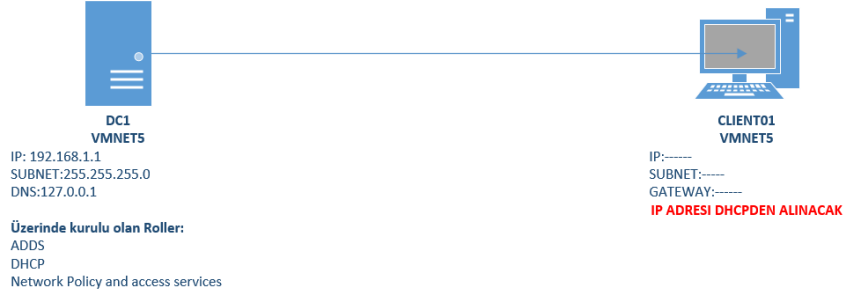


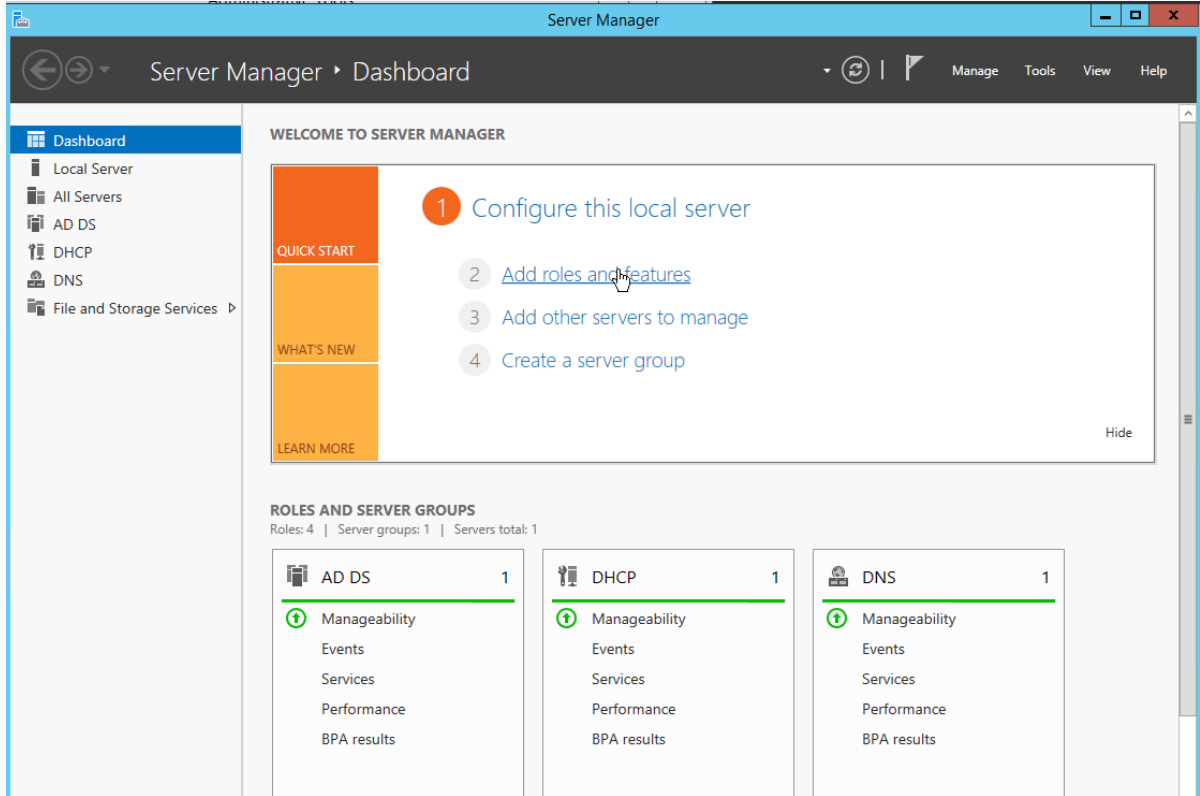
NAP SERVER KURULUMU



*DC1 Üzerinde DHCP önceden kurulmuştur ve scope oluşturulmuştur

*CLIENT01 örnek başlangıcında DOMAINe dâhil değildir



ÖNCELİKLE DC1 ÜZERİNDE NAP (NETWORK ACCESS PROTECTION) KURULUMU YAPILACAKTIR. İLGİLİ ROL **NETWORK POLICY AND ACCESS SERVICES**



Add Roles and Features Wizard

Before you begin

DESTINATION SERVER
dc1.altan.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.



☐ Skip this page by default

< Previous

Next >

Install

Cancel

Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
dc1.altan.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel

Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
dc1.altan.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool

☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
dc1.altan.local	192.168.1.1	Microsoft Windows Server 2012 R2 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

Cancel

Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
dc1.altan.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

Description

☐ Active Directory Federation Services

☐ Active Directory Lightweight Directory Services

☐ Active Directory Rights Management Services

☐ Application Server

☒ DHCP Server (Installed)

☒ DNS Server (Installed)

☐ Fax Server

☒ File and Storage Services (2 of 12 installed)

☐ Hyper-V

☐ Network Policy and Access Services

☐ Print and Document Services

☐ Remote Access

☐ Remote Desktop Services

☐ Volume Activation Services

☐ Web Server (IIS)

☐ Windows Deployment Services

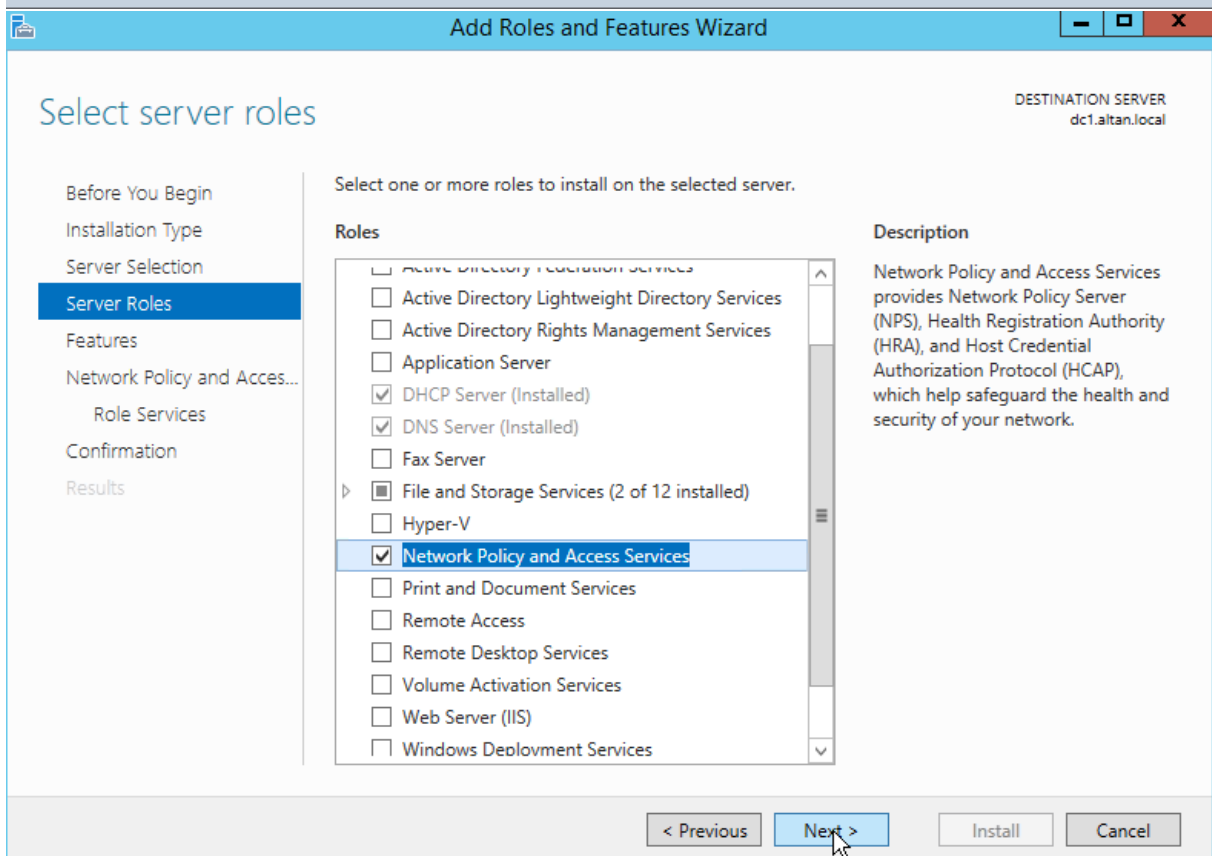
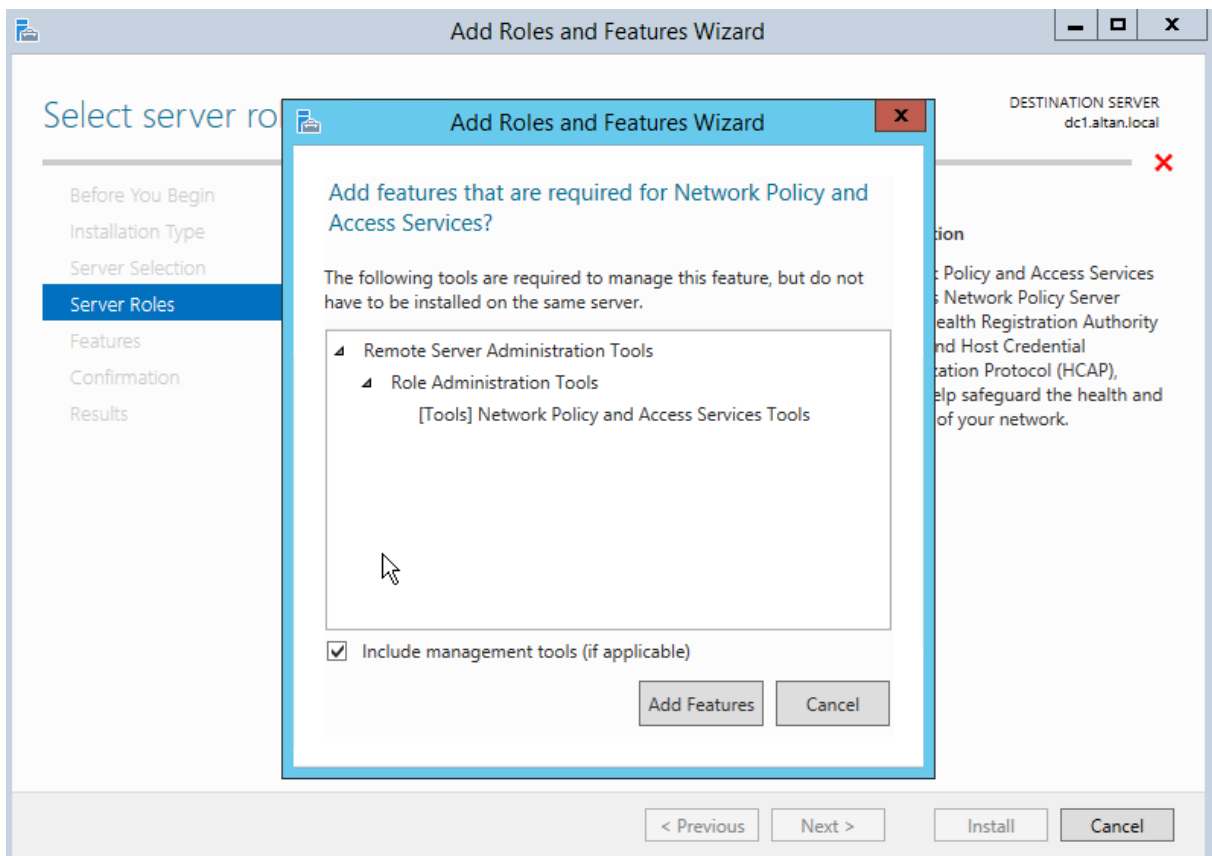
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

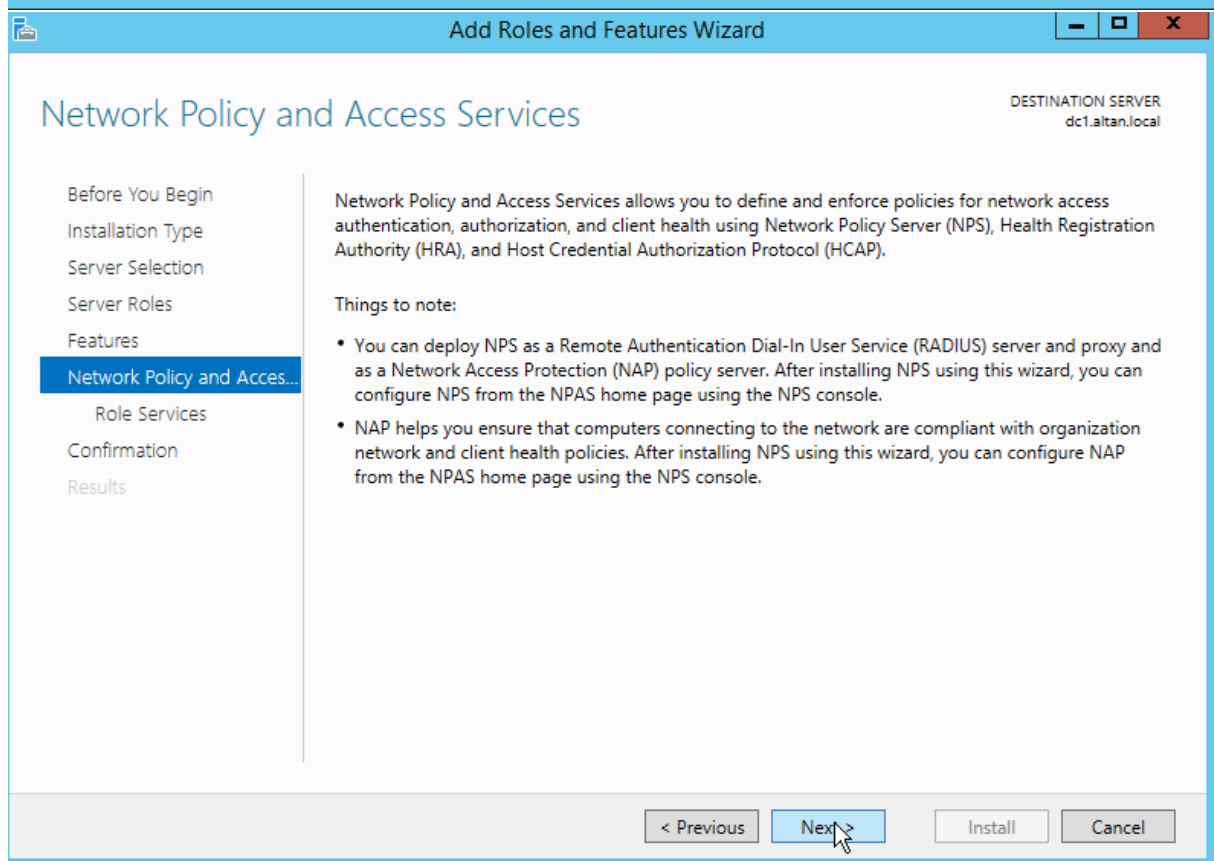
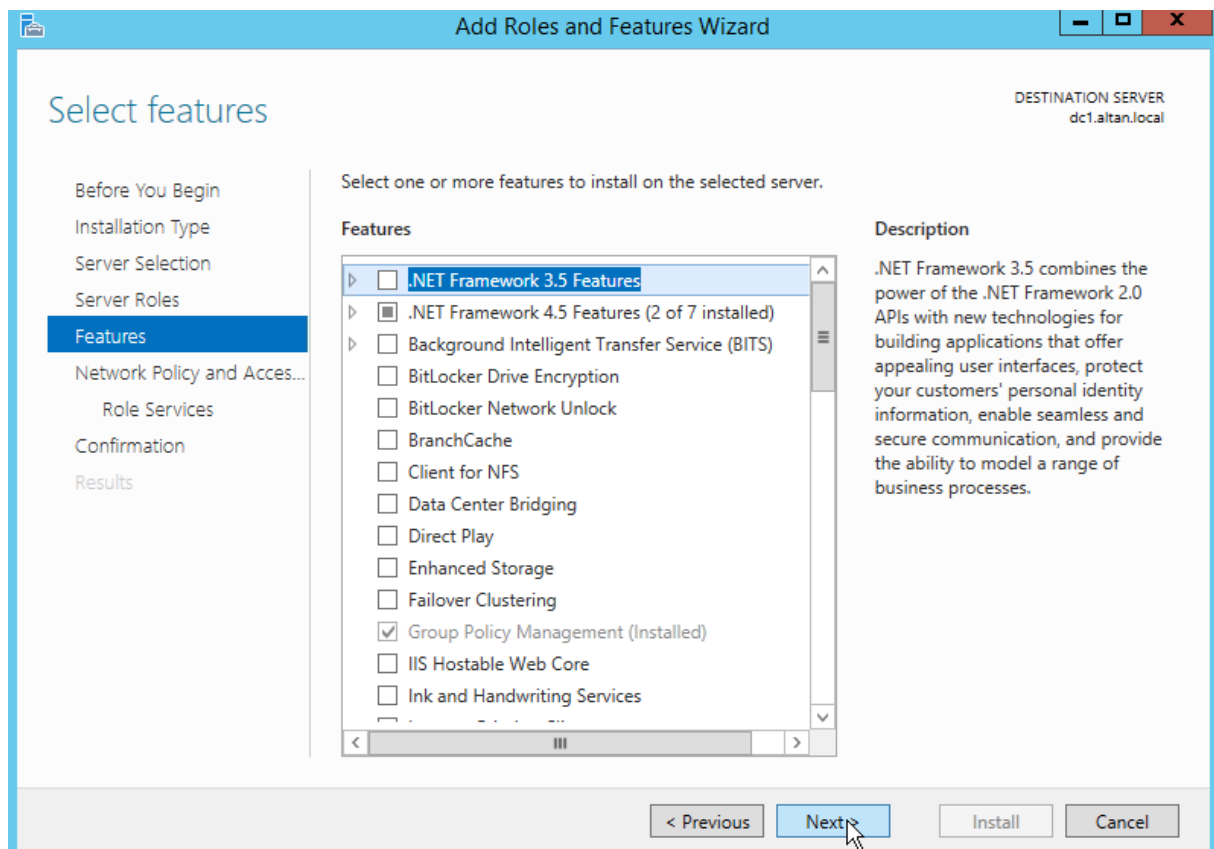
< Previous

Next >

Install

Cancel





Add Roles and Features Wizard

Select role services

DESTINATION SERVER
dc1.altan.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Network Policy and Acces...

Role Services

Confirmation

Results

Select the role services to install for Network Policy and Access Services

Role services

☒ Network Policy Server

☐ Health Registration Authority

☐ Host Credential Authorization Protocol

Description

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.

< Previous

Next >

Install

Cancel

Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
dc1.altan.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Network Policy and Acces...

Role Services

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Network Policy and Access Services
Network Policy Server

Remote Server Administration Tools
Role Administration Tools
Network Policy and Access Services Tools

Export configuration settings

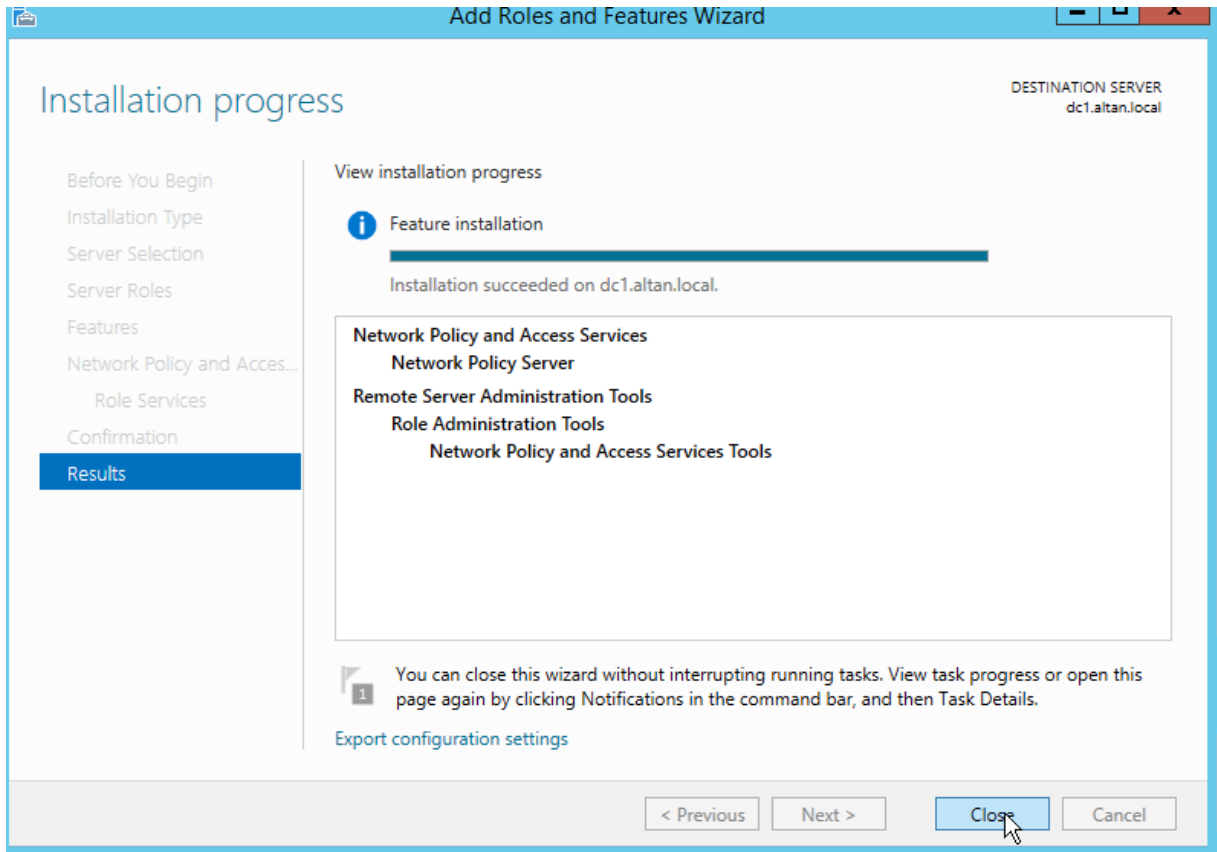
Specify an alternate source path

< Previous

Next >

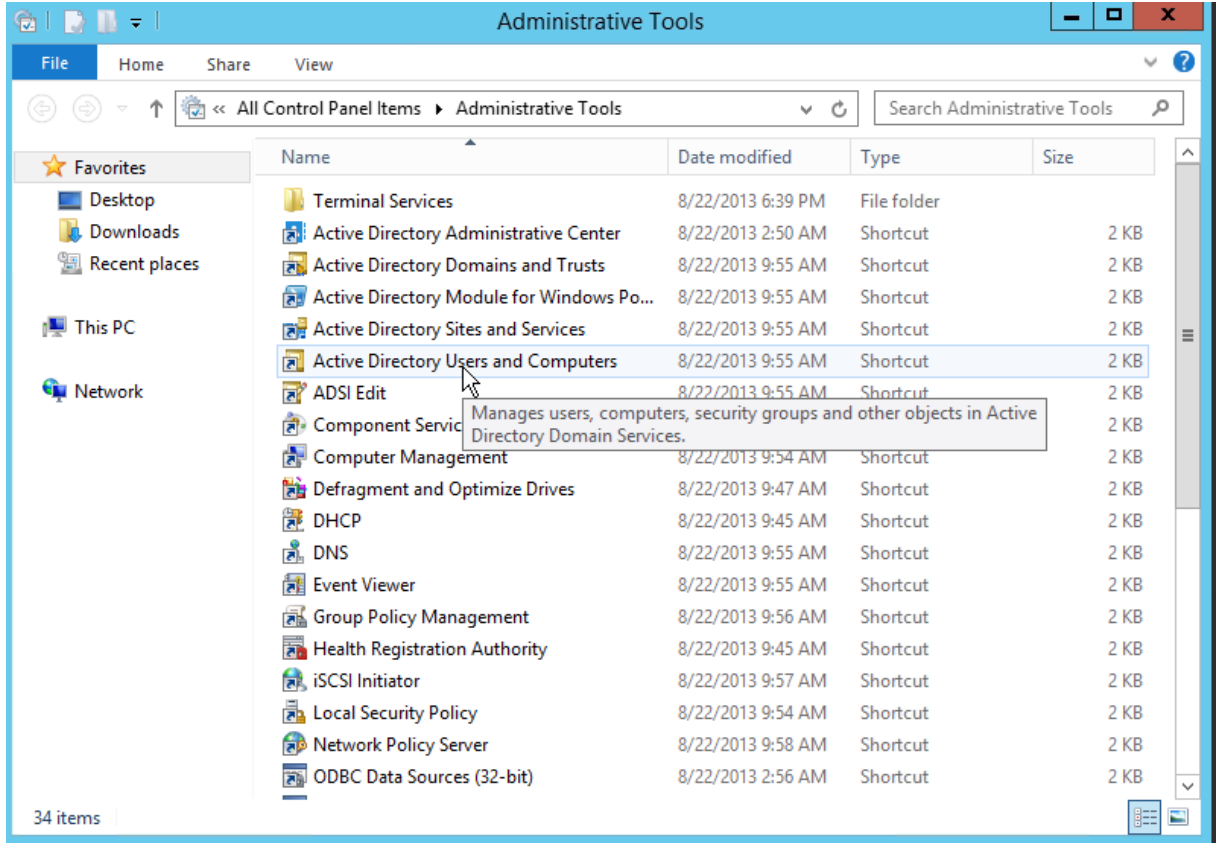
Install

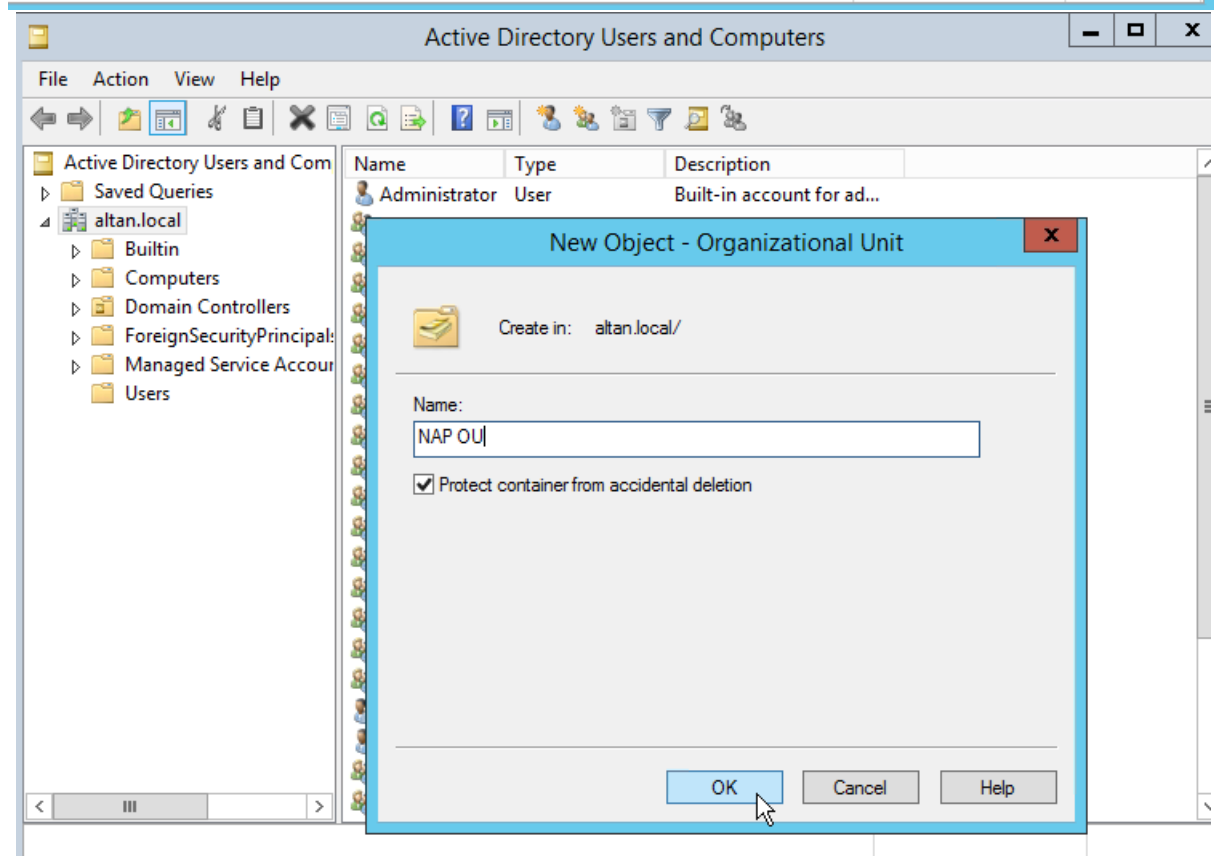
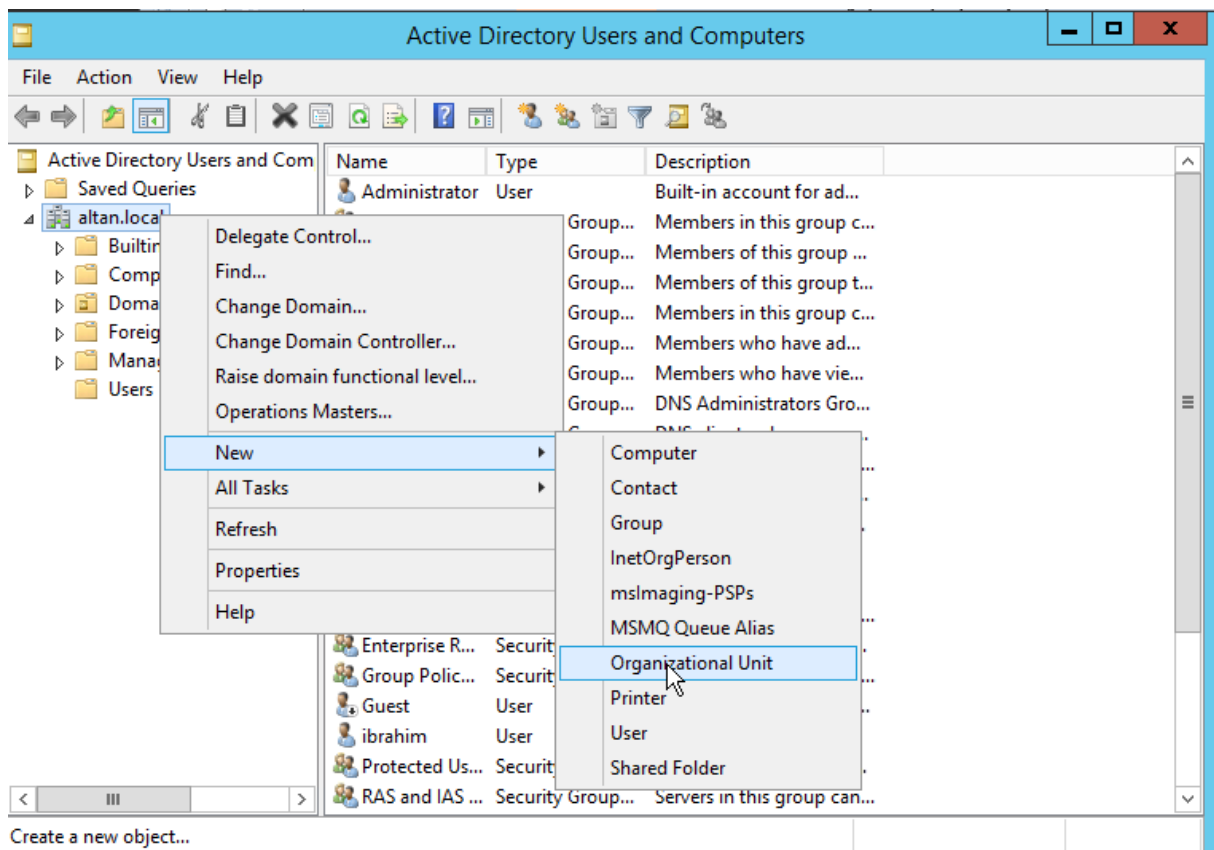
Cancel

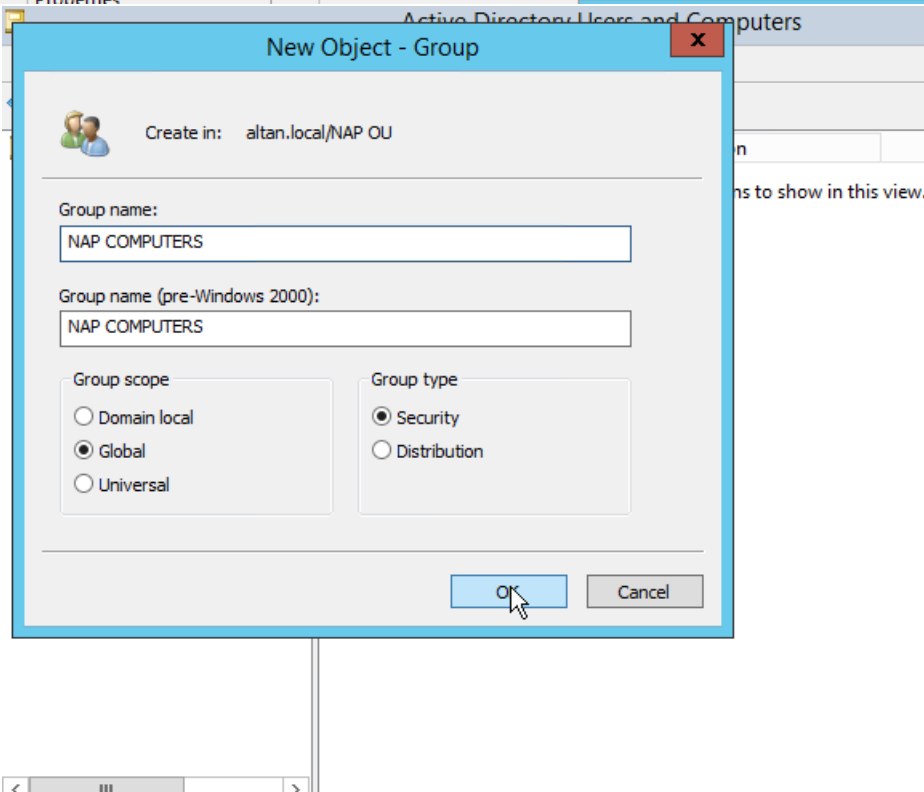
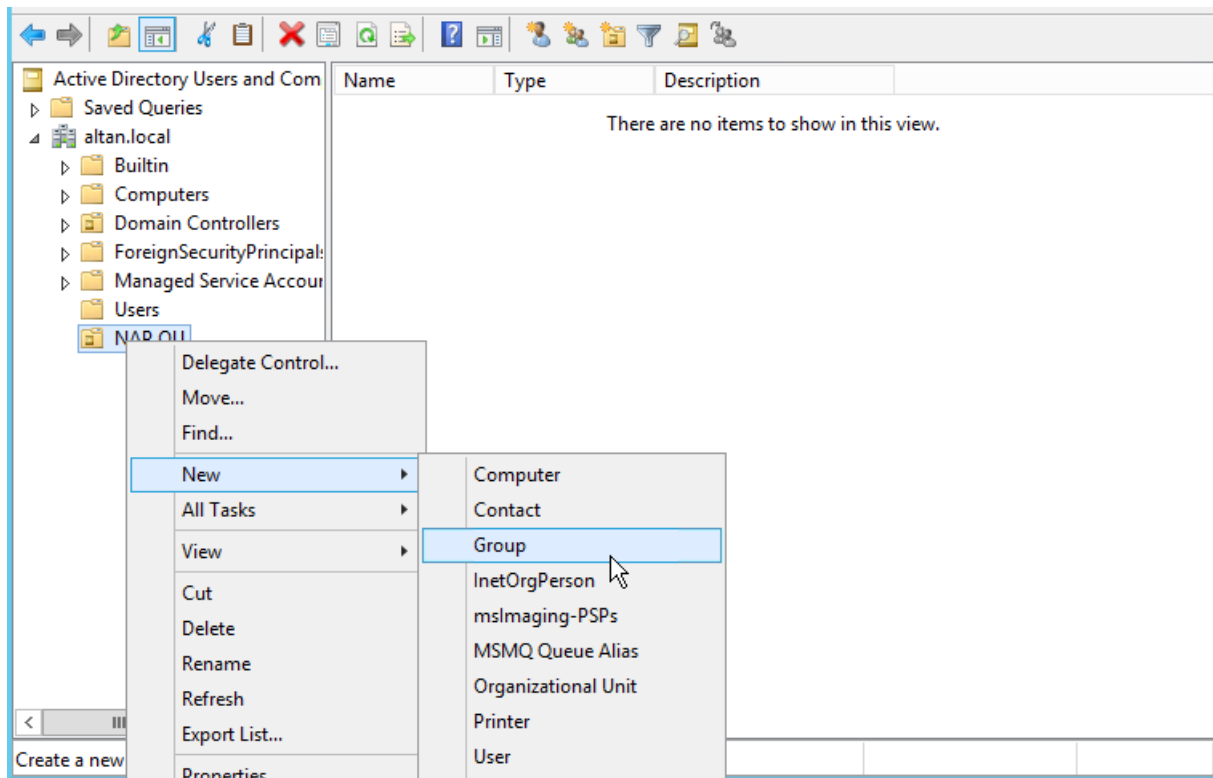


KURULUM BİTTİKTEN SONRA **ACTIVE DIRECTORY USER AND COMPUTERS**'TAN NAP COMPUTERS İÇİN GROUP VE ORGANIZATIONAL UNIT OLUŞTURUYORUZ.

BU İŞLEM CLIENT PC DOMAINE DAHİL EDİLDİKTEN SONRA NAP İLE YÖNETEBİLMEMİZ İÇİN GEREKLİ OLACAK.







SIRADAKİ İŞLEMİMİZ NAP KONFIGURASYONUNU YAPMAK

The image shows a Windows Administrative Tools window with a list of system tools. The 'Network Policy Server' tool is selected, and a tooltip indicates it 'Configures and manages Network Policy Server settings'. Below this, the 'Network Policy Server' configuration window is open, showing the 'Standard Configuration' section. The 'Network Access Protection (NAP)' scenario is selected, and the 'Configure NAP' link is highlighted.

Name	Date modified	Type	Size
Terminal Services	8/22/2013 6:39 PM	File folder	
Active Directory Administrative Center	8/22/2013 2:50 AM	Shortcut	2 KB
Active Directory Domains and Trusts	8/22/2013 9:55 AM	Shortcut	2 KB
Active Directory Module for Windows Po...	8/22/2013 9:55 AM	Shortcut	2 KB
Active Directory Sites and Services	8/22/2013 9:55 AM	Shortcut	2 KB
Active Directory Users and Computers	8/22/2013 9:55 AM	Shortcut	2 KB
ADSI Edit	8/22/2013 9:55 AM	Shortcut	2 KB
Component Services	8/22/2013 9:57 AM	Shortcut	2 KB
Computer Management	8/22/2013 9:54 AM	Shortcut	2 KB
Defragment and Optimize Drives	8/22/2013 9:47 AM	Shortcut	2 KB
DHCP	8/22/2013 9:45 AM	Shortcut	2 KB
DNS	8/22/2013 9:55 AM	Shortcut	2 KB
Event Viewer	8/22/2013 9:55 AM	Shortcut	2 KB
Group Policy Management	8/22/2013 9:56 AM	Shortcut	2 KB
Health Registration Authority	8/22/2013 9:45 AM	Shortcut	2 KB
iSCSI Initiator	8/22/2013 9:57 AM	Shortcut	2 KB
Local Security Policy	8/22/2013 9:54 AM	Shortcut	2 KB
Network Policy Server	8/22/2013 9:58 AM	Shortcut	2 KB
ODBC Data Sources (32-b...			2 KB

34 items | 1 item selected 1.06 KB

Network Policy Server

File Action View Help

NPS (Local)

- ▶ RADIUS Clients and Servers
- ▶ Policies
- ▶ Network Access Protection
- ▶ Accounting
- ▶ Templates Management

Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

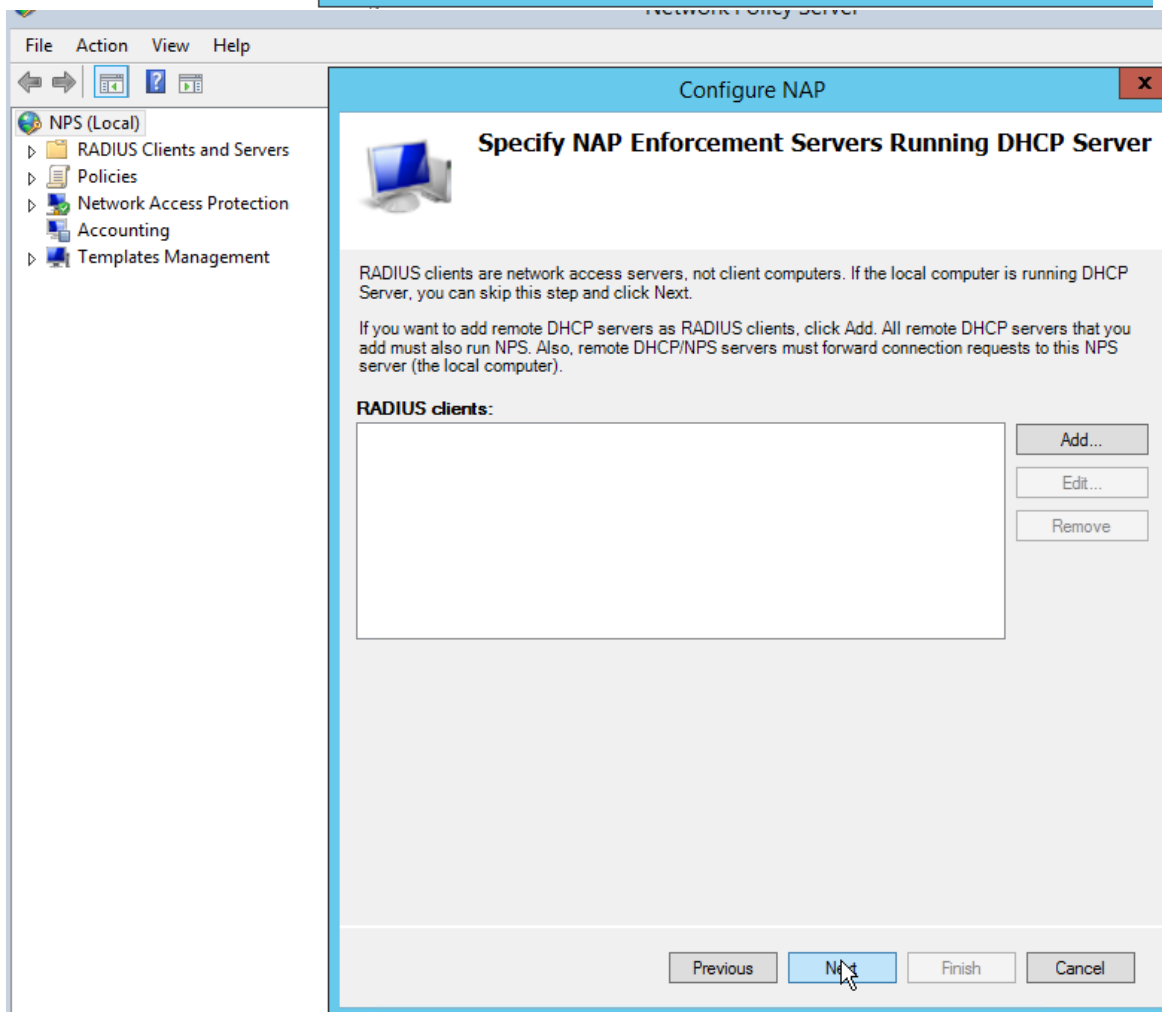
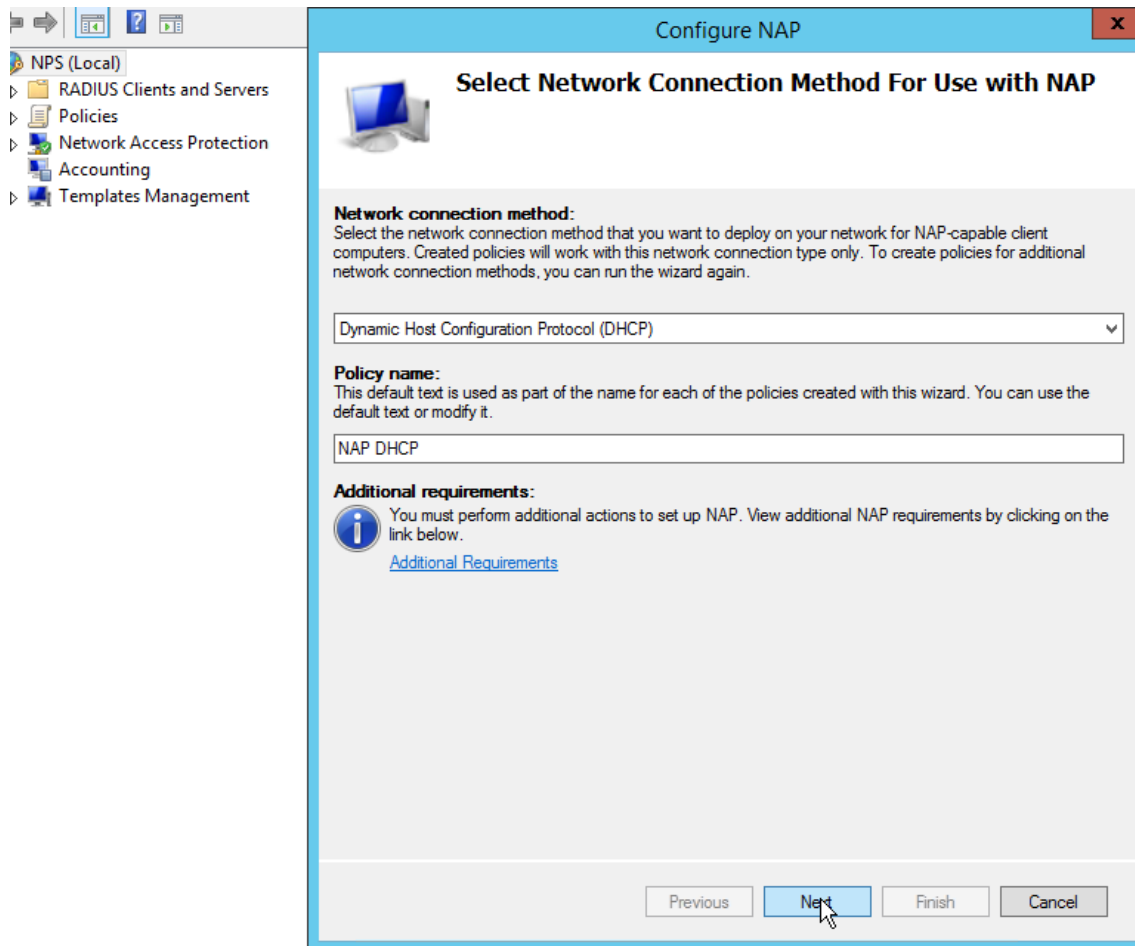
Network Access Protection (NAP)

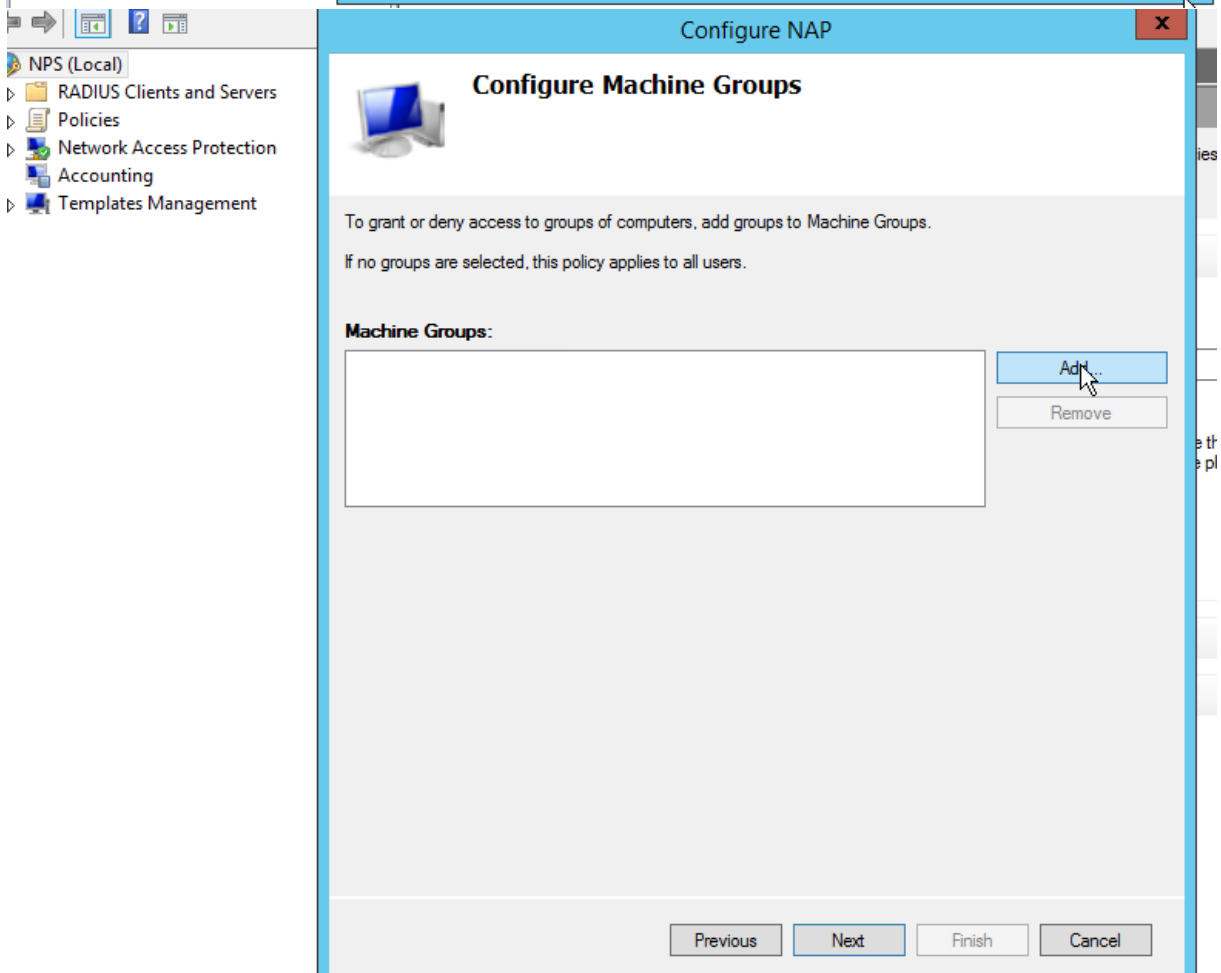
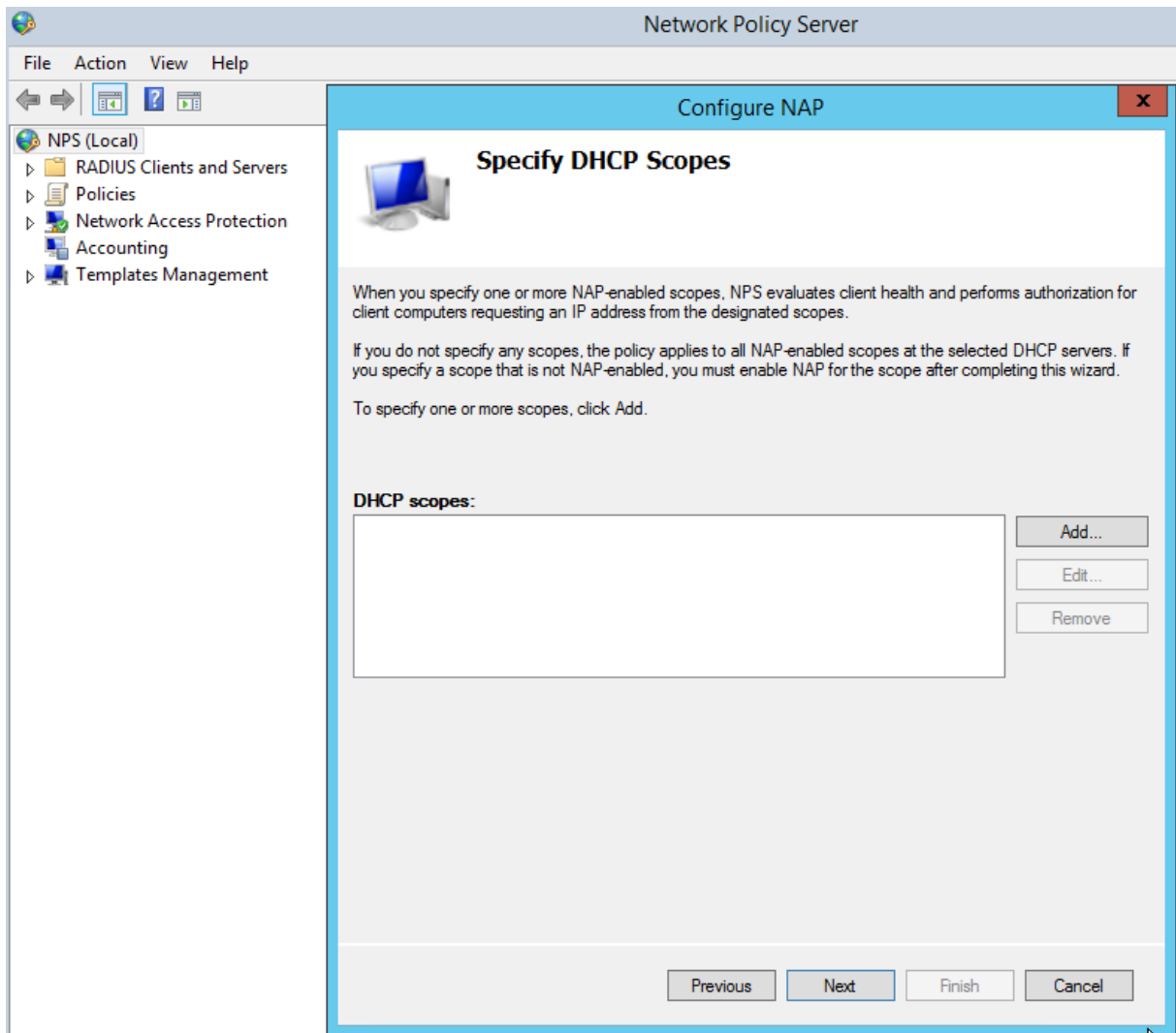
When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

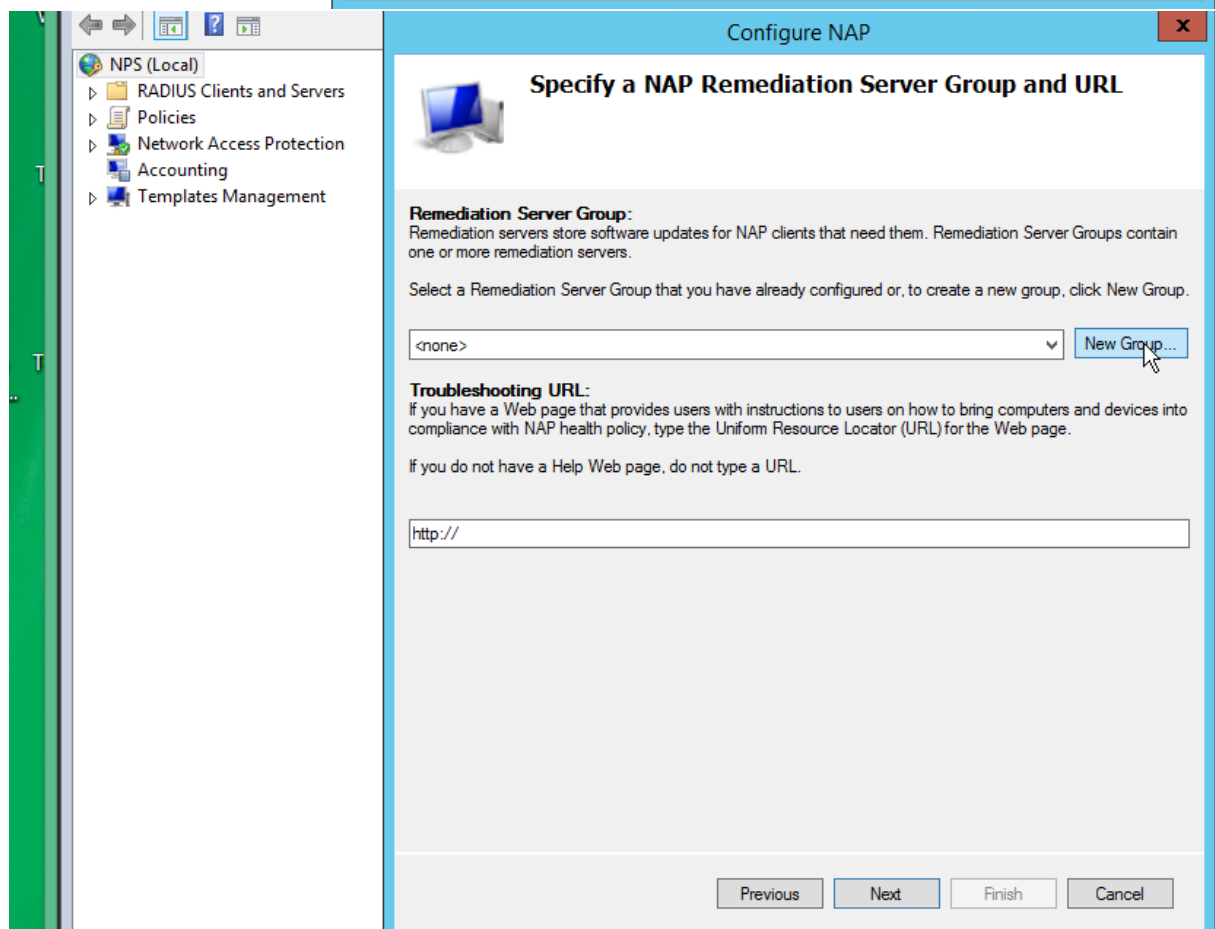
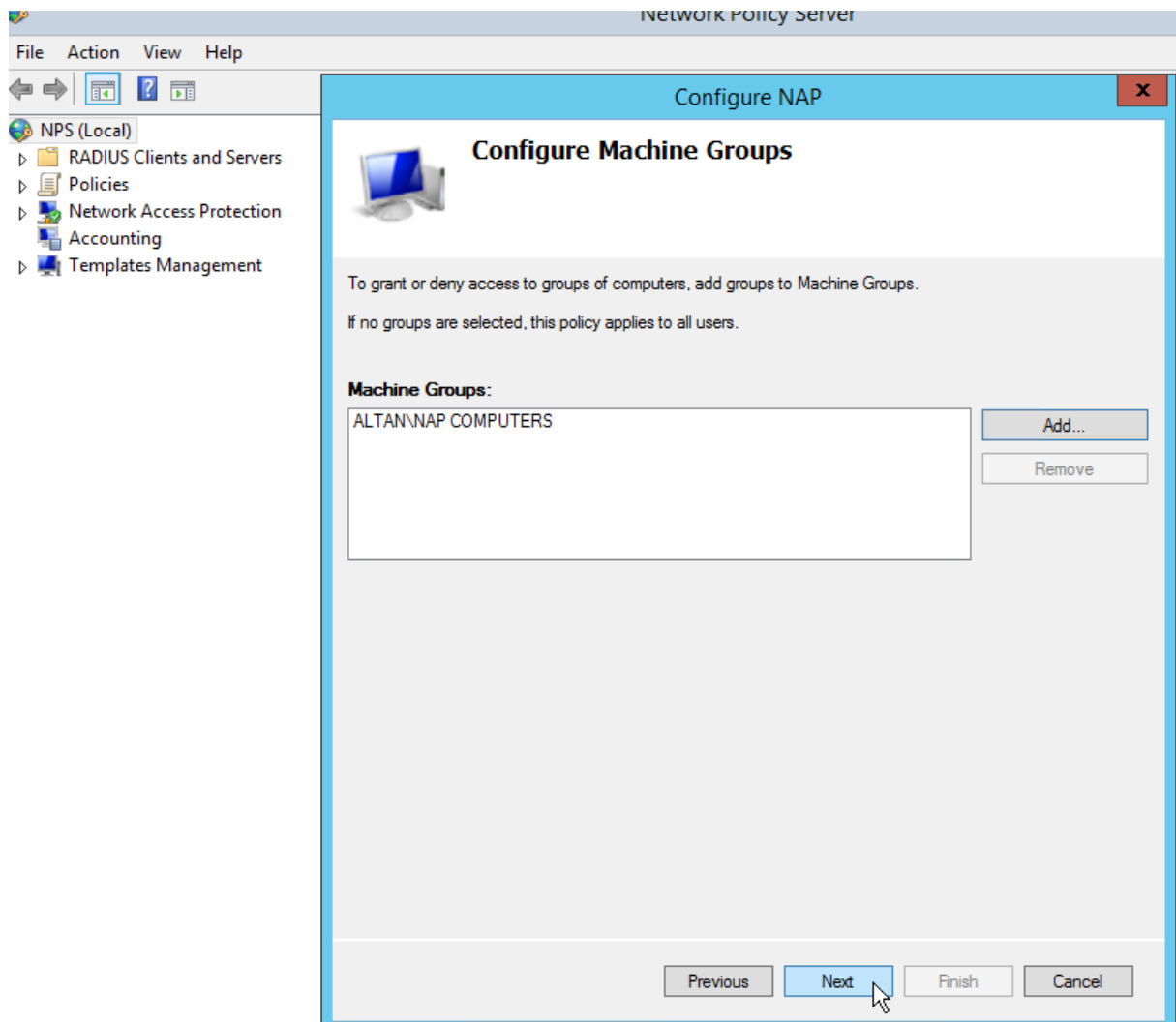
[Configure NAP](#) [Learn more](#)

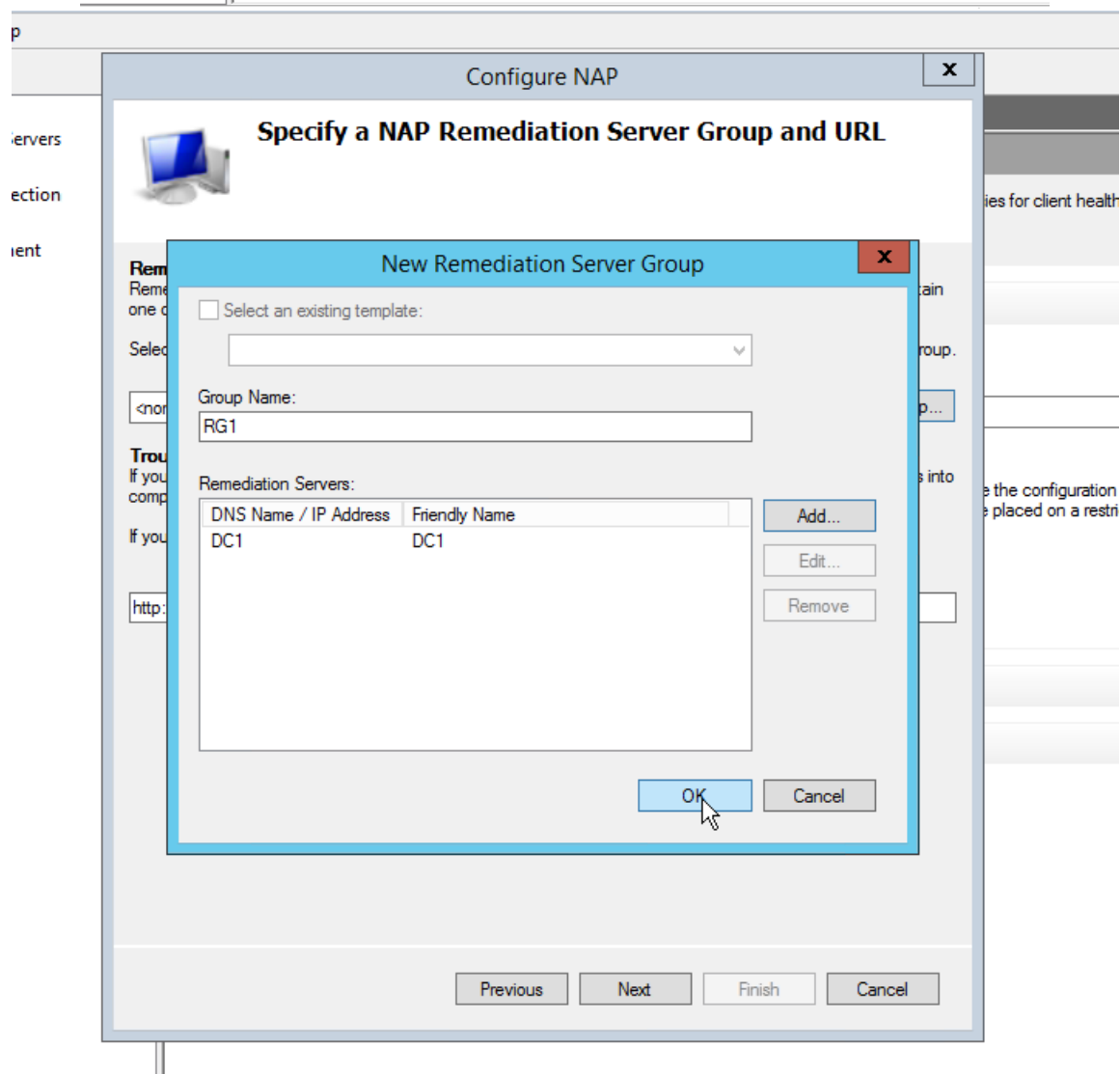
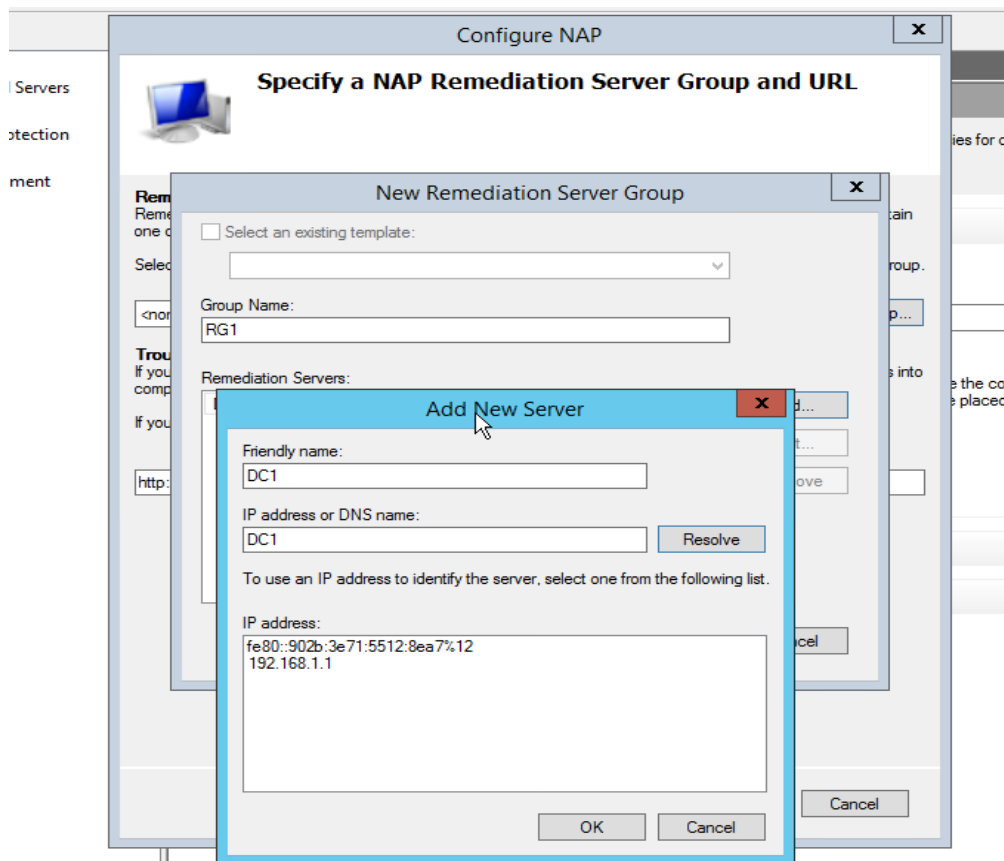
Advanced Configuration

Templates Configuration









File Action View Help

NPS (Local)

- RADIUS Clients and Servers
- Policies
- Network Access Protection
- Accounting
- Templates Management

Configure NAP

Specify a NAP Remediation Server Group and URL

Remediation Server Group:
Remediation servers store software updates for NAP clients that need them. Remediation Server Groups contain one or more remediation servers.

Select a Remediation Server Group that you have already configured or, to create a new group, click New Group.

RG1 New Group...

Troubleshooting URL:
If you have a Web page that provides users with instructions to users on how to bring computers and devices into compliance with NAP health policy, type the Uniform Resource Locator (URL) for the Web page.
If you do not have a Help Web page, do not type a URL.

http://TEST.DC1|

Previous Next Finish Cancel

Configure NAP

Define NAP Health Policy

The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy.

Name
<input checked="" type="checkbox"/> Windows Security Health Validator

☒ Enable auto-remediation of client computers

If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers.

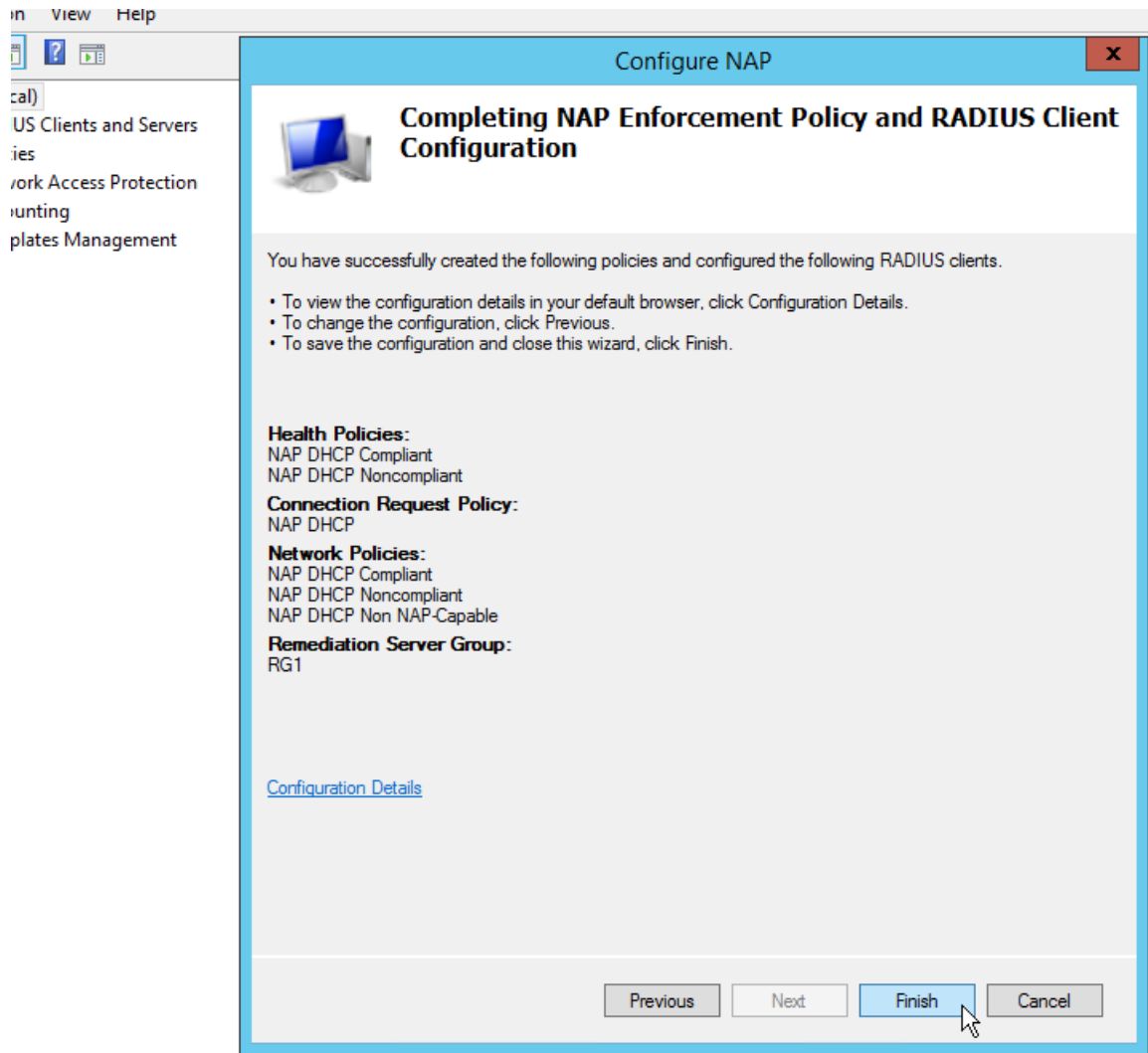
If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated.

Network access restrictions for NAP-ineligible client computers:

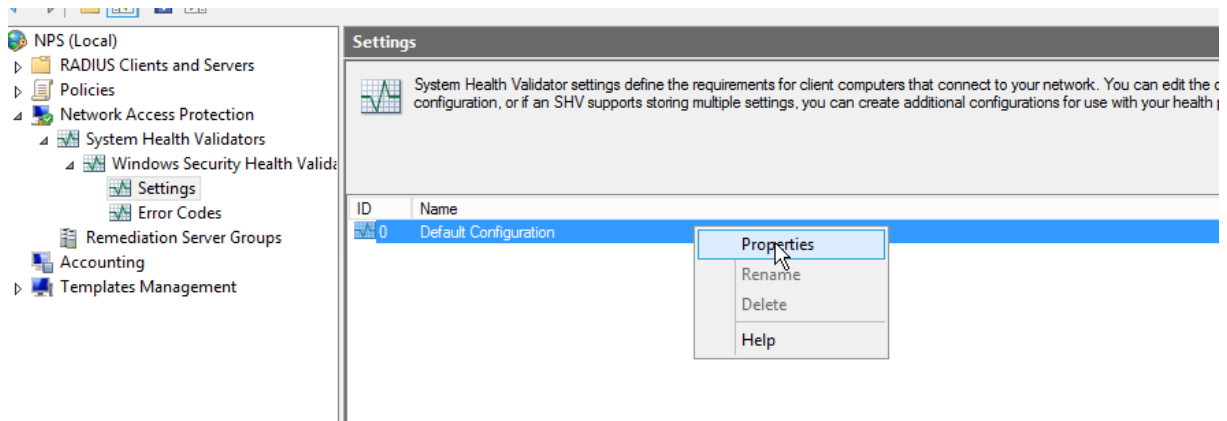
☒ Deny full network access to NAP-ineligible client computers. Allow access to a restricted network only.

☐ Allow full network access to NAP-ineligible client computers.

Previous Next Finish Cancel



YAPILANDIRMAMIZ TAMAMLANDIKTAN SONRA KULLANICILAR İÇİN HANGİ GÜVENLİK KONTROLLERİNİN YAPILACAĞINI SEÇİYORUZ.



Windows Security Health Validator

Windows 8/Windows 7/Win
Windows XP

 Choose policy settings for Windows Security Health Validator

Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.

[How do I configure a security health policy?](#)

Firewall Settings

☒ A firewall is enabled for all network connections

Antivirus Settings

☐ An antivirus application is on

☐ Antivirus is up to date

Spyware Protection Settings

☐ An antispyware application is on

☒ Antispyware is up to date

Automatic Updates Settings

OK Cancel

Windows Security Health Validator

Windows 8/Windows 7/Win
Windows XP

 Choose policy settings for Windows Security Health Validator

Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.

[How do I configure a security health policy?](#)

Firewall Settings

☒ A firewall is enabled for all network connections

Antivirus Settings

☐ An antivirus application is on

☐ Antivirus is up to date

Automatic Updates Settings

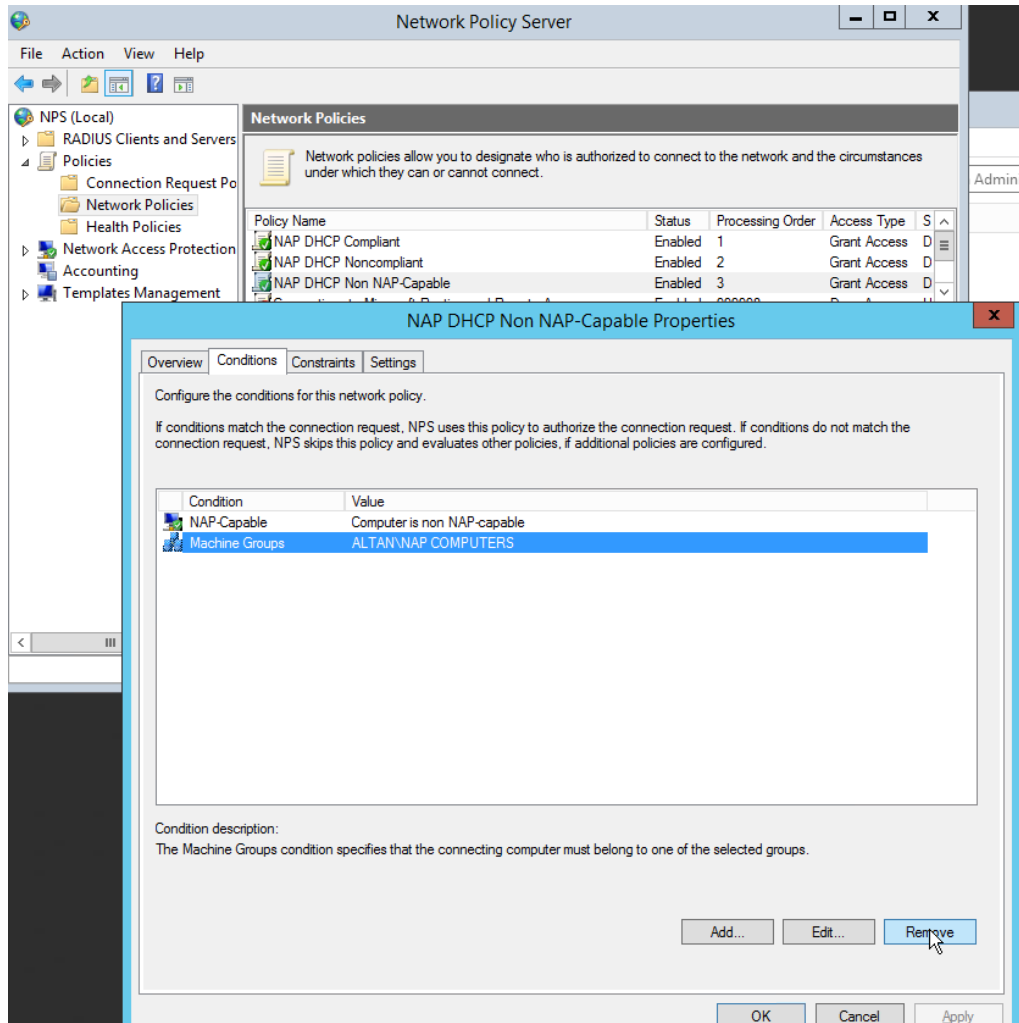
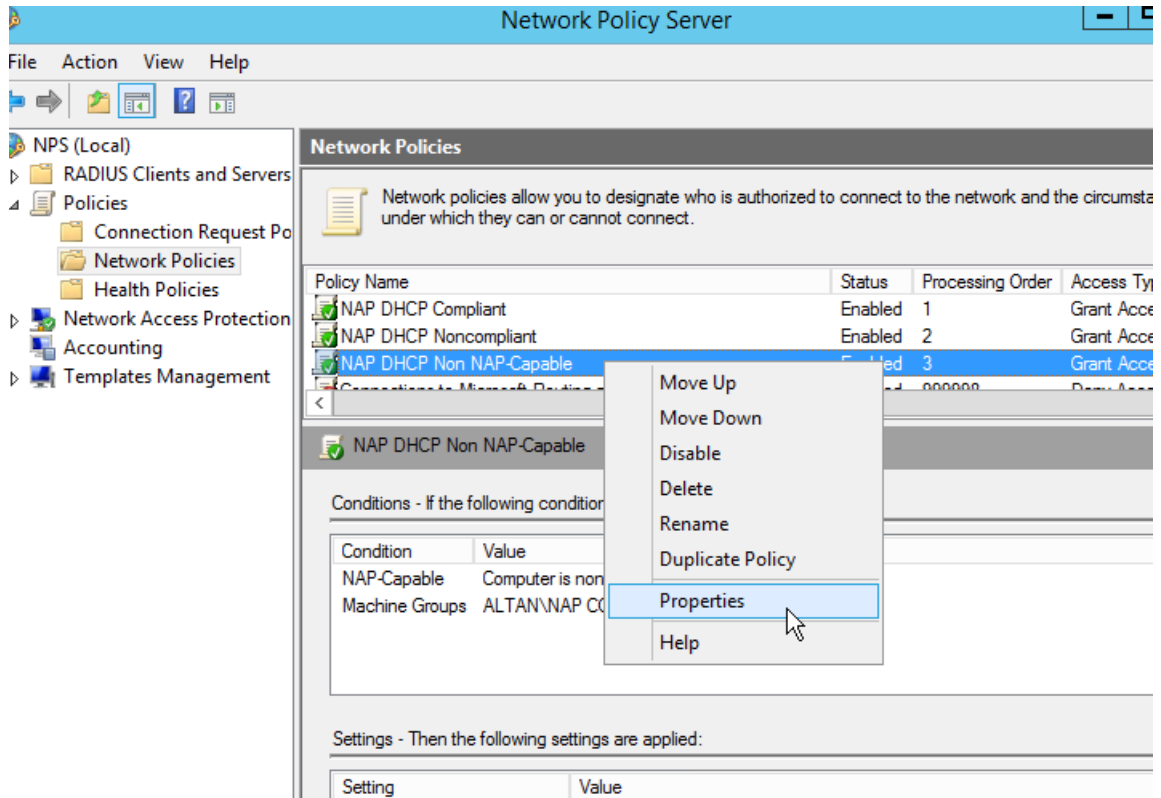
☐ Automatic updating is enabled

Security Updates Settings

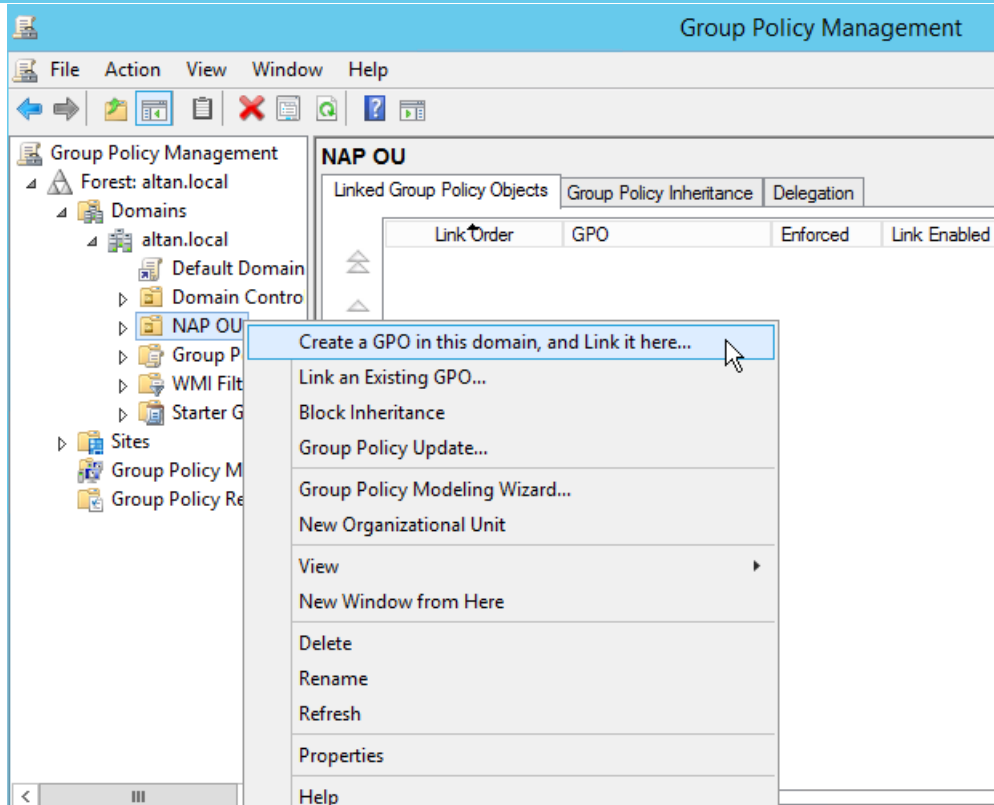
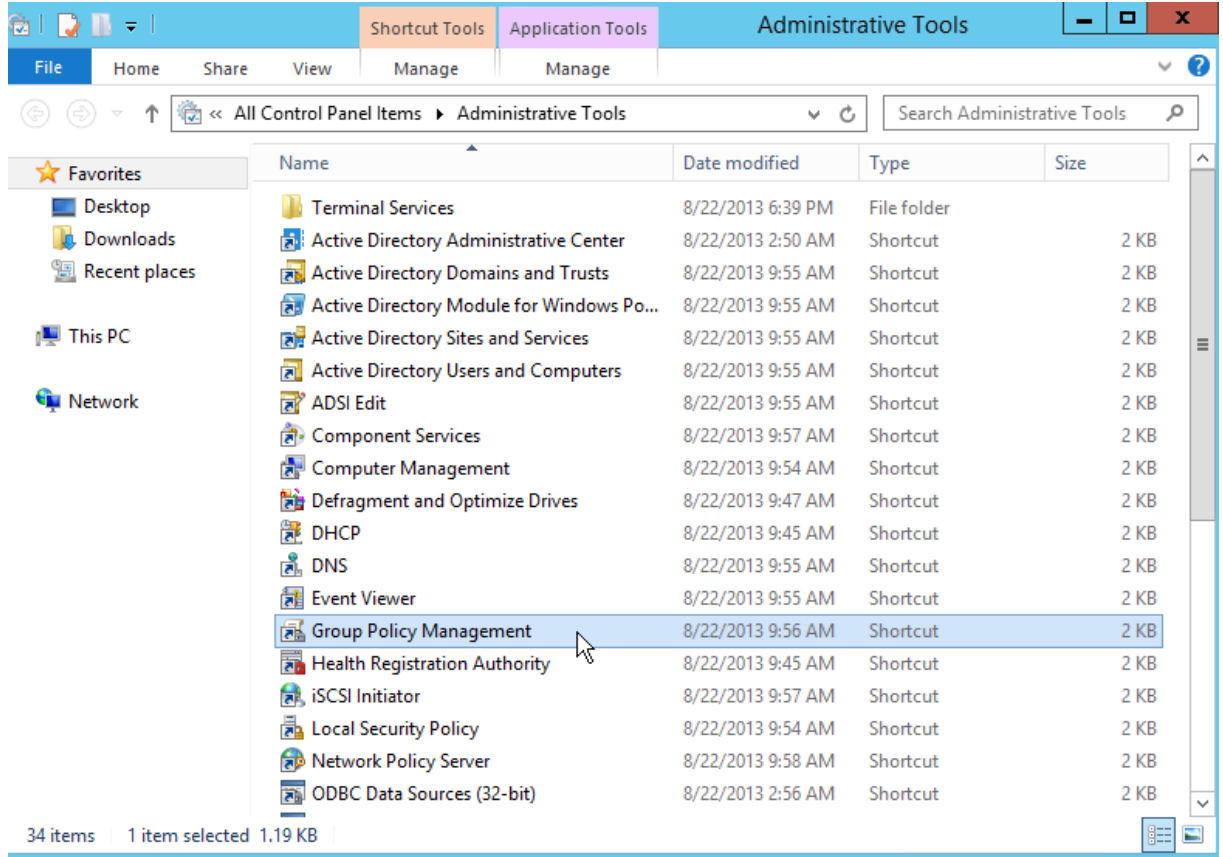
☐ Restrict access for clients that do not have all available security updates installed

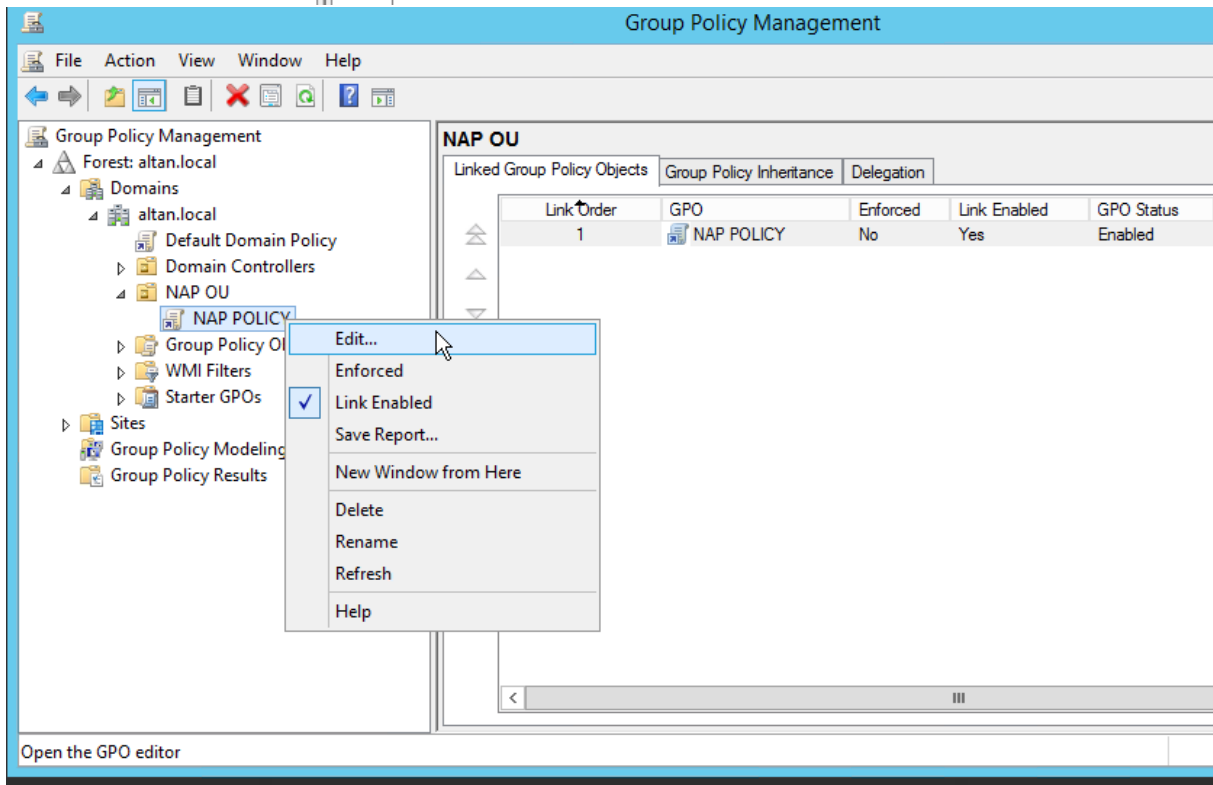
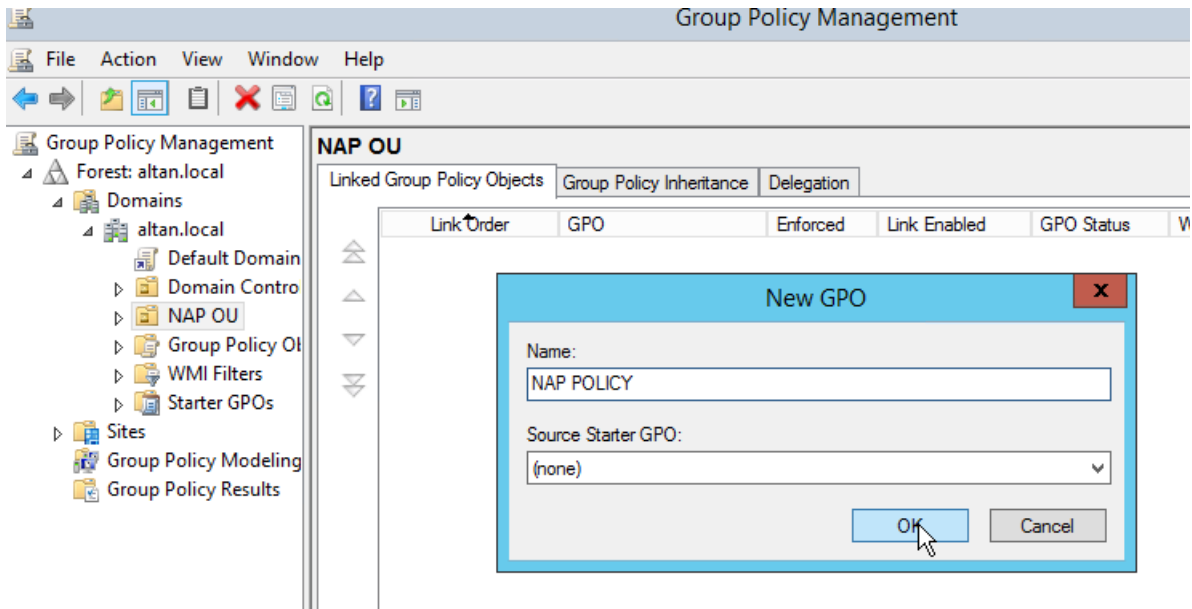
OK Cancel

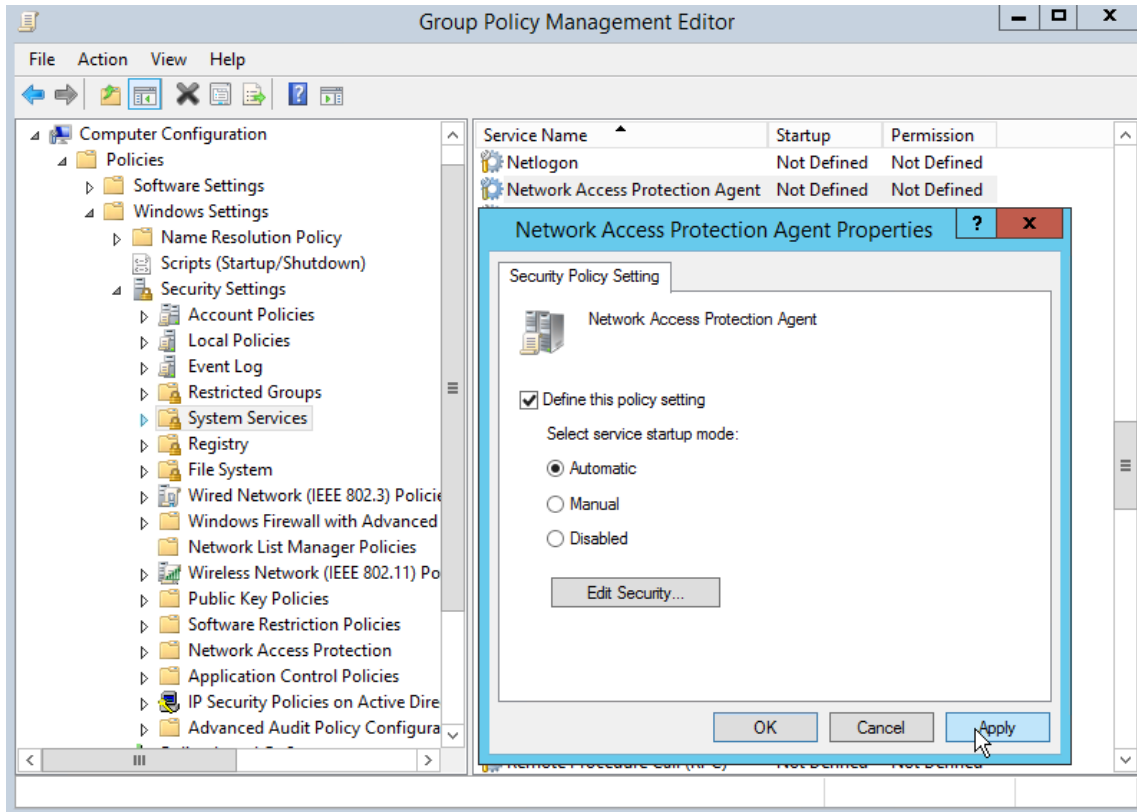
SIRADAKİ İŞLEM DOMAINDE OLMAYAN KONTROL EDEMEYECEĞİMİZ MAKİNALAR İÇİN **NAP COMPUTERS GROUP** KONTROLUNU KALDIRIYORUZ.



DOMAINDEKİ PCLERİ NAP İLE KONTROL EDEBİLMEK İÇİN **GROUP POLICY MANAGEMENT**TEN İLGİLİ AYARLARI YAPIYORUZ



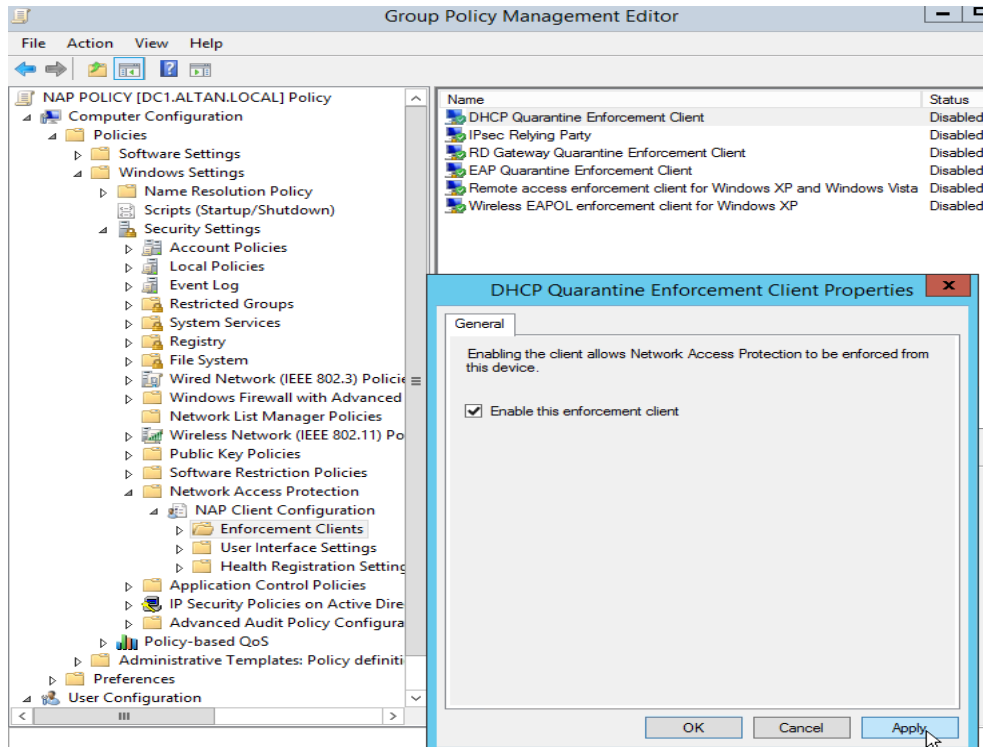




GPO>COMPUTER CONFIGURATION>POLICIES> WINDOWS SETTINGS > SECURITY SETTINGS> SYSTEM SERVICES

ALANINA GELİP **NETWORK ACCESS PROTECTION AGENT** AYARLARINI RESİMDEKİ GİBİ YAPIYORUZ.

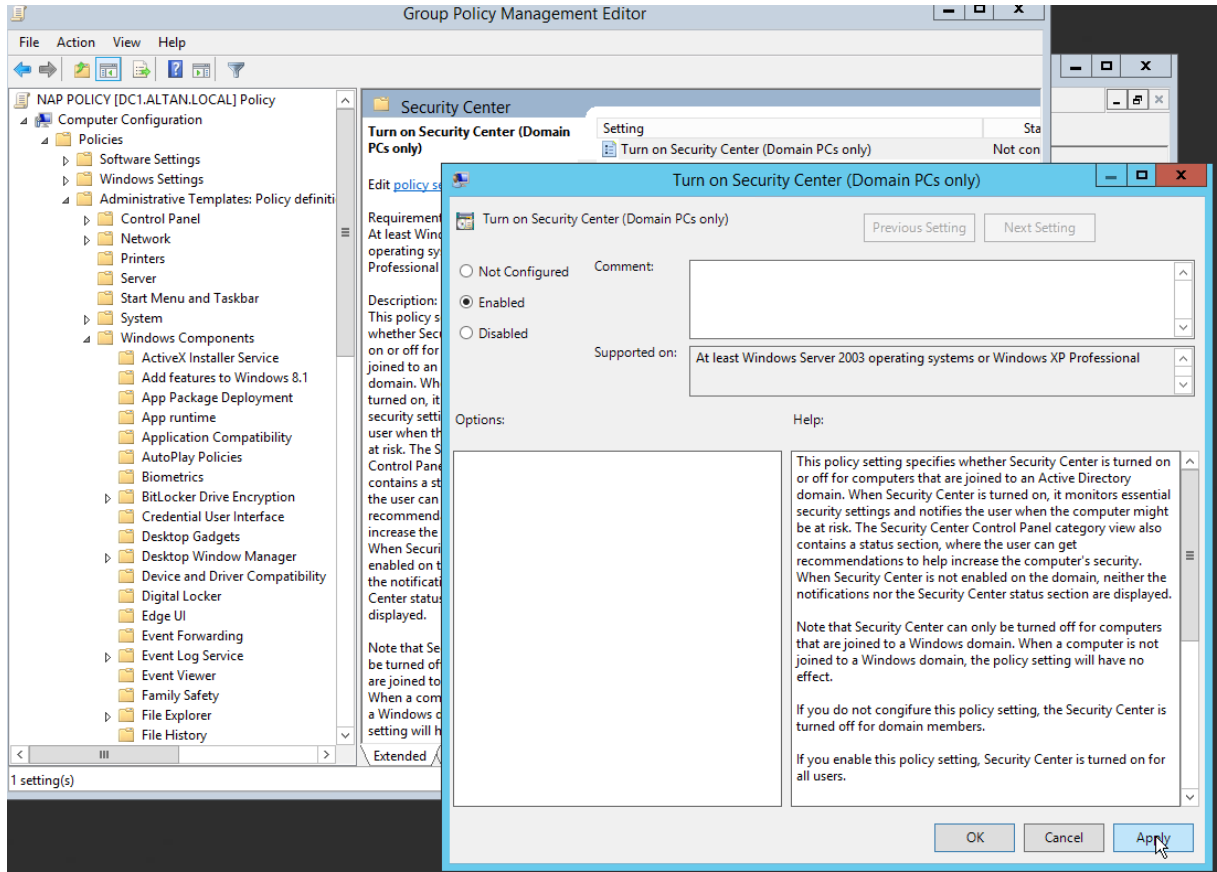
BURDAKİ AMACIMIZ; DOMAINDEKİ PCLERE GPO ARACILIĞIYLA NETWORK ACCESS PROTECTION AGENT SERVİSİNİN BAŞLAMASINI SAĞLAMAK.



GPO>COMPUTER CONFIGURATION>POLICIES> WINDOWS SETTINGS > SECURITY SETTINGS>NETWORK ACCESS PROTECTION> NAP CLIENT CONFIGURATION > ENFORCEMENT CLIENTS

ALANINA GELİP **DHCP QUARANTINE ENFORCEMENT CLIENT** AYARINI ENABLE YAPIYORUZ.

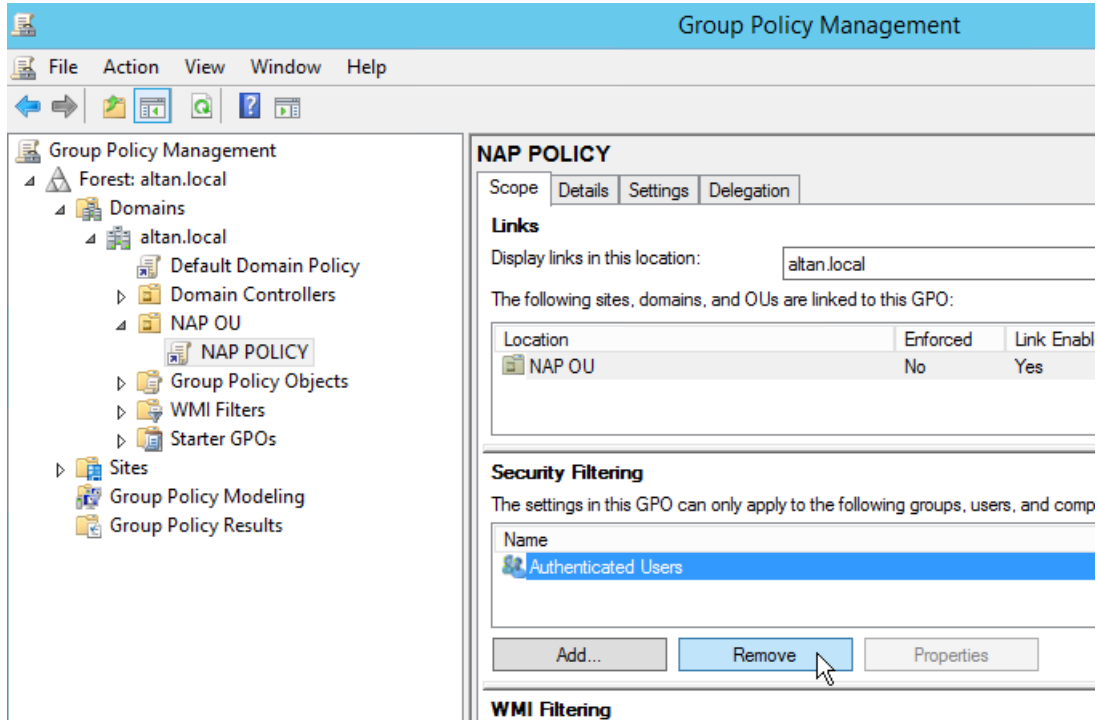
BURADAKİ AMACIMIZ DOMAINDEKİ PCLER EĞER BELİRLDİĞİMİZ GÜVENLİK ŞARTLARINA UYMUYORSA DHCP TARAFINDA KISITLI KONFIG ATANMASINI SAĞLAMAK.



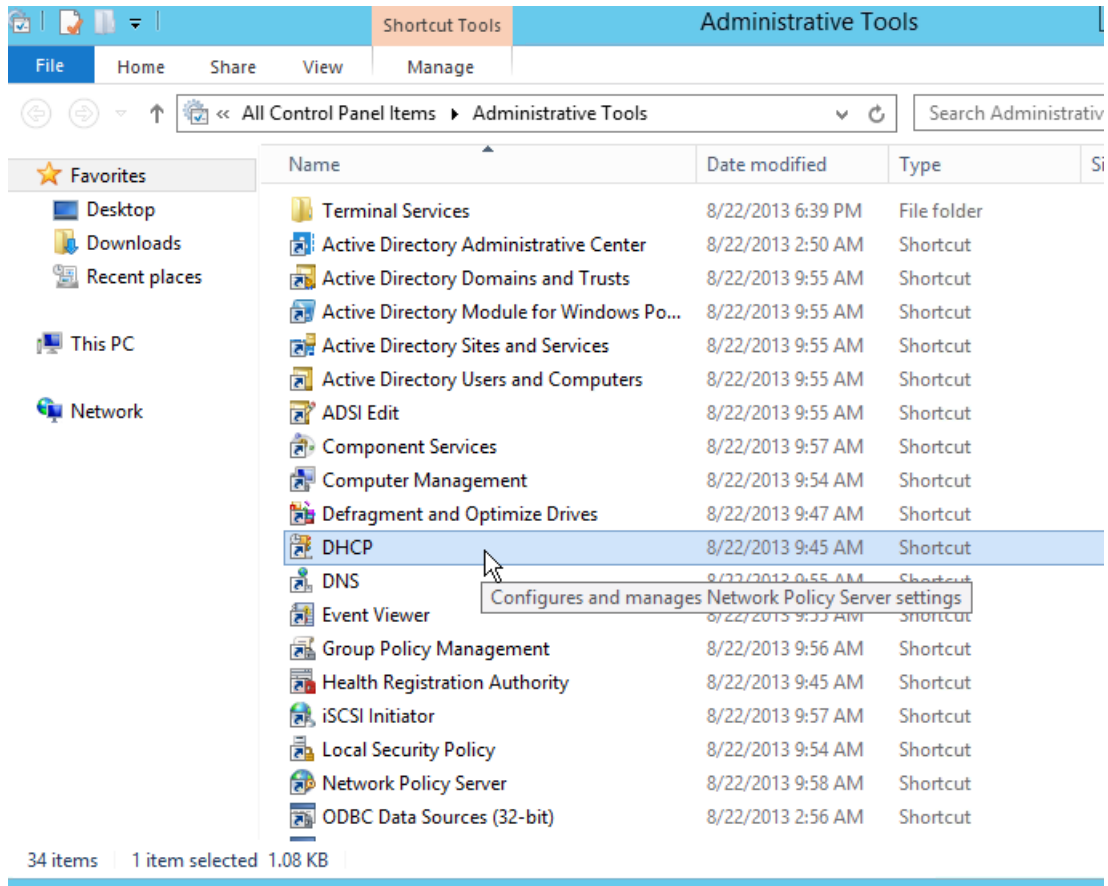
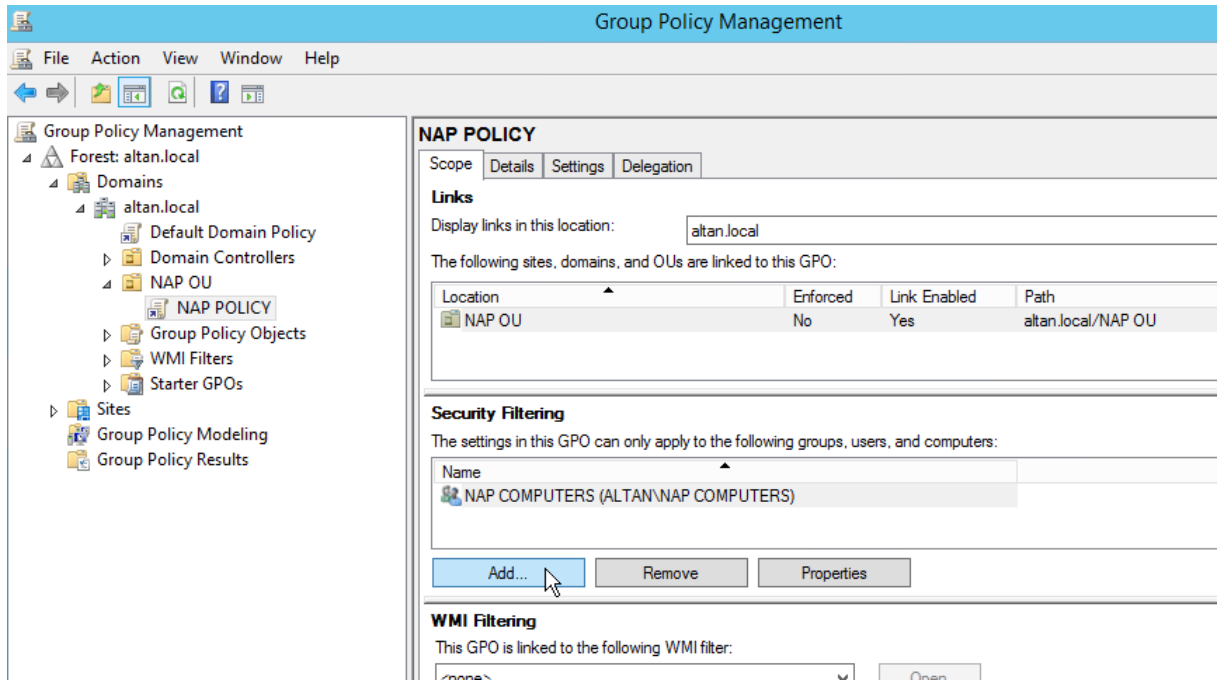
GPO>COMPUTER CONFIGURATION> POLICIES> ADMINISTRATIVE TEMPLATES> WINDOWS COMPONENTS> SECURITY CENTER

ALANINDA **TURN ON SECURITY CENTER (DOMAIN PCS ONLY)** AYARI ENABLE DURUMUNA GETİRİLİR.

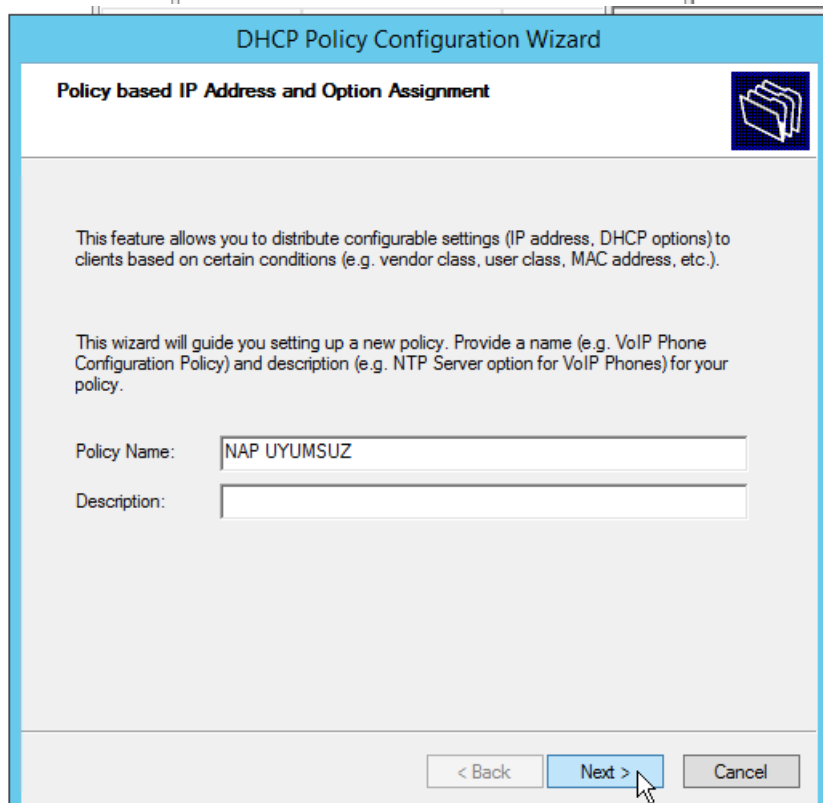
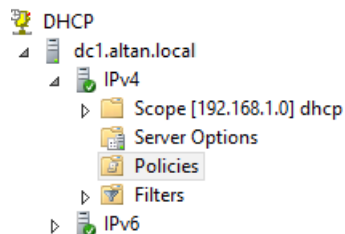
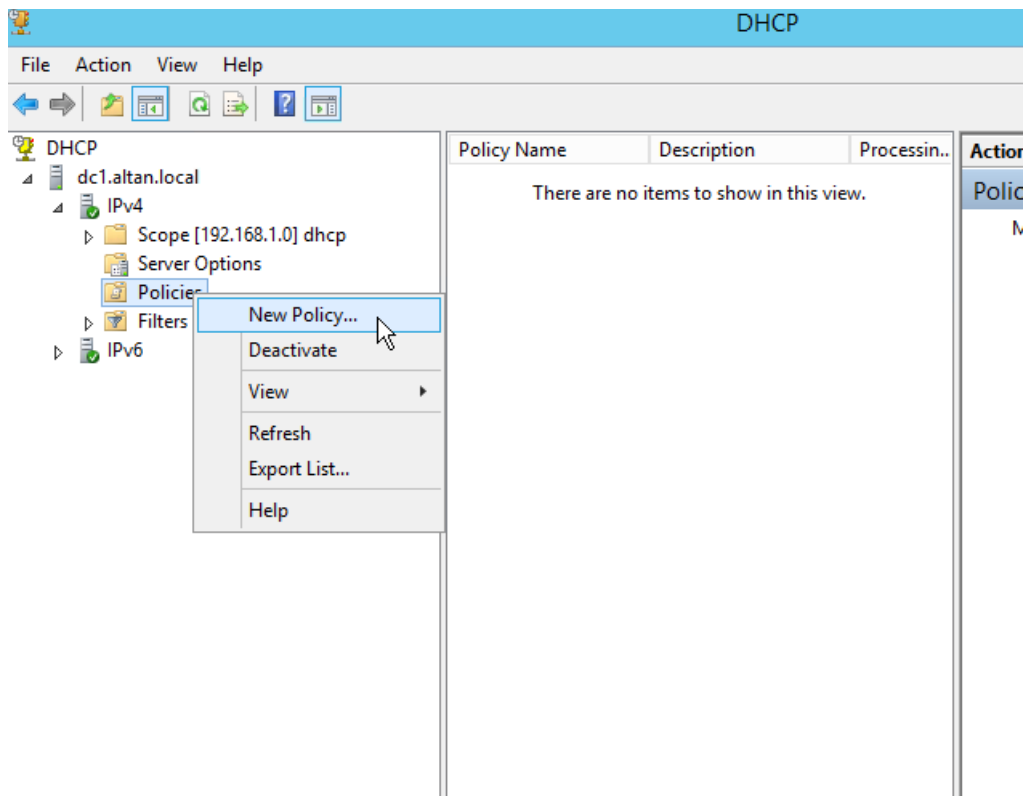
BURADAKİ AMAÇ DOMAINDEKİ PCLER EĞER BELİRTTİĞİMİZ GÜVENLİK ŞARTLARINA UYMUYORSA SECURITY CENTER TARAFINDAN UYARI VERMESİ.

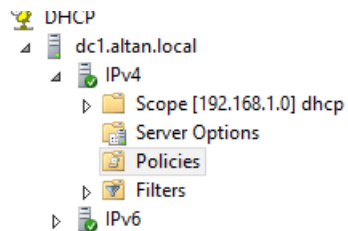


GROUP POLICYDE DAHA ÖNCEDEN EKLEMİŞ OLDUĞUMUZ GPO İÇİN SECURITY FILTERING KISMINDAN **AUTHENTICATED USERS** ÇIKARILIP **NAP COMPUTERS** GRUBU EKLENİR



DHCP DE DOMAINDE OLMAYAN YA DA DOMAINDE OLUP İSTEDİĞİMİZ GÜVENLİK ŞARTLARINA UYMAYAN PCLER İÇİN POLICY YAZILIR.





DHCP Policy Configuration Wizard

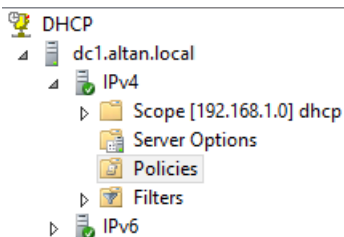
Configure Conditions for the policy

A policy consists of one or more conditions and a set of configuration settings (options, IP Address) that are distributed to the client. The DHCP server delivers these specific settings to clients that match these conditions.

! A policy with conditions based on fully qualified domain name can have configuration settings for DNS but not for options or IP address ranges.

Conditions	Operator	Value
------------	----------	-------

☐ AND ☒ OR



DHCP Policy Configuration Wizard

Add/Edit Condition

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

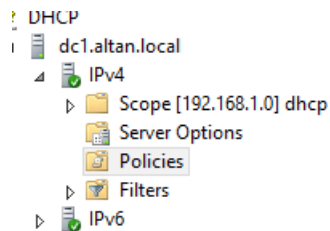
Criteria:

Operator:

Value(s)

Value:

☐ Prefix wildcard(*)
☐ Append wildcard(*)



DHCP Policy Configuration Wizard

Configure settings for the policy
If the conditions specified in the policy match a client request, the settings will be applied.

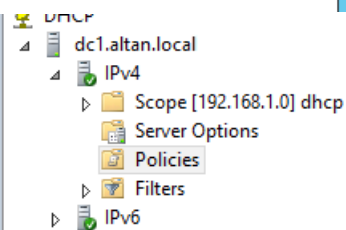
Vendor class: DHCP Standard Options

Available Options	Description
<input type="checkbox"/> 002 Time Offset	UTC offset in seconds
<input checked="" type="checkbox"/> 003 Router	Array of router addresses order
<input type="checkbox"/> 004 Time Server	Array of time server addresses

Data entry

Server name:

IP address:



DHCP Policy Configuration Wizard

Configure settings for the policy
If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class: DHCP Standard Options

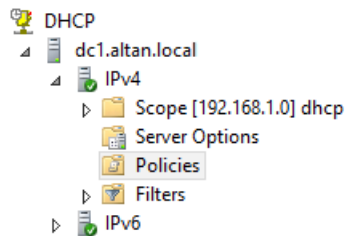
Available Options	Description
<input type="checkbox"/> 005 Name Servers	Array of name servers [IEN 110]
<input checked="" type="checkbox"/> 006 DNS Servers	Array of DNS servers, by preference
<input type="checkbox"/> 007 Log Servers	Array of MIT LCS UDP log servers

Data entry

Server name:

IP address:

< Back Next > Cancel



DHCP Policy Configuration Wizard

Configure settings for the policy
If the conditions specified in the policy match a client request, the settings will be applied.

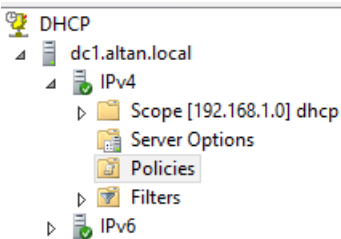
Vendor class:

Available Options	Description
<input type="checkbox"/> 014 Merit Dump File	Path name for crash dump file
<input checked="" type="checkbox"/> 015 DNS Domain Name	DNS Domain name for client request
<input type="checkbox"/> 016 Swap Server	Address of client's swap server

Data entry

String value:

< Back **Next >** Cancel



DHCP Policy Configuration Wizard

Summary

A new policy will be created with the following properties. To configure DNS settings, view properties of the policy and click the DNS tab.

Name: **NAP UYUMSUZ**

Description:

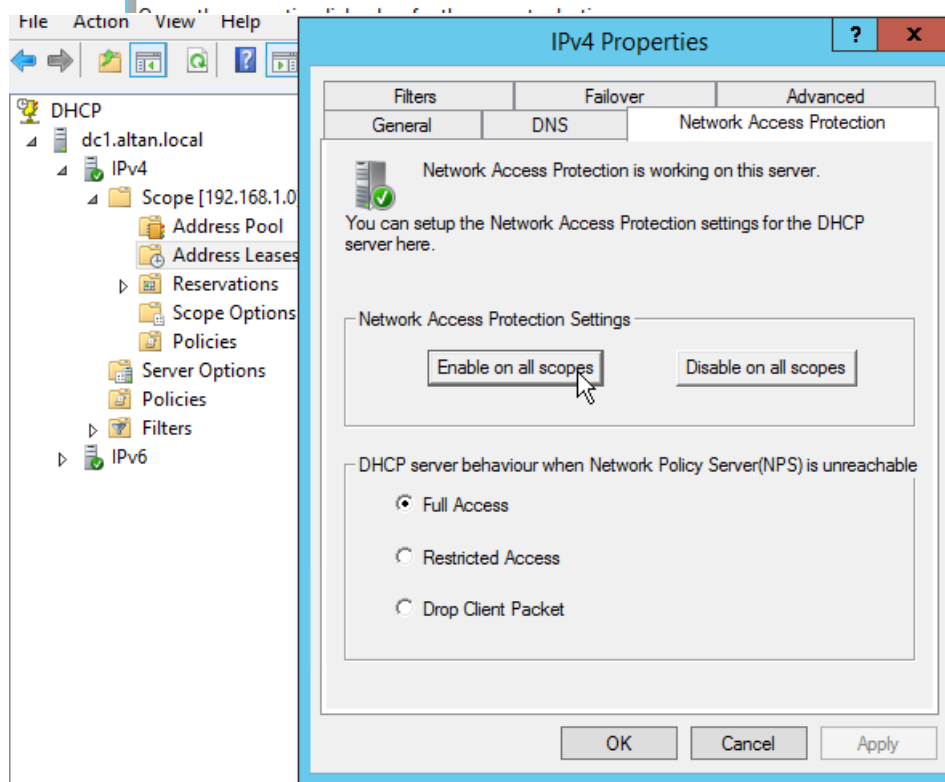
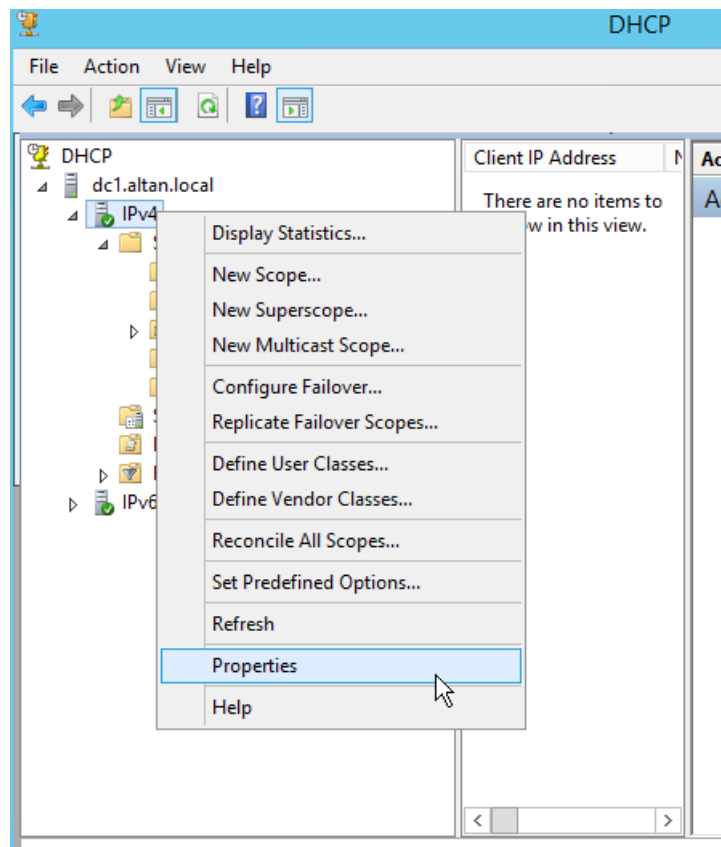
Conditions: **OR of**

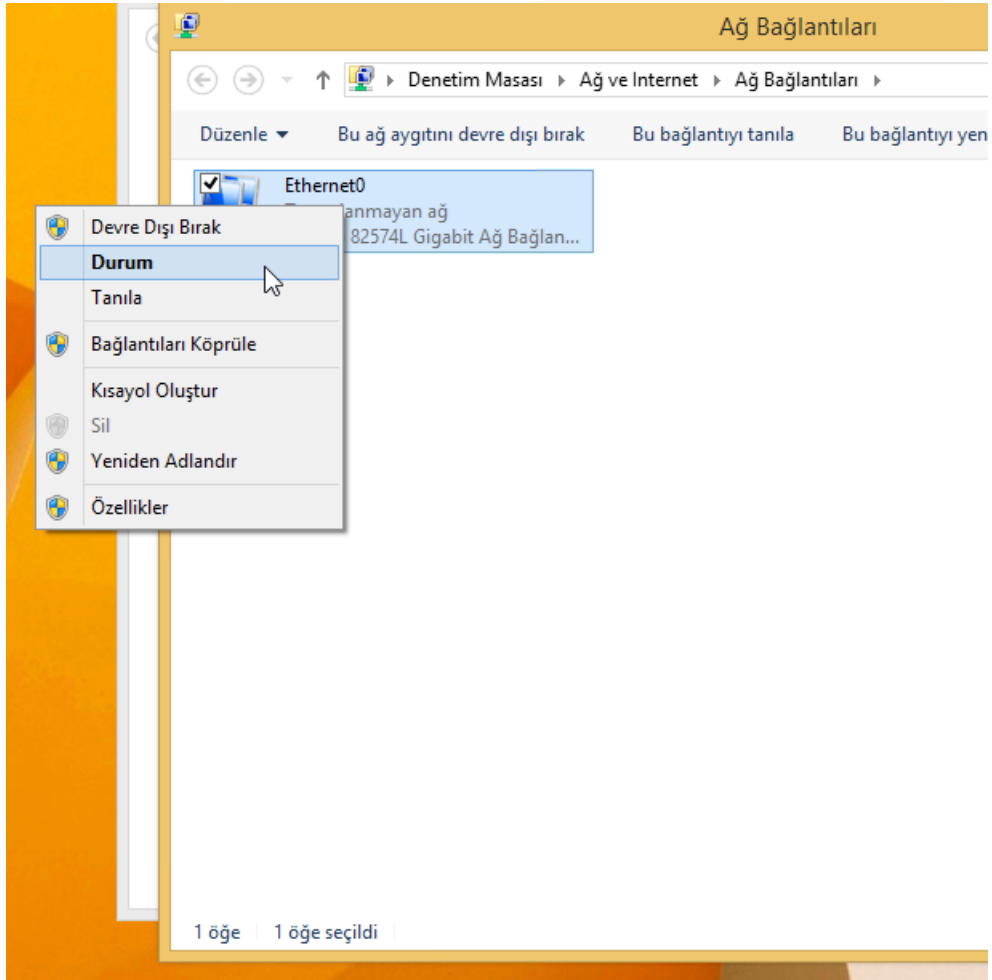
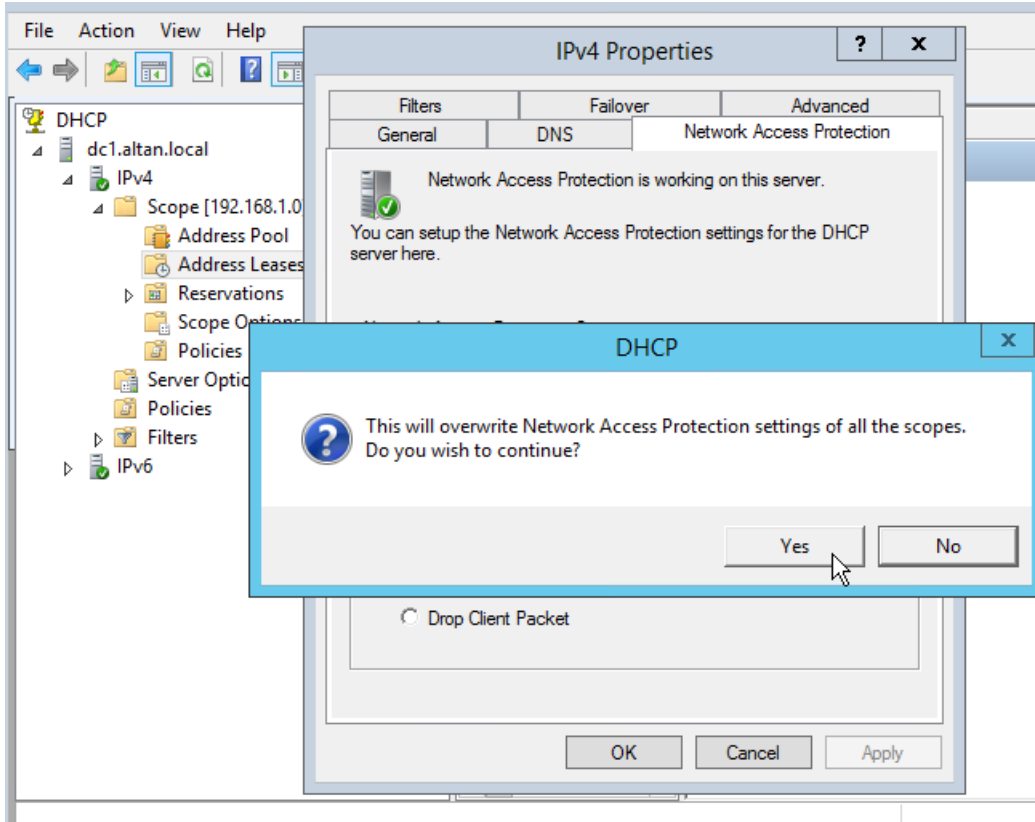
Conditions	Operator	Value
User Class	Equals	Default Network Access Protec...

Settings:

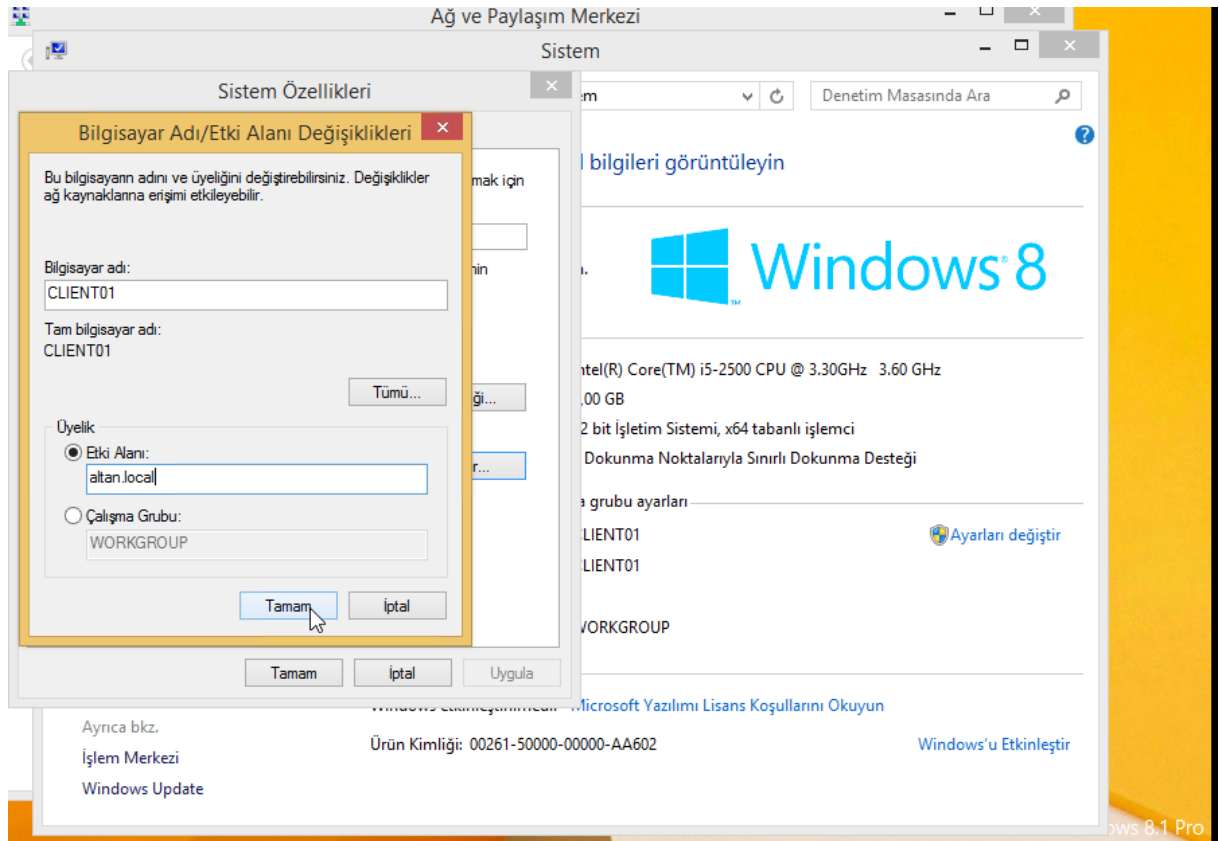
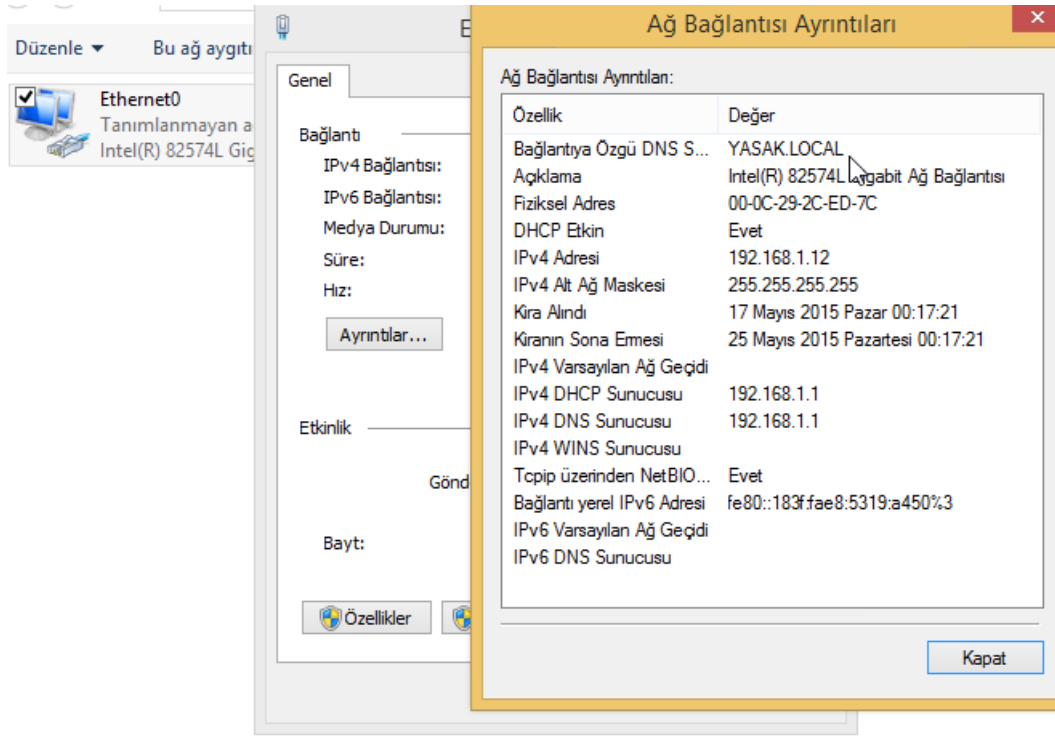
Option Name	Vendor Class	Value
Router		192.168.1.1
DNS Servers		192.168.1.1
DNS Domain Name		YASAK.LOCAL

< Back **Finish** Cancel

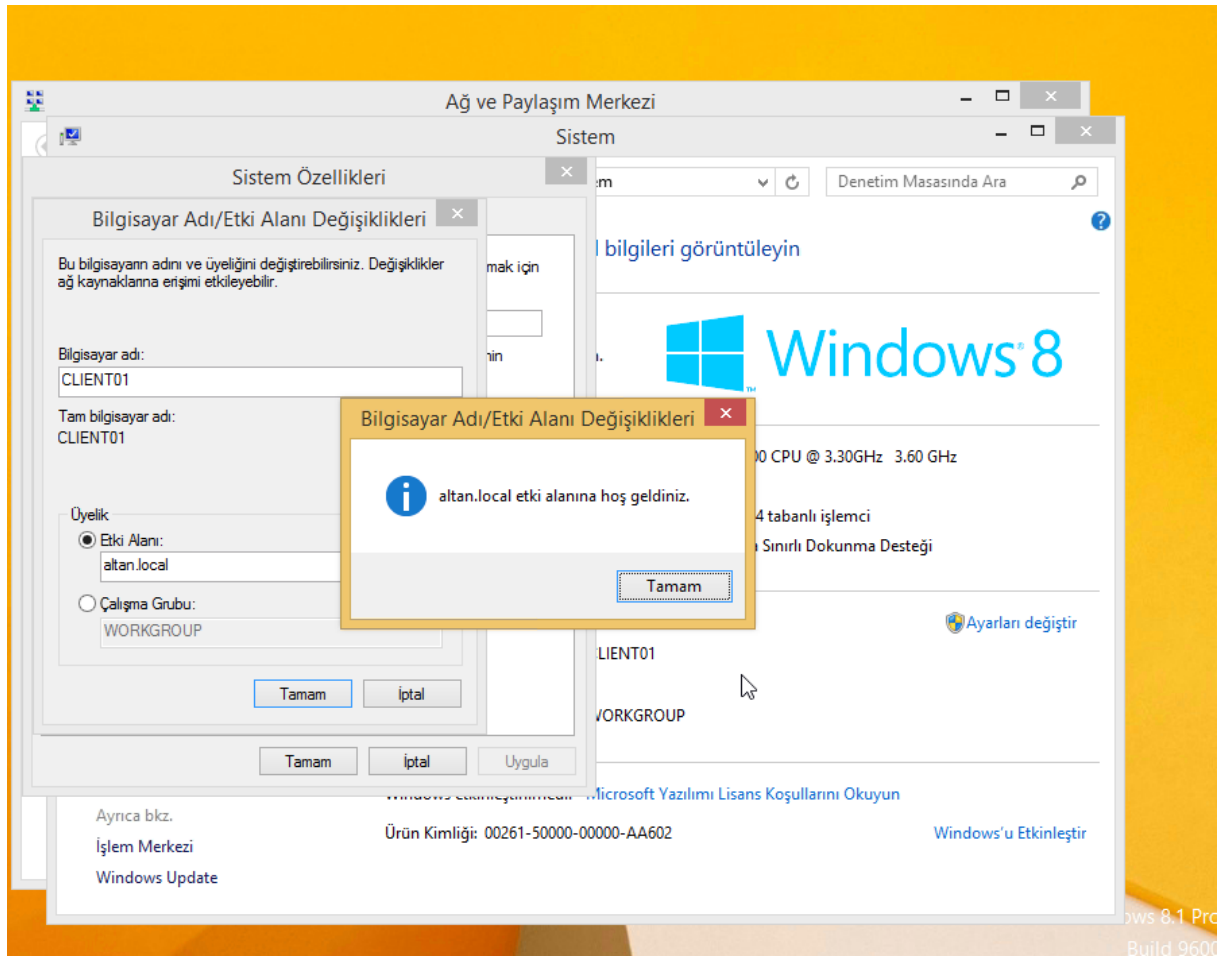




DOMAİNDE OLMAYAN WINDOWS 8 CLIENT01 MAKİNAMIZIN IP KONFIGURASYONU KONTROL EDİLİR. VE DHCP POLICY İLE BELİRTTİĞİMİZ GİBİ AYARLARIN ALDIĞI GÖZLENİR.

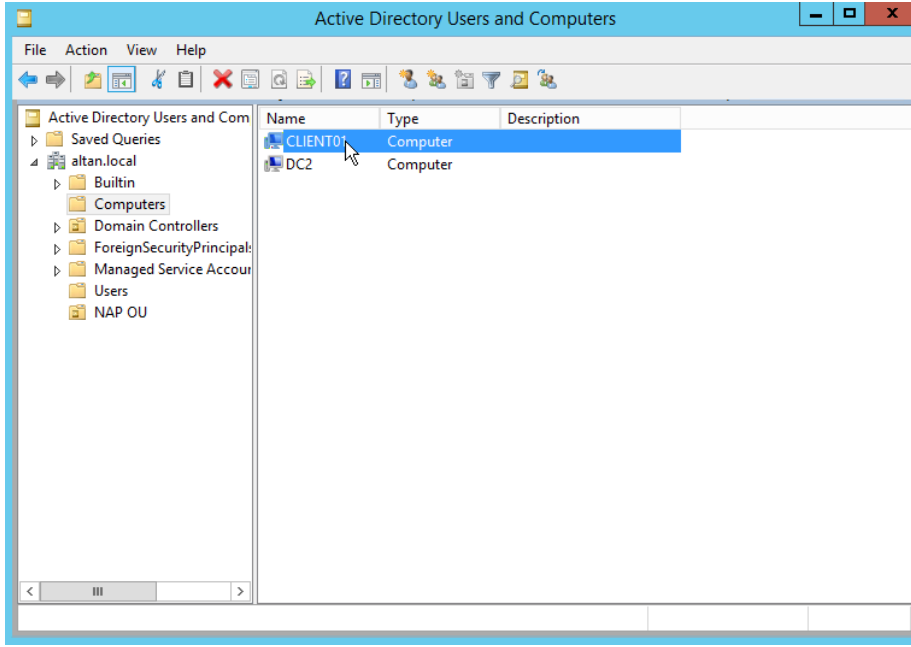


CLIENT01 İ DOMAİNE DAHİL EDİYORUZ.

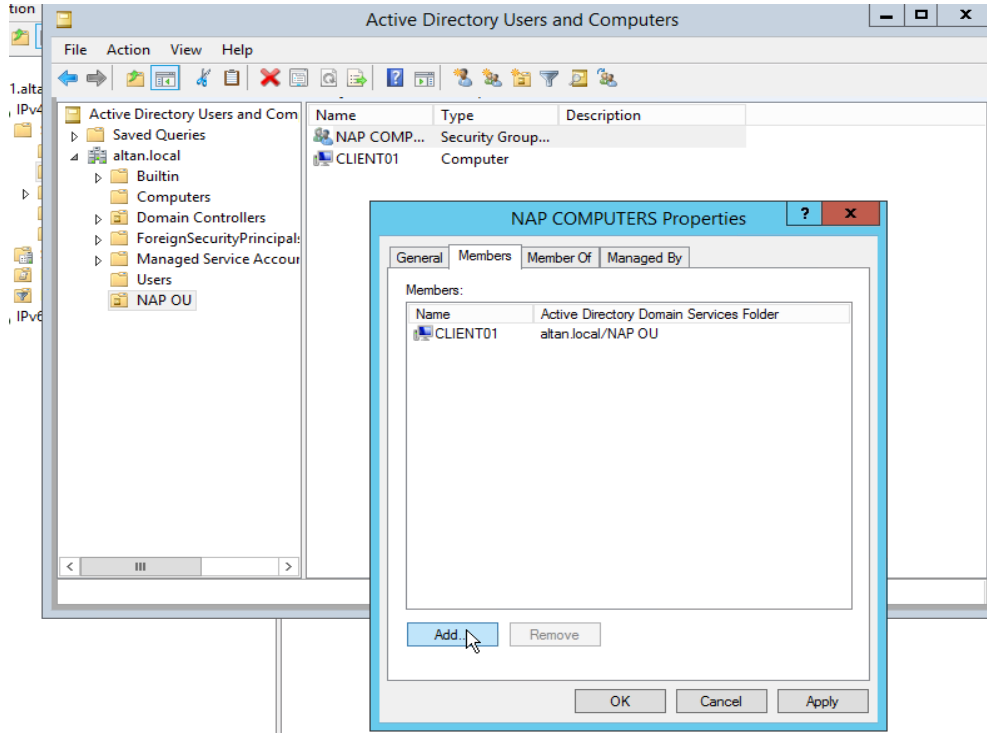


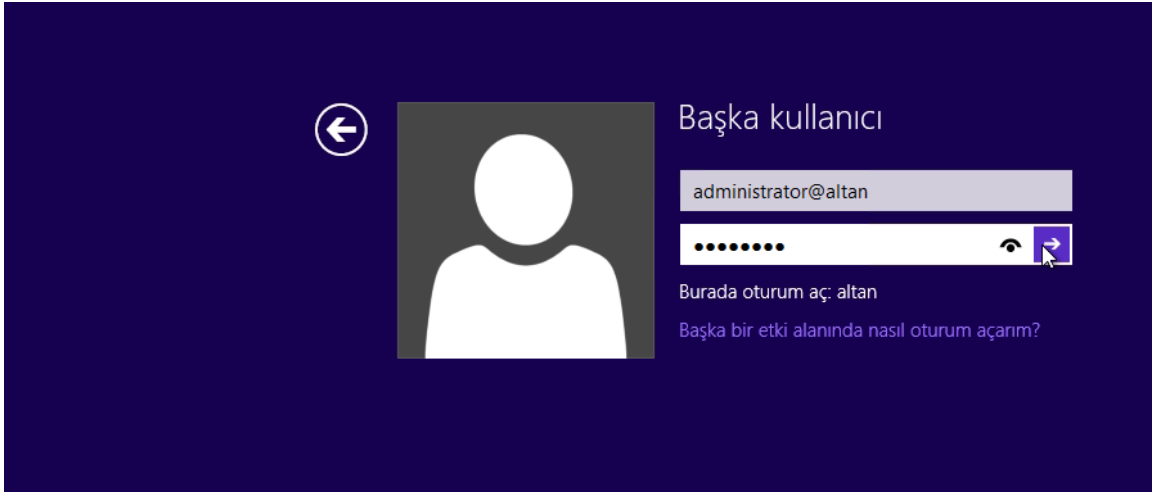
DHCP									
File Action View Help									
Client IP Address	Name	Lease Expiration	Type	Unique ID	Description	Network Access Protection	Probation Expiration	Filter	
192.168.1.12	CLIENT01.altan.local	5/25/2015 12:20:12 AM	DHCP	000c292ce...		Restricted Access	N/A	Nc	

DC1 ÜZERİNDEKİ DHCPDE CLIENT01İN BELİRTTİĞİMİZ ÜZERE KISITLI ALANDA OLDUĞU TEYİT EDİLİR. GÖRÜLDÜĞÜ ÜZERE **NETWORK ACCESS PROTECTION** TABINDA **RESTRICTED ACCESS** GÖRÜNÜYOR



AZ EVVEL DOMAINE DAHİL ETTİĞİMİZ CLIENT01 MAKINASINI ACTIVE DIRECTORYDE COMPUTERS ALANINDAN **NAP OU** ORGANIZATIONAL UNITINE SÜREKLE BIRAK YÖNTEMİYLE TAŞIYORUZ. VE BİLGİSAYARI **NAP COMPUTERS** GRUBUNA ÜYE YAPIYORUZ

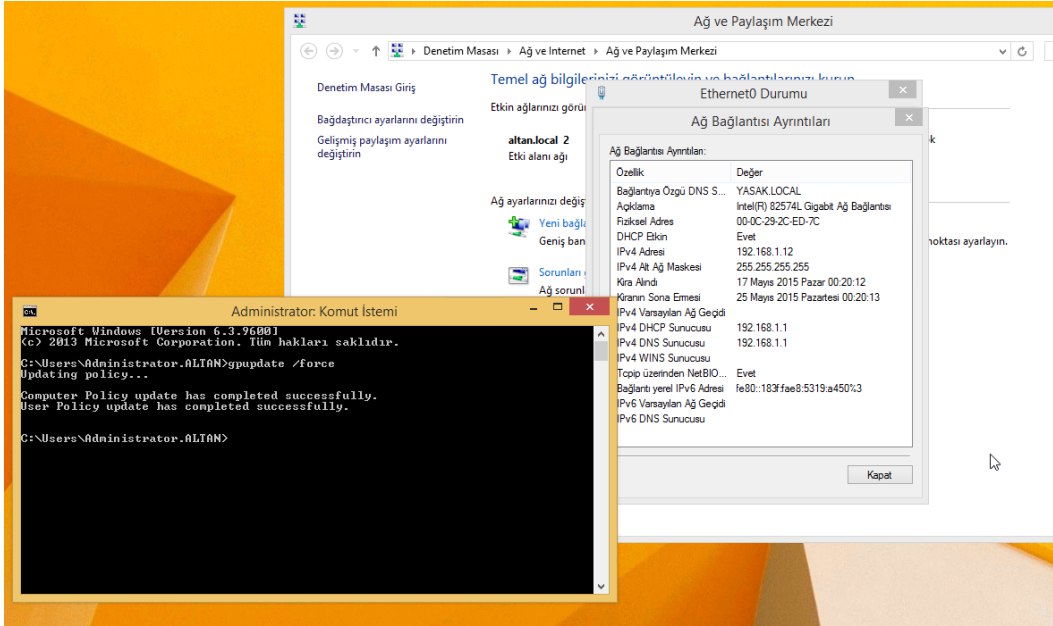


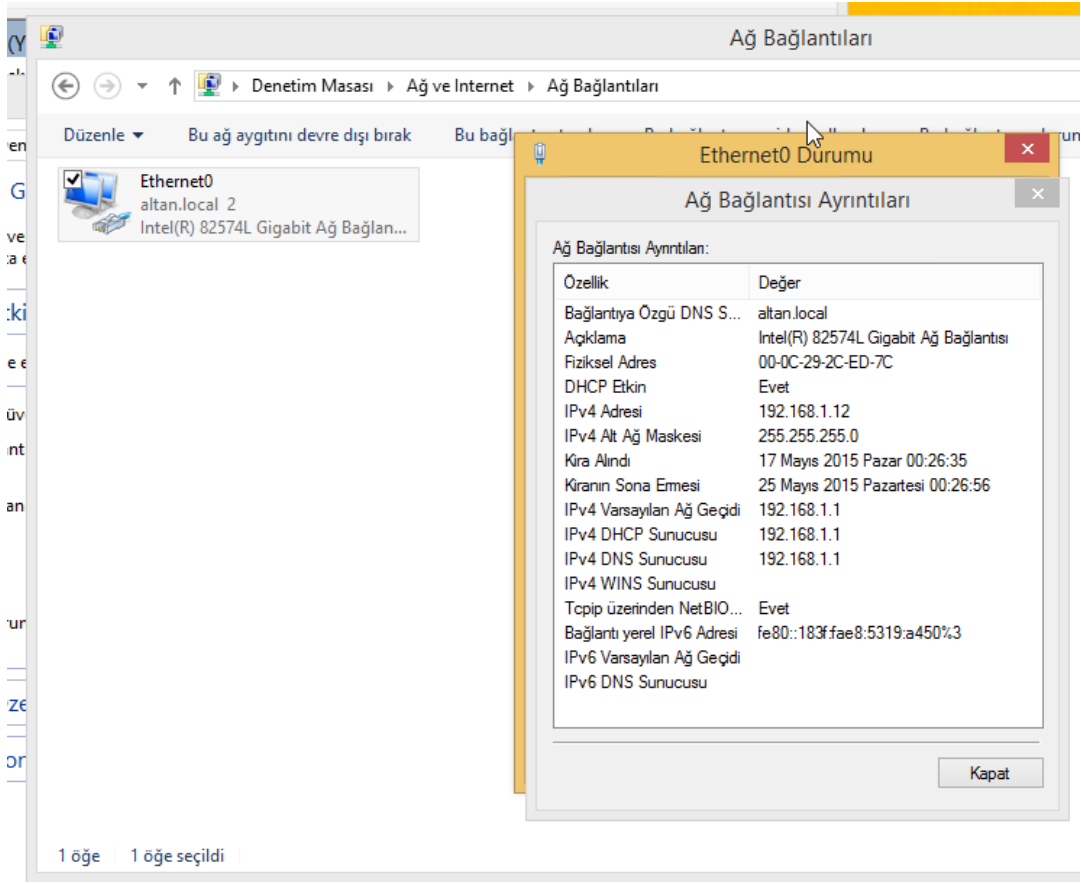


WINDOWS 8.1 CLIENT01DE DOMAINDE OTURUM AÇIYORUZ. VE IP KONFIGURASYONUMUZU KONTROL EDİYORUZ. AYARLARIMIZIN AYNI OLDUĞU GÖRÜLECEKTİR. GPUPDATE /FORCE KOMUTUNU ÇALIŞTIRIP PCYİ YENİDEN BAŞLATIYORUZ.

HALA AYNI AYARLARI GÖRÜYORSAK :

CMD > SERVICES.MSC KOMUTUYLA HİZMETLERE **NETWORK ACCESS PROTECTION AGENT** SERVİSİNİ KONTROL EDİYORUZ. EĞER SERVİS OTOMATİK VE ÇALIŞIYOR OLARAK GÖRÜNÜYORSA GPOYU ALMIŞ DEMEKTİR. ETHERNET KARTIMIZI DEVRE DIŞI BIRAKIP TEKRAR AKTİF EDİYORUZ. HALA AYNI AYARLARI GÖRÜYORSAK :





KONFIGURASYONUMUZ DOĞRU OLARAK AYARLANDI.

ŞİMDİ PC ÜZERİNDE NAP AGENTİMİZİN DOĞRU ÇALIŞIP ÇALIŞMADIĞINI KONTROL EDECEĞİZ.

WINDOWS FIREWALLI DEVRE DIŞI BIRAKIP OTOMATİK OLARAK AKTİF HALE GELİYORSA YAPILANDIRMAMIZ SORUNSUZ DEMEKTİR.

Ayarları Özelleştir

Denetim Masası > Tüm Denetim Masası Öğeleri > Windows Güvenlik Duvarı > Ayarları Özelleştir

Her ağ türü için ayarları özelleştir

Kullandığınız her ağ türü için güvenlik duvarı ayarlarını değiştirebilirsiniz.

Etki alanı ağ ayarları

- ☒ Windows Güvenlik Duvarı'nı aç
- ☐ İzin verilen uygulamalar listesindekiler de dahil gelen tüm bağlantıları engelle
- ☒ Windows Güvenlik Duvarı yeni bir uygulamayı engellediğinde bana bildir
- ☒ Windows Güvenlik Duvarı'nı kapat (önerilmez)

Özel ağ ayarları

- ☒ Windows Güvenlik Duvarı'nı aç
- ☐ İzin verilen uygulamalar listesindekiler de dahil gelen tüm bağlantıları engelle
- ☒ Windows Güvenlik Duvarı yeni bir uygulamayı engellediğinde bana bildir
- ☒ Windows Güvenlik Duvarı'nı kapat (önerilmez)

Ortak ağ ayarları

- ☒ Windows Güvenlik Duvarı'nı aç
- ☐ İzin verilen uygulamalar listesindekiler de dahil gelen tüm bağlantıları engelle
- ☒ Windows Güvenlik Duvarı yeni bir uygulamayı engellediğinde bana bildir
- ☒ Windows Güvenlik Duvarı'nı kapat (önerilmez)

Tamam

İptal

Windows Güvenlik Duvarı

Denetim Masası > Tüm Denetim Masası Öğeleri > Windows Güvenlik Duvarı

Denetim Masası Giriş

Bir uygulamanın veya özelliğin Windows Güvenlik Duvarını geçmesine izin ver

Bildirim ayarlarını değiştir

Windows Güvenlik Duvarı'nı etkinleştir veya devre dışı bırak

Varsayılanları geri yükle

Gelişmiş ayarlar

Ağımda sorun gider

Windows Güvenlik Duvarı ile kişisel bilgisayarınızın korunmasına yardımcı olun

Windows Güvenlik Duvarı, korsanların veya kötü amaçlı yazılımların İnternet veya ağ üzerinden kişisel bilgisayarınıza erişmesini engellemeye yardımcı olabilir.

Etki alanı ağları		Bağlandı
Bir iş yerinde etki alanına bağlanmış ağlar		
Windows Güvenlik Duvarı durumu:	Açık	
Gelen bağlantılar:	İzin verilen uygulamalar listesinde olmayan uygulamalara yönelik tüm bağlantıları engelle	
Etkin etki alanı ağları:	<div>altan.local 2</div> <div>altan.local 2</div> <div>altan.local 2</div>	
Bildirim durumu:	Windows Güvenlik Duvarı yeni bir uygulamayı engellediğinde bana bildir	
Özel ağlar		Bağlı değil
Konuk ağları veya ortak ağlar		Bağlı değil

Ayrıca bkz.

Windows Güvenlik Duvarı

Denetim Masası > Tüm Denetim Masası Öğeleri > Windows Güvenlik Duvarı

Denet

Denetim Masası Giriş

Bir uygulamanın veya özelliğin
Windows Güvenlik Duvarını
geçmesine izin ver

Bildirim ayarlarını değiştir

Windows Güvenlik Duvarı'nı
etkinleştir veya devre dışı bırak

Arsayılanları geri yükle

Gelişmiş ayarlar

Ağımda sorun gider

Ayrıca bkz.

Sistem Merkezi

Ağ ve Paylaşım Merkezi

Windows Güvenlik Duvarı ile kişisel bilgisayarınızın korunmasına yardımcı olun

Windows Güvenlik Duvarı, korsanların veya kötü amaçlı yazılımların İnternet veya ağ üzerinden kişisel bilgisayarınıza erişmesini engellemeye yardımcı olabilir.

Güvenlik duvarı ayarlarınızı güncelleyin

Windows Güvenlik Duvarı bilgisayarınızı korumak
için önerilen ayarları kullanmıyor.

Önerilen ayarlar nelerdir?

Önerilen ayarları kullan

Etki alanı ağları

Bağlandı

Bir iş yerinde etki alanına bağlanmış ağlar

Windows Güvenlik Duvarı durumu:

Kapalı

Gelen bağlantılar:

İzin verilen uygulamalar listesinde olmayan uygulamalara yönelik tüm bağlantıları engelle

Etkin etki alanı ağları:

altan.local 2

altan.local 2

altan.local 2

Bildirim durumu:

Windows Güvenlik Duvarı yeni bir uygulamayı engellediğinde bana bildir

Özel ağlar

Bağlı değil

Konuk ağları veya ortak ağlar

Bağlı değil

Windows Güvenlik Duvarı

Denetim Masası > Tüm Denetim Masası Öğeleri > Windows Güvenlik Duvarı

D

Denetim Masası Giriş

Bir uygulamanın veya özelliğin
Windows Güvenlik Duvarını
geçmesine izin ver

Bildirim ayarlarını değiştir

Windows Güvenlik Duvarı'nı
etkinleştir veya devre dışı bırak

Arsayılanları geri yükle

Gelişmiş ayarlar

Ağımda sorun gider

Ayrıca bkz.

Sistem Merkezi

Ağ ve Paylaşım Merkezi

Windows Güvenlik Duvarı ile kişisel bilgisayarınızın korunmasına yardımcı olun

Windows Güvenlik Duvarı, korsanların veya kötü amaçlı yazılımların İnternet veya ağ üzerinden kişisel bilgisayarınıza erişmesini engellemeye yardımcı olabilir.

Etki alanı ağları

Bağlandı

Bir iş yerinde etki alanına bağlanmış ağlar

Windows Güvenlik Duvarı durumu:

Açık

Gelen bağlantılar:

İzin verilen uygulamalar listesinde olmayan uygulamalara yönelik tüm bağlantıları engelle

Etkin etki alanı ağları:

altan.local 2

altan.local 2

altan.local 2

Bildirim durumu:

Windows Güvenlik Duvarı yeni bir uygulamayı engellediğinde bana bildir

Özel ağlar

Bağlı değil

Konuk ağları veya ortak ağlar

Bağlı değil