Progress®
Kemp® LoadMaster®

Technical Note RADIUS Authentication and Authorization

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 4

Document Purpose 4

Intended Audience 5

Chapter 2: Prerequisites for Authentication and Authorization 6

Add a RADIUS Client 6

Chapter 3: Configure Authentication and Authorization 9

Local Authentication and Authorization 10

Specify the RADIUS Server Details 10

Specifying RADIUS Authentication for an Individual User 10

Specifying Local Authorization for an Individual User 11

RADIUS Authentication and Authorization 13

Specify the RADIUS Server Details 13

Specifying RADIUS permissions for Groups and All Users 16

Chapter 4: References 43

1

Introduction

The Remote Access Dial In User Service (RADIUS) server can be used to authenticate users who log in to the LoadMaster. The LoadMaster passes the user's details to the RADIUS server and the RADIUS server informs the LoadMaster whether the user is authenticated or not.

RADIUS in Windows Server 2008 R2 is done with network policy and access services.

Note: The steps in this document have been tested and validated on Windows Server 2008 R2.

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience

Document Purpose

The purpose of this document is to provide further information and steps on configuring RADIUS authentication and authorization.

Intended Audience

This document is intended to be used by anyone who is interested in learning more about using RADIUS authentication and authorization in the LoadMaster.

2

Prerequisites for Authentication and Authorization

Before performing these steps, ensure there is an Active Directory group to add to the network policy. This needs to be done on the domain controller.

The steps in this document outline how to give the users/groups certain permissions to the LoadMaster.

Note: It is not possible to use RADIUS authentication and authorization if you are using a FIPS LoadMaster.

Related Links

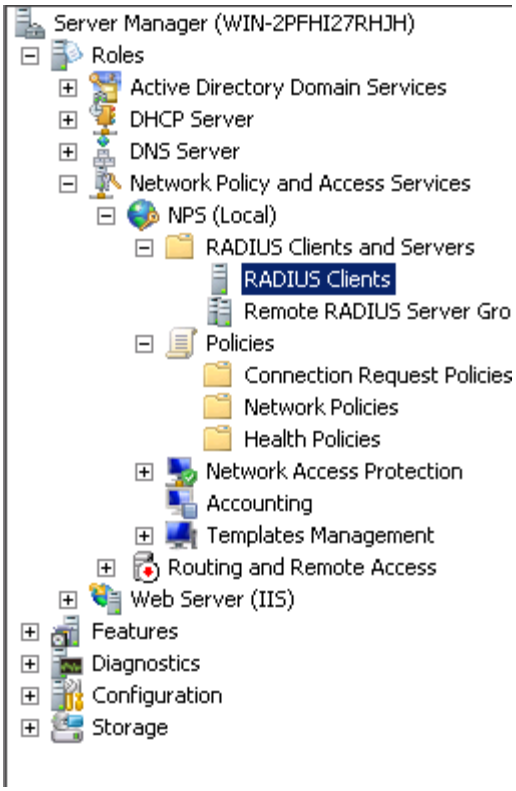
For details, see the following topics:

- Add a RADIUS Client

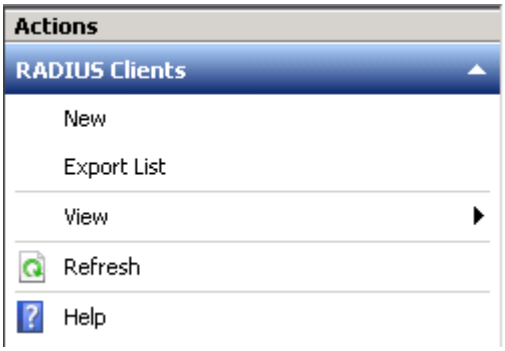
Add a RADIUS Client

A RADIUS client needs to be created so that the LoadMaster can authenticate. Create a RADIUS client by following the steps below:

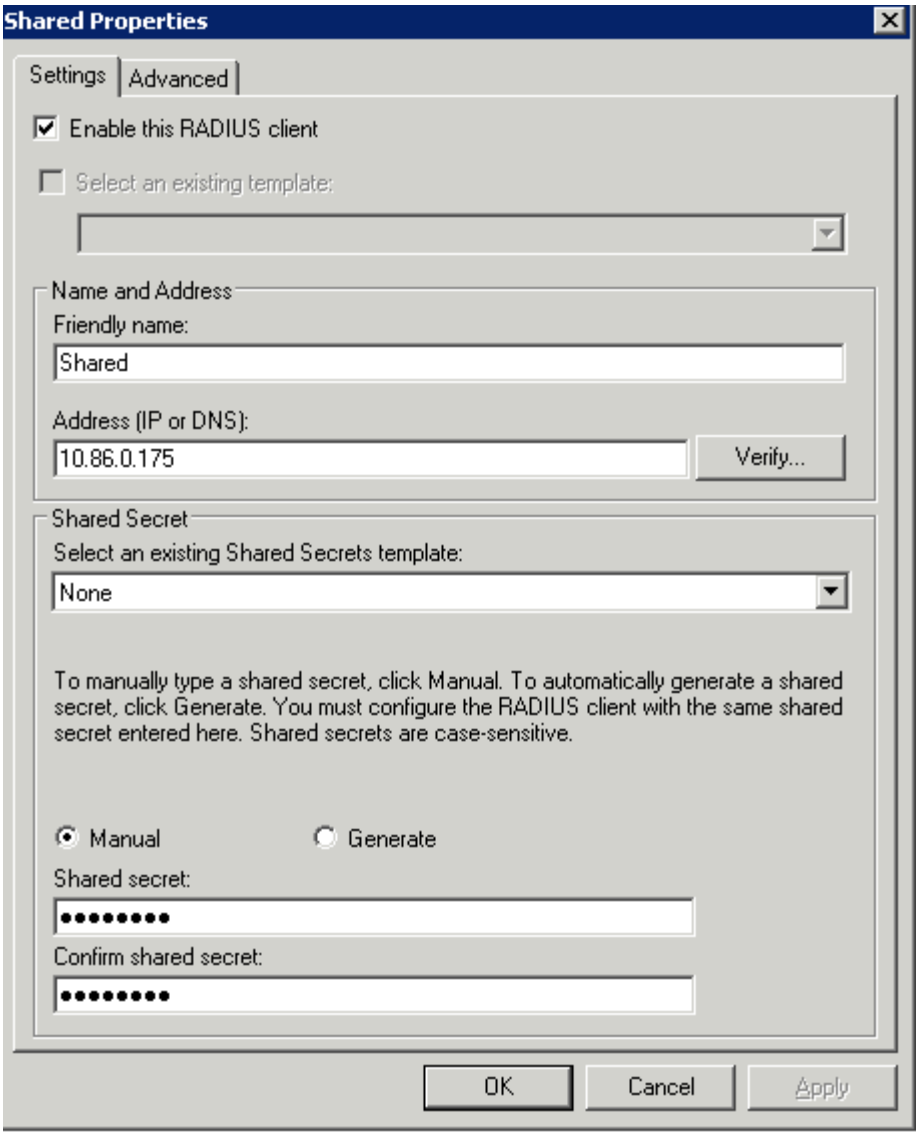
1. Open the **Server Manager** application.



2. Navigate to the following option: **Roles > Network Policy and Access Services > NPS (Local) > RADIUS Clients and Servers > RADIUS Clients**.



3. Click **New** in the panel on the right.



4. Enter a **Friendly name**.
5. Enter the IP **Address** of the LoadMaster.

Note: If using a High Availability (HA) pair, add all three IP addresses (unit 1, unit 2 and the shared IP address).

---

6. Enter a **Shared secret**.

Note: The **Shared secret** has a 48-character limit.

---

7. Enter the same shared secret in the **Confirm shared secret** text box and click **OK**.
8. When the LoadMaster contacts the RADIUS server, it uses the active physical interface. Therefore, two RADIUS clients must also be configured in addition to the shared address. Follow the steps above (using a different IP address) to create the additional RADIUS clients.

3

Configure Authentication and Authorization

LoadMaster allows the users to be authorized by either RADIUS or Local User authorization. The user's authorization decides what level of permissions the user has and what functions on the LoadMaster they are allowed to perform.

When both authorization methods are selected, the LoadMaster initially attempts to authorize the user using RADIUS. If this authorization method is not available, the LoadMaster attempts to authorize the user using the Local User authorization.

In addition to configuring RADIUS authentication in the Server Manager, the LoadMaster also needs to be configured to use it. Configuration of RADIUS authentication in the LoadMaster varies depending on what method you want to use:

- **Local Authentication and Authorization** means that the LoadMaster contacts the RADIUS server for authentication and will use local authorization.
- **RADIUS Authentication and Authorization** means that the LoadMaster contacts the RADIUS server for authentication and will use reply messages sent back from the RADIUS server to authorize.

Note: The maximum character length for RADIUS authentication passwords that are used to log in to the Edge Security Pack (ESP) form is 128 alphanumeric characters. If non-alphanumeric or other characters are used that require multi-byte encoding, the maximum number of characters that can be used reduces.

Follow the steps in the relevant section below, depending on the chosen method.

For further details on what each of the LoadMaster fields mean, refer to the Web User Interface,

Configuration Guide.

Related Links

For details, see the following topics:

- Local Authentication and Authorization
- RADIUS Authentication and Authorization

Local Authentication and Authorization

Follow the steps below to configure the local authentication and authorization settings in the LoadMaster.

Note: Session Management must be disabled in order to use this method. If Session Management is enabled, the RADIUS server options mentioned in this section will not be available.

Specify the RADIUS Server Details

To enter the details of the RADIUS server, follow the steps below:

1. In the main menu of the LoadMaster Web User Interface (WUI), navigate to **Certificates & Security > Remote Access**.
2. Enter the IP address of the **Radius Server** and click the **Radius Server** button.

   Note: If you do not see this option, ensure to disable **Session Management** in **Certificates & Security > Admin WUI Access**.

3. Enter the **Shared Secret** and click the **Set Secret** button.

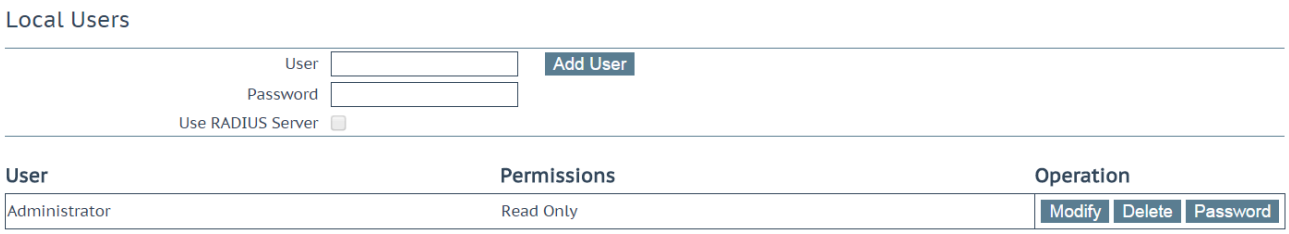
   Note: The **Shared Secret** should be the same as the one entered in the Add a RADIUS Client section.

4. Enter the Revalidation Interval and click Set Interval.

Specifying RADIUS Authentication for an Individual User

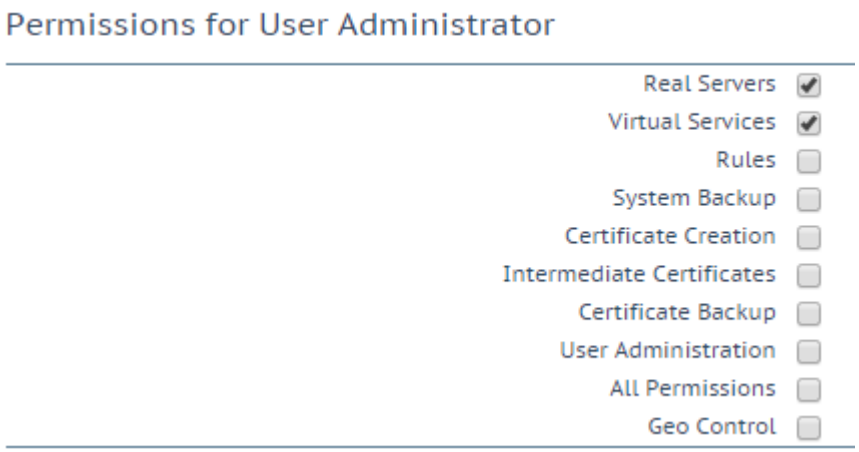
When adding a new user in the **System Configuration** > **System Administration** > **User Management** screen, the **Use RADIUS Server** check box can be selected.

Selecting this check box will mean that RADIUS authentication is used when that user logs in to the LoadMaster. The RADIUS server details must be set up before this option can be used.



Specifying Local Authorization for an Individual User

After a user has been added, you can specify what permissions they have by clicking the **Modify** button in the **Action** column.



The level of user permissions can be set in this screen. This determines what configuration changes the user is allowed to perform. The primary user, bal, always has full permissions. Secondary users may be restricted to certain functions.

There are two permissions relating to Virtual Services - **Virtual Services** and **Add Virtual Services**.

The **Add Virtual Services** permission is only visible when the **Allow Extended Permissions** check box is selected on the **User Management** screen.

The Virtual Service operations allowed differ based on what combination of options you have selected. For a summary of these connotations, refer to the table below:

Allow Extended Permissions	Virtual Services	Add Virtual Service	Operations Allowed	Operations not Allowed
Enabled	Enabled	Disabled	• View existing Virtual Services • Modify existing Virtual Services • Change Virtual Service port	• Add Virtual Service • Duplicate Virtual Service • Change Address • Export template
Enabled	Disabled	Enabled	• View existing Virtual Services	• Add Virtual Service • Duplicate Virtual Service • Change Address

Allow Extended Permissions	Virtual Services	Add Virtual Service	Operations Allowed	Operations not Allowed
				• Export template • Modify existing Virtual Services • Change Virtual Service port
Enabled	Enabled	Enabled	• Add Virtual Service • Duplicate Virtual Service • Change address • Export template • View existing Virtual Services • Modify existing Virtual Services • Change Virtual Service port	Not applicable
Enabled	Disabled	Disabled	View existing Virtual Services	Not applicable
Disabled	Enabled	Disabled	• Add Virtual Service • Duplicate Virtual Service • Change address • Export template • View existing Virtual Services • Modify existing Virtual Services • Change Virtual Service port	Not applicable
Disabled	Disabled	Disabled	View existing Virtual Services	• Add Virtual Service • Duplicate Virtual

Allow Extended Permissions	Virtual Services	Add Virtual Service	Operations Allowed	Operations not Allowed
				Service • Change address • Export template • Modify existing Virtual Service • Change Virtual Service port

RADIUS Authentication and Authorization

This is an alternative option to using local authentication and authorization. In order to use this method, session management must be enabled. Session management settings are configurable in **Certificates & Security > Admin WUI Access**. If session management is disabled, the RADIUS options mentioned in this section will not be available.

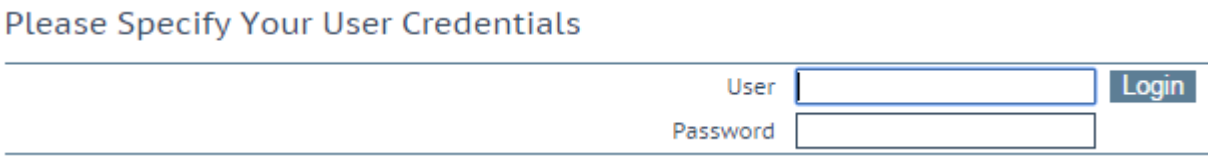
Specify the RADIUS Server Details

To use the RADIUS Authentication and Authorization method, **Session Management** must be enabled. To enable **Session Management**, follow the steps below:

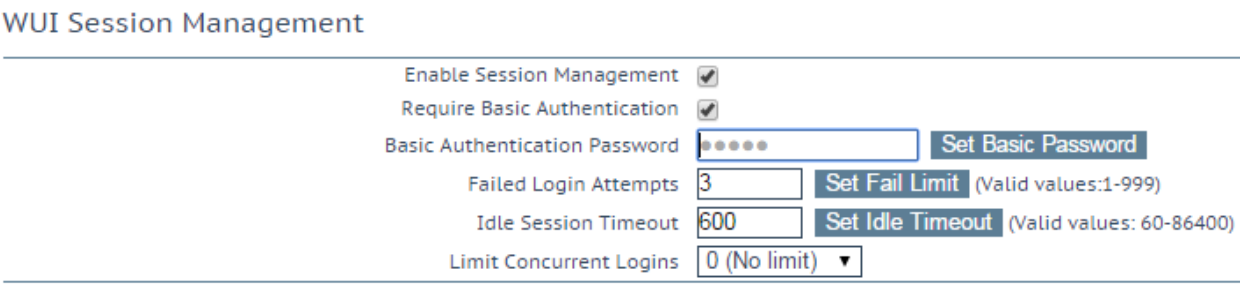
1. In the main menu of the LoadMaster WUI, select **Certificates & Security**.



2. Select the **Enable Session Management** check box.



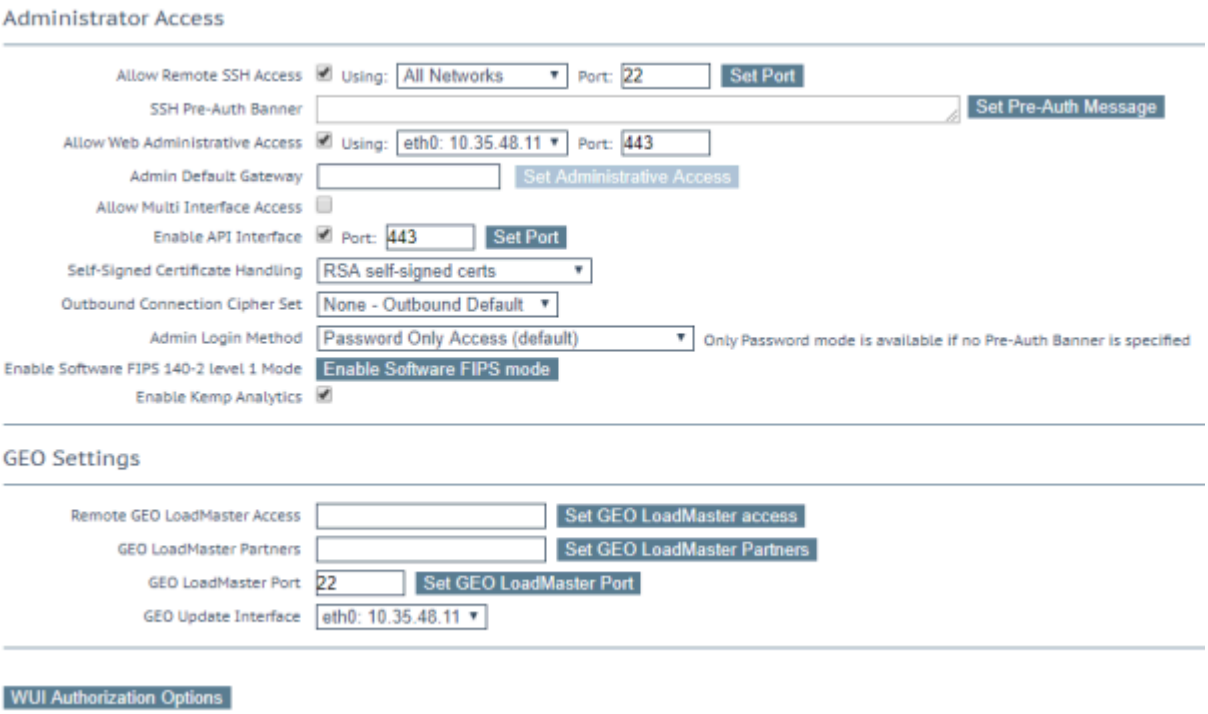
3. Enter **User** and **Password** details and click the **Login** button.



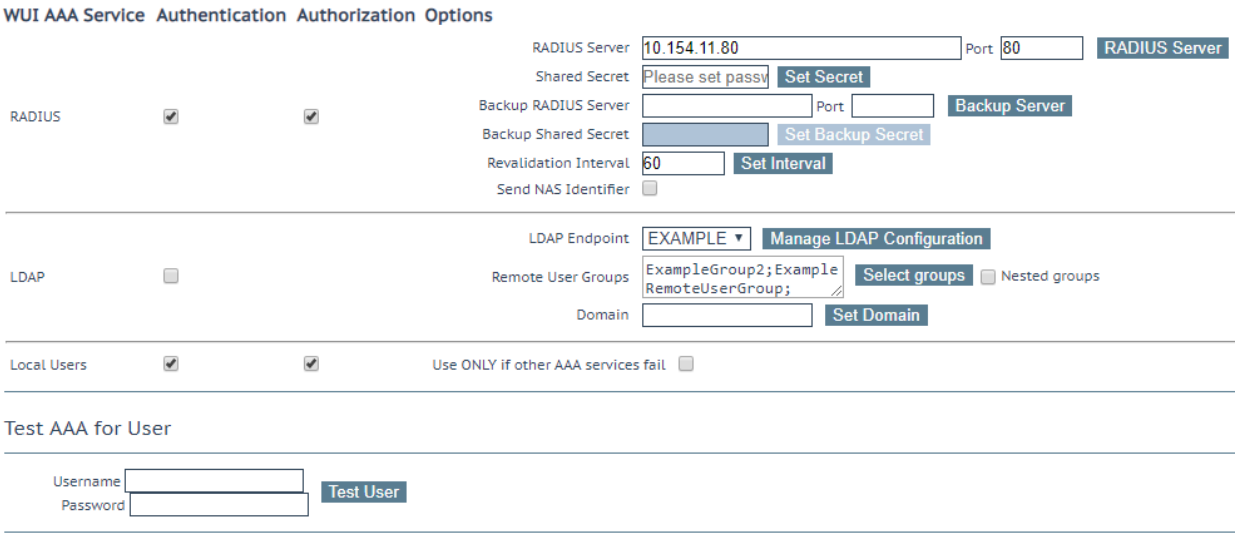
4. In the main menu of the LoadMaster WUI, select **Certificates & Security > Admin WUI Access**.

   When **Session Management** is enabled on the LoadMaster, follow the steps below to configure RADIUS authentication:

5. In the main menu of the LoadMaster WUI, navigate to **Certificates & Security > Remote Access**.



6. Click **WUI Authorization Options**.



7. Enter the **Radius Server** IP address and **Port**.

   Note: IPv6 is not supported for RADIUS authentication.

8. Select the **Radius Authentication** check box.
9. Select the **Radius Authorization** check box.
10. Click **Radius Server**.
11. Enter the **Shared Secret**.

    Note: The **Shared Secret** should be the same as the one entered during the Add a RADIUS Client section.

12. Click **Set Secret**.
13. If necessary, fill out details for a **Backup Radius Server**.
14. Enter the **Revalidation Interval**.
15. Click the **Set Interval** button.

Note: The RADIUS authorization method can only be used if the RADIUS authentication method is selected.

Note: There is a **Test AAA for User** section at the bottom of this screen. When session management is enabled, you can enter a valid **Username** and **Password** to test.

1. Decide whether or not to enable the **Send NAS Identifier** check box.

   Note: If this check box is disabled (default), a NAS identifier is not sent to the RADIUS server. If it is enabled, a Network Access Server (NAS) identifier string is sent to the RADIUS server. By default, this is the hostname. Alternatively, if a value is specified in the **RADIUS NAS Identifier** text box, this value is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed.

2. If you enabled the **Send NAS Identifier** check box, decide whether or not to specify the **RADIUS NAS Identifier**.

Note: If the **Send NAS Identifier** check box is selected, the **RADIUS NAS Identifier** field is shown. When specified, this value is used as the NAS identifier. Otherwise, the hostname is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed.

3. Decide whether or not to enable the **Send Vendor Specific** check box.

Note: When this is enabled and a user is logging into the LoadMaster UI using RADIUS authentication with Cisco Access Control Server (ACS) or Identity Services Engine (IDE), the LoadMaster sends an Attribute Value Pair (AVP) to the server as part of the login request which contains Progress Kemp's vendor ID. The server can use this AVP upon receipt to identify the LoadMaster device. The format and requirements for this attribute are in Section 5.26 of RFC 2865. The Progress Kemp vendor ID is 12196.

Specifying RADIUS permissions for Groups and All Users

Permissions can be set up to apply to all users, or to groups:

- **Connection request policies:** Sets of conditions and settings that allow network administrators to designate which RADIUS servers perform the authentication and authorization of connection request that the Network Policy Server (NPS) receives from RADIUS clients. Connection request policies can be configured to designate which RADIUS servers are used for RADIUS accounting.
- **Network policies:** Sets of conditions, constraints and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect. When you deploy Network Access Protection (NAP), health policy is added to the network policy configuration so that NPS performs client health checks during the authorization process.

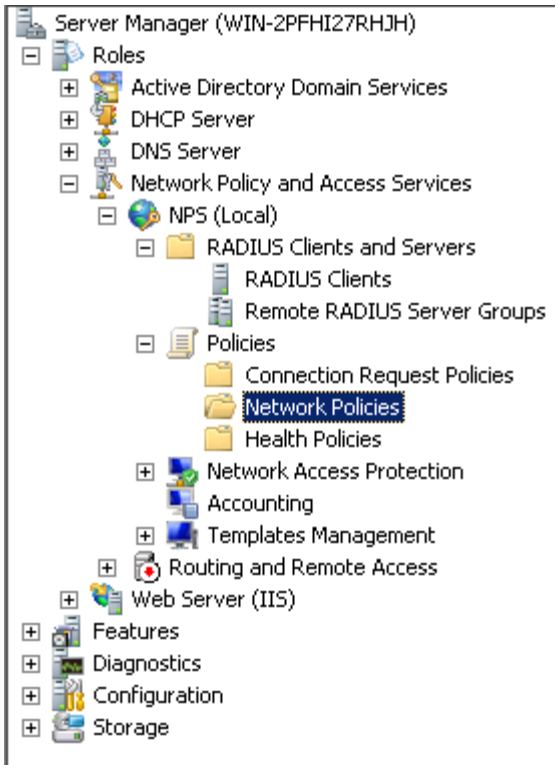
Connection request policies apply to all users. Network policies apply to groups.

Refer to the relevant section below depending on what level of permissions are needed.

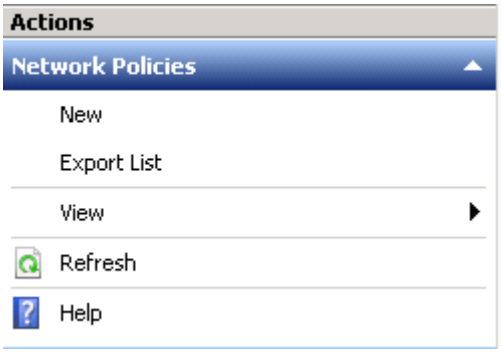
Specifying RADIUS Authentication and Authorization for a Group (Network Request Policy)

Specifying RADIUS Authentication for a Group

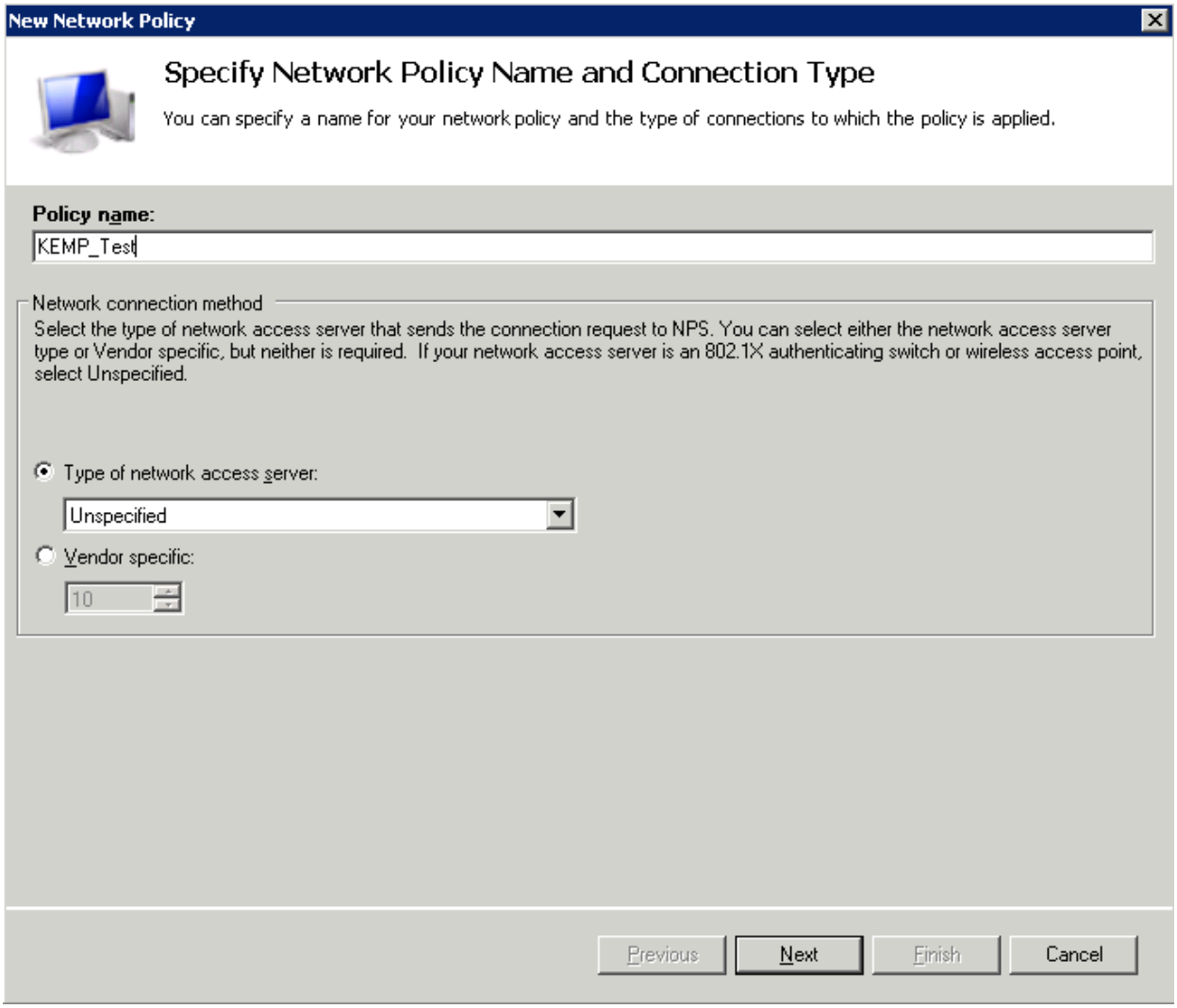
To set up a network policy, follow the steps below in the **Server Manager**.



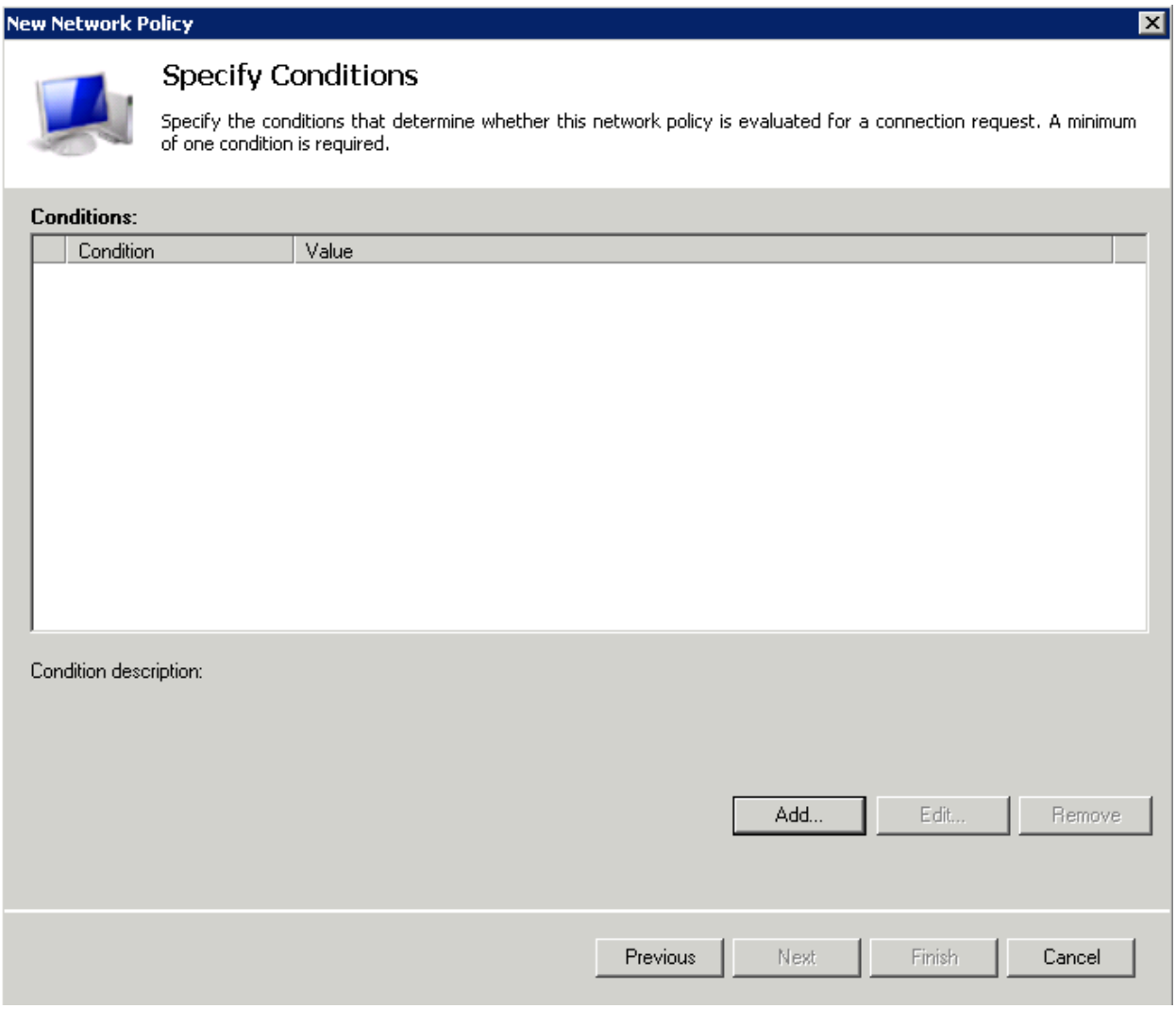
1. In the panel on the left, go to **Policies > Network Policies**.



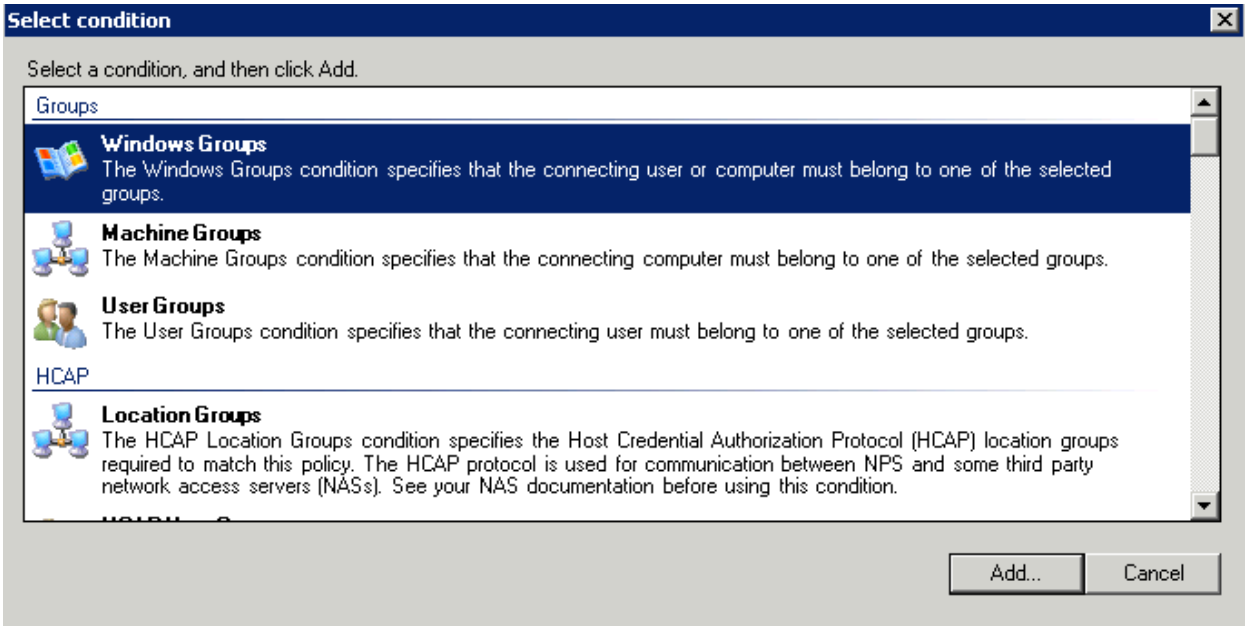
2. Click **New** in the panel on the right.



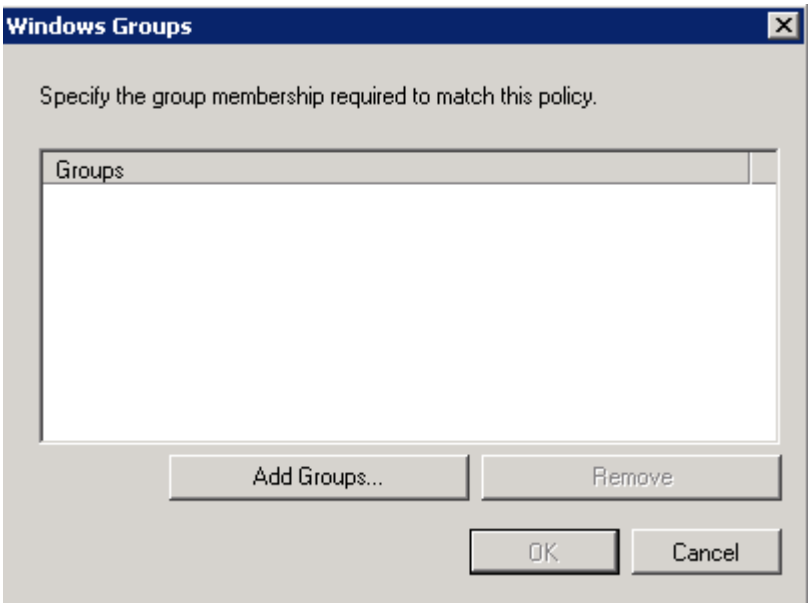
3. Enter a **Policy name**.
4. Click **Next**.



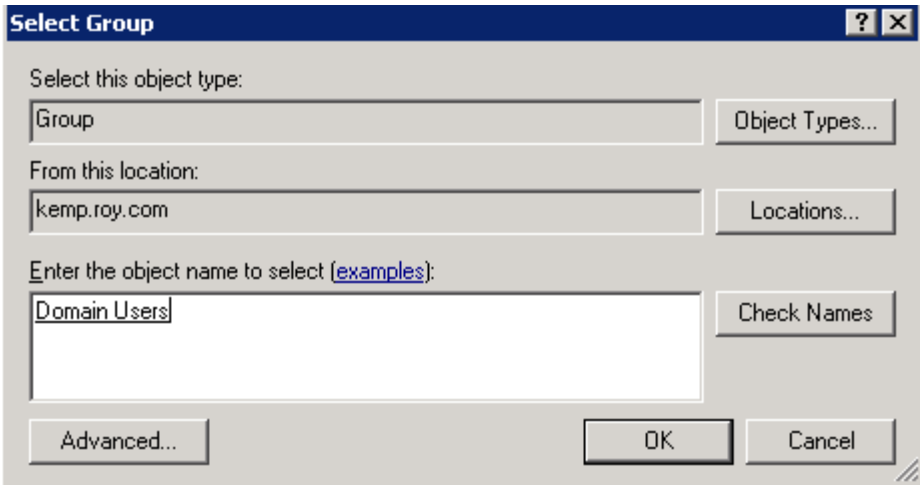
5. Click the **Add…** button.



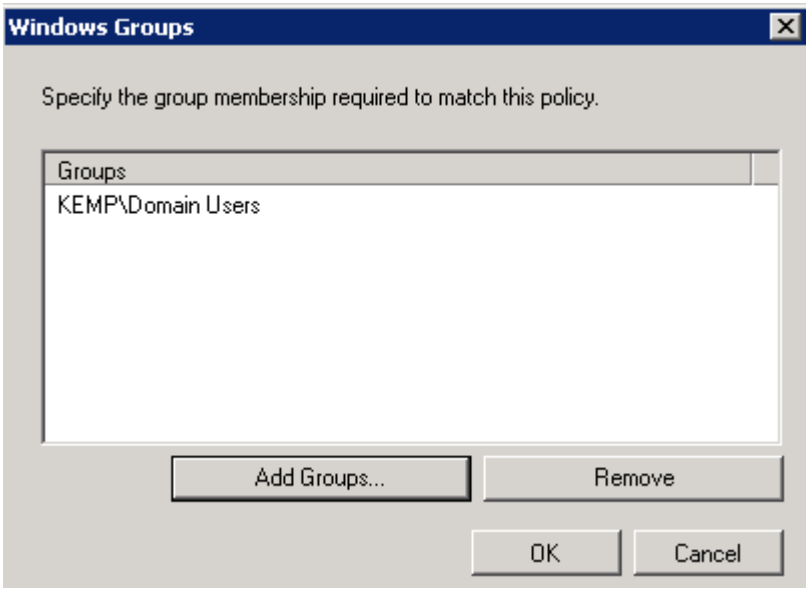
6. Select the relevant group type.
7. Click the **Add…** button.



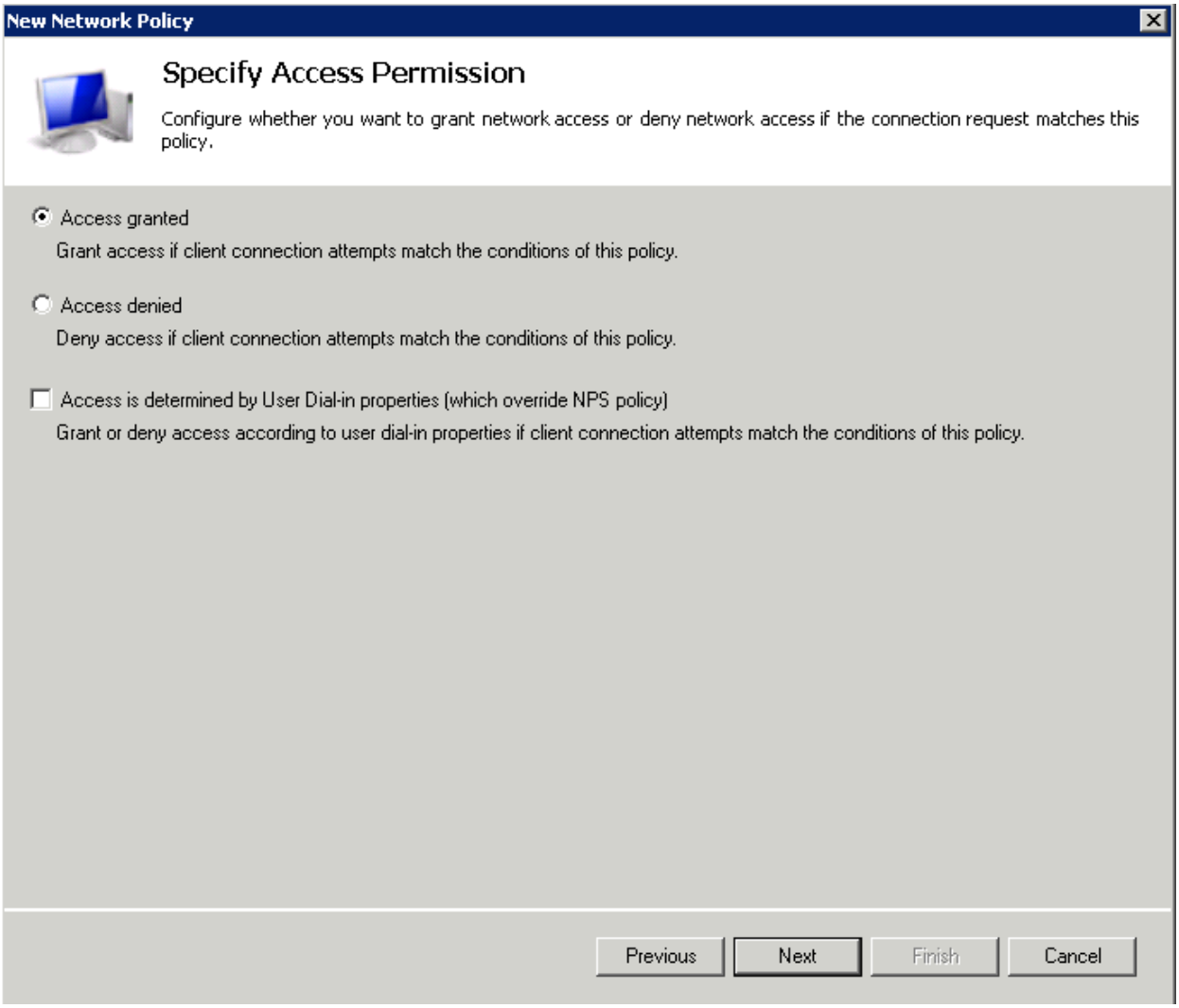
8. Click the **Add Groups…** button.



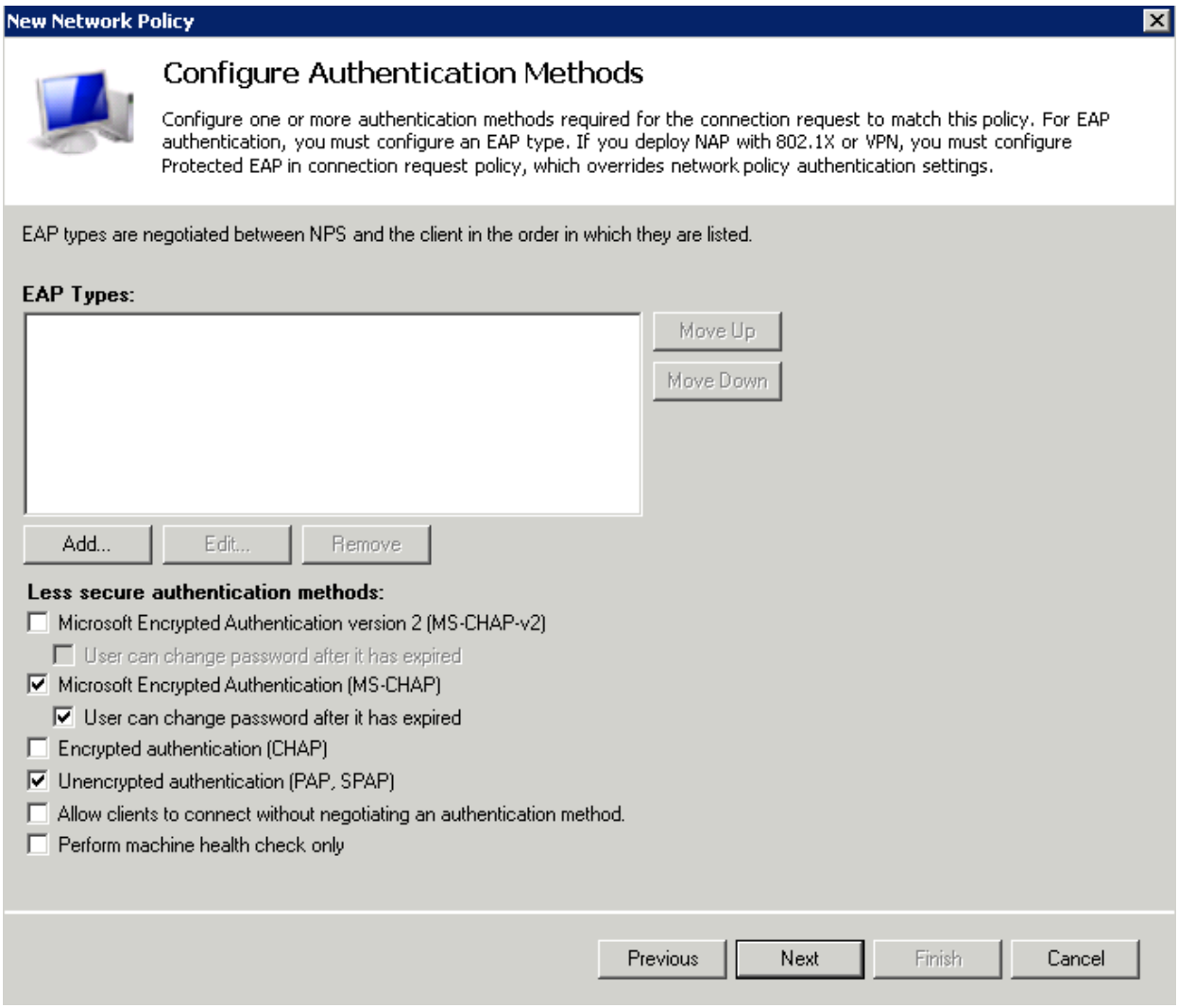
9. Enter the group name in the text area provided.
10. Click **Check Names**.
11. If the name is alright, click **OK**.



12. Click **OK**.
13. Click **Next**.

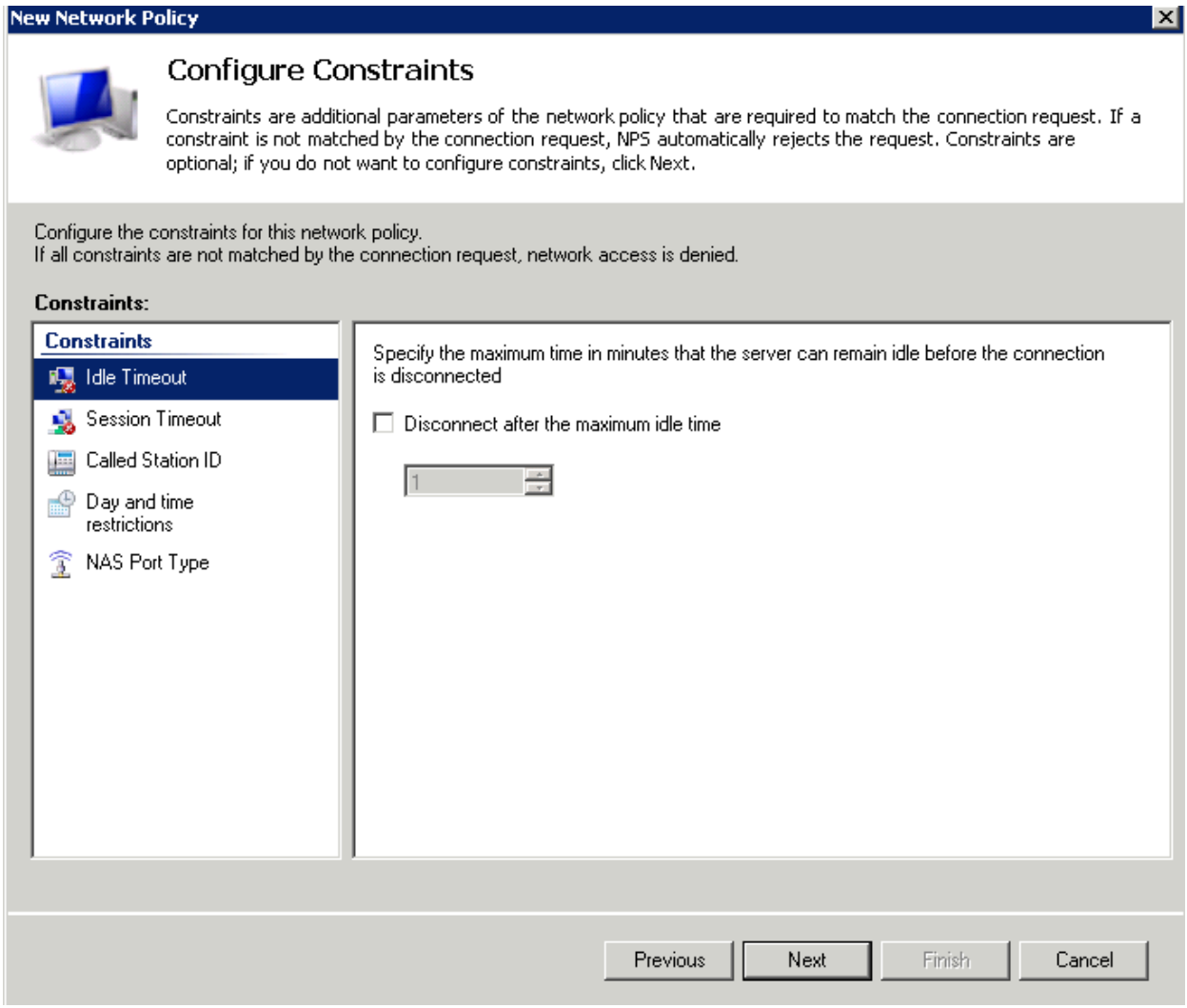


14. Select the relevant Access Permission option.
15. Click **Next**.



16. Remove the tick from the **Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)** check box.
17. Ensure that **Microsoft Encrypted Authentication (MS-CHAP)** is selected.
18. Ensure that **User can change password after it has expired** is selected.
19. Select the **Unencrypted authentication (PAP, SPAP)** check box.
20. Click **Next**.

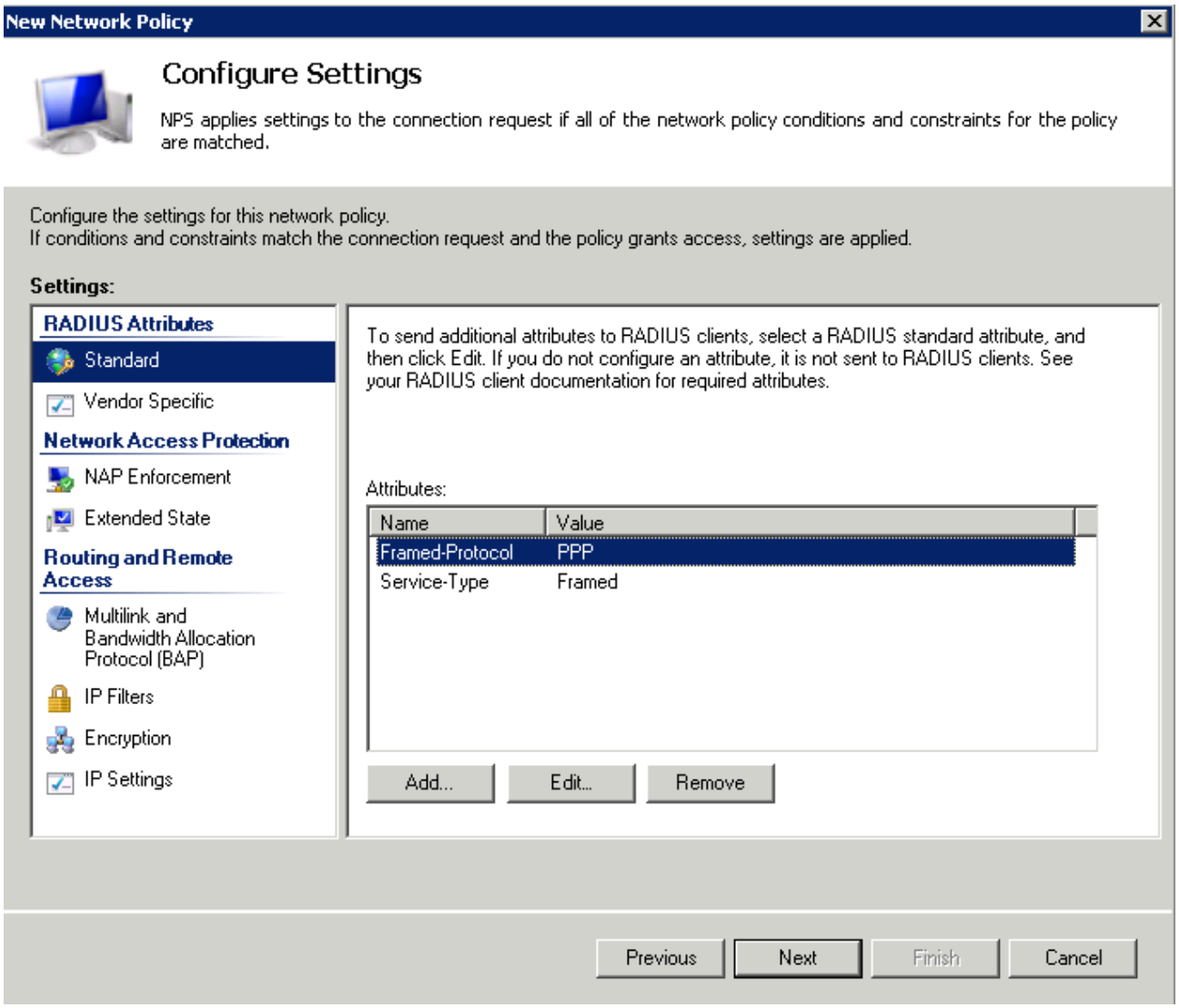
Note: If idle timeout is used on the server it should match the idle timeout settings in the LoadMaster. Generally, we recommend not setting this on the server.



21. Click **Next**.

Note: The Progress Kemp RADIUS policies should be moved to the top of the policy list on the Windows RADIUS server. The policies are executed in the order they are displayed.

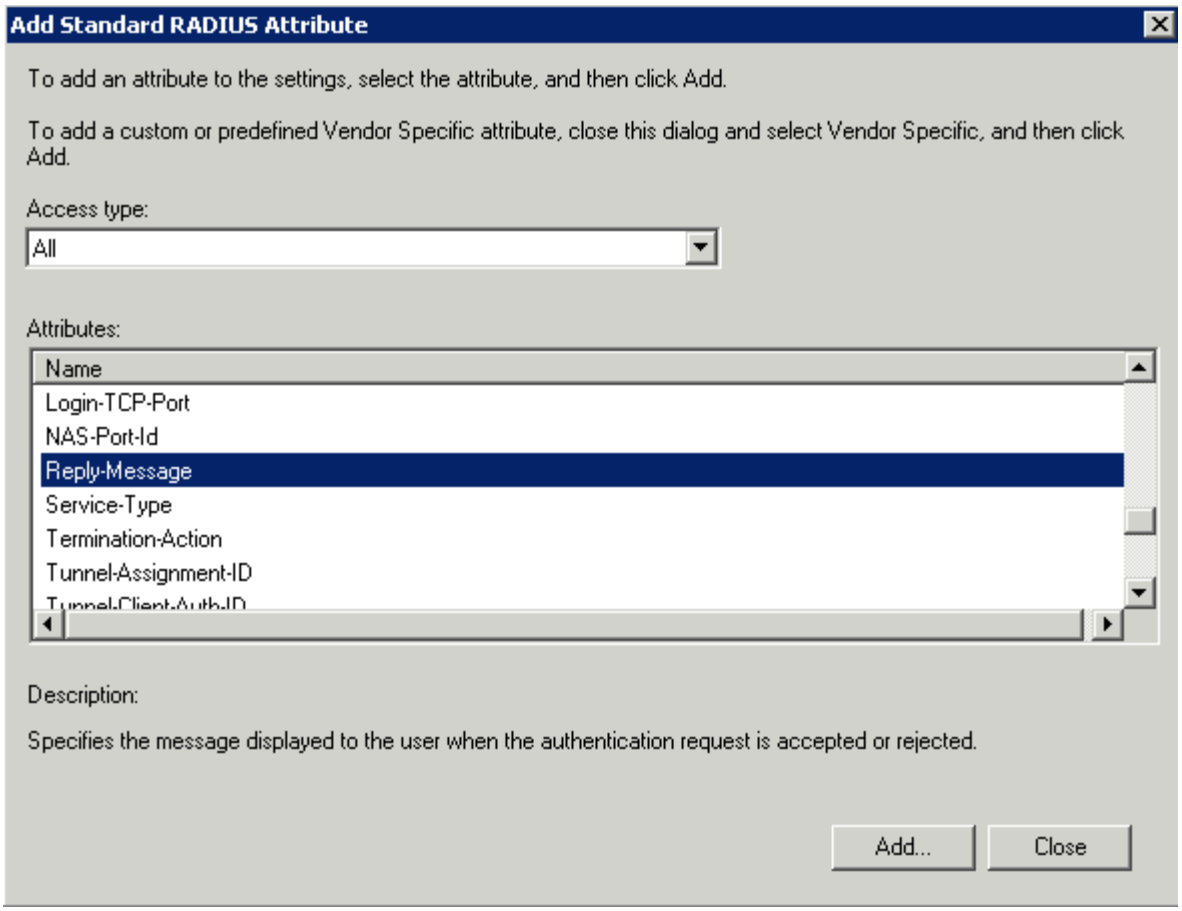
Specify RADIUS Authorization for a Group



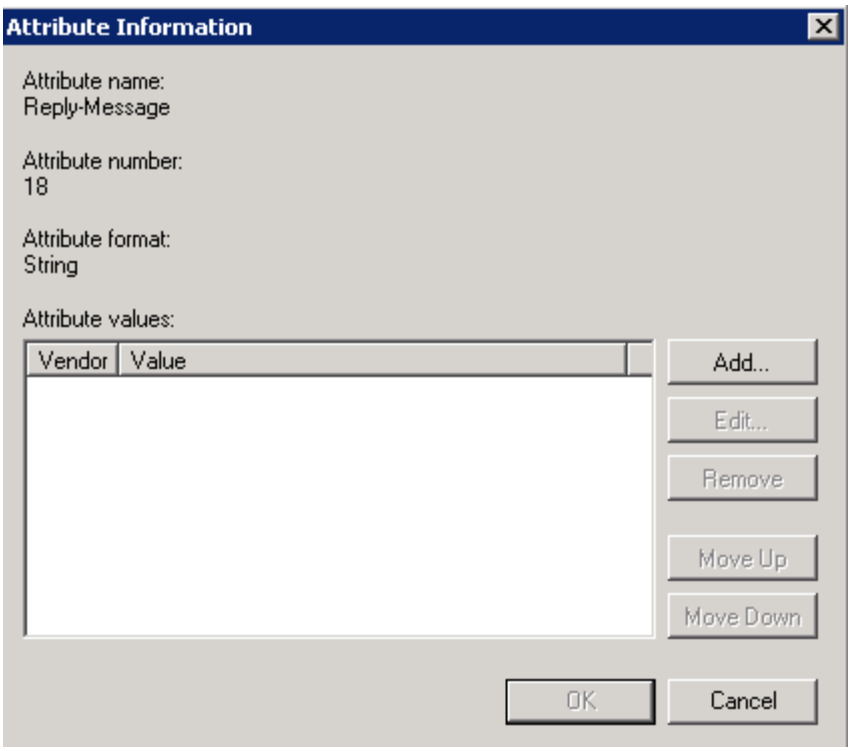
Note: The **Attributes** on this screen need to be in a certain order for the settings to work correctly. The order is as follows: **1. Reply-Message2. Framed-Protocol3. Service-Type**

Note: Unfortunately, these attributes are not movable. So, to order these attributes correctly, you need to **Remove** and then **Add** them.

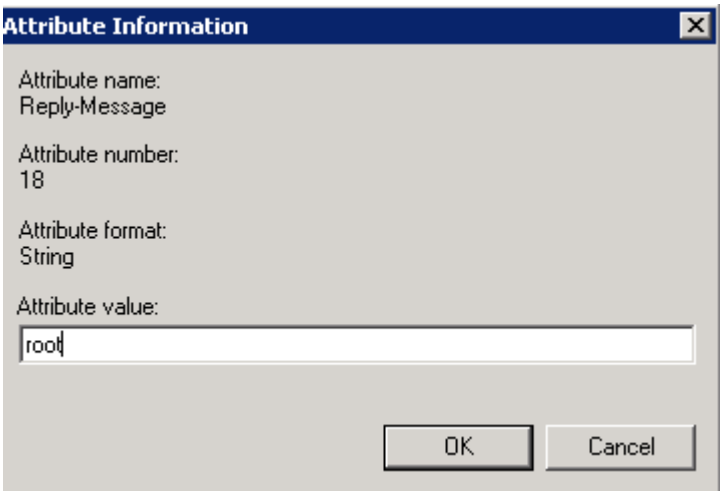
1. Select **Framed-Protocol** and click **Remove**.
2. Select **Service-Type** and click **Remove**.
3. Click the **Add…** button.



4. Select **Reply-Message**.
5. Click the **Add…** button.



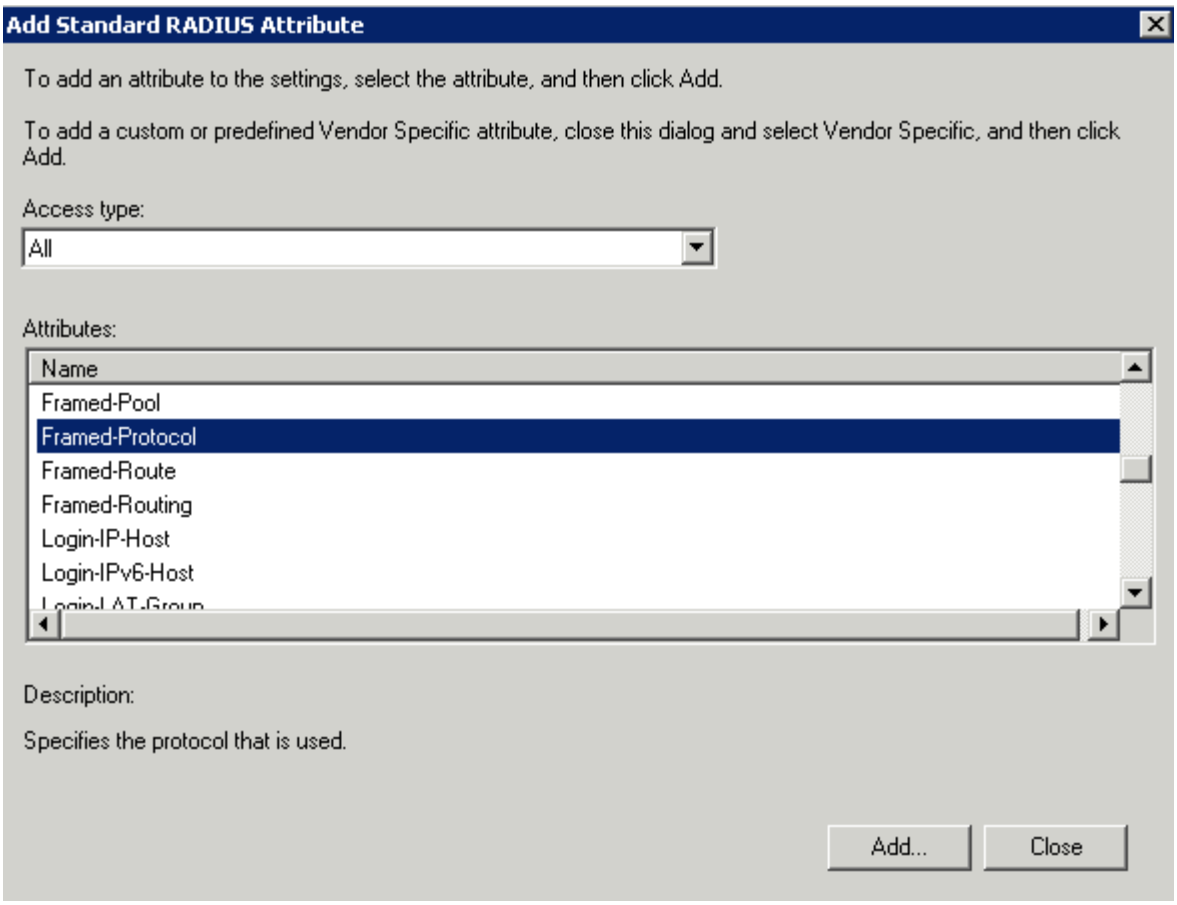
6. Click the **Add…** button.



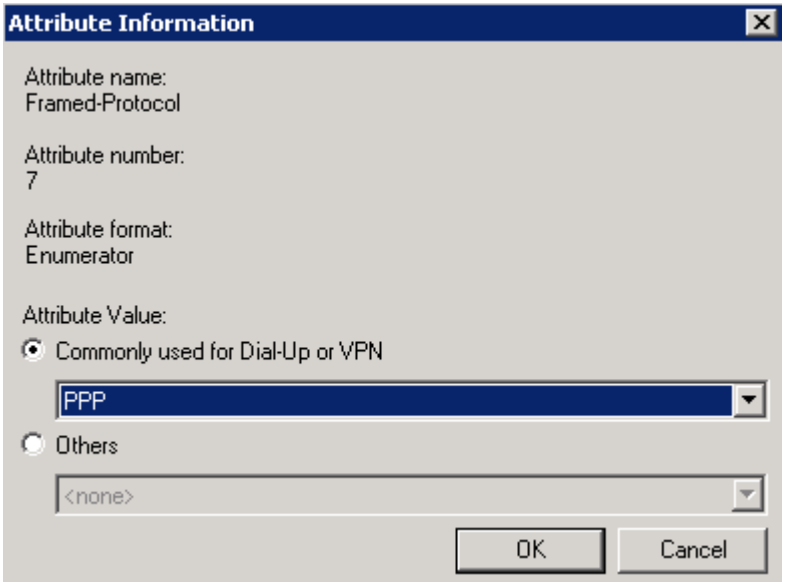
7. Enter the relevant permission option(s) and click **OK**.

Note: The available permission options are as follows:**real,vs,rules,backup,certs,cert3,certbackup,users,root,addvs**These correspond to the permission options in the LoadMaster Web User Interface (WUI). The **root** permission grants all permissions. Multiple attributes can be specified here, but they must be separated by a comma (with no space).

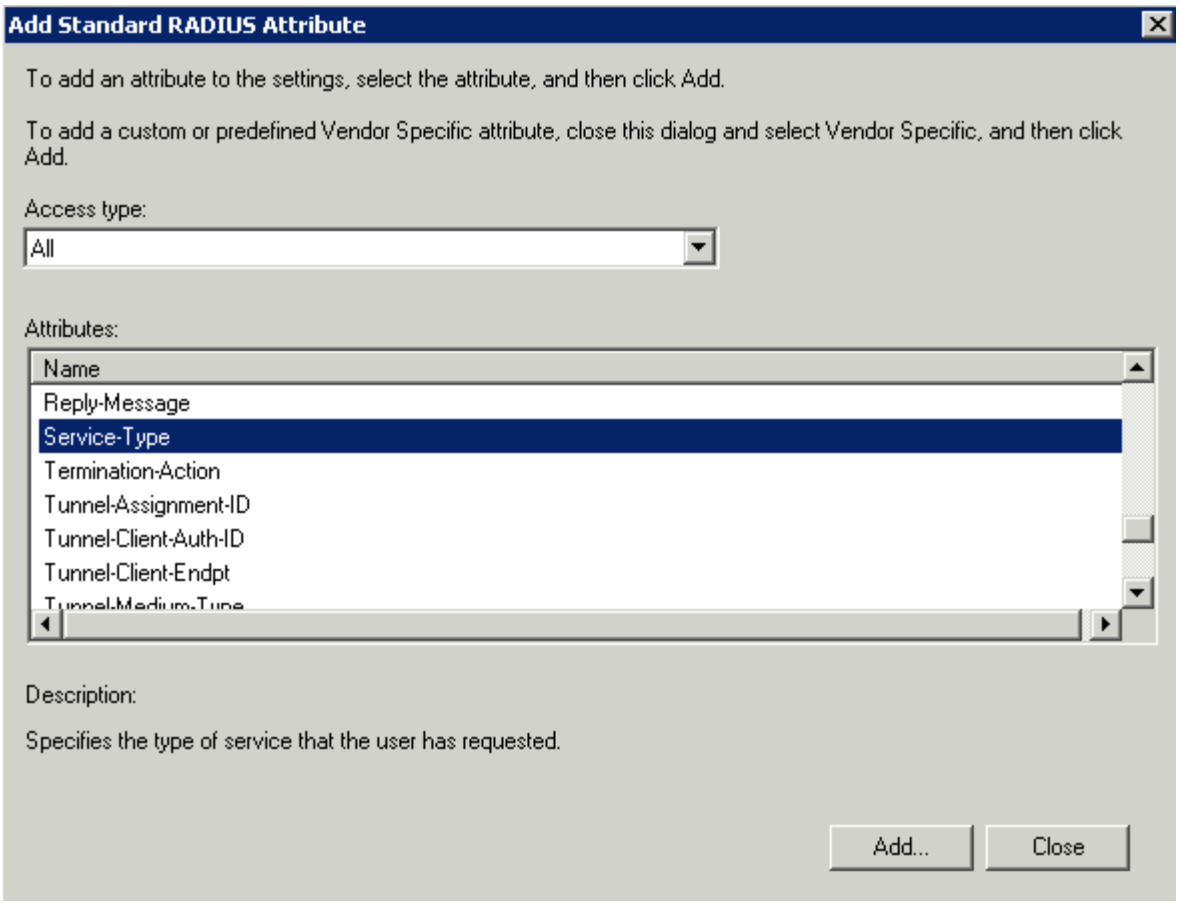
8. Click **OK** again.
9. Select **Framed-Protocol**.



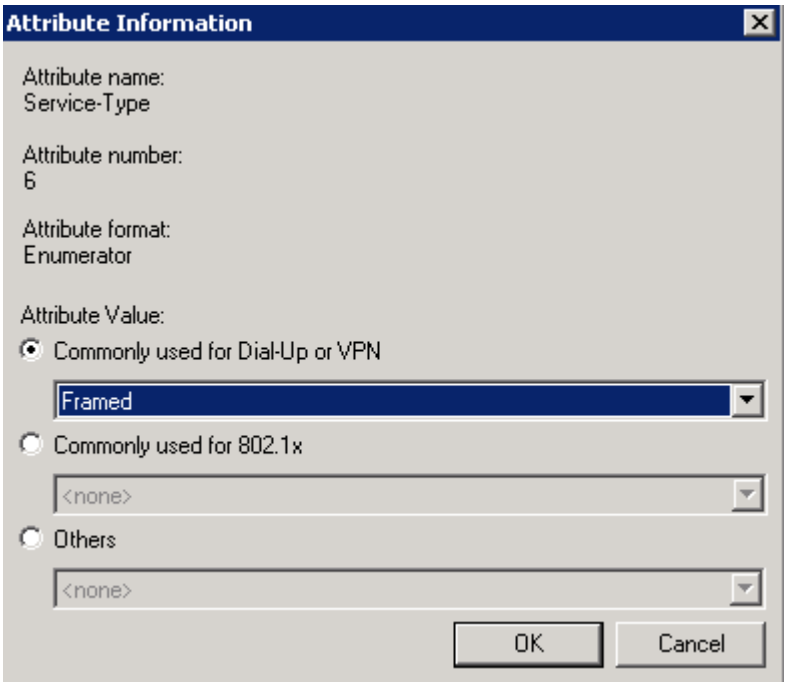
10. Click the **Add…** button.



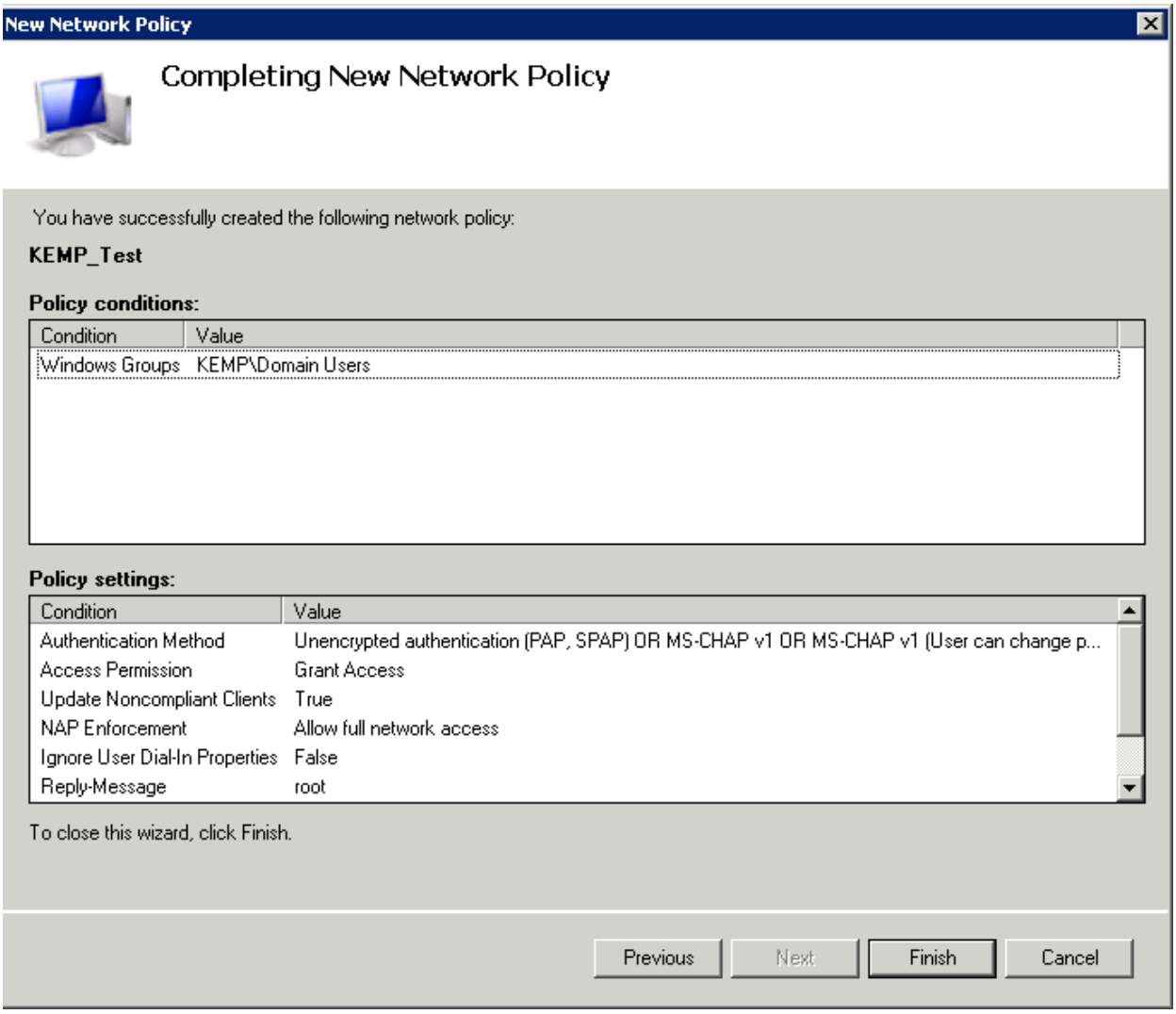
11. Select **PPP** from the **Commonly used for Dial-Up or VPN drop-down** list.
12. Click **OK**.



13. Select **Service-Type**.
14. Click the **Add…** button.



15. Select **Framed** from the **Commonly used for Dial-Up or VPN** drop-down list.
16. Click **OK**.
17. Click **Close**.
18. Click **Next**.



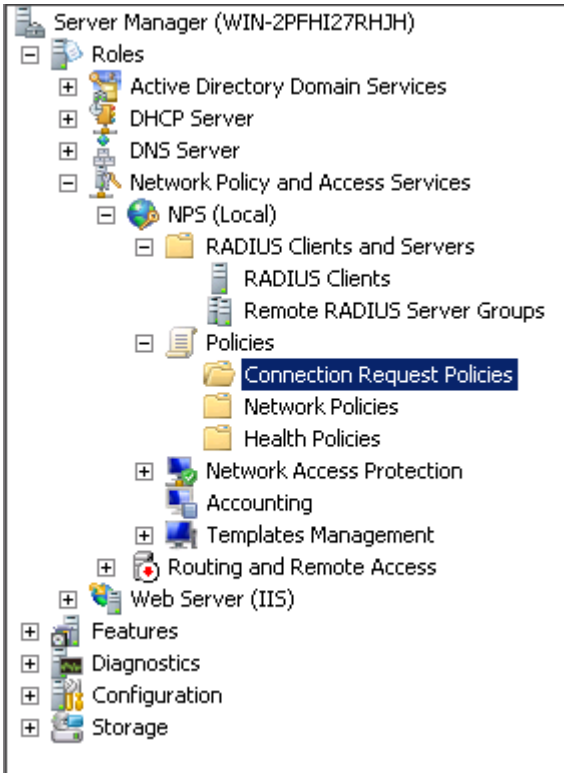
19. Click **Finish**.
20. Repeat this process as needed to set permissions for other groups.

Specify RADIUS Authentication and Authorization for All Users

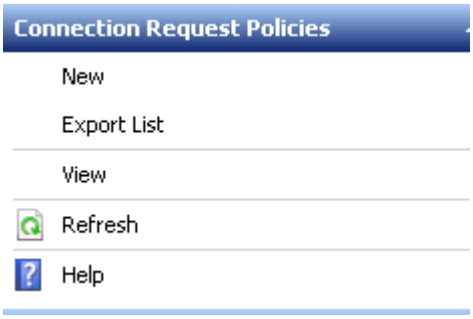
Specify RADIUS Authentication for All Users (Connection Request Policy)

Note: Permissions set in the connection request policy apply to all users.

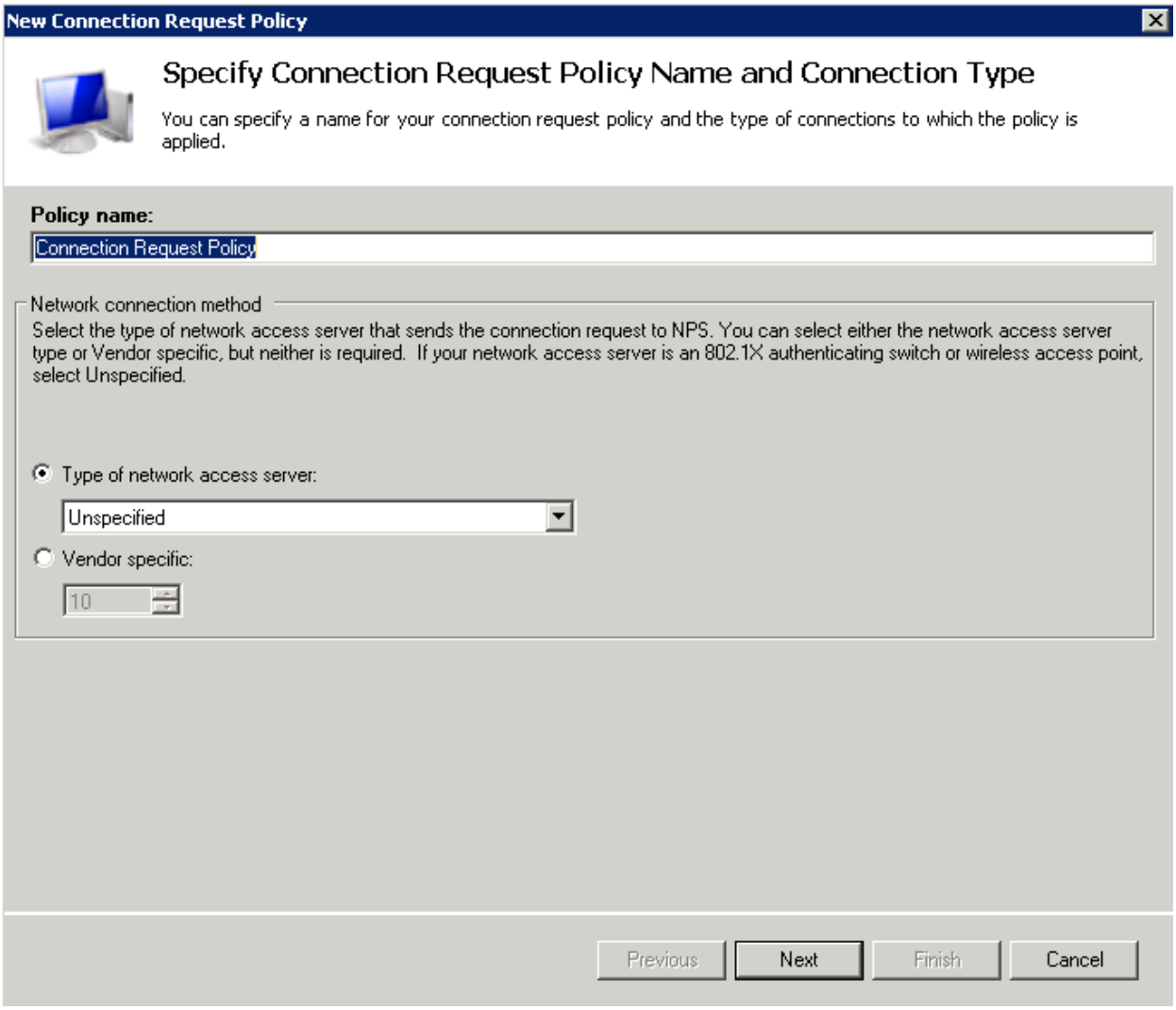
To set up a connection request policy, follow the steps below.



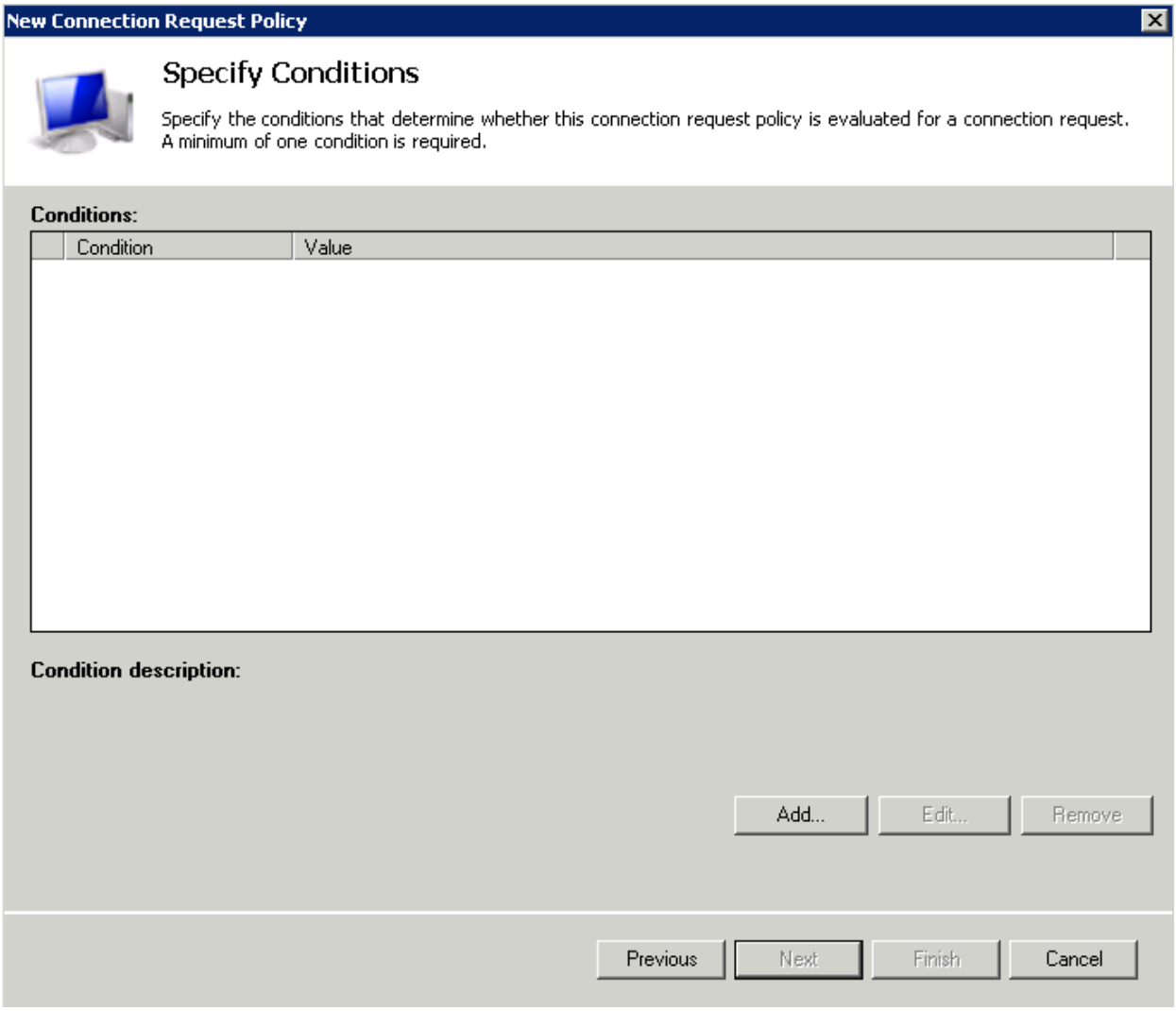
1. Navigate to **Roles > Network Policy and Access Services > Policies > Connection Request Policies**.



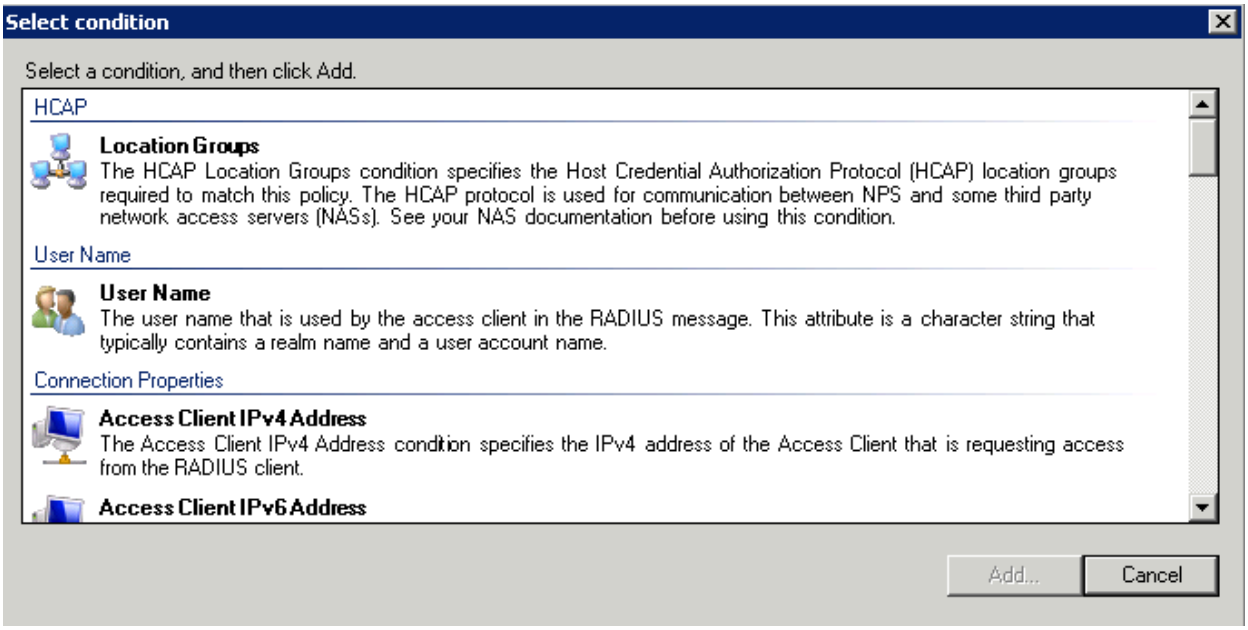
2. Click **New** in the panel on the right.



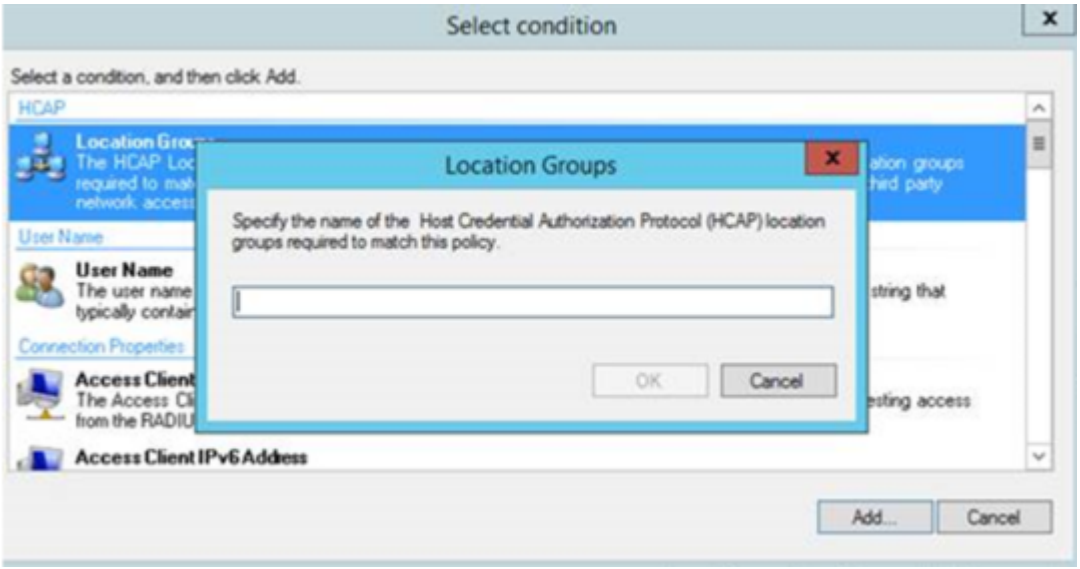
3. Enter a **Policy name.**
4. Click **Next**.



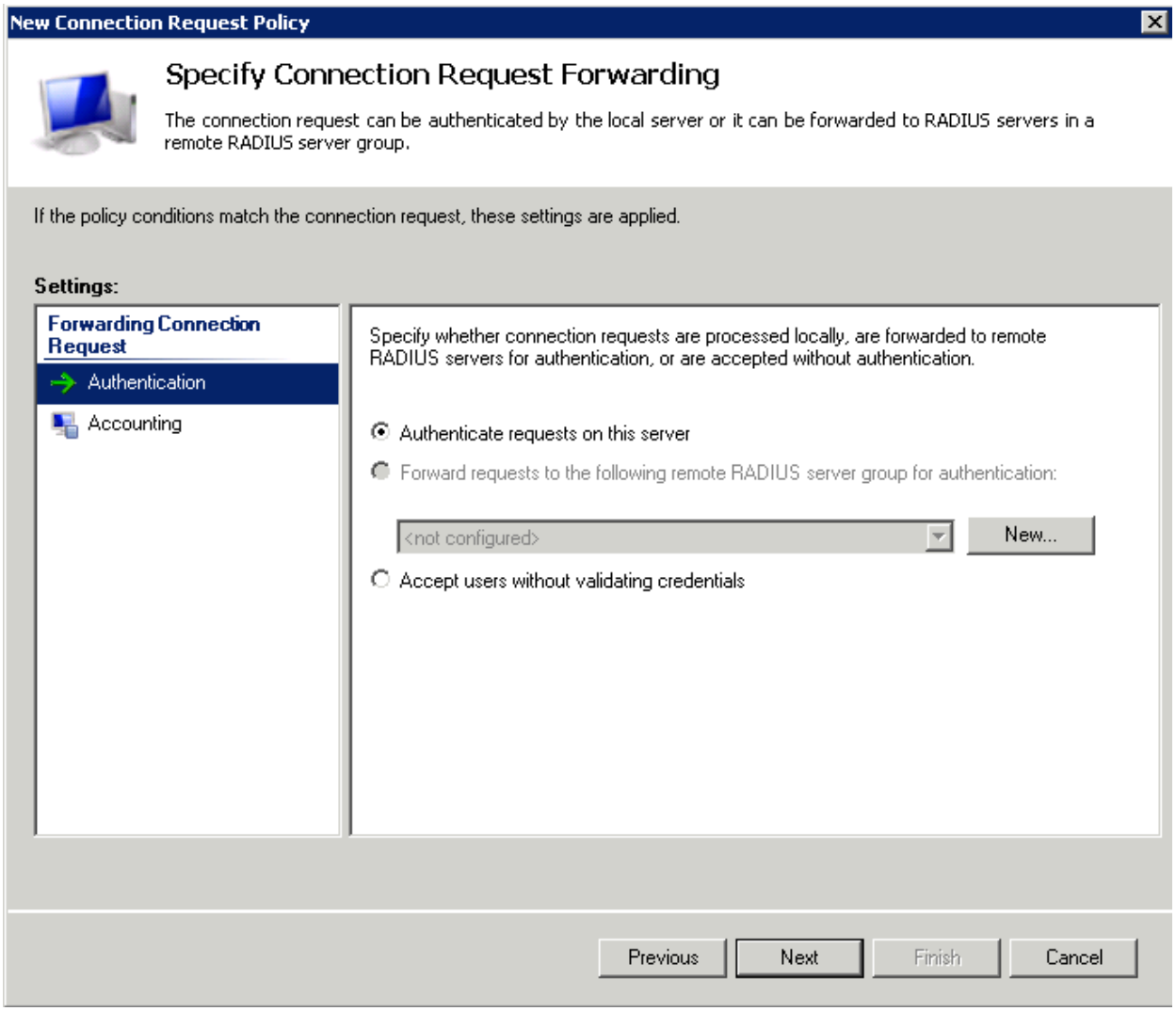
5. Click the **Add…** button.



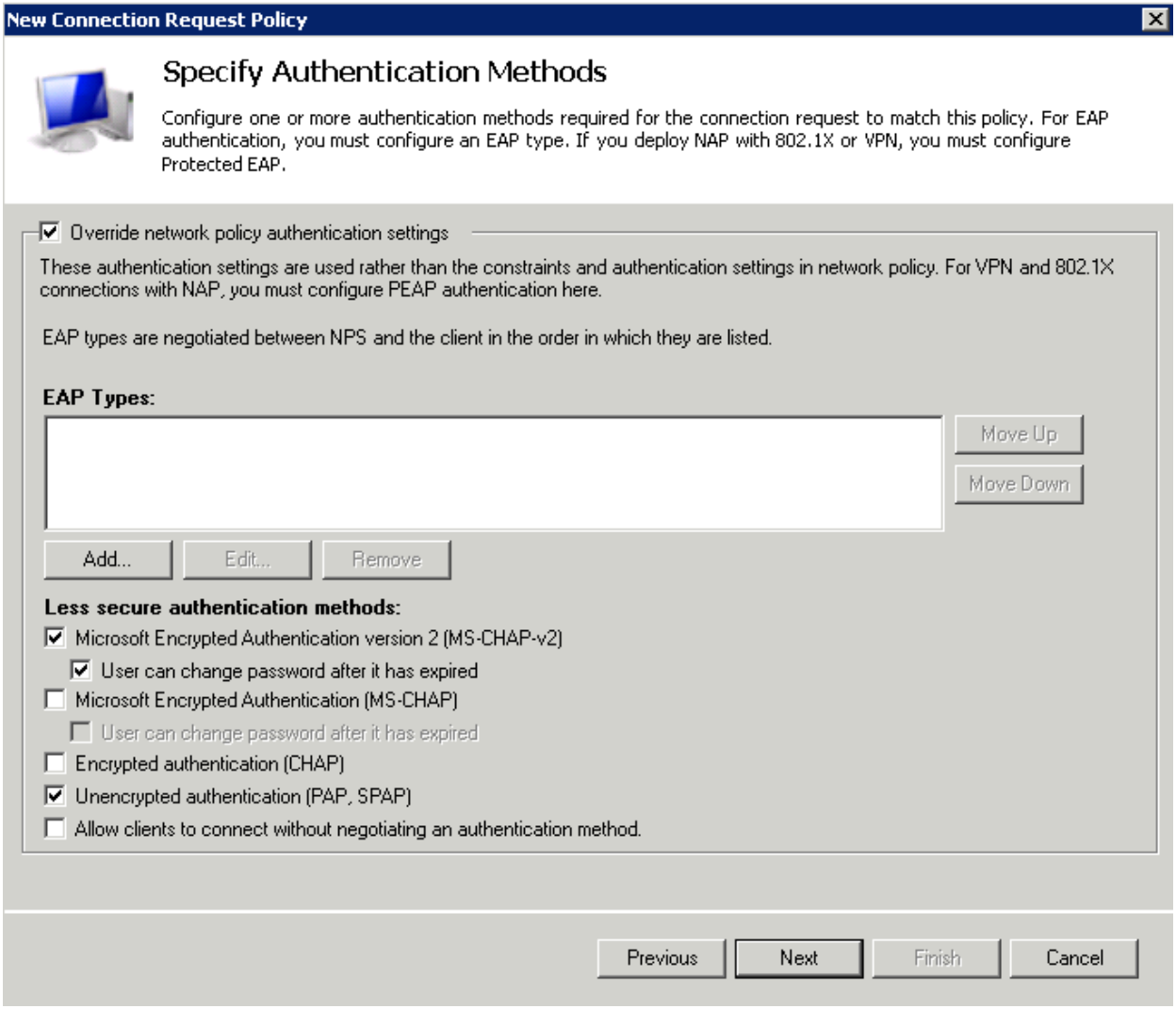
6. Select the **Location Groups** option.
7. Click the **Add…** button.



8. Type **Domain users** and click **OK**.
9. Click **Next**.

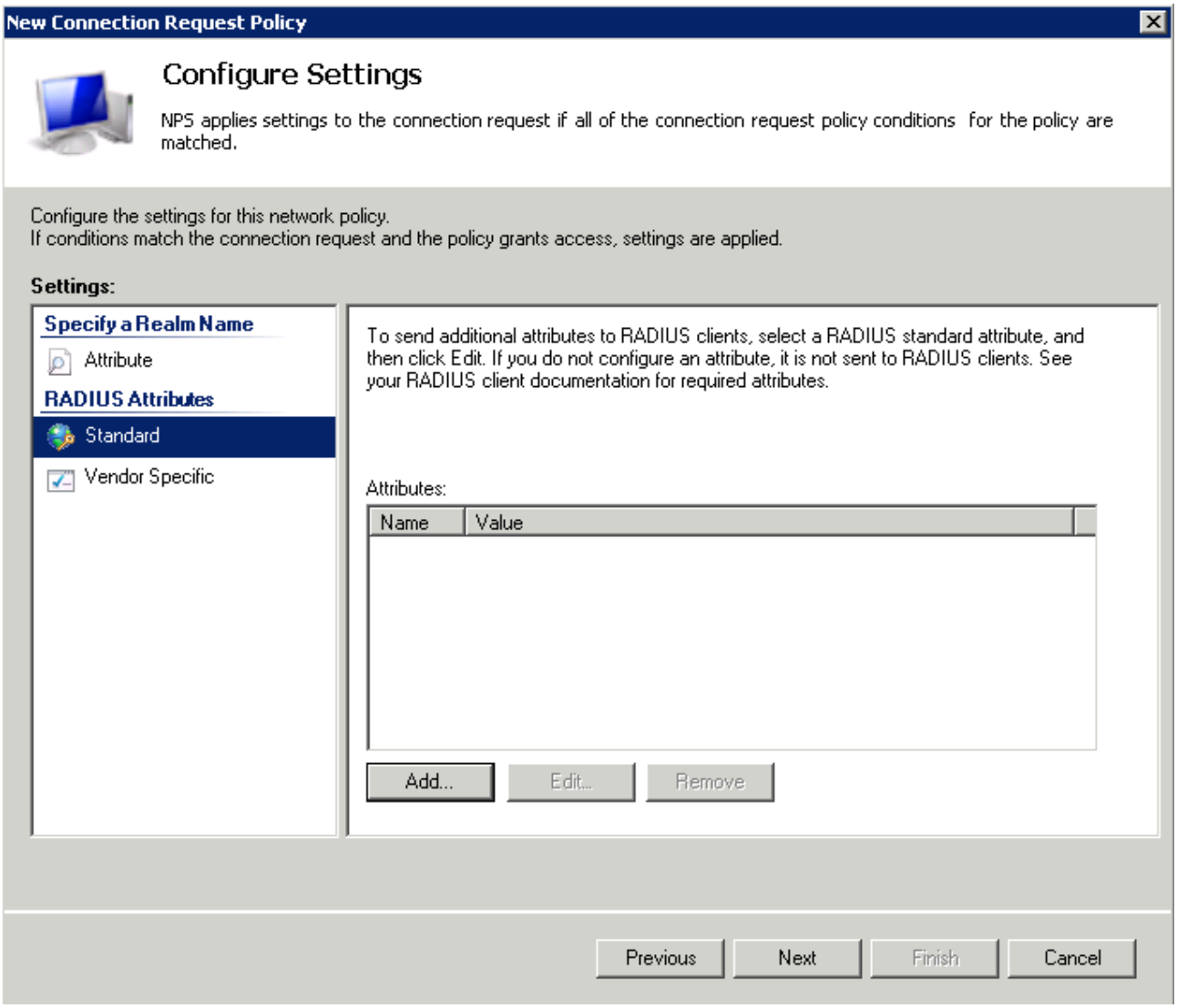


10. Click **Next**.

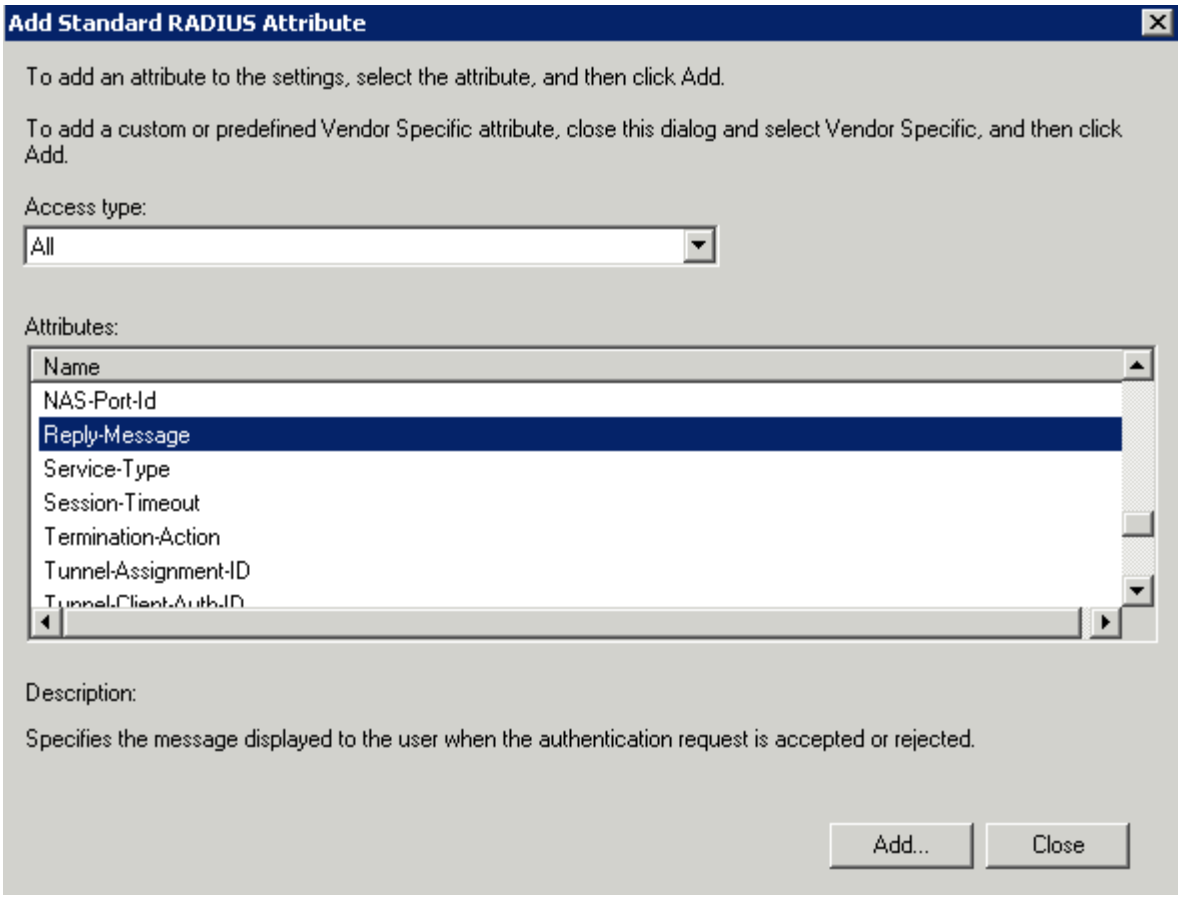


11. Select the **Override network policy authentication settings** check box.
12. Select the **Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)** check box.
13. Select the **User can change password after it has expired** check box.
14. Select the **Unencrypted authentication (PAP, SPAP) check** box.

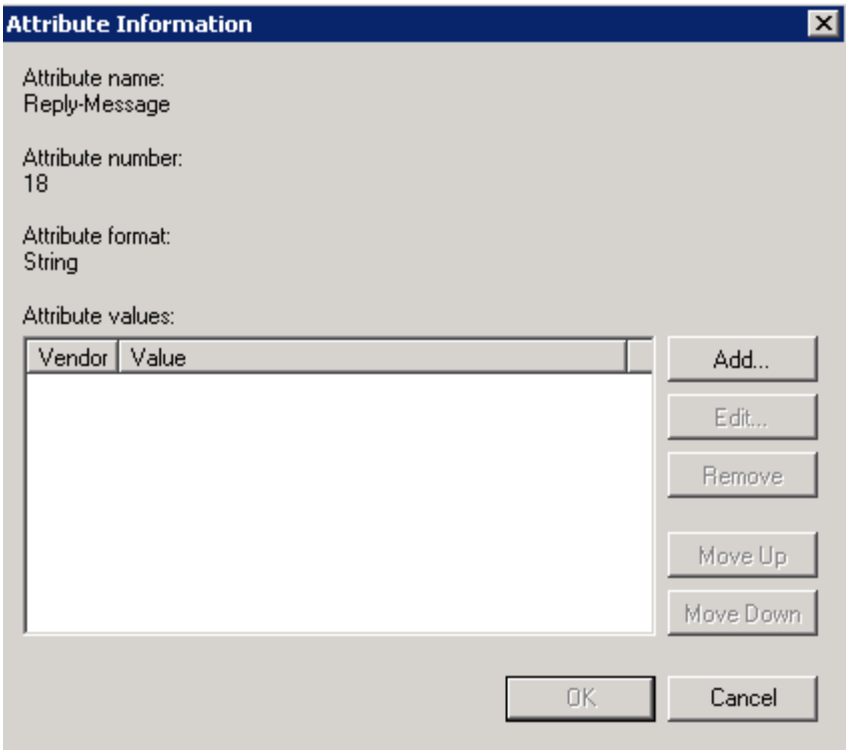
Specifying RADIUS Authorization for All Users



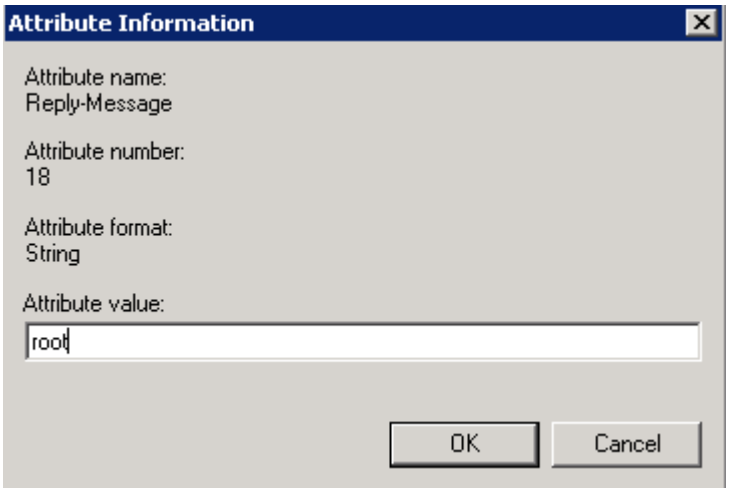
1. Select **Standard** in the panel on the left.
2. Click the **Add…** button.



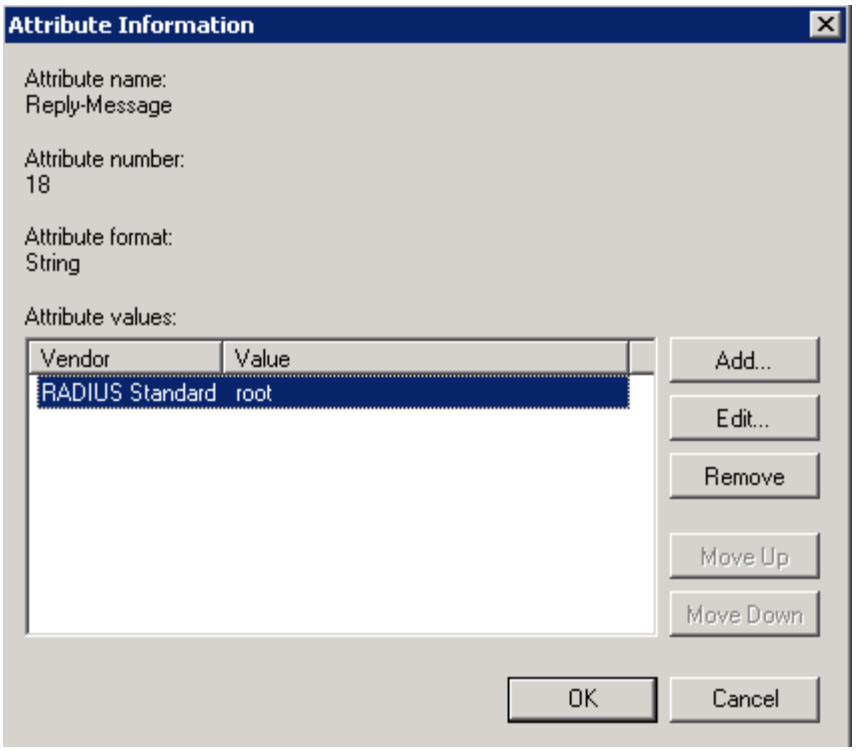
3. Select **Reply-Message**.
4. Click the **Add…** button.



5. Click the **Add…** button.

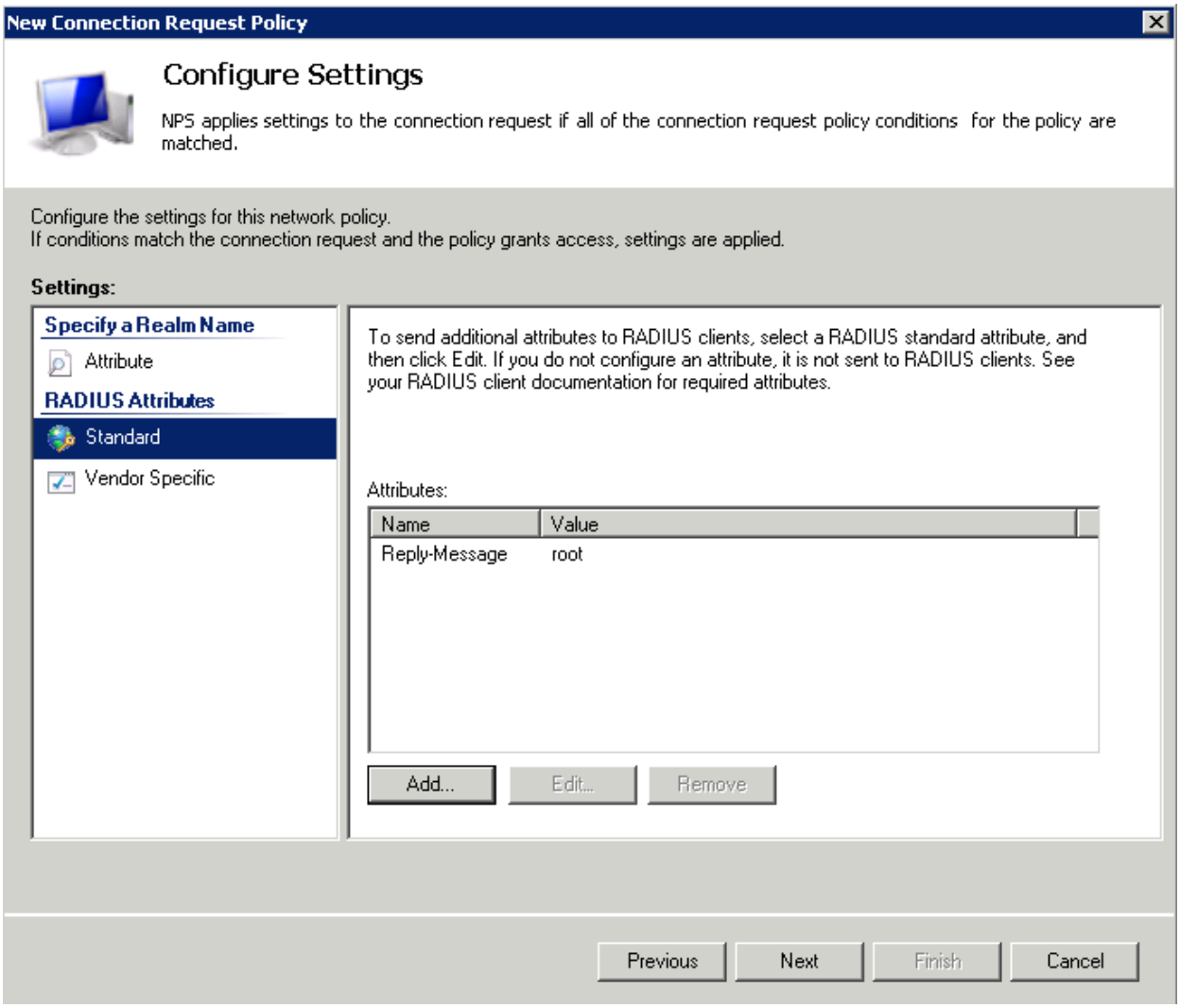


6. Enter the relevant permission(s) and click **OK**.

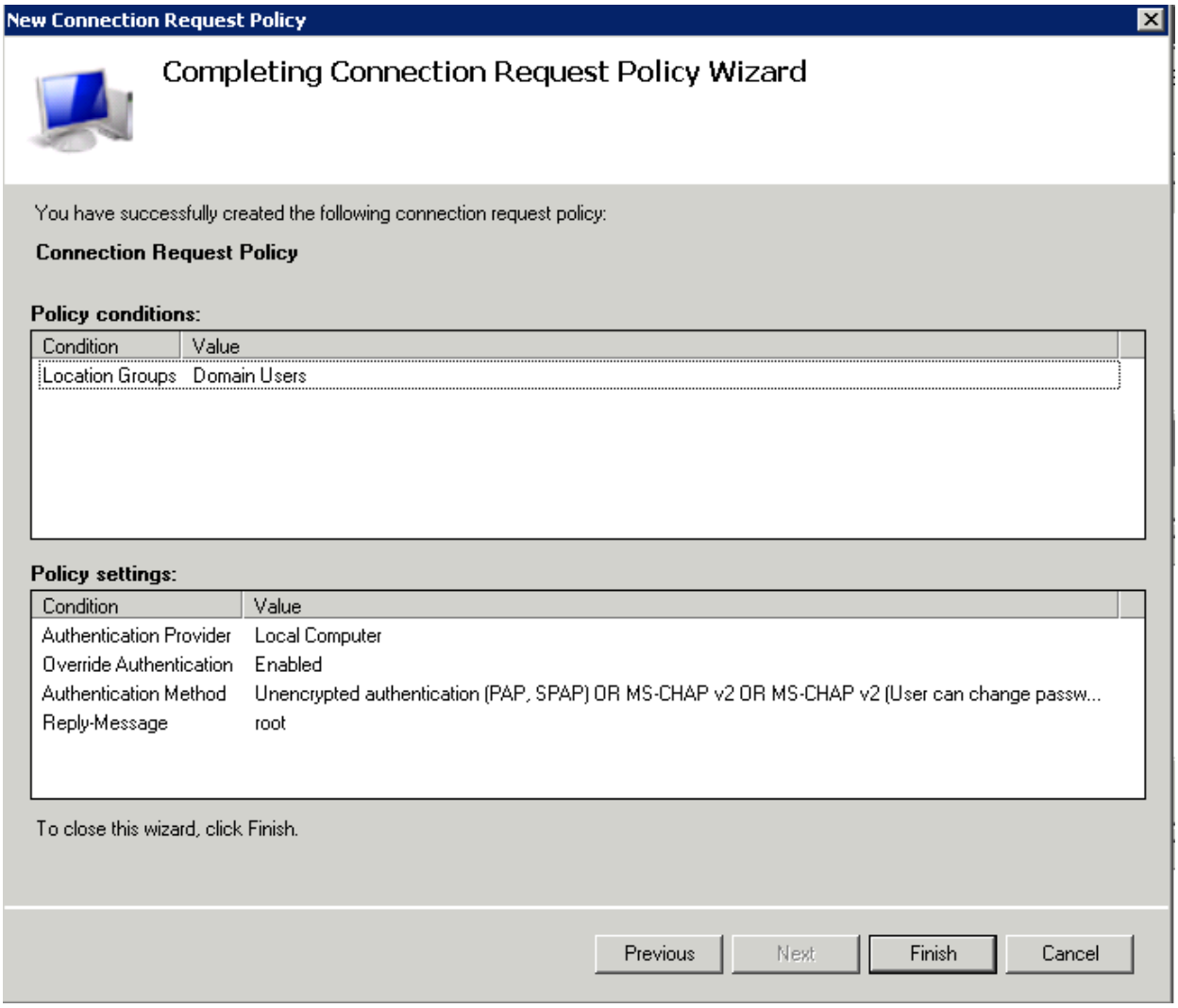


Note: The available permission options are as follows: **real,vs,rules,backup,certs,cert3,certbackup,users,root,geo**These correspond to the permission options in the LoadMaster Web User Interface (WUI). The **root** permission grants all permissions. Multiple attributes can be specified here, but they must be separated by a comma (with no space).

7. Select the attribute and click **OK**.
8. Click **OK** again.
9. Click **Close**.



10. Click **Next**.



11. Click **Finish**.

4

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

Web User Interface, Configuration Guide