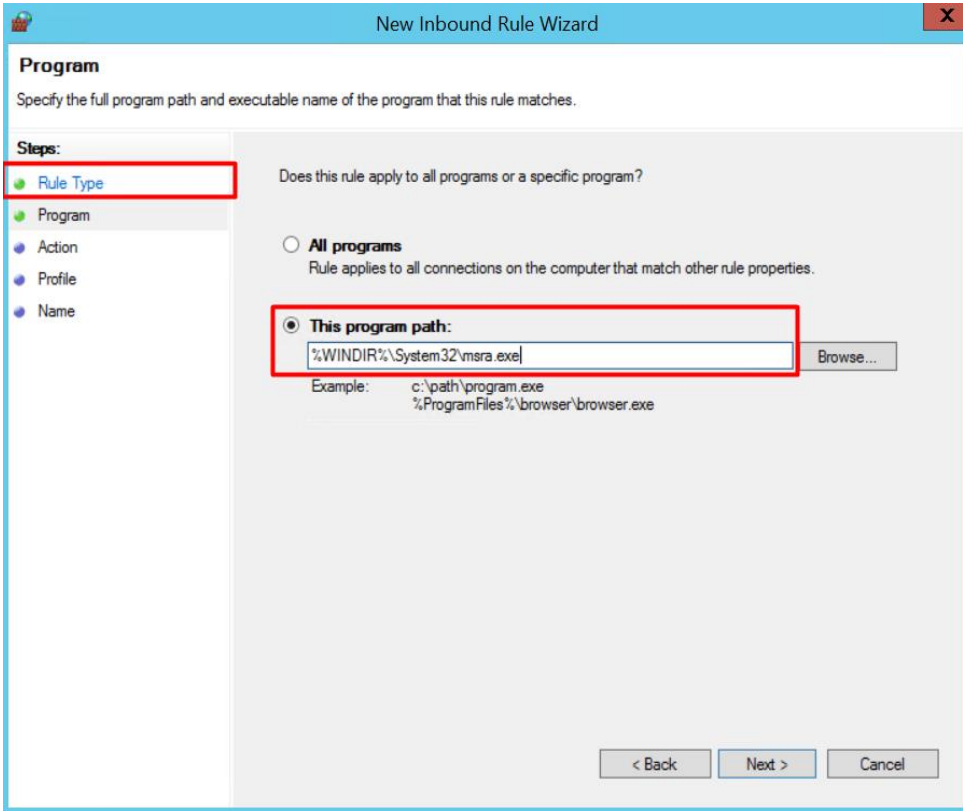
☐ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
Active Directory Domain Services
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back Next > Cancel

Yeniden firewall **inbound** kuralı oluşturuyoruz, 2.Firewall inbound kuralımız ise bağlantı sağlayacak exelerin çalışması ile ilgilidir.



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Program' step. The 'Steps' list on the left has 'Rule Type' highlighted with a red box. The main area asks 'Does this rule apply to all programs or a specific program?'. The 'All programs' option is unselected. The 'This program path:' option is selected and highlighted with a red box. Below it, a text box contains '%WINDIR%\System32\msra.exe' and a 'Browse...' button is to its right. Examples of paths are listed below: 'c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

New Inbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

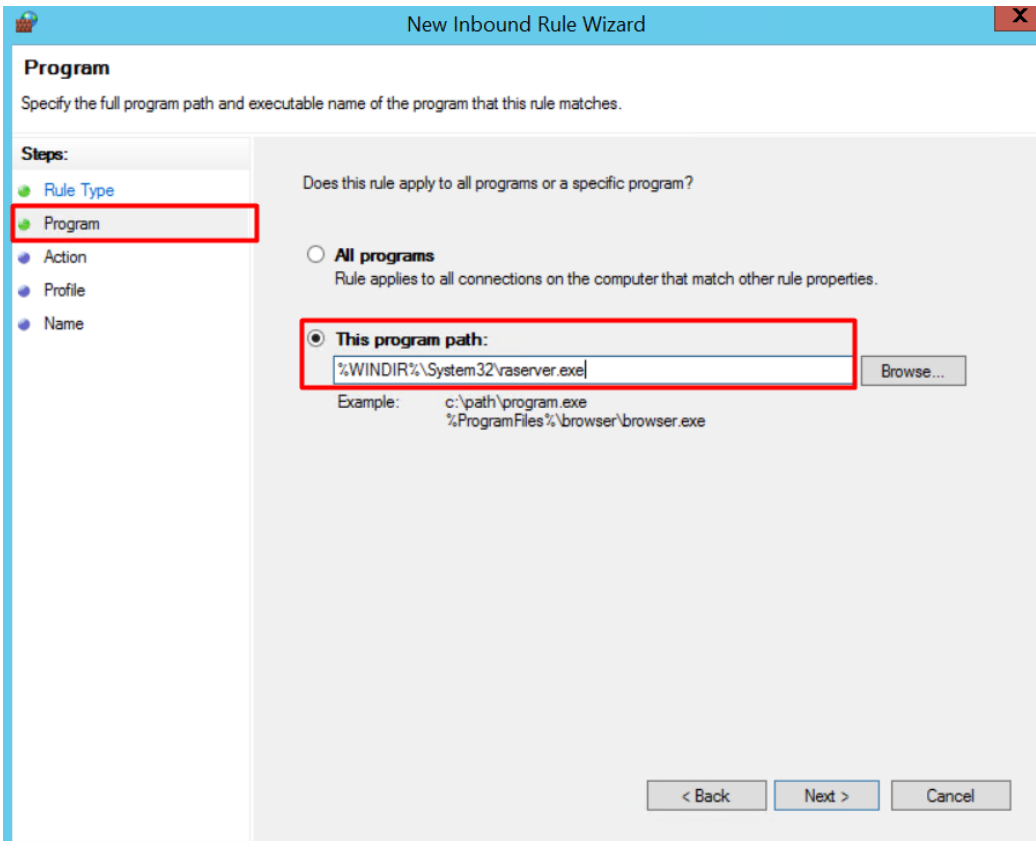
☐ All programs
Rule applies to all connections on the computer that match other rule properties.

☒ This program path:
%WINDIR%\System32\msra.exe Browse...

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

< Back Next > Cancel

İzin vereceğimiz msra.exe dir.
This program path bölümüne
%WINDIR%\System32\msra.exe
yazarak programa izin vermesini
sağlıyoruz.



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Program' step. The 'Steps' list on the left has 'Program' highlighted with a red box. The main area asks 'Does this rule apply to all programs or a specific program?'. The 'All programs' option is unselected. The 'This program path:' option is selected and highlighted with a red box. Below it, a text box contains '%WINDIR%\System32\raserver.exe' and a 'Browse...' button is to its right. Examples of paths are listed below: 'c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

New Inbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

☐ All programs
Rule applies to all connections on the computer that match other rule properties.

☒ This program path:
%WINDIR%\System32\raserver.exe Browse...

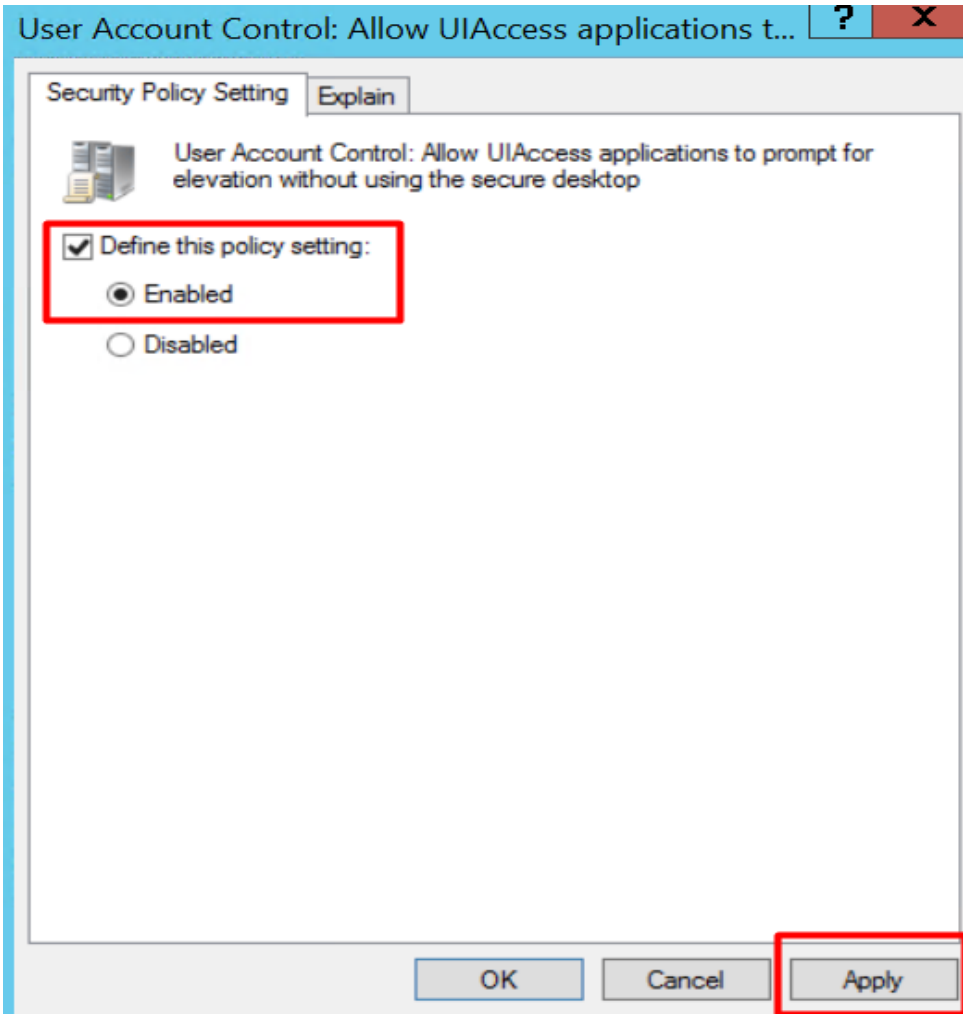
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

< Back Next > Cancel

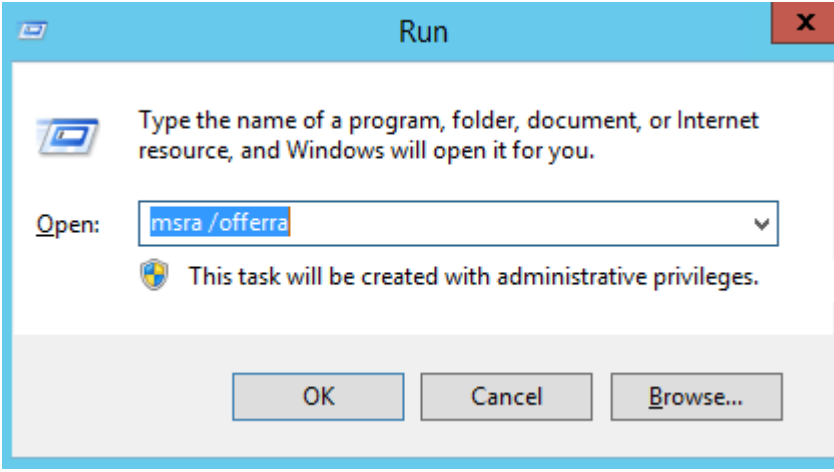
3. inbound kuralımız da
yine bir program kuralı, bu
sefer This program path
bölümümüzü
%WINDIR%\System32
raserver.exe şeklinde
doldurarak izin veriyoruz.

Policy	Policy Setting
Network security: Force logoff when logon hours expire	Not Defined
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Not Defined
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Not Defined
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Not Defined
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Not Defined
Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
Shutdown: Allow system to be shut down without having to log on	Not Defined
Shutdown: Clear virtual memory pagefile	Not Defined
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Not Defined
System objects: Require case insensitivity for non-Windows subsystems	Not Defined
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Not Defined
System settings: Optional subsystems	Not Defined
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Not Defined
User Account Control: Admin Approval Mode for the Built-in Administrator account	Not Defined
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Not Defined

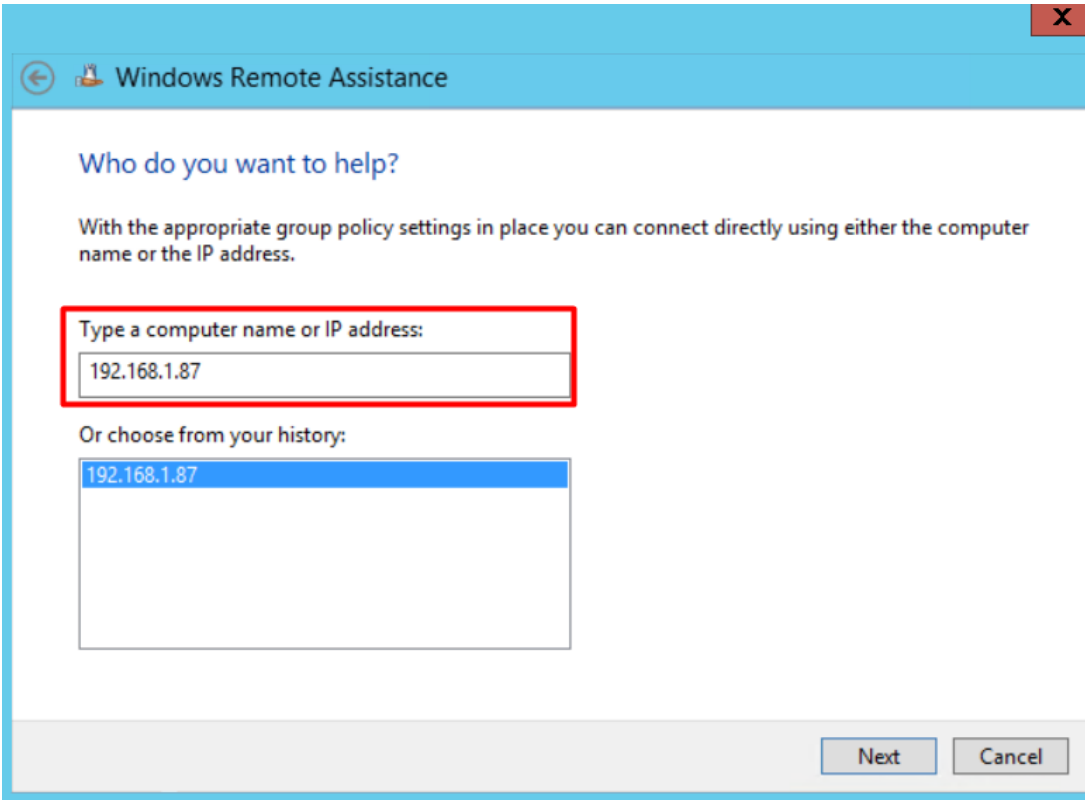
3 firewall inbound kuralımızı da oluşturduktan sonra GPO tarafında yapmamız gereken bir ayar daha kaldı. Onun için yapılandırdığımız GPOmuzda **Computer Configuration – Policies – Windows Settings – Security Settings – Local policy – Security Options** sekmesine geliyoruz.



Sağ tarafta açılan bölümde **User Account Control:Allow UIAccess applications to prompt for elevation without using the secure desktop** ayarına girerek Define this policy setting tikini işaretliyor ve Enable ediyoruz.



Uzak bağlantı desteği vereceğimiz bilgisayarda çalıştır bölümüne veya dos ekranına **msra /offerra** yazarak uzak bağlantı yöneticimizi çalıştırırız.



Açılan ekranda Type a computer name or IP adress yazan bölüme uzak bağlantı sağlayacağınız bilgisayarın IP adresi veya bilgisayar adını yazarak bağlantı sağlayabilirsiniz.

Windows Uzaktan Yardım



Bağlantı talebi gönderdiğinizde kullanıcı ekranında bu şekilde bir uyarı verecektir. Kullanıcıya uzak bağlantının sağlanabilmesi için Evet temesi gerekmektedir.

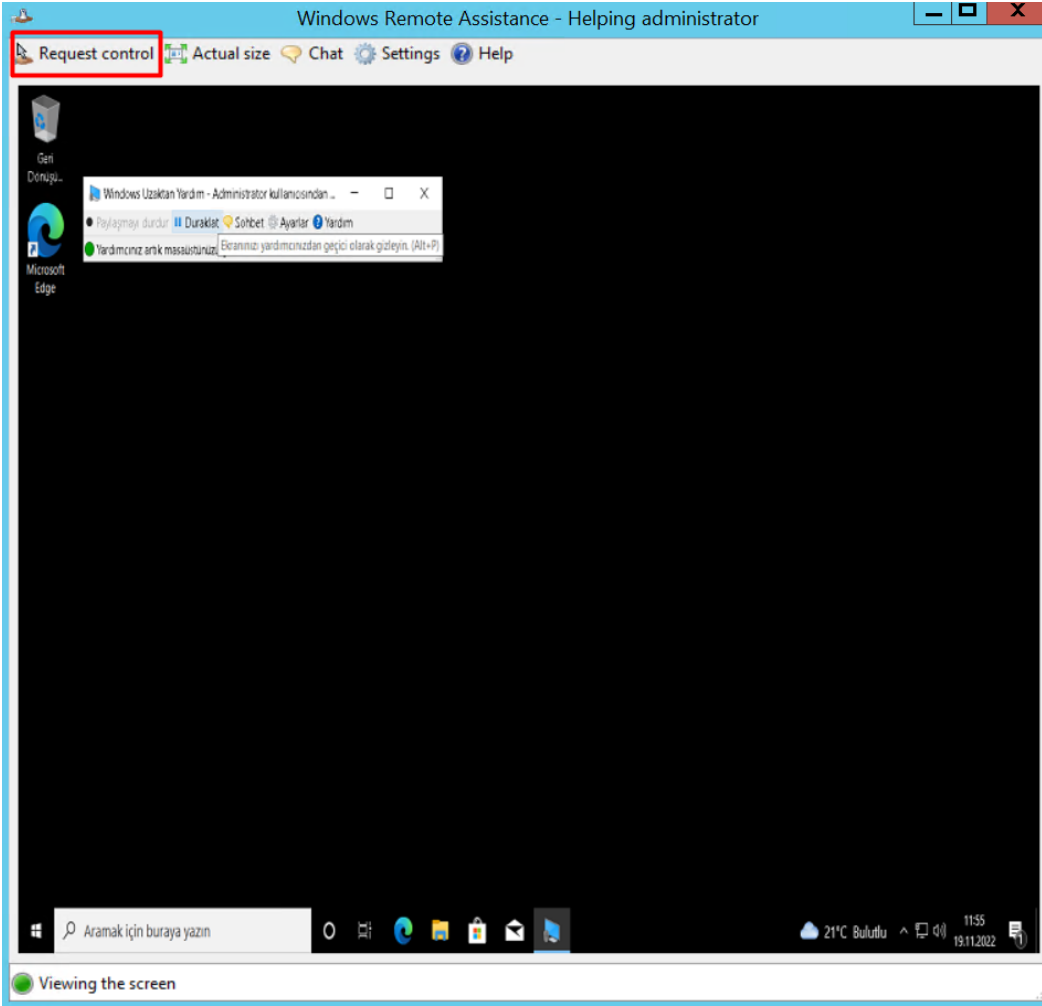
Administrator kullanıcısının bilgisayarınıza bağlanmasına izin vermek istiyor musunuz?

Bağlandıktan sonra, Administrator masaüstünüzdeki her şeyi görebilecek.

Evet

Hayır

[Gizlilik ve güvenlik sorunları nelerdir?](#)



Bağlantıyı sağlayan Remote Admin ekranında toolun görünümü bu şekildedir, Request control diyerek uzak bağlantı sağlanan kullanıcının aşağıda belirtilen uyarıya Evet demesiyle uzak bağlantı yönetim işlemi de başlayacaktır.

Windows Uzaktan Yardım



Administrator kullanıcısının, masaüstünüzün denetimini paylaşmasına izin vermek istiyor musunuz?

Denetimi paylaşmayı durdurmak için, Uzaktan Yardım iletişim kutusunda Paylaşımı durdur'u tıklayın.

Evet

Hayır

[Gizlilik ve güvenlik sorunları nelerdir?](#)