

NAP DHCP CONFIGURATION

SERVER 2012

NAP DHCP

One of the services that can be well-integrated with NAP is DHCP. If the client trying to receive an IP address does not pass the health validation check, it is not allowed to receive an IP address and therefore is not able to connect to the network.

Of course one of the disadvantages of using DHCP integrated with NAP is that it could be easily bypassed if the client avoided using a dynamic IP address configuration and the user set its IP address manually and joined the network.

- NPS (Local)
- ▷ RADIUS Clients and Servers
- ▷ Policies
- ▷ Network Access Protection
- ▷ Accounting
- ▷ Templates Management

NPS (Local)

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



Select Network Connection Method For Use with NAP

Network connection method:

Select the network connection method that you want to deploy on your network for NAP-capable client computers. Created policies will work with this network connection type only. To create policies for additional network connection methods, you can run the wizard again.

Dynamic Host Configuration Protocol (DHCP) ▾

Policy name:

This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it.

NAP DHCP

Additional requirements:

You must perform additional actions to set up NAP. View additional NAP requirements by clicking on the link below.

[Additional Requirements](#)

Previous

Next

Finish

Cancel



Specify NAP Enforcement Servers Running DHCP Server

RADIUS clients are network access servers, not client computers. If the local computer is running DHCP Server, you can skip this step and click Next.

If you want to add remote DHCP servers as RADIUS clients, click Add. All remote DHCP servers that you add must also run NPS. Also, remote DHCP/NPS servers must forward connection requests to this NPS server (the local computer).

RADIUS clients:

RadiusClient1
radius server2
classtemplateclient
dhcp Server (1)

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

New RADIUS Client



Settings

Select an existing template:

template3

Name and Address

Friendly name:

dhcp Server (1)

Address (IP or DNS):

10.10.10.7

Verify...

Shared Secret

Select an existing Shared Secrets template:

secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual

Generate

Shared secret:

••••••••

Confirm shared secret:

••••••••

OK

Cancel

Configure NAP



Specify DHCP Scopes

When you specify one or more NAP-enabled scopes, NPS evaluates client health and performs authorization for client computers requesting an IP address from the designated scopes.

If you do not specify any scopes, the policy applies to all NAP-enabled scopes at the selected DHCP servers. If you specify a scope that is not NAP-enabled, you must enable NAP for the scope after completing this wizard.

To specify one or more scopes, click Add.

DHCP scopes:

Add...

Edit...

Remove

MS-Service Class



Specify the profile name that identifies your DHCP scope.

OK

Cancel

Previous

Next

Finish

Cancel



Specify DHCP Scopes

When you specify one or more NAP-enabled scopes, NPS evaluates client health and performs authorization for client computers requesting an IP address from the designated scopes.

If you do not specify any scopes, the policy applies to all NAP-enabled scopes at the selected DHCP servers. If you specify a scope that is not NAP-enabled, you must enable NAP for the scope after completing this wizard.

To specify one or more scopes, click **Add**.

DHCP scopes:

scope1

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

Configure NAP



Configure Machine Groups

To grant or deny access to groups of computers, add groups to Machine Groups.

If no groups are selected, this policy applies to all users.

Machine Groups:

Add...

Remove

Previous

Next

Finish

Cancel

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.

<none>



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://

Previous

Next

Finish

on, and connection request authorization.

before they connect to your network. Clients that are not compliant with

New Remediation Server Group



Select an existing template:

Dropdown menu

Group Name:

remediation group1

Remediation Servers:

DNS Name / IP Address	Friendly Name
10.10.10.9	Rem server

Add...

Edit...

Remove

OK

Cancel



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.

remediation group 1

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://



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

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



Completing NAP Enforcement Policy and RADIUS Client Configuration

You have successfully created the following policies and configured the following RADIUS clients.

- To view the configuration details in your default browser, click Configuration Details.
- To change the configuration, click Previous.
- To save the configuration and close this wizard, click Finish.

RADIUS clients:

dhcp Server (1) (10.10.10.7)

Health Policies:

NAP DHCP Compliant

NAP DHCP Noncompliant

Connection Request Policy:

NAP DHCP

Network Policies:

NAP DHCP Compliant

NAP DHCP Noncompliant

NAP DHCP Non NAP-Capable

Remediation Server Group:

remediation group 1

[Configuration Details](#)

Previous

Next

Finish

Cancel