



Technical Note RADIUS Authentication and Authorization

8 January 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. 44

Introduction

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

- [Document Purpose](#)
- [Intended Audience](#)

Document Purpose

Document Purpose

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

Intended Audience

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.

Prerequisites for Authentication and Authorization

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

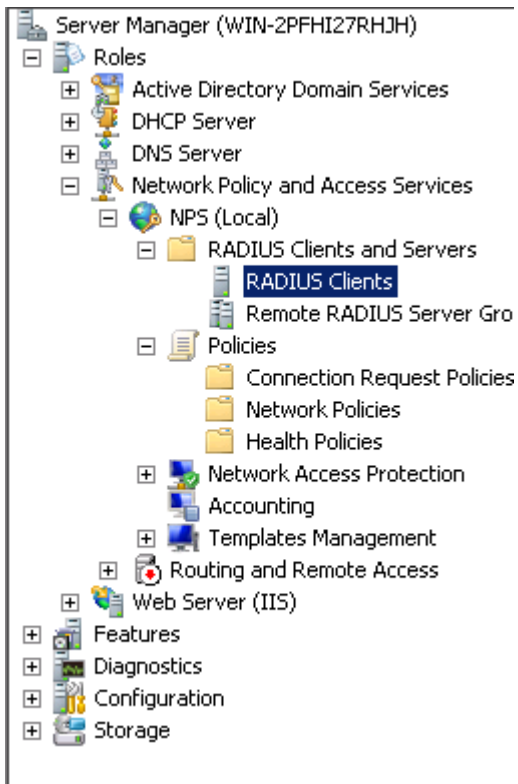
- [Add a RADIUS Client](#)

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.

The screenshot shows the 'Shared Properties' dialog box with the 'Advanced' tab selected. The 'Settings' section has 'Enable this RADIUS client' checked. Below it is an unchecked checkbox for 'Select an existing template:' followed by an empty dropdown menu. The 'Name and Address' section contains a 'Friendly name:' field with the text 'Shared' and an 'Address (IP or DNS):' field with the text '10.86.0.175'. A 'Verify...' button is to the right of the address field. The 'Shared Secret' section has a 'Select an existing Shared Secrets template:' dropdown menu currently set to 'None'. Below this is a text block explaining manual and automatic secret generation. There are two radio buttons: 'Manual' (selected) and 'Generate'. Below the radio buttons are two text fields: 'Shared secret:' and 'Confirm shared secret:', both containing masked characters (dots). At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

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.

Configure Authentication and Authorization

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

- [Local Authentication and Authorization](#)
- [RADIUS Authentication and Authorization](#)

Local 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.

Related Links

- [Specify the RADIUS Server Details](#)
- [Specifying RADIUS Authentication for an Individual User](#)
- [Specifying Local Authorization for an Individual User](#)

Specify the RADIUS Server Details

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

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="password"/>	
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"/>

Specifying Local Authorization for an Individual User

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.

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	<ul style="list-style-type: none"> View existing Virtual Services 	<ul style="list-style-type: none"> Add Virtual Service

Allow Extended Permissions	Virtual Services	Add Virtual Service	Operations Allowed	Operations not Allowed
			<ul style="list-style-type: none"> • Modify existing Virtual Services • Change Virtual Service port 	<ul style="list-style-type: none"> • Duplicate Virtual Service • Change Address • Export template
Enabled	Disabled	Enabled	<ul style="list-style-type: none"> • View existing Virtual Services 	<ul style="list-style-type: none"> • Add Virtual Service • Duplicate Virtual Service • Change Address • Export template • Modify existing Virtual Services • Change Virtual Service port
Enabled	Enabled	Enabled	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Add Virtual Service • Duplicate Virtual Service • Change address • Export template • View existing Virtual Services 	Not applicable

Allow Extended Permissions	Virtual Services	Add Virtual Service	Operations Allowed	Operations not Allowed
			<ul style="list-style-type: none"> • Modify existing Virtual Services • Change Virtual Service port 	
Disabled	Disabled	Disabled	View existing Virtual Services	<ul style="list-style-type: none"> • Add Virtual Service • Duplicate Virtual Service • Change address • Export template • Modify existing Virtual Service • Change Virtual Service port

RADIUS Authentication and Authorization

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.

Related Links

- [Specify the RADIUS Server Details](#)
- [Specifying RADIUS permissions for Groups and All Users](#)

Specify the RADIUS Server Details

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"/>	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"/>	Set Basic Password
Failed Login Attempts	<input type="text" value="3"/>	Set Fail Limit (Valid values:1-999)
Idle Session Timeout	<input type="text" value="600"/>	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**.

Administrator Access

Allow Remote SSH Access	<input checked="" type="checkbox"/>	Using: <input type="text" value="All Networks"/>	Port: <input type="text" value="22"/>	Set Port
SSH Pre-Auth Banner		<input type="text"/>		
		Set Pre-Auth Message		
Allow Web Administrative Access	<input checked="" type="checkbox"/>	Using: <input type="text" value="eth0: 10.35.48.11"/>	Port: <input type="text" value="443"/>	
Admin Default Gateway		<input type="text"/>		
		Set Administrative Access		
Allow Multi Interface Access	<input type="checkbox"/>			
Enable API Interface	<input checked="" type="checkbox"/>	Port: <input type="text" value="443"/>	Set Port	
Self-Signed Certificate Handling		<input type="text" value="RSA self-signed certs"/>		
Outbound Connection Cipher Set		<input type="text" value="None - Outbound Default"/>		
Admin Login Method		<input type="text" value="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	<input checked="" type="checkbox"/>			

GEO Settings

Remote GEO LoadMaster Access	<input type="text"/>	Set GEO LoadMaster access
GEO LoadMaster Partners	<input type="text"/>	Set GEO LoadMaster Partners
GEO LoadMaster Port	<input type="text" value="22"/>	Set GEO LoadMaster Port
GEO Update Interface	<input type="text" value="eth0: 10.35.48.11"/>	

WUI Authorization Options

6. Click **WUI Authorization Options**.

WUI AAA Service Authentication Authorization Options

RADIUS		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	RADIUS Server <input type="text" value="10.154.11.80"/> Port <input type="text" value="80"/> RADIUS Server Shared Secret <input type="text" value="Please set passv"/> Set Secret Backup RADIUS Server <input type="text"/> Port <input type="text"/> Backup Server Backup Shared Secret <input type="text"/> Set Backup Secret Revalidation Interval <input type="text" value="60"/> Set Interval Send NAS Identifier <input type="checkbox"/>
LDAP		<input type="checkbox"/>		LDAP Endpoint <input type="text" value="EXAMPLE"/> Manage LDAP Configuration Remote User Groups <input type="text" value="ExampleGroup2;ExampleRemoteUserGroup;"/> Select groups <input type="checkbox"/> Nested groups Domain <input type="text"/> Set Domain
Local Users		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Use ONLY if other AAA services fail <input type="checkbox"/>

Test AAA for User

Username	<input type="text"/>	Test User
Password	<input type="text"/>	

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

Note: IPv6 is not supported for RADIUS authentication.

- Select the **Radius Authentication** check box.
- Select the **Radius Authorization** check box.
- Click **Radius Server**.
- Enter the **Shared Secret**.

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

- Click **Set Secret**.
- If necessary, fill out details for a **Backup Radius Server**.
- Enter the **Revalidation Interval**.
- 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.

- 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

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.

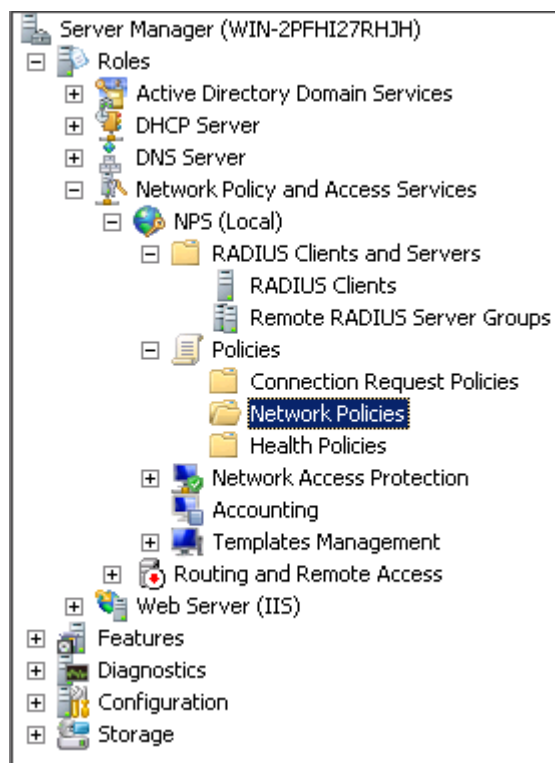
Connection request policies apply to all users. Network policies apply to groups.

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

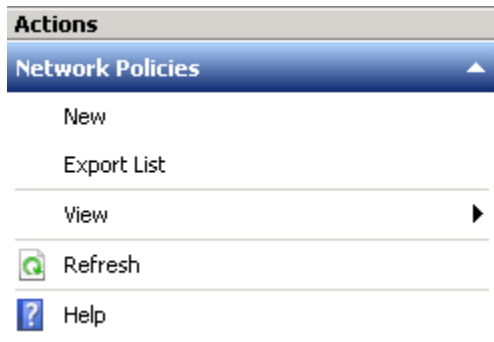
Specifying RADIUS Authentication and Authorization for a Group (Network Request Policy)

Specifying RADIUS Authentication for a Group

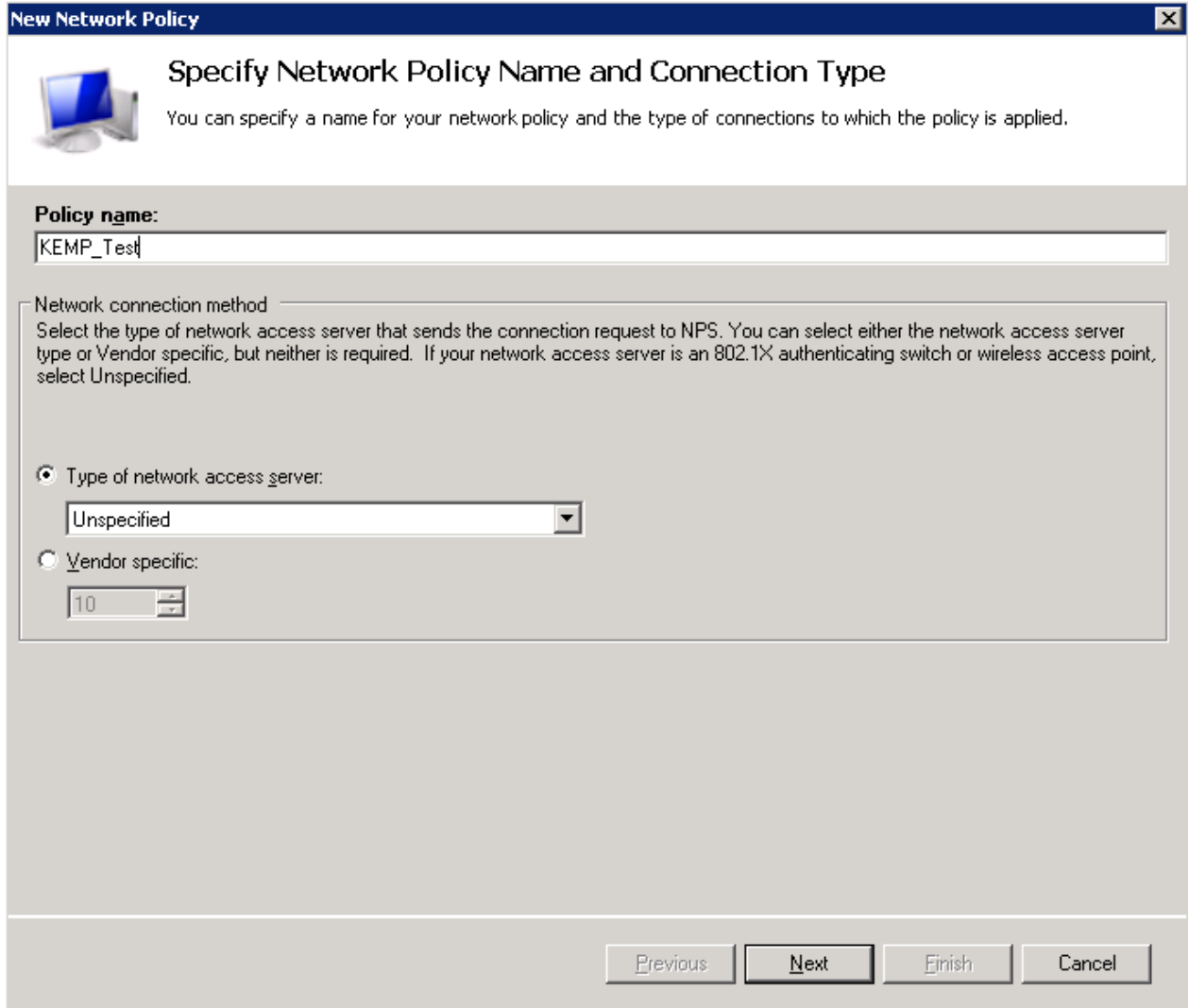
To set up a network policy, follow the steps below in the **Server Manager**.



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



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



The image shows a Windows-style dialog box titled "New Network Policy". It has a blue header bar with the title and a close button (X). Below the header, there is a small icon of a computer monitor and the text "Specify Network Policy Name and Connection Type". A subtitle reads: "You can specify a name for your network policy and the type of connections to which the policy is applied." Below this, there is a section labeled "Policy name:" with a text input field containing "KEMP_Test". Underneath, there is a section titled "Network connection method" with a descriptive paragraph: "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." There are two radio buttons: "Type of network access server:" (selected) and "Vendor specific:". The "Type of network access server:" option has a dropdown menu showing "Unspecified". The "Vendor specific:" option has a text input field containing "10". At the bottom right, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

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**.

New Network Policy [X]

 **Specify Conditions**

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

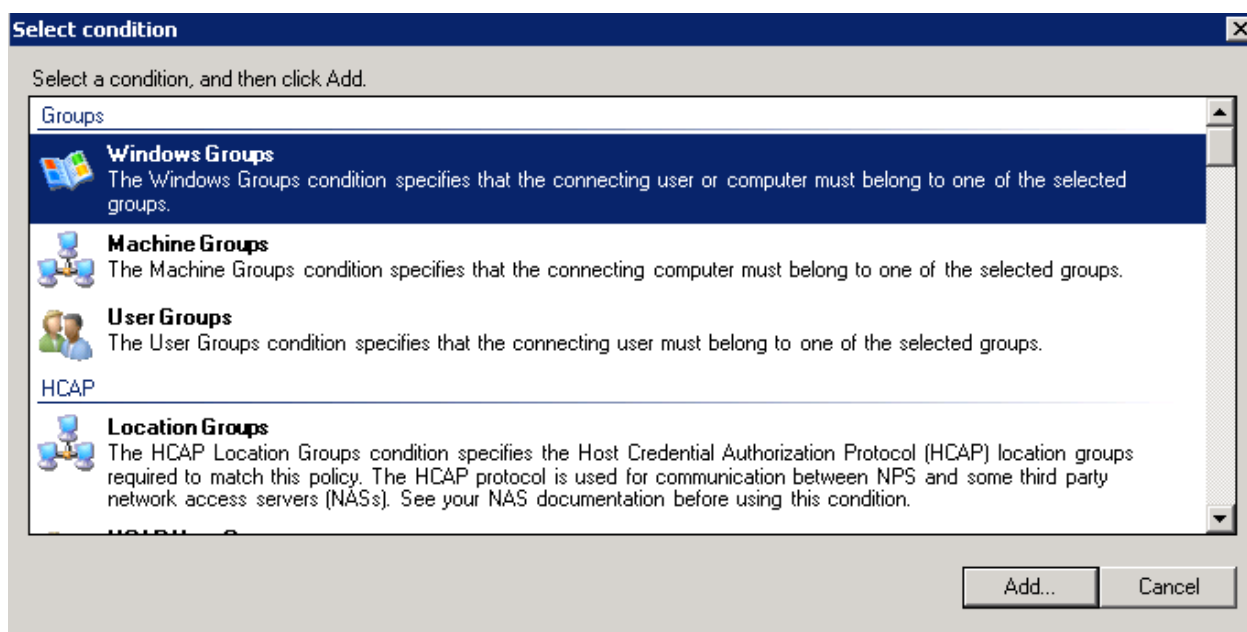
Condition	Value
-----------	-------

Condition description:

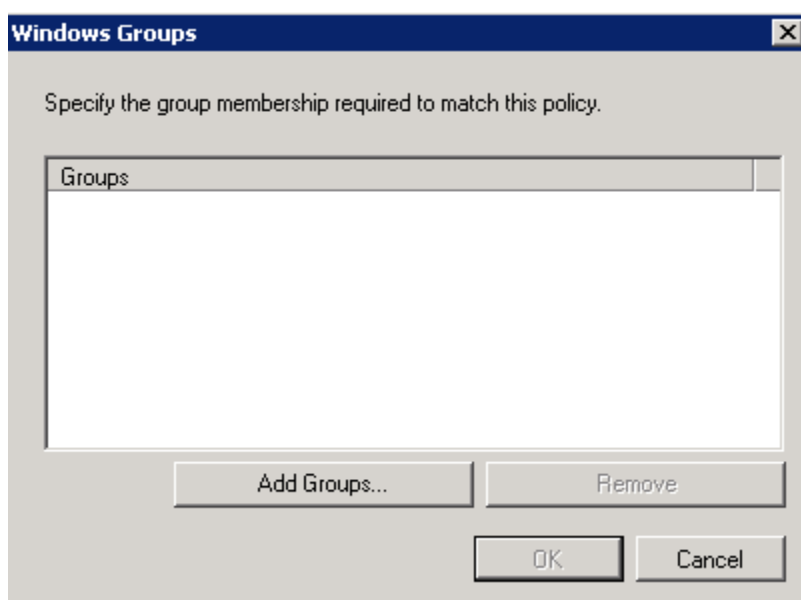
[Add...] [Edit...] [Remove]

[Previous] [Next] [Finish] [Cancel]

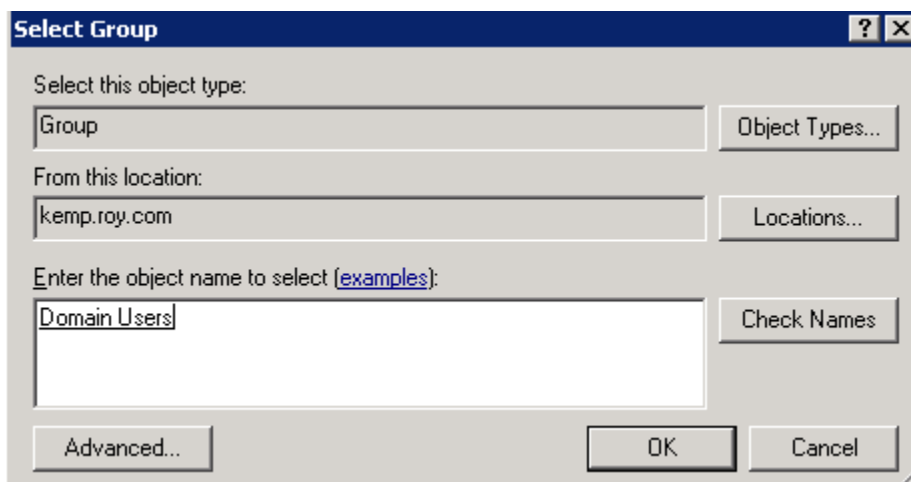
5. Click the **Add...** button.



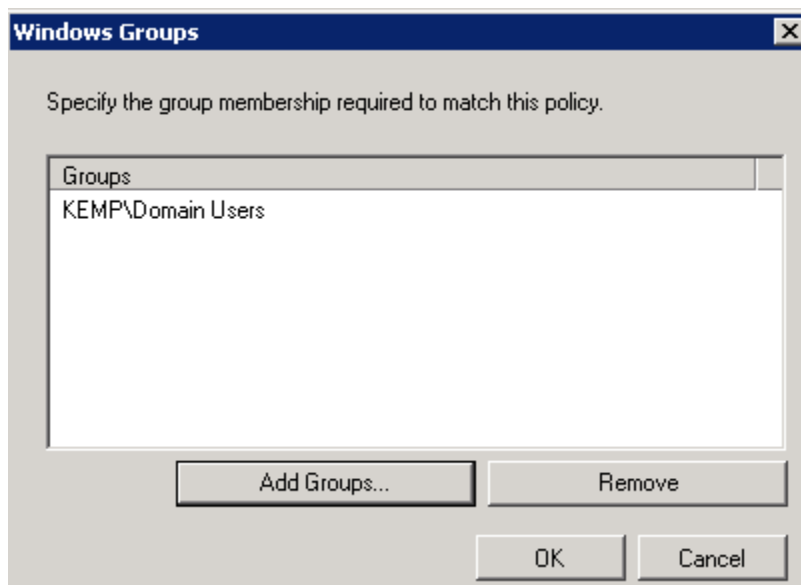
6. Select the relevant group type.
7. Click the **Add...** button.



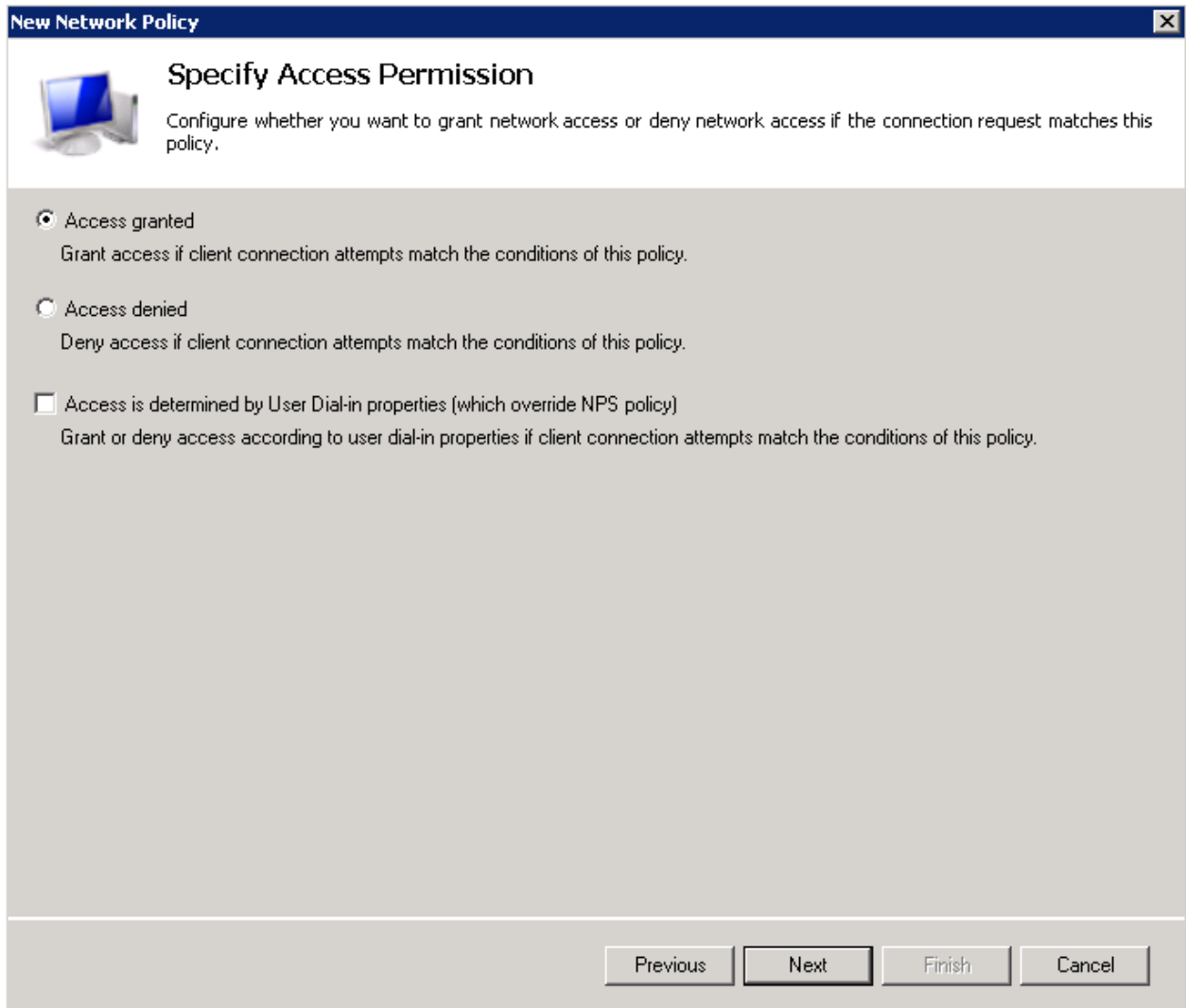
8. Click the **Add Groups...** button.



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**.



The image shows a Windows-style dialog box titled "New Network Policy". It has a blue header bar with the title and a close button (X). Below the header, there is a small icon of a computer monitor and the title "Specify Access Permission". A descriptive text says: "Configure whether you want to grant network access or deny network access if the connection request matches this policy." There are three radio button options: "Access granted" (selected), "Access denied", and "Access is determined by User Dial-in properties (which override NPS policy)". Each option has a sub-description. At the bottom right, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

☒ Access granted
Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

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:

Move Up
Move Down

Add... Edit... Remove

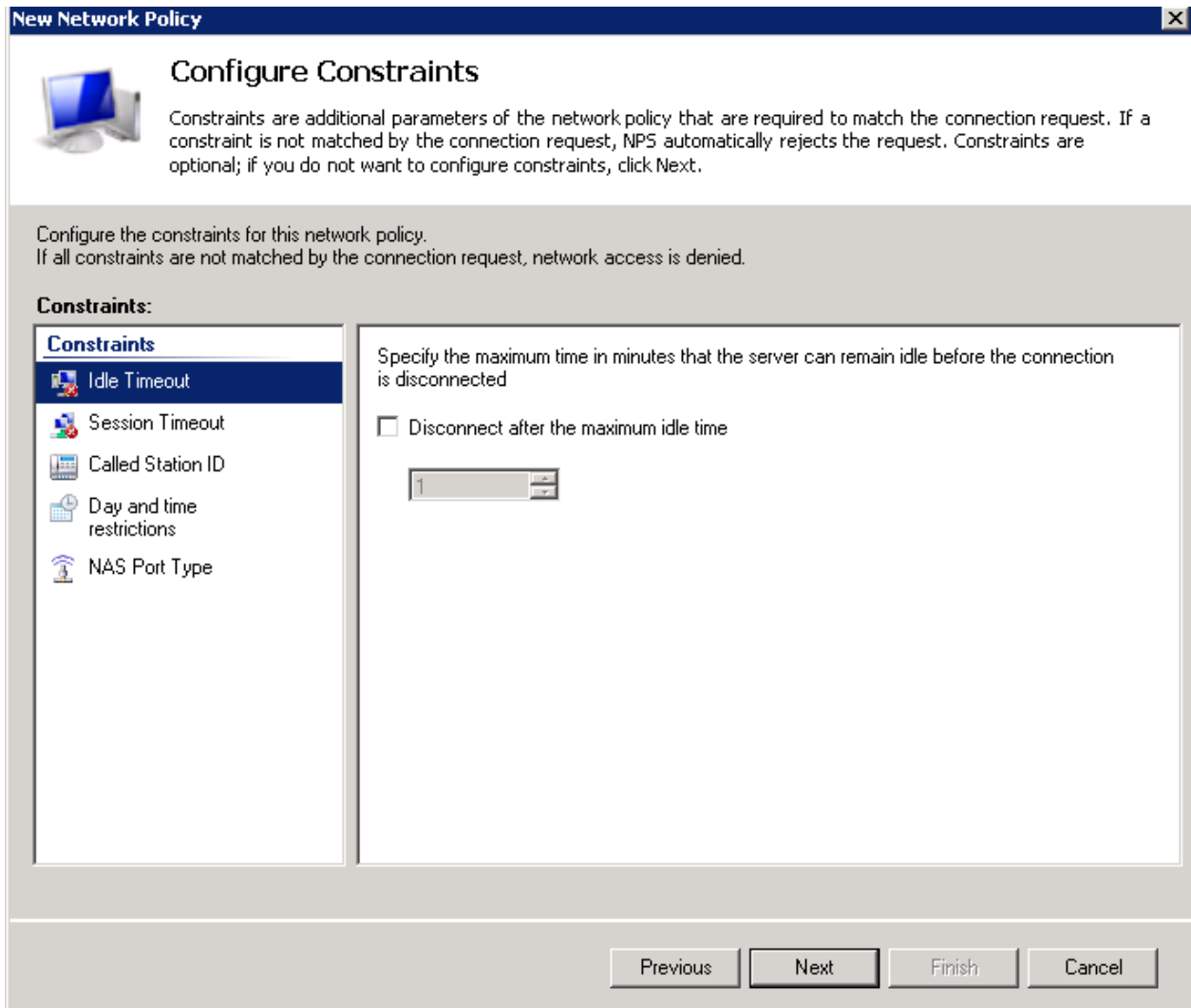
Less secure authentication methods:

- ☐ 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.
- ☐ Perform machine health check only

Previous Next Finish Cancel

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.



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

- Constraints**
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

1

Previous Next Finish Cancel

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

New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

- ☒ Standard
- ☒ Vendor Specific

Network Access Protection

- ☒ NAP Enforcement
- ☒ Extended State

Routing and Remote Access

- ☒ Multilink and Bandwidth Allocation Protocol (BAP)
- ☒ IP Filters
- ☒ Encryption
- ☒ IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

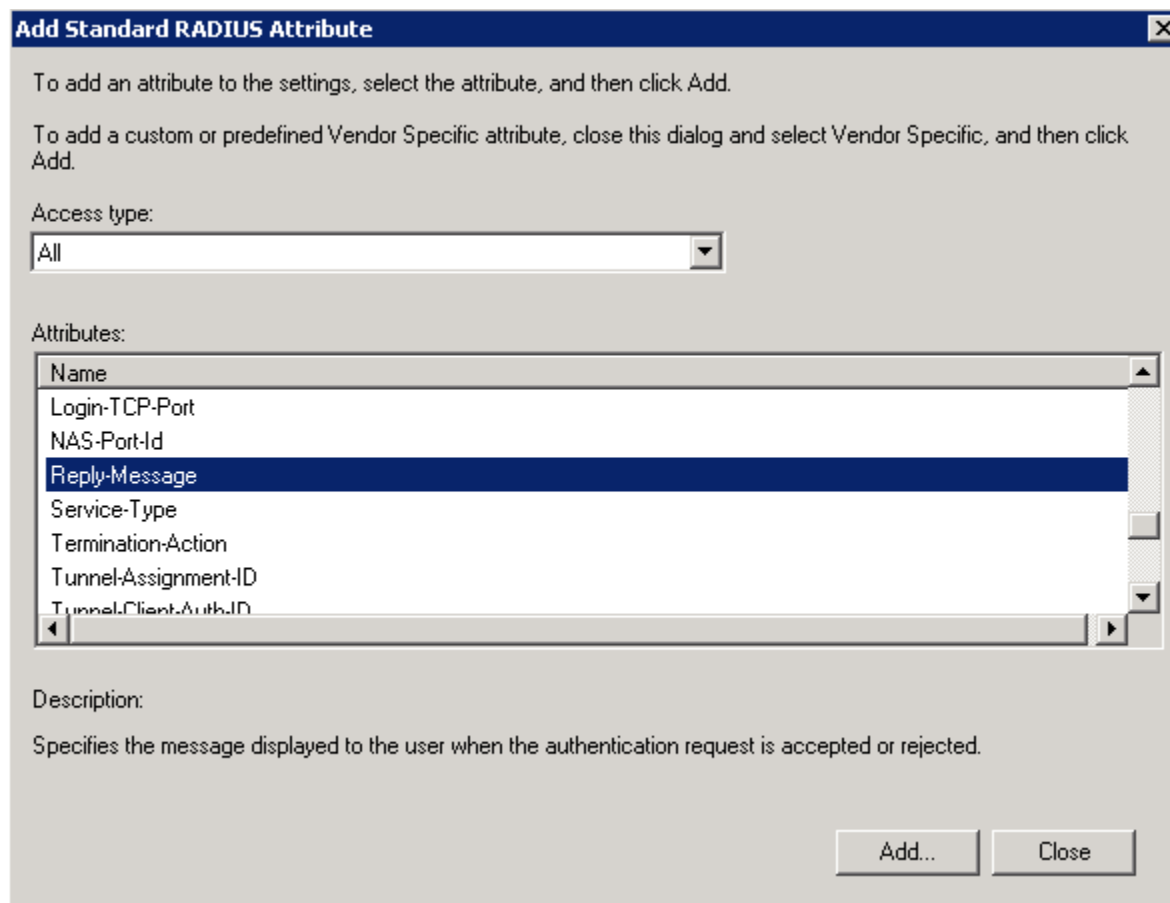
Add... Edit... Remove

Previous Next Finish Cancel

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-Message****2. Framed-Protocol****3. 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.



Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:

All

Attributes:

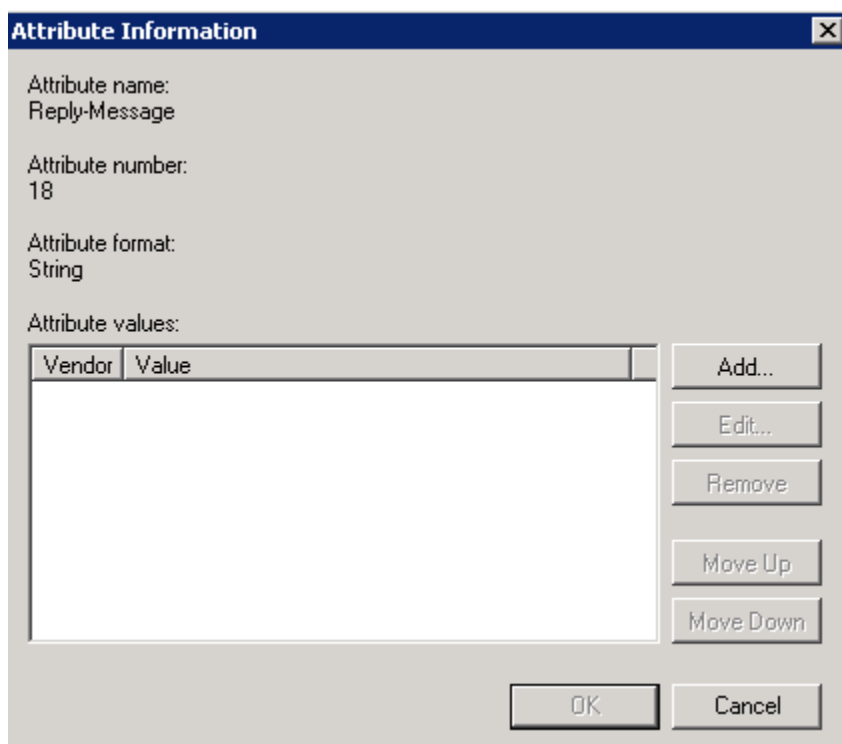
Name
Login-TCP-Port
NAS-Port-Id
Reply-Message
Service-Type
Termination-Action
Tunnel-Assignment-ID
Tunnel-Client-Auth-ID

Description:

Specifies the message displayed to the user when the authentication request is accepted or rejected.

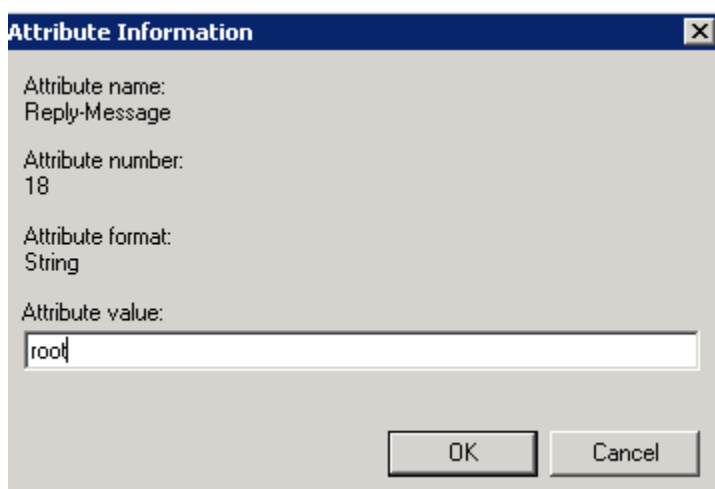
Add... Close

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



The 'Attribute Information' dialog box is shown. It has a title bar with a close button. The fields are: 'Attribute name:' with the value 'Reply-Message', 'Attribute number:' with the value '18', and 'Attribute format:' with the value 'String'. Below these is the 'Attribute values:' section, which contains a table with two columns: 'Vendor' and 'Value'. The table is currently empty. To the right of the table are five buttons: 'Add...', 'Edit...', 'Remove', 'Move Up', and 'Move Down'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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

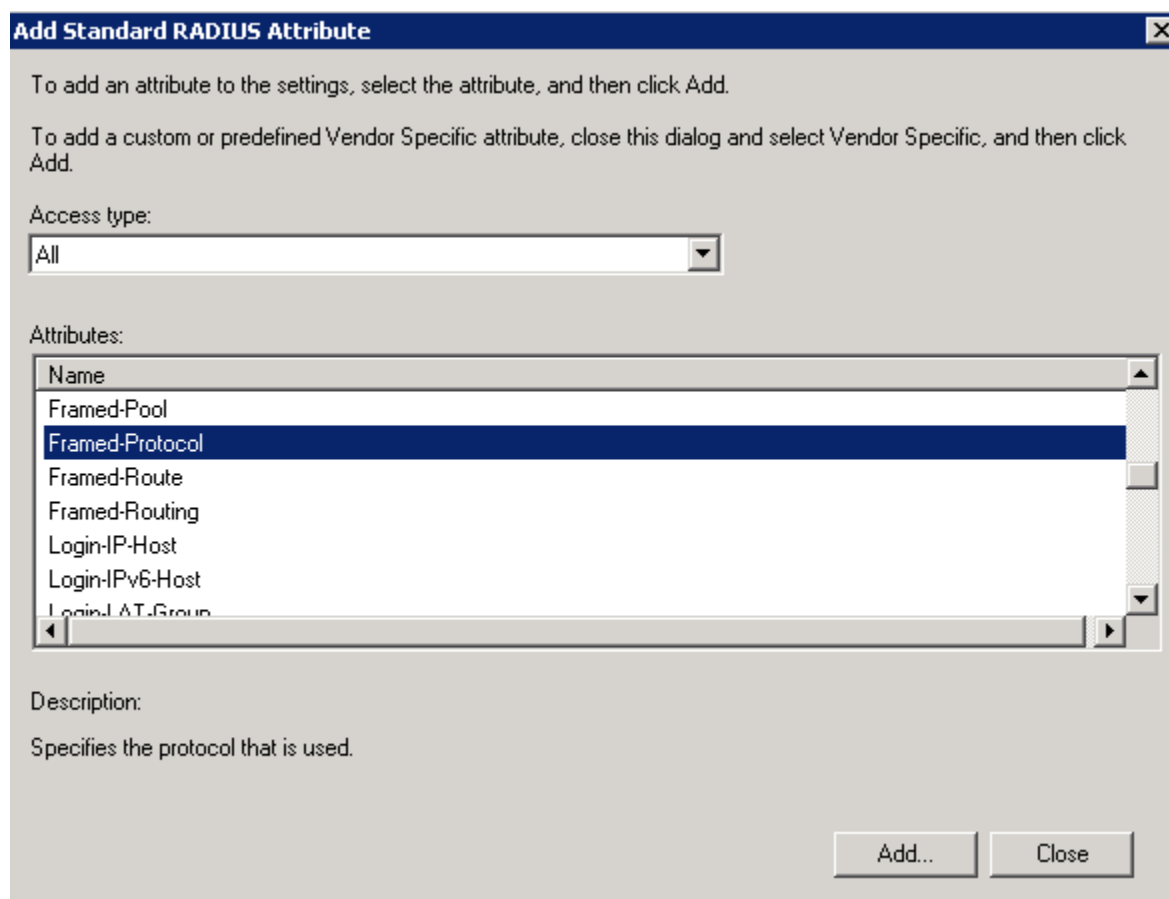


The 'Attribute Information' dialog box is shown again. The 'Attribute name:' is 'Reply-Message', 'Attribute number:' is '18', and 'Attribute format:' is 'String'. The 'Attribute value:' field now contains the text 'root'. The 'Add...' button is no longer visible, and the 'OK' and 'Cancel' buttons are at the bottom.

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**.



Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

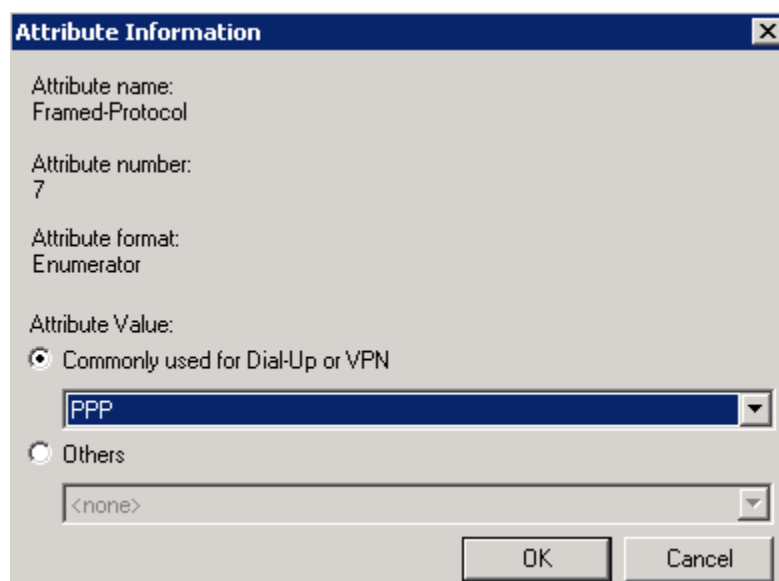
Access type:

Attributes:

Name
Framed-Pool
Framed-Protocol
Framed-Route
Framed-Routing
Login-IP-Host
Login-IPv6-Host
Login-AT-Group

Description:
 Specifies the protocol that is used.

- Click the **Add...** button.



Attribute Information

Attribute name:
 Framed-Protocol

Attribute number:
 7

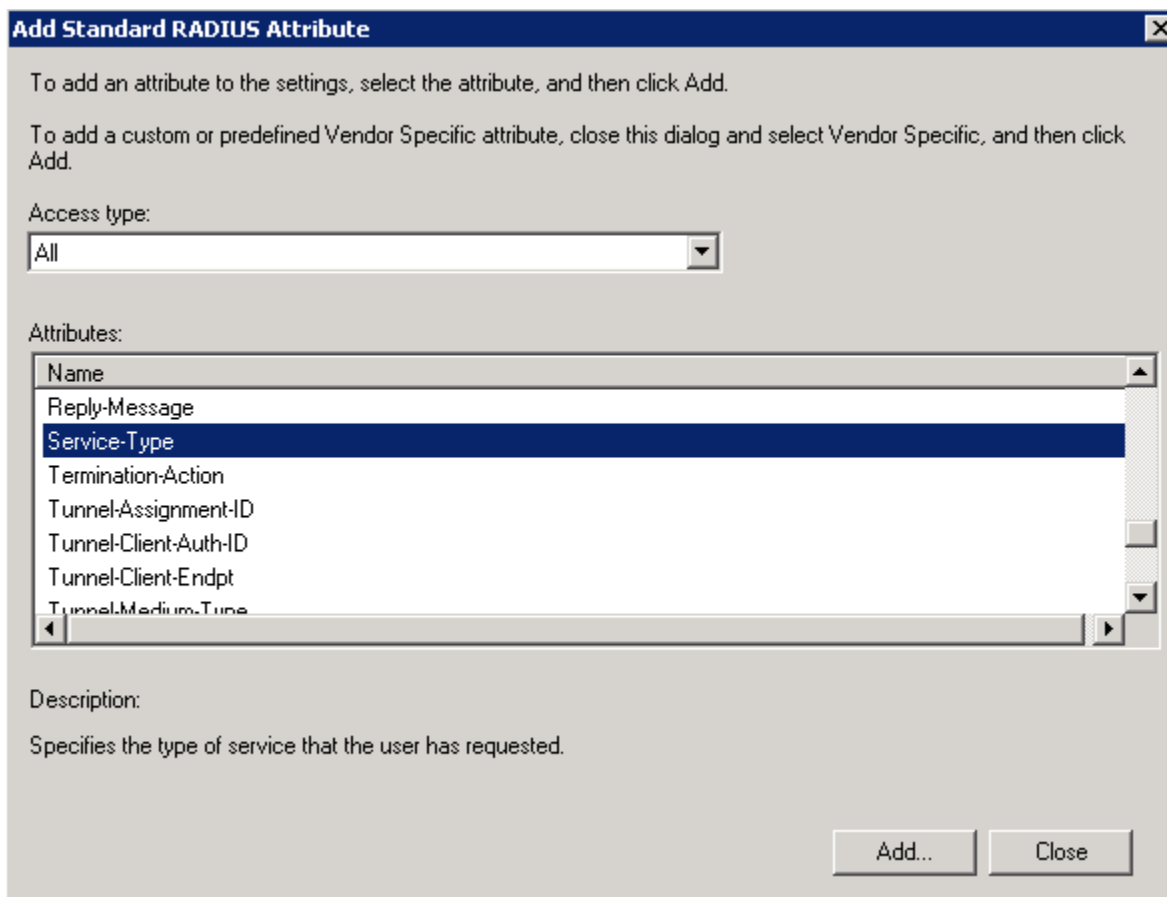
Attribute format:
 Enumerator

Attribute Value:

☒ Commonly used for Dial-Up or VPN

☐ Others

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



Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:
All

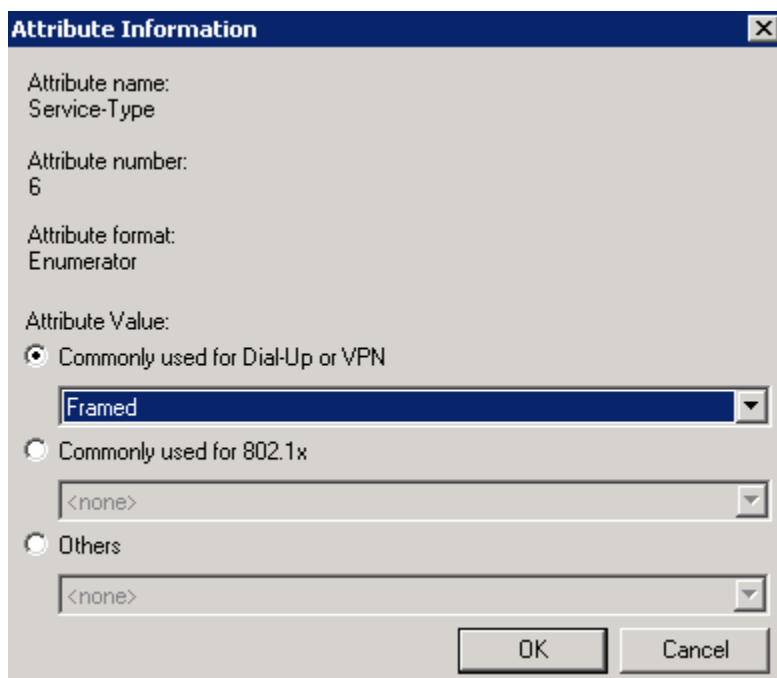
Attributes:

Name
Reply-Message
Service-Type
Termination-Action
Tunnel-Assignment-ID
Tunnel-Client-Auth-ID
Tunnel-Client-Endpt
Tunnel-Medium-Type

Description:
Specifies the type of service that the user has requested.

Add... Close

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



The image shows a Windows-style dialog box titled "Attribute Information". It contains the following fields and options:

- Attribute name: Service-Type
- Attribute number: 6
- Attribute format: Enumerator
- Attribute Value:
 - ☒ Commonly used for Dial-Up or VPN: A dropdown menu with "Framed" selected.
 - ☐ Commonly used for 802.1x: A dropdown menu with "<none>" selected.
 - ☐ Others: A dropdown menu with "<none>" selected.

At the bottom right are "OK" and "Cancel" buttons.

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

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

KEMP_Test

Policy conditions:

Condition	Value
Windows Groups	KEMP\Domain Users

Policy settings:

Condition	Value
Authentication Method	Unencrypted authentication (PAP, SPAP) OR MS-CHAP v1 OR MS-CHAP v1 (User can change p...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Ignore User Dial-In Properties	False
Reply-Message	root

To close this wizard, click Finish.

Previous Next Finish Cancel

19. Click **Finish**.

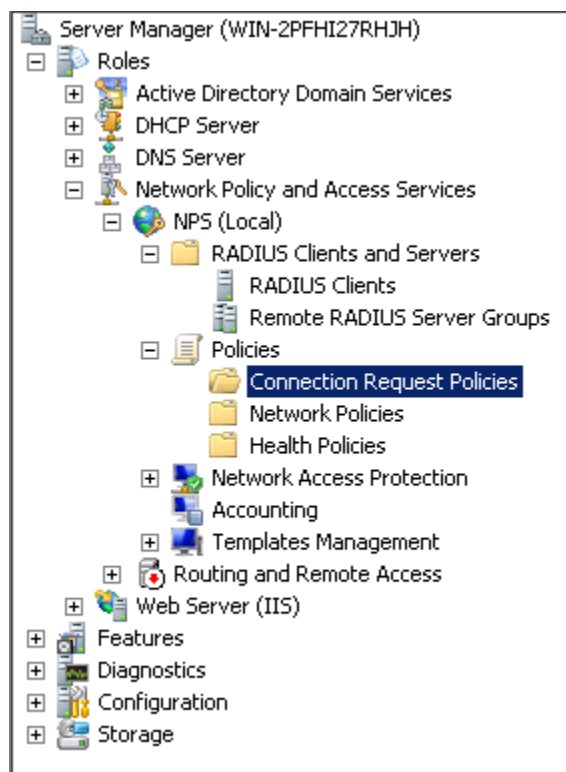
20. Repeat this process as needed to set permissions for other groups.

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.

New Connection Request Policy [X]

 **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

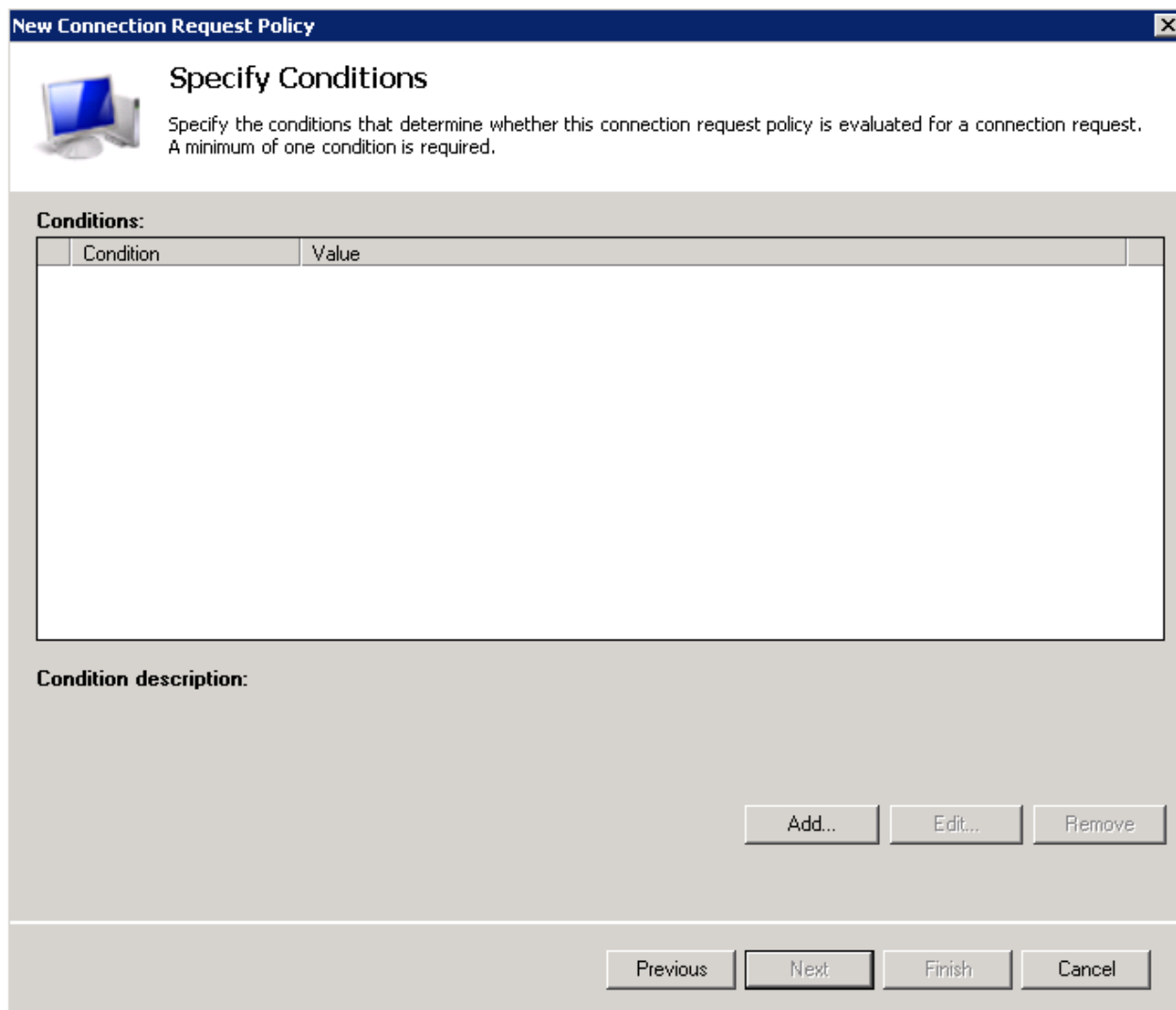
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select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

☒ Type of network access server:
Unspecified

☐ Vendor specific:
10

Previous Next Finish Cancel

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



The dialog box is titled "New Connection Request Policy" and has a close button (X) in the top right corner. Below the title bar, there is a section titled "Specify Conditions" with a computer icon. The text below the title says: "Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required." Below this text is a table with two columns: "Condition" and "Value". The table is currently empty. Below the table is a section titled "Condition description:". At the bottom right of the dialog, there are three buttons: "Add...", "Edit...", and "Remove". At the very bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

New Connection Request Policy

Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

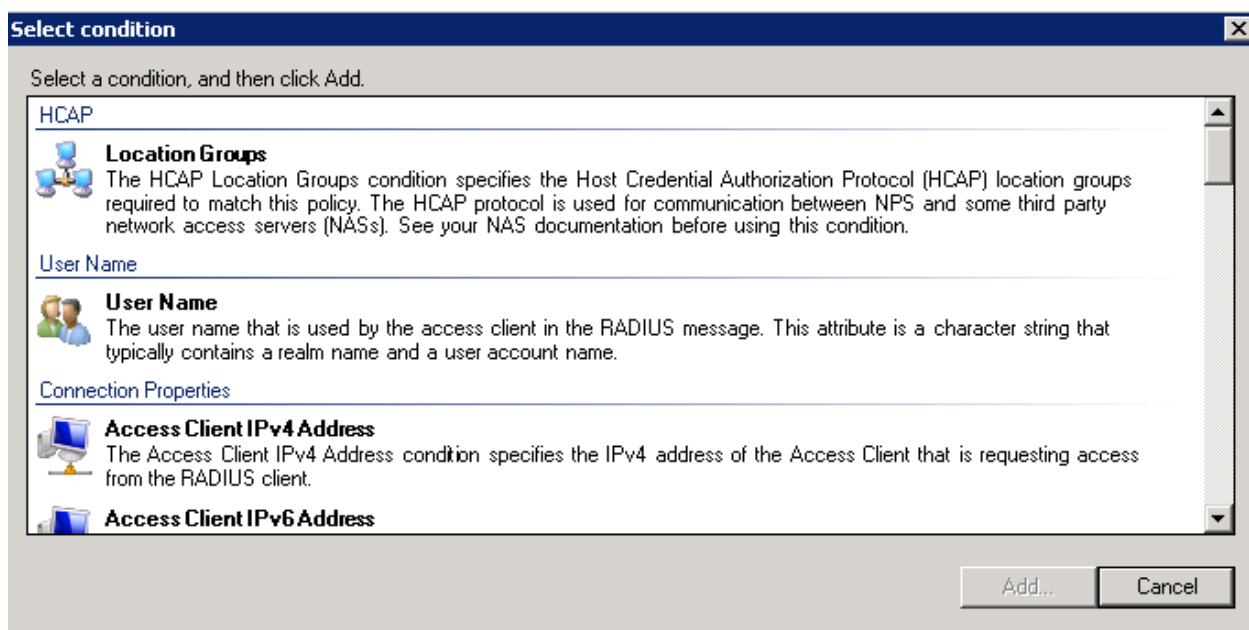
Condition	Value
-----------	-------

Condition description:

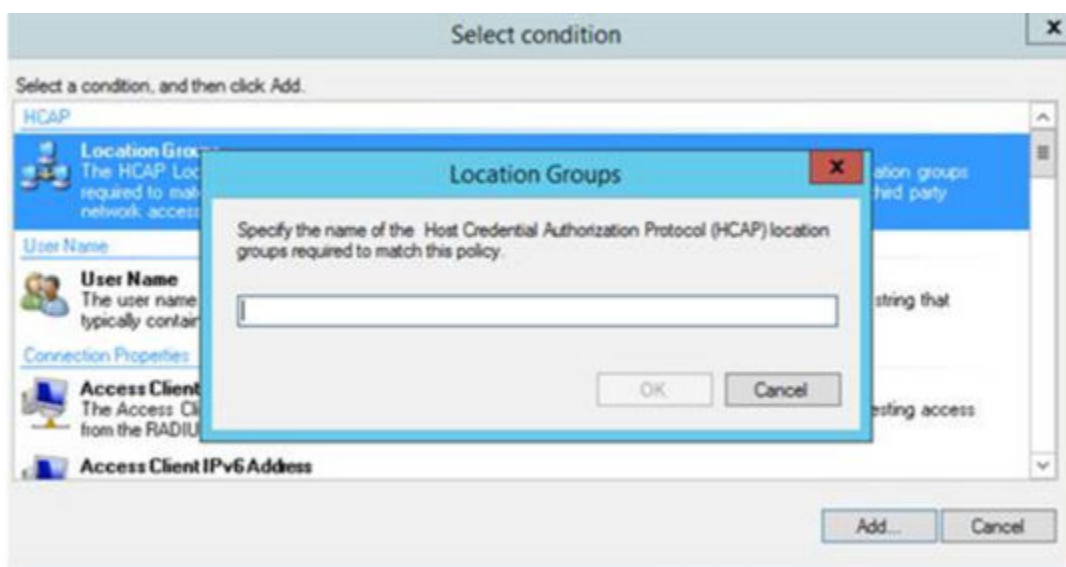
Add... Edit... Remove

Previous Next Finish Cancel

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**.

New Connection Request Policy



Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Forwarding Connection Request

→ Authentication

Accounting

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

☒ Authenticate requests on this server

☐ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

New...

☐ Accept users without validating credentials

Previous

Next

Finish

Cancel

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:

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.

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

New Connection Request Policy

Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are applied.

Settings:

Specify a Realm Name

- Attribute
- RADIUS Attributes**
 - Standard**
 - Vendor Specific

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

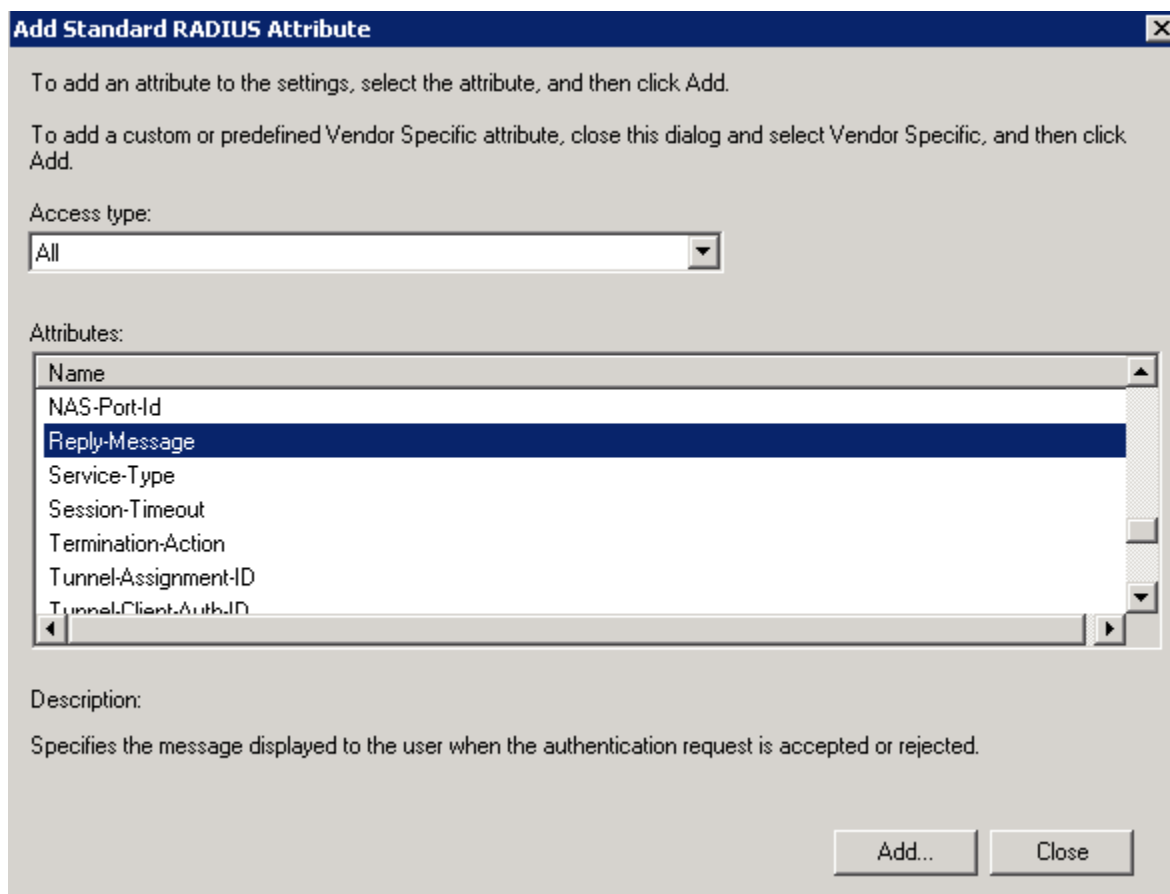
Attributes:

Name	Value
------	-------

Add... Edit... Remove

Previous Next Finish Cancel

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



Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:
All

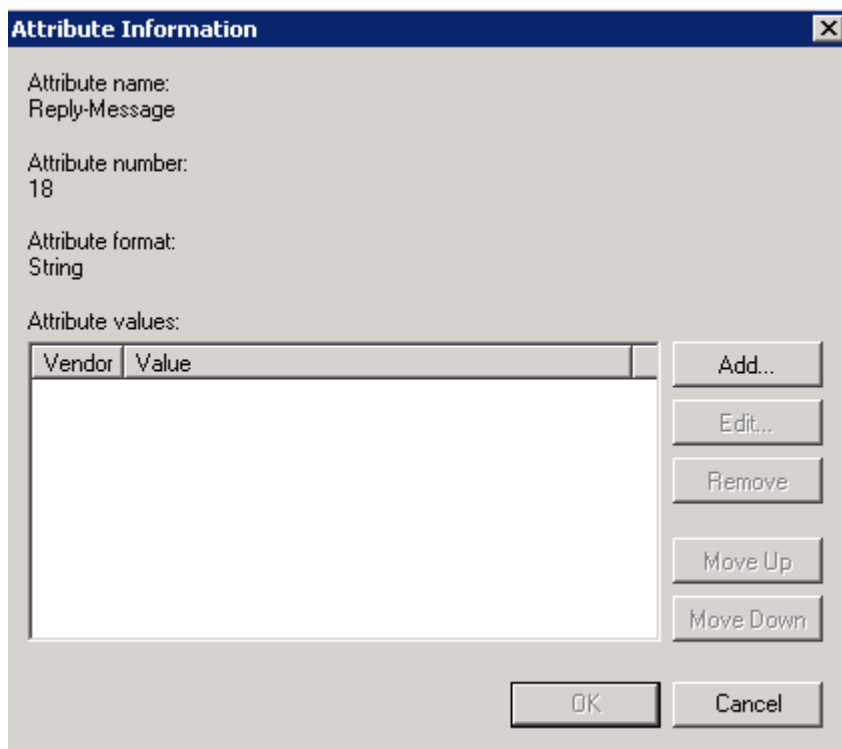
Attributes:

Name
NAS-Port-Id
Reply-Message
Service-Type
Session-Timeout
Termination-Action
Tunnel-Assignment-ID
Tunnel-Client-Auth-ID

Description:
Specifies the message displayed to the user when the authentication request is accepted or rejected.

Add... Close

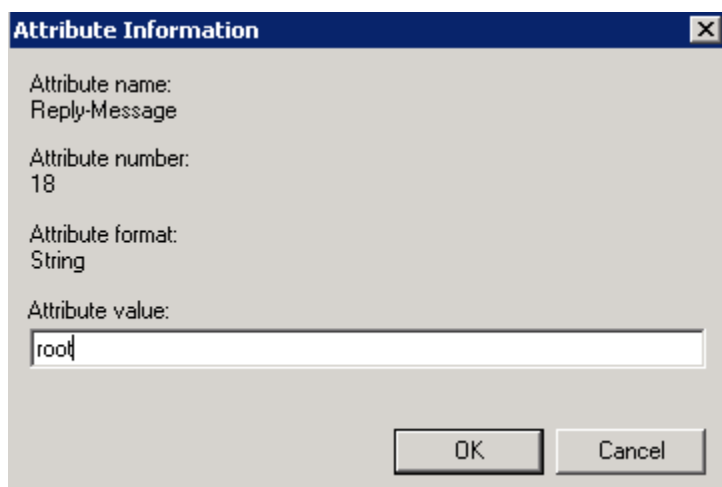
3. Select **Reply-Message**.
4. Click the **Add...** button.



The 'Attribute Information' dialog box displays the following fields and controls:

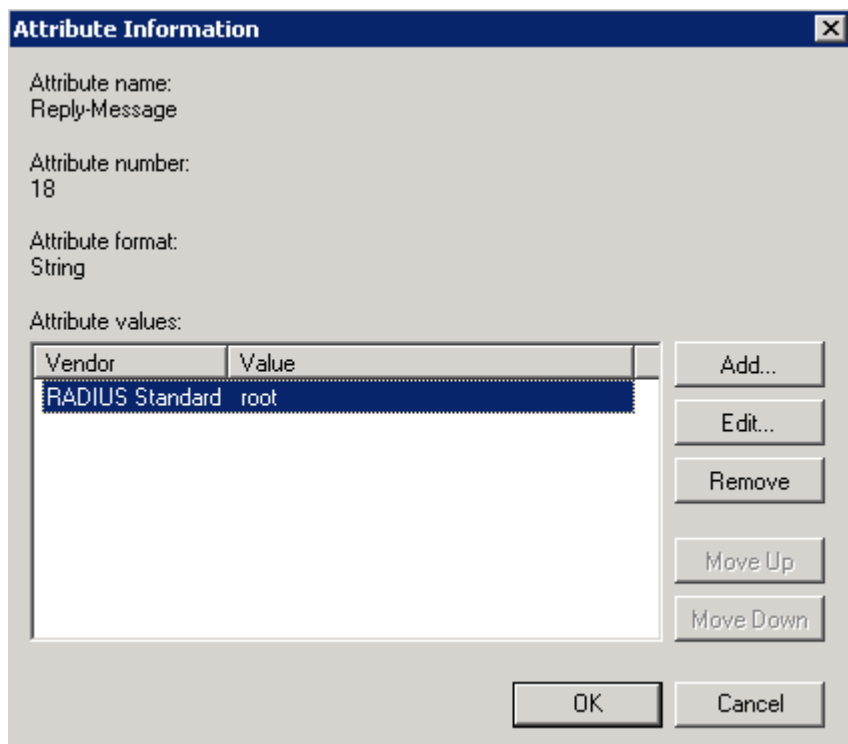
- Attribute name: Reply-Message
- Attribute number: 18
- Attribute format: String
- Attribute values: A table with two columns, 'Vendor' and 'Value', which is currently empty.
- Buttons: Add..., Edit..., Remove, Move Up, Move Down, OK, and Cancel.

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



The 'Attribute Information' dialog box is shown again, but with the 'Attribute value' field containing the text 'root'. The 'Attribute values' table is no longer visible, and the 'Add...' button is no longer present.

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



The dialog box is titled "Attribute Information" and contains the following fields and controls:

- Attribute name: Reply-Message
- Attribute number: 18
- Attribute format: String
- Attribute values: A table with two columns, "Vendor" and "Value". The first row is highlighted with a blue background and contains the text "RADIUS Standard" and "root".

Buttons on the right side of the dialog box:

- Add...
- Edit...
- Remove
- Move Up
- Move Down

Buttons at the bottom of the dialog box:


- OK
- Cancel

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**.

New Connection Request Policy



Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are applied.

Settings:

Specify a Realm Name

Attribute

RADIUS Attributes

Standard

☒ Vendor Specific

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Reply-Message	root

Add...

Edit...

Remove

Previous

Next

Finish


Cancel

10. Click **Next**.

42

Technical Note RADIUS Authentication and Authorization

New Connection Request Policy

 **Completing Connection Request Policy Wizard**

You have successfully created the following connection request policy:

Connection Request Policy

Policy conditions:

Condition	Value
Location Groups	Domain Users

Policy settings:

Condition	Value
Authentication Provider	Local Computer
Override Authentication	Enabled
Authentication Method	Unencrypted authentication (PAP, SPAP) OR MS-CHAP v2 OR MS-CHAP v2 (User can change passw...
Reply-Message	root

To close this wizard, click Finish.

Previous Next Finish Cancel

11. Click **Finish**.

References

References

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

Web User Interface, Configuration Guide