



# RADIUS Authentication and Authorization

## Technical Note

UPDATED: 19 March 2021



## **Copyright Notices**

Copyright © 2002-2021 Kemp Technologies, Inc. All rights reserved. Kemp Technologies and the Kemp Technologies logo are registered trademarks of Kemp Technologies, Inc.

Kemp Technologies, Inc. reserves all ownership rights for the LoadMaster and Kemp 360 product line including software and documentation.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933

# Table of Contents

---

<b>1 Introduction</b> .....	<b>5</b>
1.1 Document Purpose .....	5
1.2 Intended Audience .....	5
1.3 Related Firmware Version .....	5
<b>2 Prerequisites for Authentication and Authorization</b> .....	<b>6</b>
2.1 Add a RADIUS Client .....	6
<b>3 Configure Authentication and Authorization</b> .....	<b>10</b>
3.1 Local Authentication and Authorization .....	11
3.1.1 Specify the RADIUS Server Details .....	11
3.1.2 Specifying RADIUS Authentication for an Individual User .....	11
3.1.3 Specifying Local Authorization for an Individual User .....	12
3.2 RADIUS Authentication and Authorization .....	12
3.2.1 Specify the RADIUS Server Details .....	12
3.2.2 Specifying RADIUS permissions for Groups and All Users .....	16
3.2.2.1 Specifying RADIUS Authentication and Authorization for a Group (Network Request Policy) .....	16
3.2.2.1.1 Specifying RADIUS Authentication for a Group .....	16
3.2.2.1.2 Specify RADIUS Authorization for a Group .....	24
3.2.2.2 Specify RADIUS Authentication and Authorization for All Users .....	29
3.2.2.2.1 Specify RADIUS Authentication for All Users (Connection Request Policy) .....	29
3.2.2.2.2 Specifying RADIUS Authorization for All Users .....	35

---

<b>References</b> .....	<b>40</b>
<b>Last Updated Date</b> .....	<b>41</b>

# 1 Introduction

The Remote Access Dial In User Service (RADIUS) server can be used to authenticate users who log in to the Kemp 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.

---

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

---

## 1.1 Document Purpose

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

## 1.2 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.

## 1.3 Related Firmware Version

Published with LMOS version 7.2.48.4 LTS. This document has not required substantial changes since 7.2.48.4 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

# 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 Kemp LoadMaster.

---

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

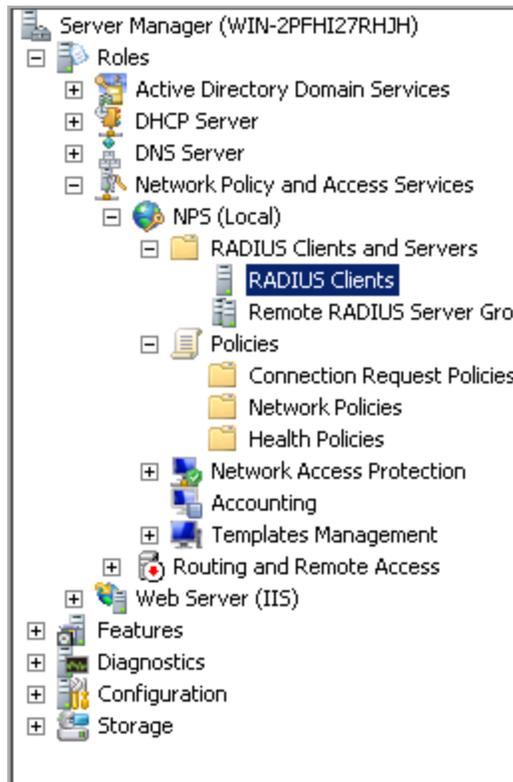
---

## 2.1 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.

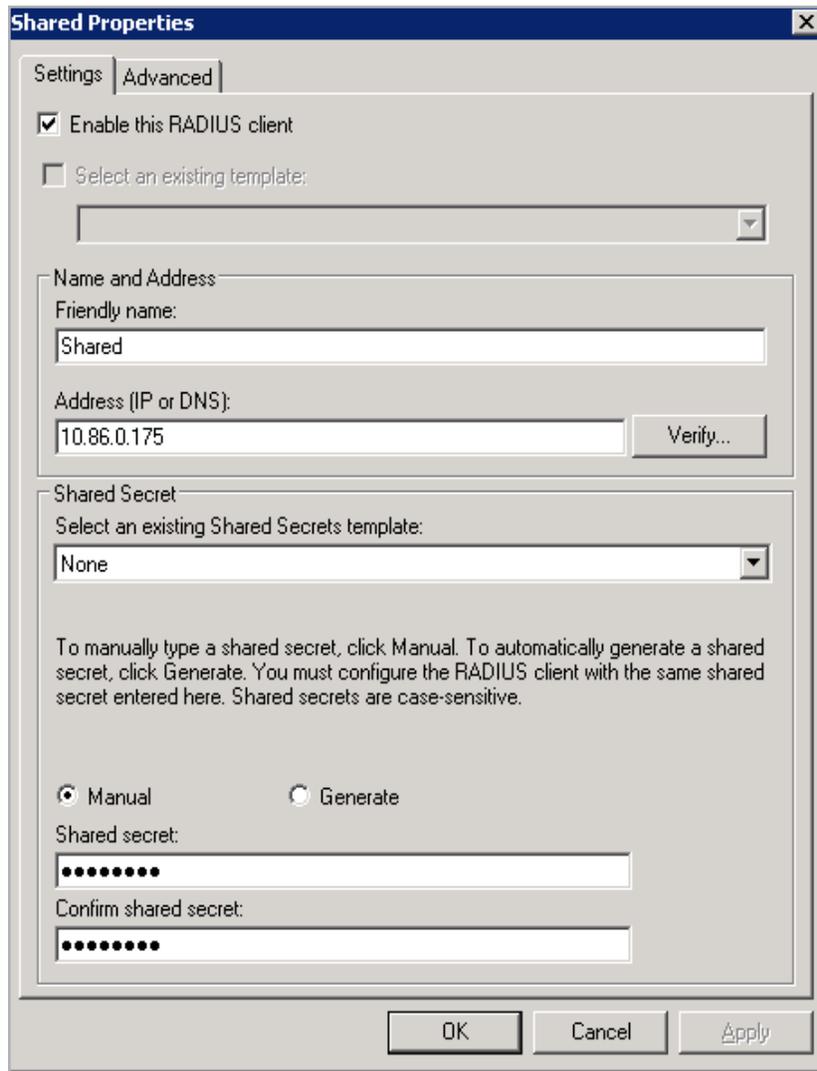
## 2 Prerequisites for Authentication and Authorization



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.

---

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**.

---

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.

---

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** .

## 3.1 Local Authentication and Authorization

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

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.

### 3.1.1 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.

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.

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.

### 3.1.2 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.

Local Users		
User	<input type="text"/>	<input type="button" value="Add User"/>
Password	<input type="text"/>	
Use RADIUS Server	<input type="checkbox"/>	
User	Permissions	Operation
Administrator	Read Only	<input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Password"/>

### 3.1.3 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.

**Permissions for User Administrator**

---

Real Servers	<input checked="" type="checkbox"/>
Virtual Services	<input checked="" type="checkbox"/>
Rules	<input type="checkbox"/>
System Backup	<input type="checkbox"/>
Certificate Creation	<input type="checkbox"/>
Intermediate Certificates	<input type="checkbox"/>
Certificate Backup	<input type="checkbox"/>
User Administration	<input type="checkbox"/>
All Permissions	<input type="checkbox"/>
Geo Control	<input type="checkbox"/>

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.

## 3.2 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.

### 3.2.1 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**.

**WUI Session Management**

---

Enable Session Management

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

Please Specify Your User Credentials

User	<input type="text"/>	<input type="button" value="Login"/>
Password	<input type="password"/>	

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

WUI Session Management

Enable Session Management	<input checked="" type="checkbox"/>	
Require Basic Authentication	<input checked="" type="checkbox"/>	
Basic Authentication Password	<input type="password" value="•••••"/>	<input type="button" value="Set Basic Password"/>
Failed Login Attempts	<input type="text" value="3"/>	<input type="button" value="Set Fail Limit (Valid values:1-999)"/>
Idle Session Timeout	<input type="text" value="600"/>	<input type="button" value="Set Idle Timeout (Valid values: 60-86400)"/>
Limit Concurrent Logins	<input type="text" value="0 (No limit)"/>	

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**.

## 3 Configure Authentication and Authorization

### Administrator Access

Allow Remote SSH Access Using: All Networks Port: 22 Set Port  
 SSH Pre-Auth Banner  Set Pre-Auth Message  
 Allow Web Administrative Access Using: eth0: 10.35.48.22 Port: 443  
 Admin Default Gateway  Set Administrative Access  
 Allow Multi Interface Access  
 Enable API Interface  
 Self-Signed Certificate Handling RSA self-signed certs  
 Outbound Connection Cipher Set None - Outbound Default  
 Admin Login Method Password Only Access (default) Only Password mode is available if no Pre-Auth Banner is specified  
 Enable Software FIPS 140-2 Level 1 Mode Enable Software FIPS mode  
 Enable Kemp Analytics

---

### GEO Settings

Remote GEO LoadMaster Access  Set GEO LoadMaster access  
 GEO LoadMaster Partners  Set GEO LoadMaster Partners  
 GEO LoadMaster Port 22 Set GEO LoadMaster Port  
 GEO Update Interface eth0: 10.35.48.22

---

WUI Authorization Options

6. Click **WUI Authorization Options**.

### WUI AAA Service Authentication Authorization Options

RADIUS

RADIUS Server 10.154.11.80 Port 80 RADIUS Server  
 Shared Secret Please set passw Set Secret  
 Backup RADIUS Server  Port  Backup Server  
 Backup Shared Secret  Set Backup Secret  
 Revalidation Interval 60 Set Interval  
 Send NAS Identifier

---

LDAP

LDAP Endpoint EXAMPLE Manage LDAP Configuration  
 Remote User Groups ExampleGroup2; ExampleRemoteUserGroup; Select groups  Nested groups  
 Domain  Set Domain

---

Local Users   Use ONLY if other AAA services fail

---

### Test AAA for User

Username  Test User  
 Password

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

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**.

---

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.

---

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

---

---

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.

---

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

---

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.

---

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

---

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.

---

In LoadMaster firmware version 7.2.51 and above, there is an option to include the Kemp vendor specific attribute in the RADIUS request sent to the server doing the authentication against the user trying to log in to the LoadMaster WUI. For further details, refer to the following article: [Send Kemp Vendor Specific Attribute In RADIUS Requests](#).

### 3.2.2 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.

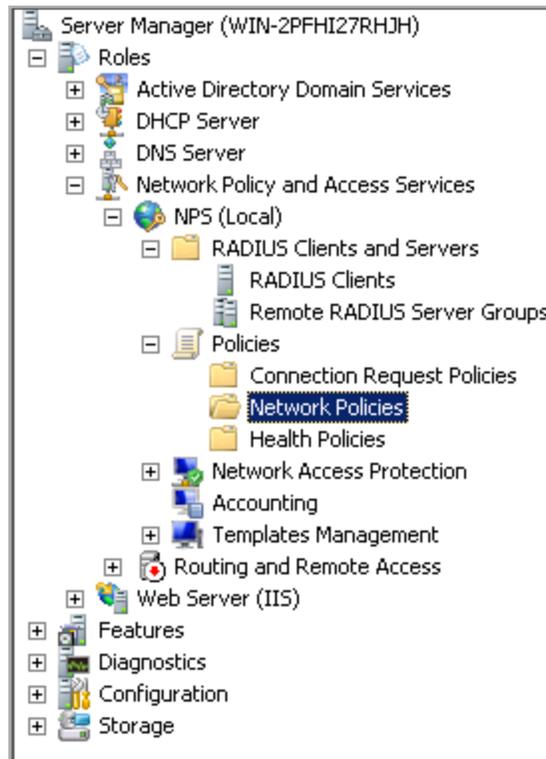
Connection request policies apply to all users. Network policies apply to groups.

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

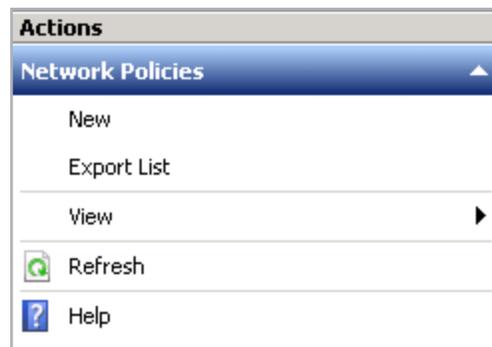
#### 3.2.2.1 Specifying RADIUS Authentication and Authorization for a Group (Network Request Policy)

##### 3.2.2.1.1 Specifying RADIUS Authentication for a Group

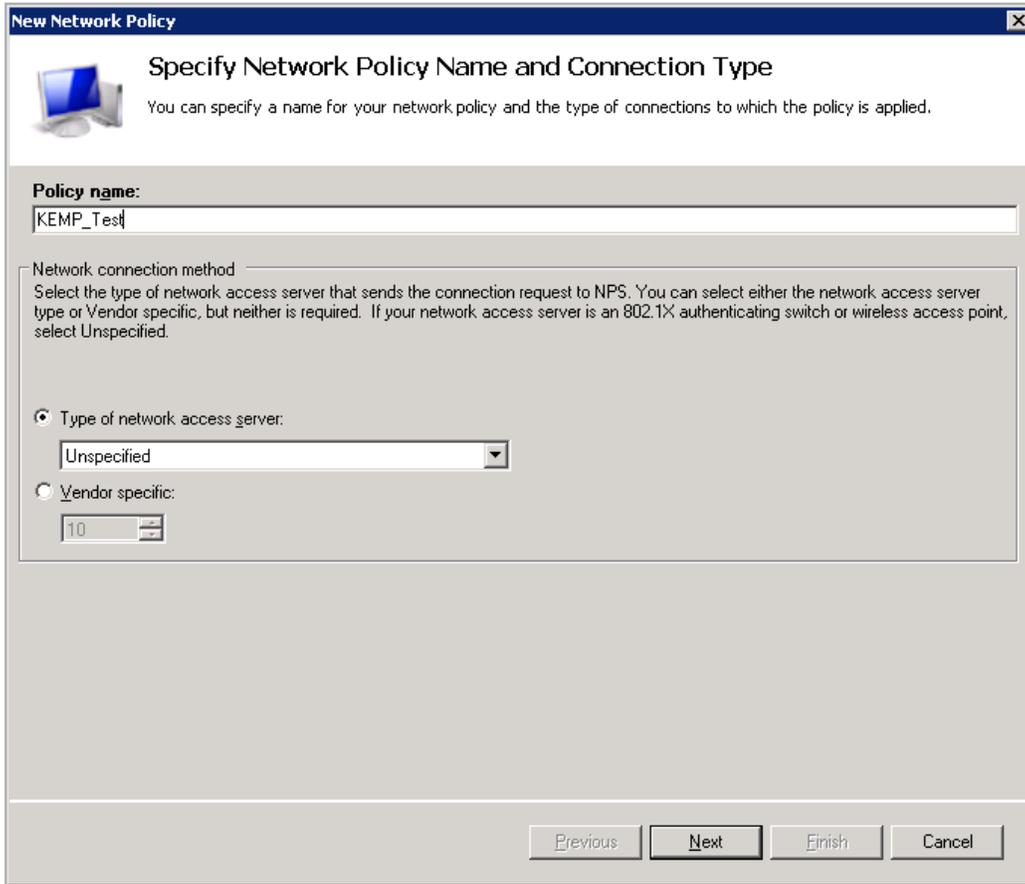
To set up a network policy, follow the steps below in the **Server Manager**.



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



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



**New Network Policy**

**Specify Network Policy Name and Connection Type**

You can specify a name for your network policy and the type of connections to which the policy is applied.

**Policy name:**  
KEMP\_Test

**Network connection method**  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

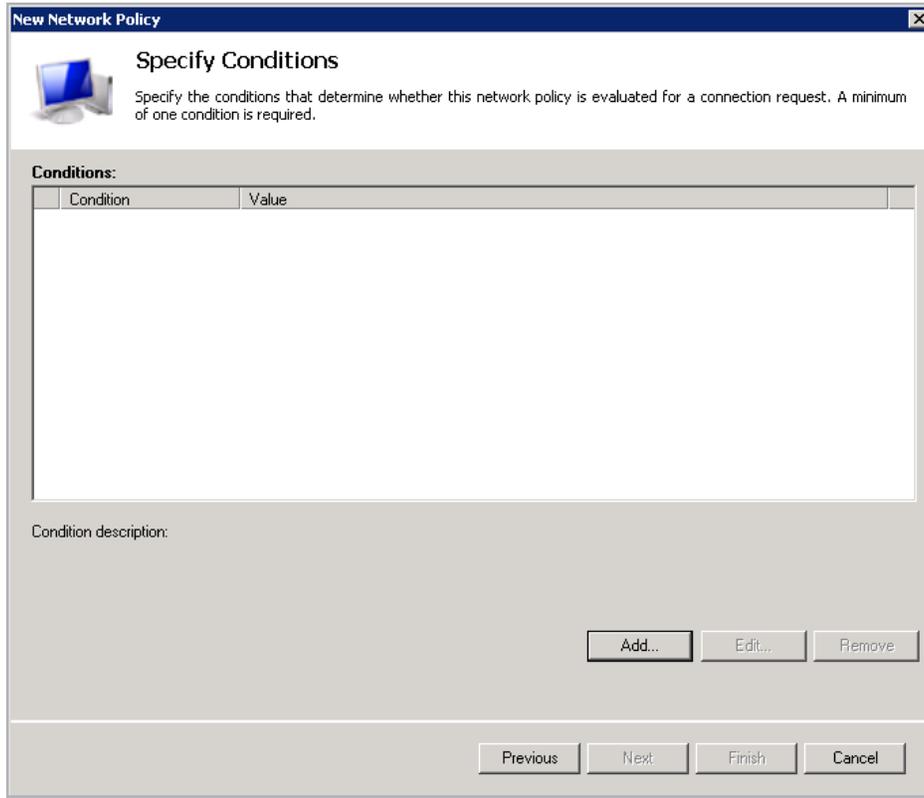
**Type of network access server:**  
Unspecified

**Vendor specific:**  
10

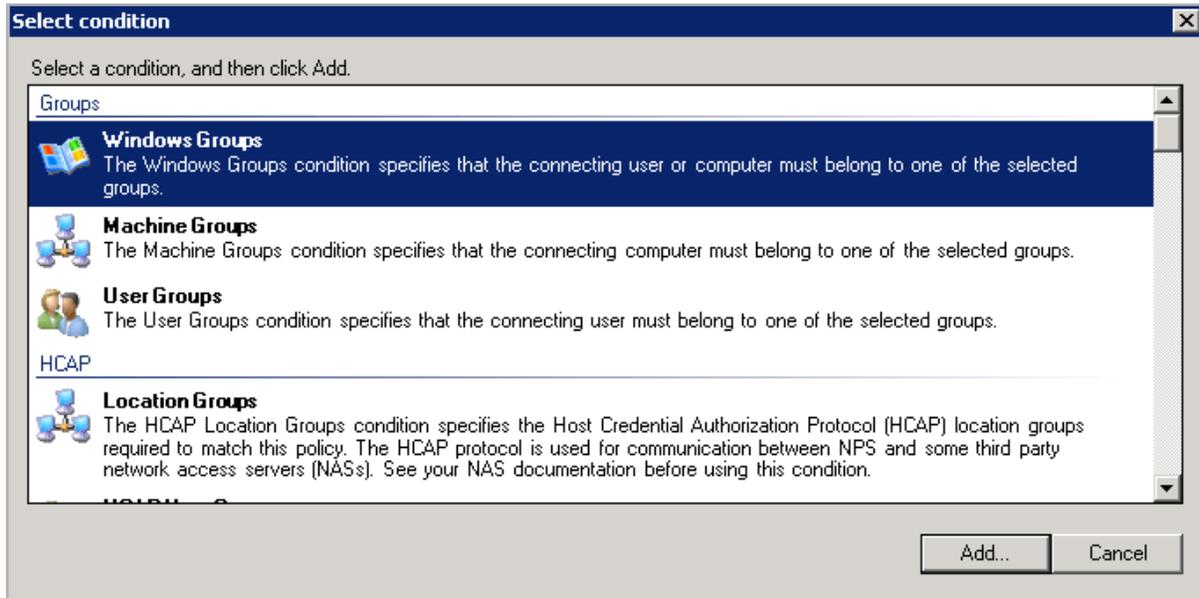
Previous Next Finish Cancel

3. Enter a **Policy name**.

4. Click **Next**.



5. Click the **Add...** button.

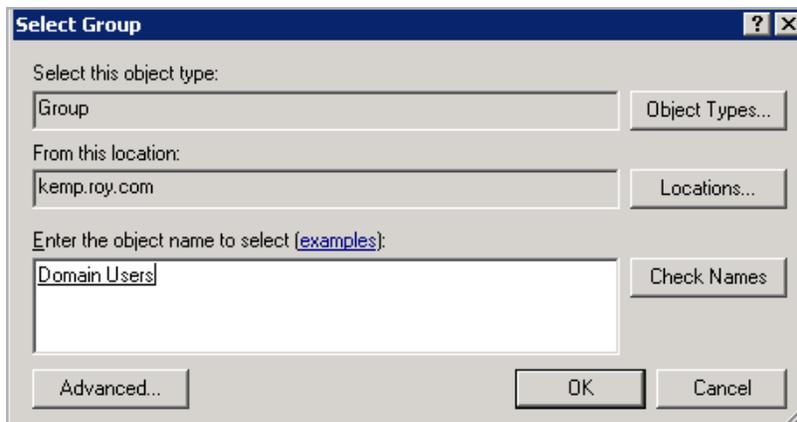


6. Select the relevant group type.

7. Click the **Add...** button.



8. Click the **Add Groups...** button.



9. Enter the group name in the text area provided.

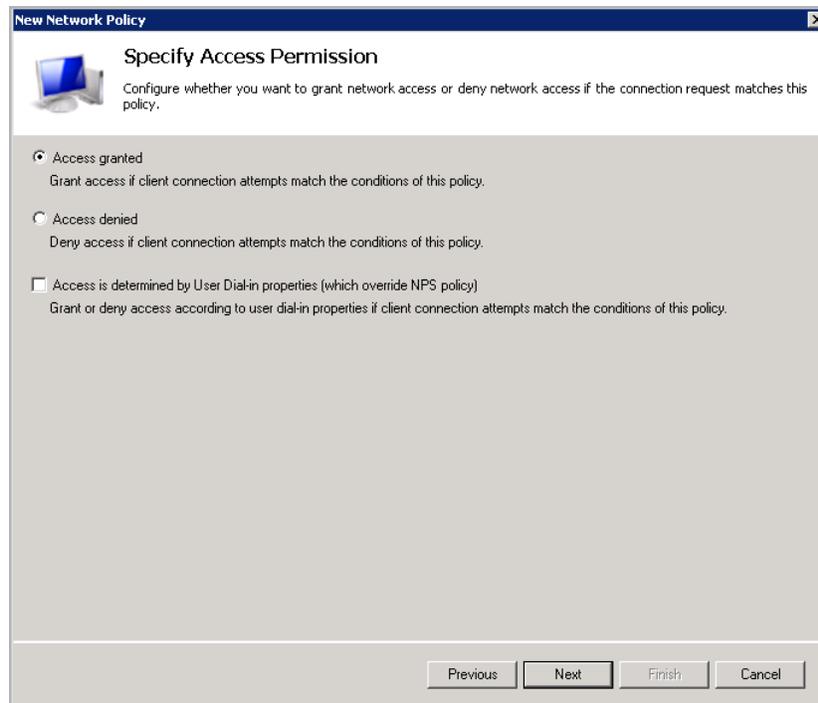
10. Click **Check Names**.

11. If the name is alright, click **OK**.



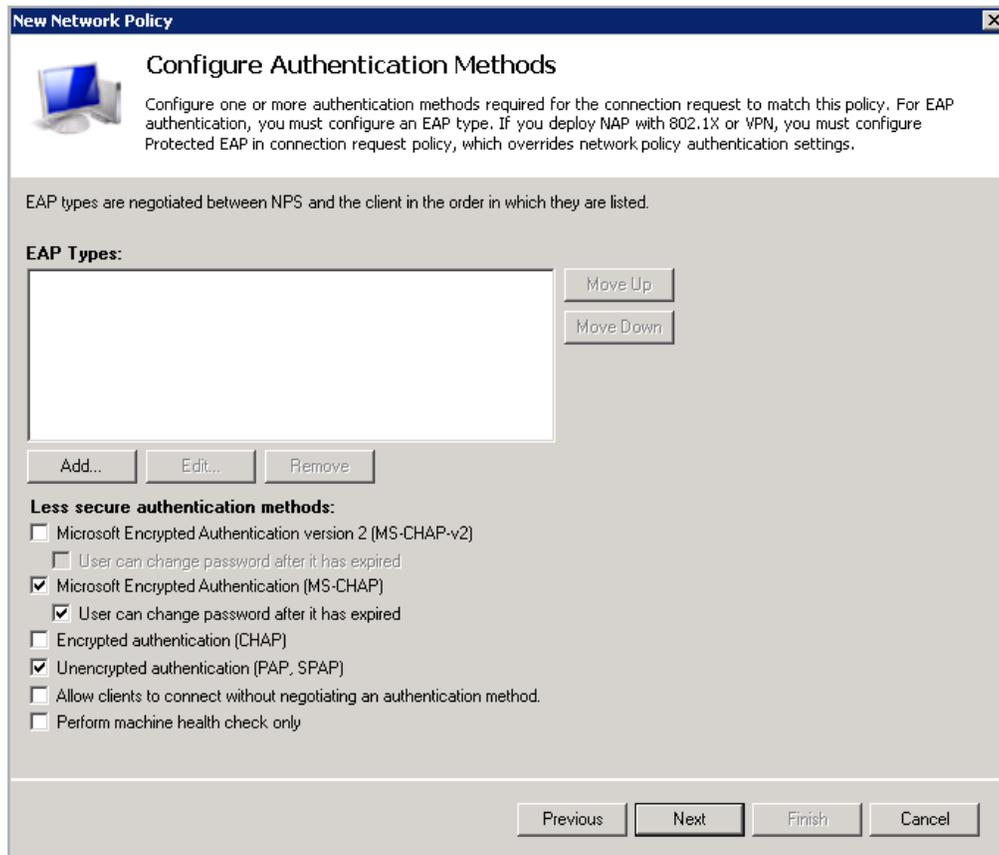
12. Click **OK**.

13. Click **Next**.



14. Select the relevant Access Permission option.

15. Click **Next**.



**New Network Policy**

### Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

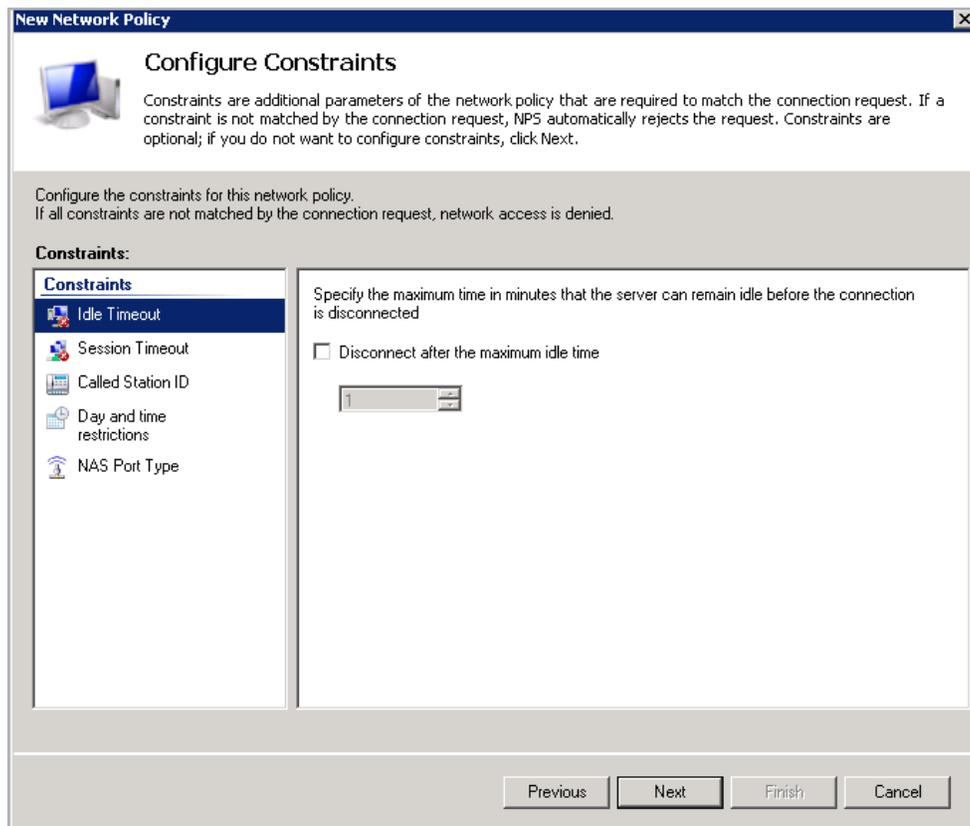
EAP types are negotiated between NPS and the client in the order in which they are listed.

**EAP Types:**

**Less secure authentication methods:**

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
  - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.
- Perform machine health check only

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**.



---

If idle timeout is used on the server it should match the idle timeout settings in the LoadMaster. Generally, Kemp recommends not setting this on the server.

---

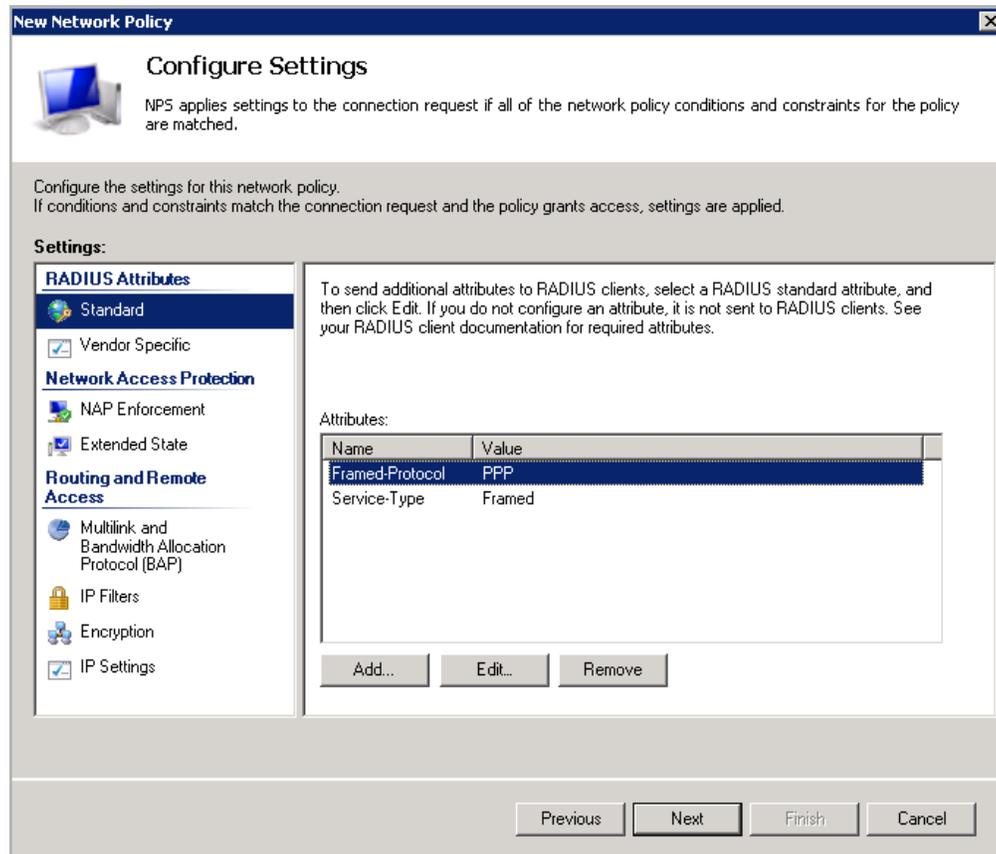
21. Click **Next**.

---

The 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.

---

## 3.2.2.1.2 Specify RADIUS Authorization for a Group



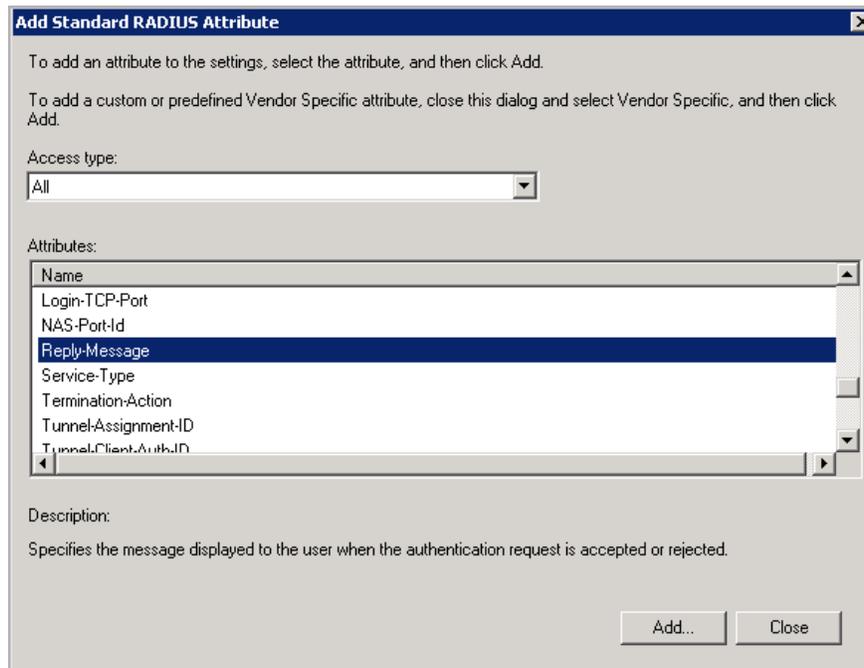
The **Attributes** on this screen need to be in a certain order for the settings to work correctly. The order is as follows:

1. **Reply-Message**
2. **Framed-Protocol**
3. **Service-Type**

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

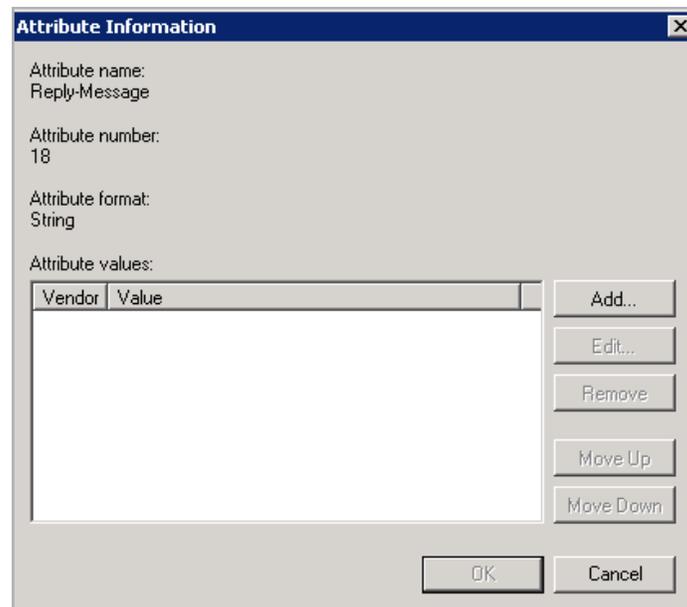
1. Select **Framed-Protocol** and click **Remove**.
2. Select **Service-Type** and click **Remove**.
3. Click the **Add...** button.

## 3 Configure Authentication and Authorization

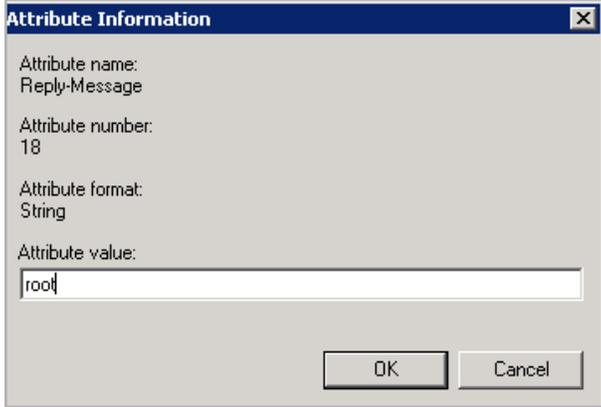


4. Select **Reply-Message**.

5. Click the **Add...** button.



6. Click the **Add...** button.



The image shows a dialog box titled "Attribute Information" with a close button (X) in the top right corner. It contains the following fields:

- Attribute name: Reply-Message
- Attribute number: 18
- Attribute format: String
- Attribute value: root

At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

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

---

The available permission options are as follows:

**real,vs,rules,backup,certs,cert3,certbackup,users,root,adv**s

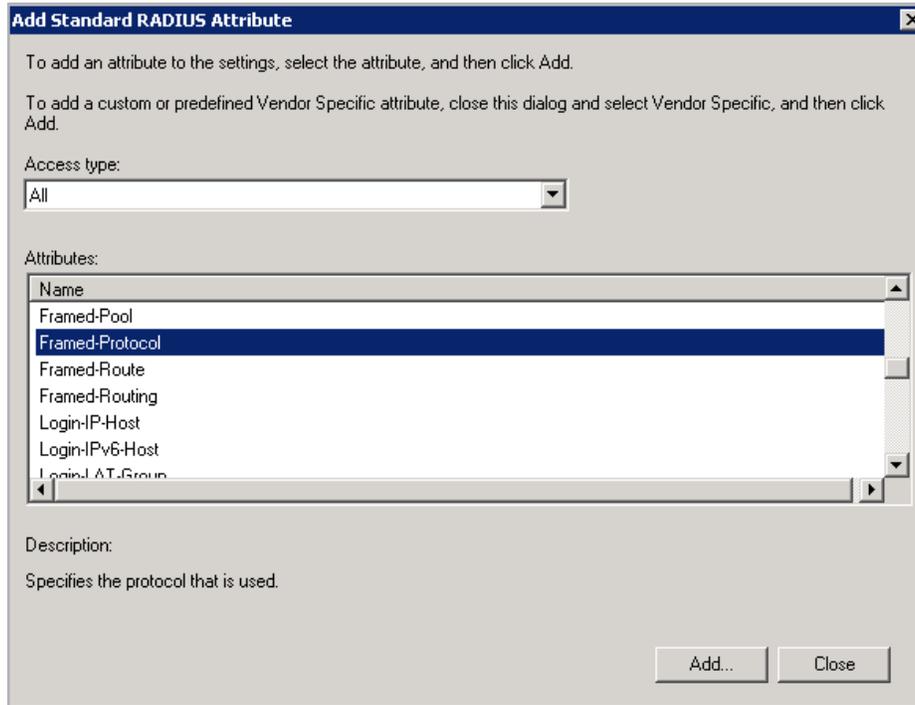
These correspond to the permission options in the LoadMaster Web User Interface (WUI).

The **root** permission grants all permissions.

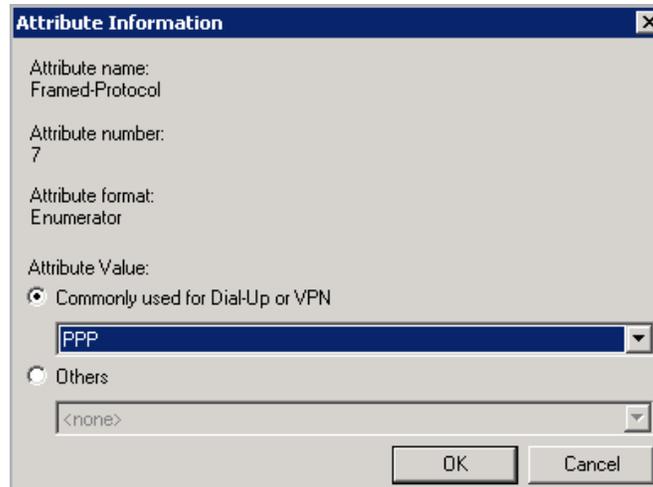
Multiple attributes can be specified here, but they must be separated by a comma (with no space).

---

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



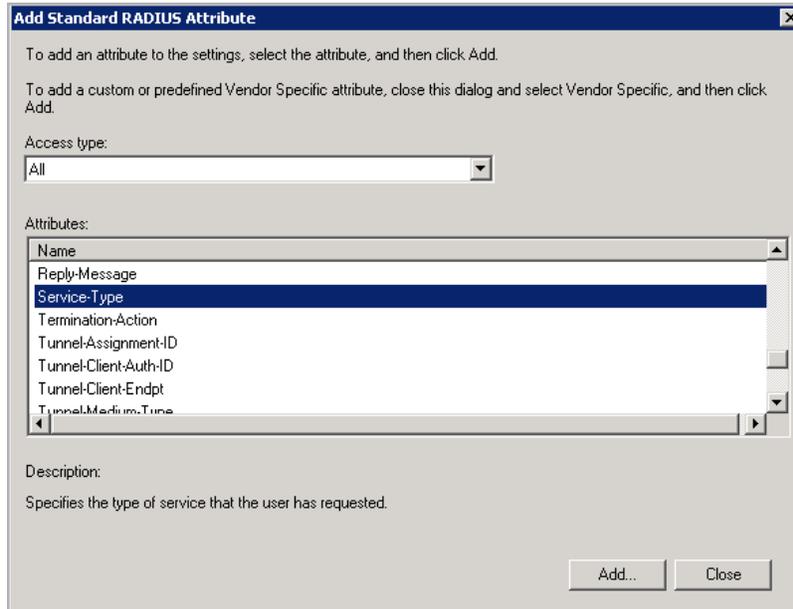
10. Click the **Add...** button.



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

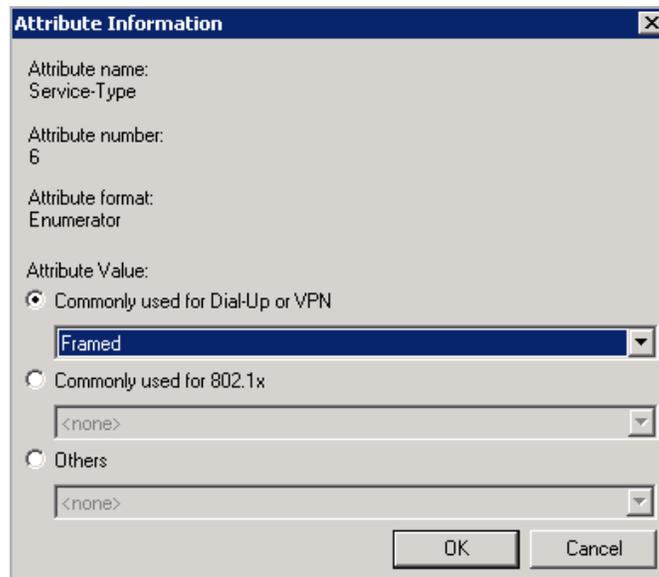
12. Click **OK**.

## 3 Configure Authentication and Authorization



13. Select **Service-Type**.

14. Click the **Add...** button.

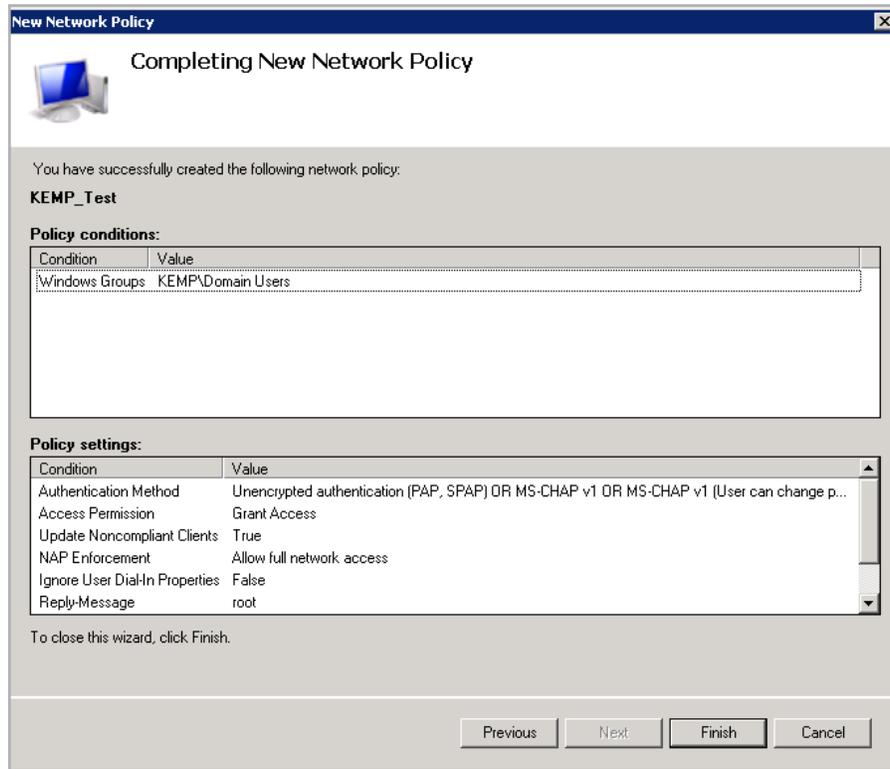


15. Select **Framed** from the **Commonly used for Dial-Up or VPN** drop-down list.

16. Click **OK**.

17. Click **Close**.

18. Click **Next**.



19. Click **Finish**.

20. Repeat this process as needed to set permissions for other groups.

### 3.2.2.2 Specify RADIUS Authentication and Authorization for All Users

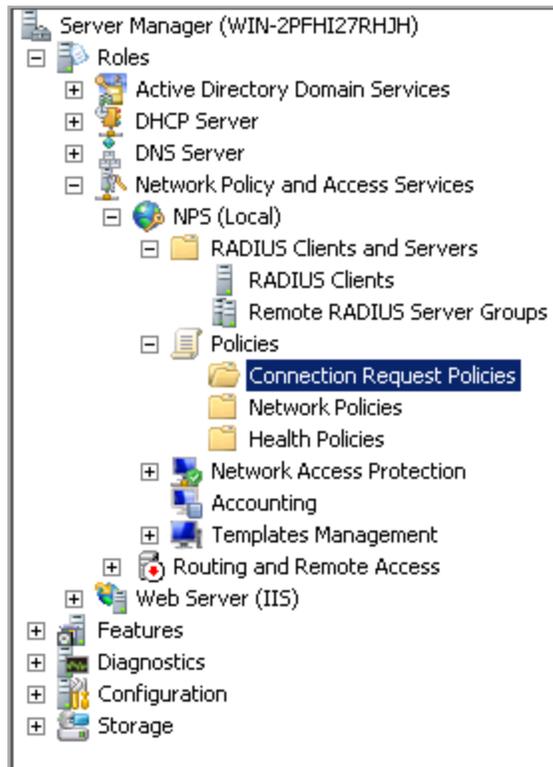
#### 3.2.2.2.1 Specify RADIUS Authentication for All Users (Connection Request Policy)

---

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

---

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

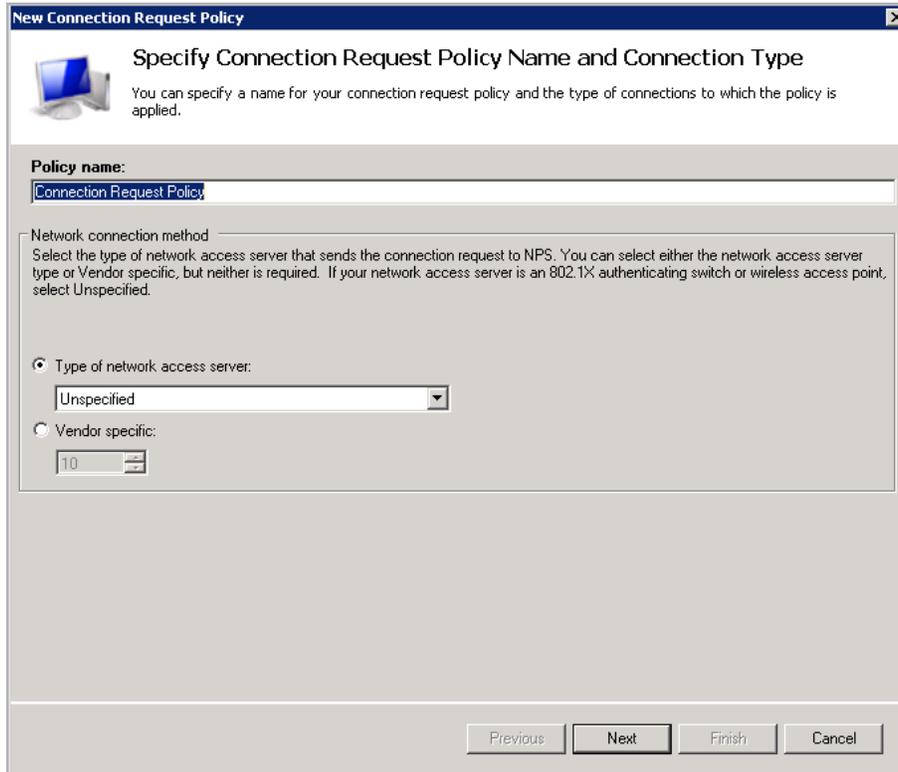


1. Navigate to **Roles > Network Policy and Access Services > Policies > Connection Request Policies**.



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

## 3 Configure Authentication and Authorization



**New Connection Request Policy**

**Specify Connection Request Policy Name and Connection Type**

You can specify a name for your connection request policy and the type of connections to which the policy is applied.

**Policy name:**  
Connection Request Policy

**Network connection method**  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

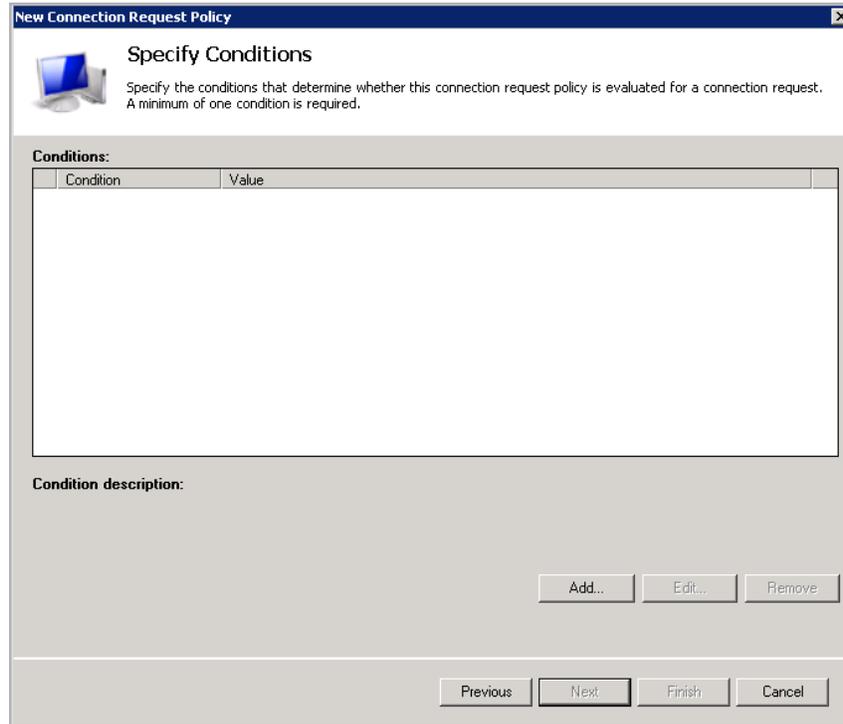
Type of network access server:  
Unspecified

Vendor specific:  
10

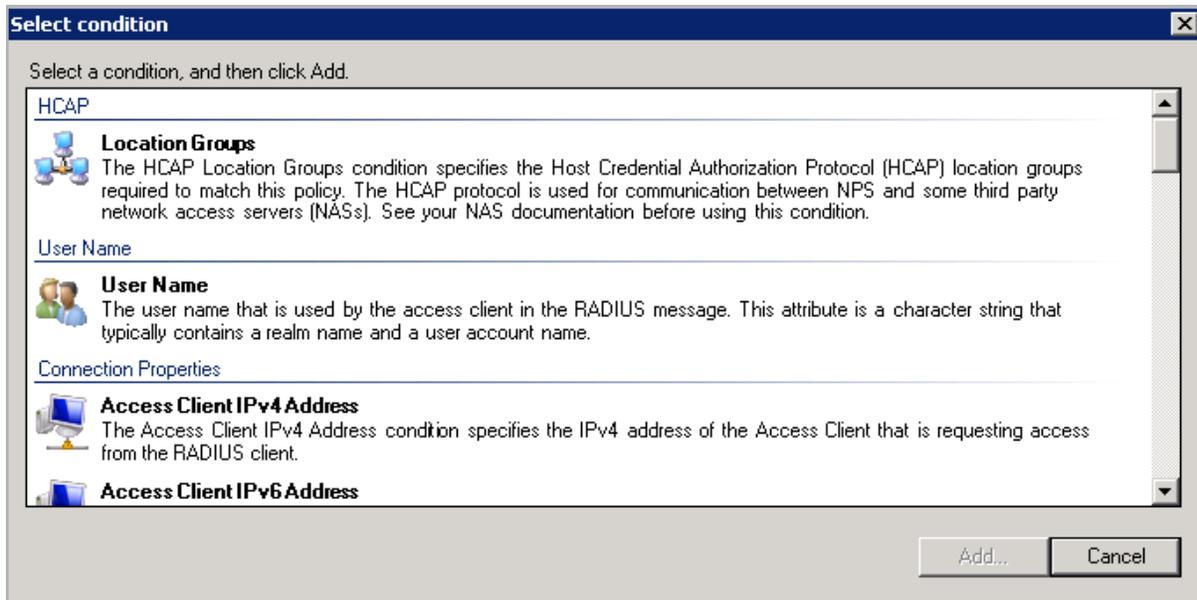
Previous Next Finish Cancel

3. Enter a **Policy name**.

4. Click **Next**.



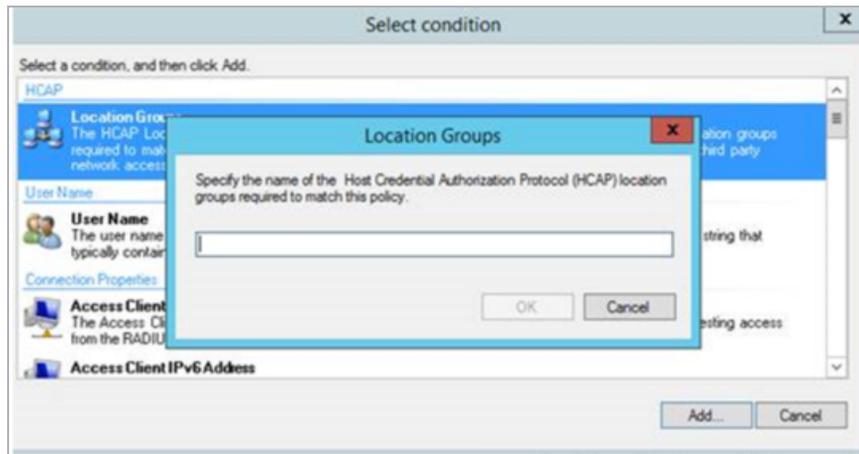
5. Click the **Add...** button.



6. Select the **Location Groups** option.

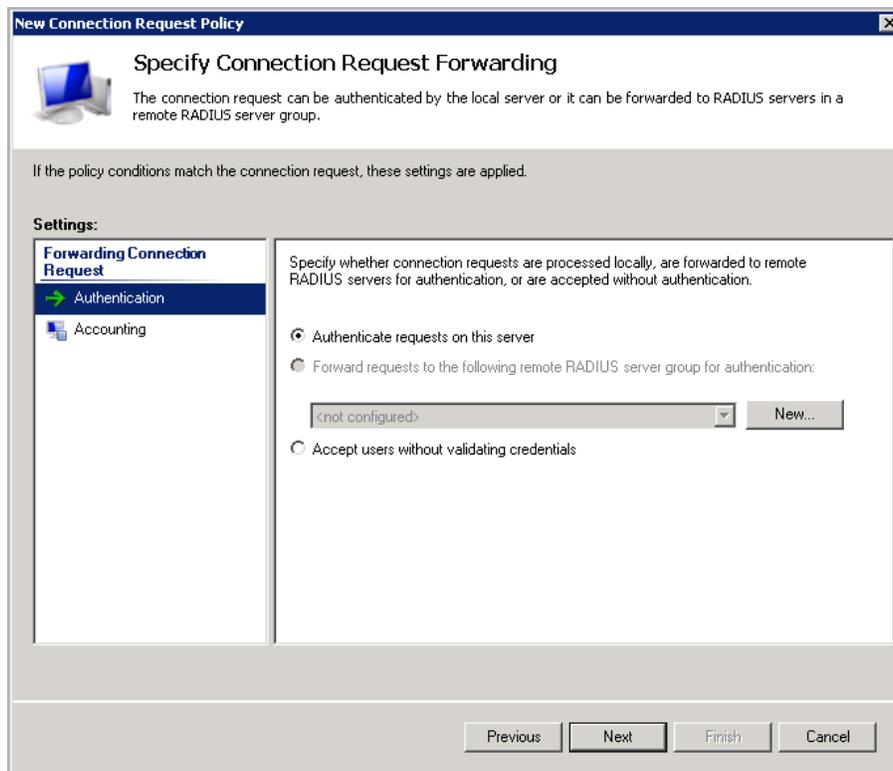
7. Click the **Add...** button.

## 3 Configure Authentication and Authorization

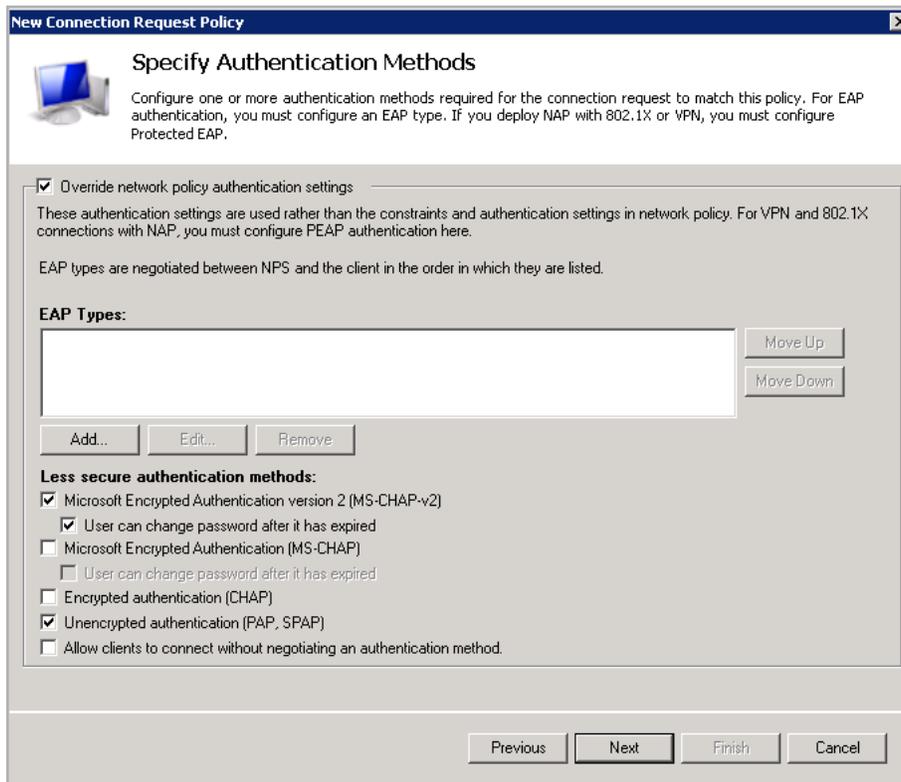


8. Type **Domain users** and click **OK**.

9. Click **Next**.



10. Click **Next**.



**New Connection Request Policy**

**Specify Authentication Methods**

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP.

**Override network policy authentication settings**

These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.

EAP types are negotiated between NPS and the client in the order in which they are listed.

**EAP Types:**

[Empty list box]

Move Up  
Move Down

Add... Edit... Remove

**Less secure authentication methods:**

Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

- User can change password after it has expired

Microsoft Encrypted Authentication (MS-CHAP)

- User can change password after it has expired

Encrypted authentication (CHAP)

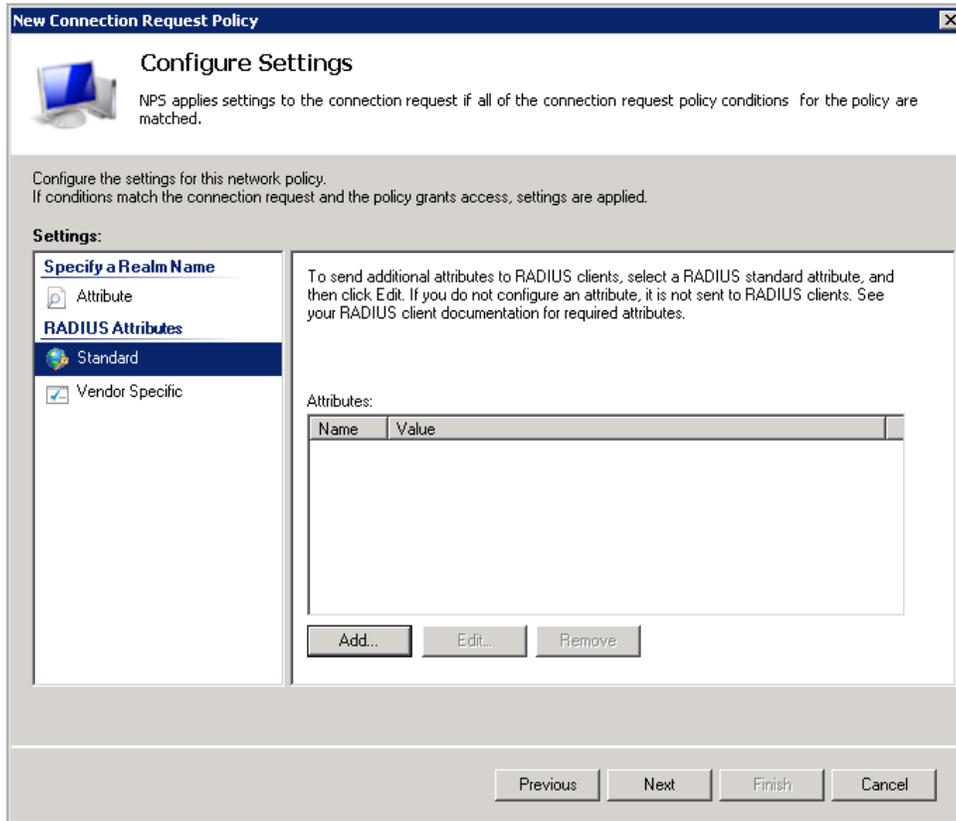
Unencrypted authentication (PAP, SPAP)

Allow clients to connect without negotiating an authentication method.

Previous Next Finish Cancel

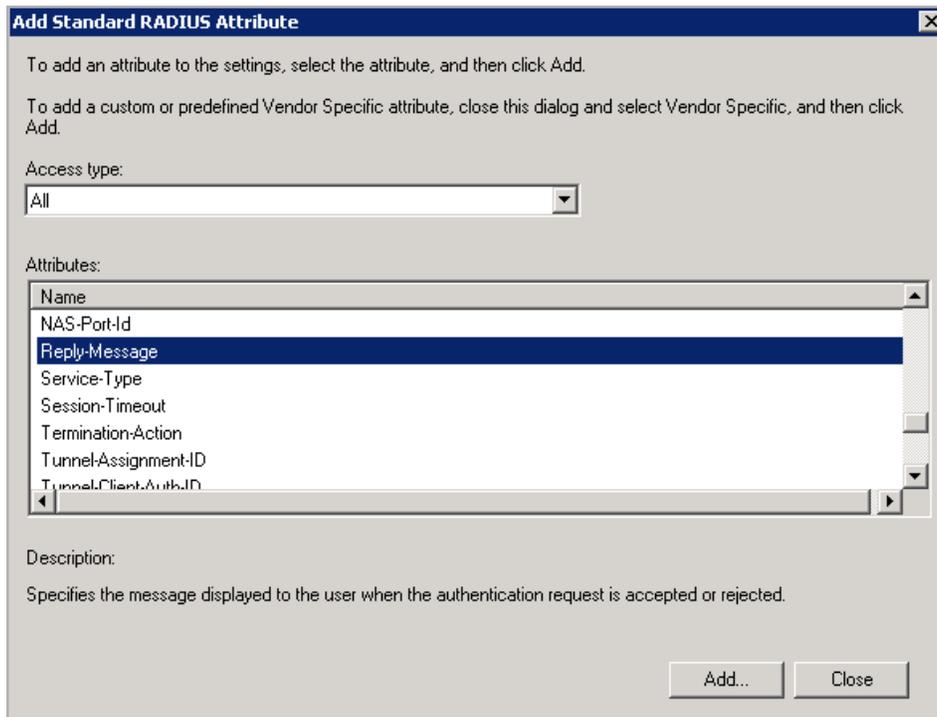
11. Select the **Override network policy authentication settings** check box.
12. Select the **Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)** check box.
13. Select the **User can change password after it has expired** check box.
14. Select the **Unencrypted authentication (PAP, SPAP)** check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

### 3.2.2.2 Specifying RADIUS Authorization for All Users



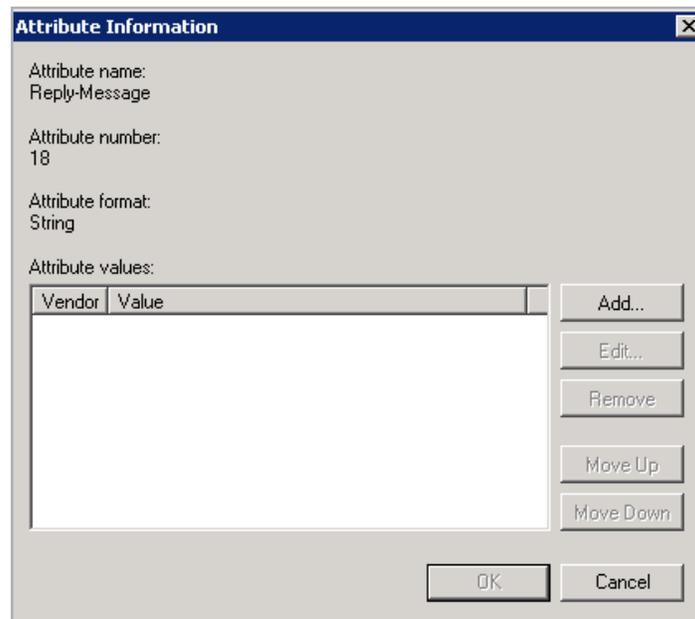
1. Select **Standard** in the panel on the left.
2. Click the **Add...** button.

## 3 Configure Authentication and Authorization

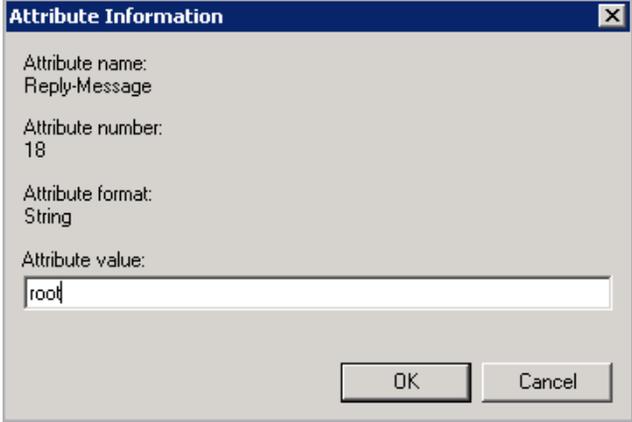


3. Select **Reply-Message**.

4. Click the **Add...** button.



5. Click the **Add...** button.



The image shows a dialog box titled "Attribute Information" with a close button (X) in the top right corner. It contains the following fields:

- Attribute name: Reply-Message
- Attribute number: 18
- Attribute format: String
- Attribute value: root

At the bottom right, there are two buttons: "OK" and "Cancel".

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

---

The available permission options are as follows:

**real,vs,rules,backup,certs,cert3,certbackup,users,root,geo**

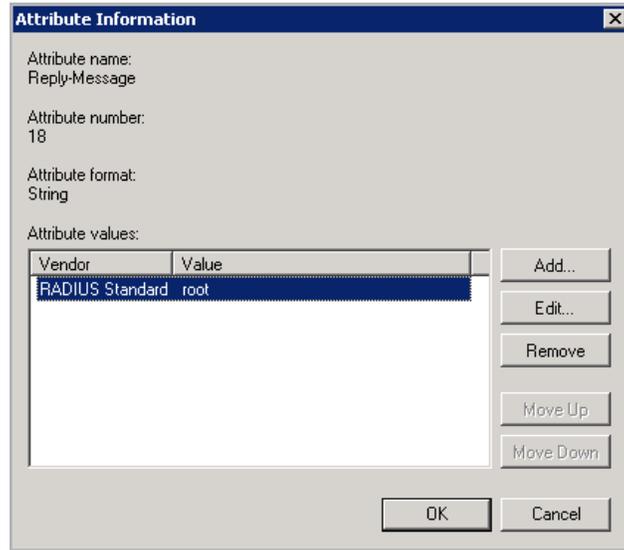
These correspond to the permission options in the LoadMaster Web User Interface (WUI).

The **root** permission grants all permissions.

Multiple attributes can be specified here, but they must be separated by a comma (with no space).

---

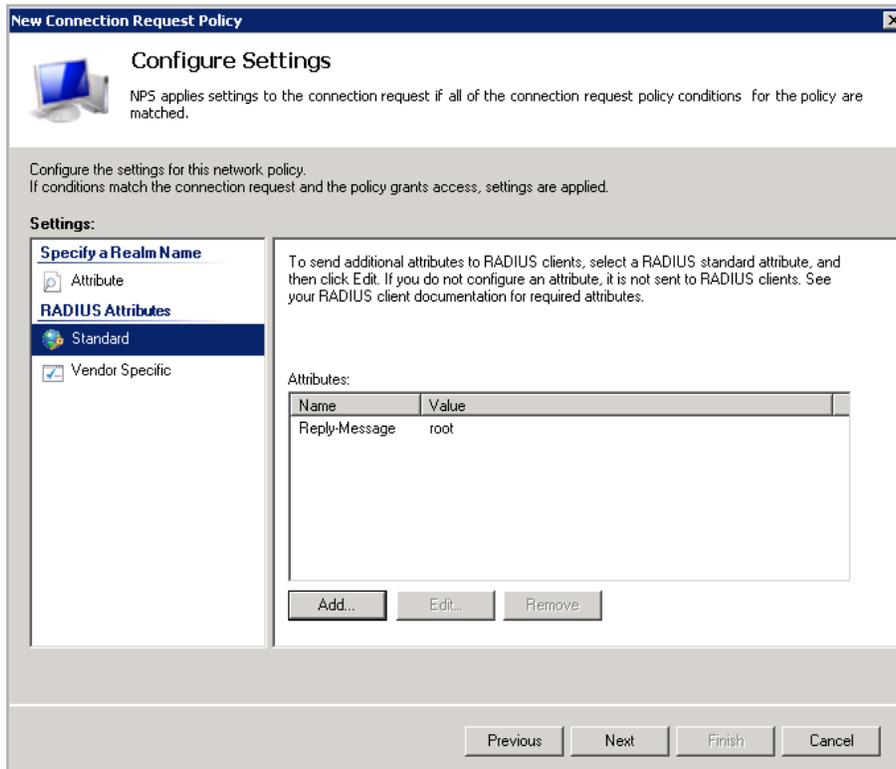
## 3 Configure Authentication and Authorization



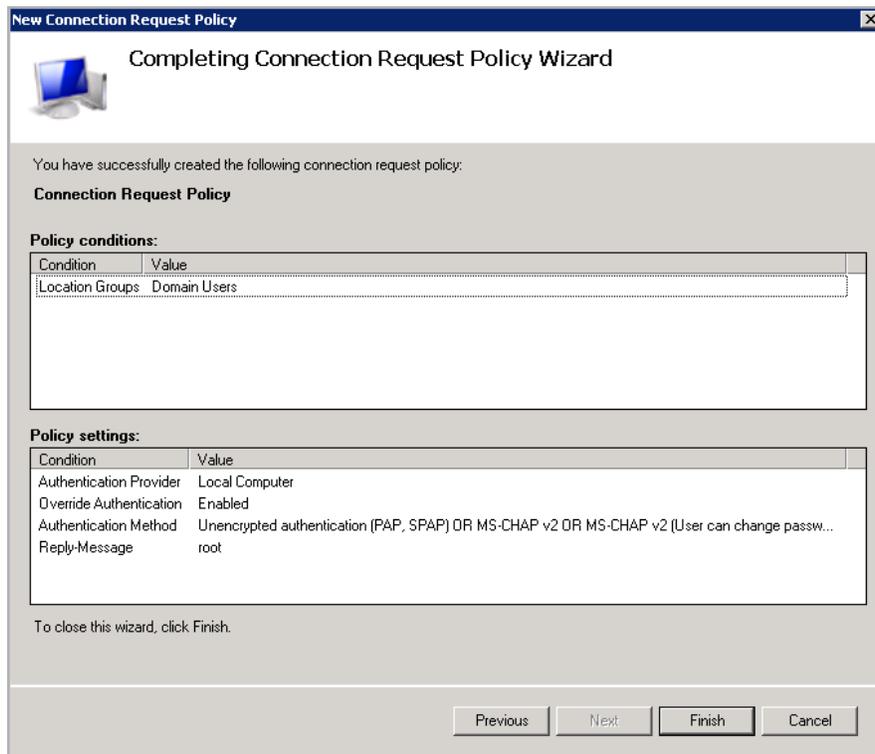
7. Select the attribute and click **OK**.

8. Click **OK** again.

9. Click **Close**.



10. Click **Next**.



11. Click **Finish**.

# References

Unless otherwise specified, the following documents can be found at <http://kemptechnologies.com/documentation>.

**Web User Interface, Configuration Guide**

# Last Updated Date

This document was last updated on 19 March 2021.