



RADIUS Authentication and Authorization

Technical Note

UPDATED: 28 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

Table of Contents

1 Introduction	5
1.1 Document Purpose	5
1.2 Intended Audience	5
2 Prerequisites for Authentication and Authorization	6
2.1 Add a RADIUS Client	6
3 Configure Authentication and Authorization	10
3.1 Local Authentication and Authorization	10
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	11
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	15
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	23
3.2.2.2 Specify RADIUS Authentication and Authorization for All Users	28
3.2.2.2.1 Specify RADIUS Authentication for All Users (Connection Request Policy)	28
3.2.2.2.2 Specifying RADIUS Authorization for All Users	34
References	39

Last Updated Date	40
--------------------------------	-----------

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.

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.

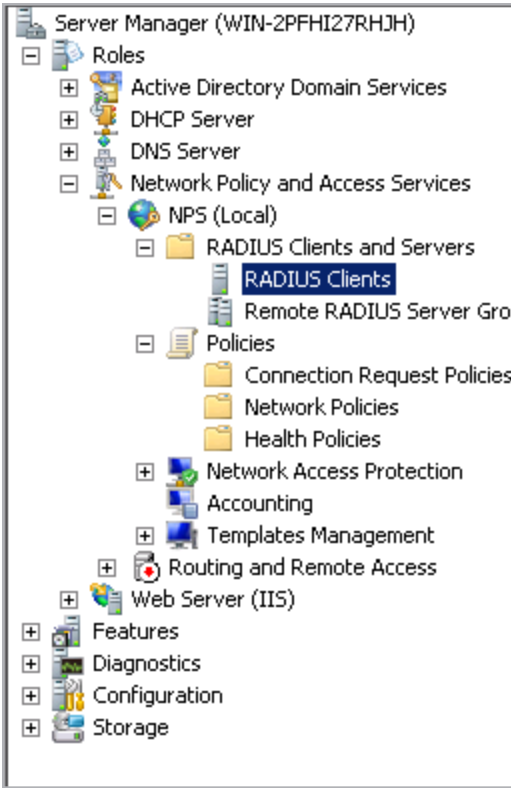
It is not possible to use RADIUS authentication and authorization if you are using a FIPS LoadMaster.

2.1 Add a RADIUS Client

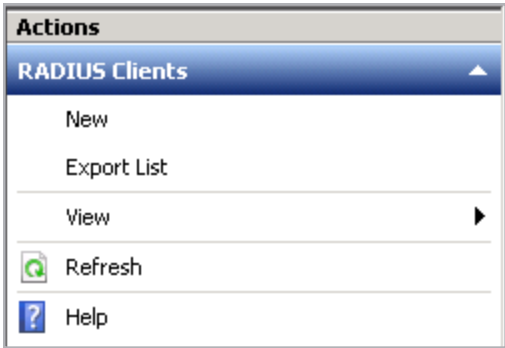
A RADIUS client needs to be created so that the LoadMaster can authenticate. Create a RADIUS client by following the steps below:

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

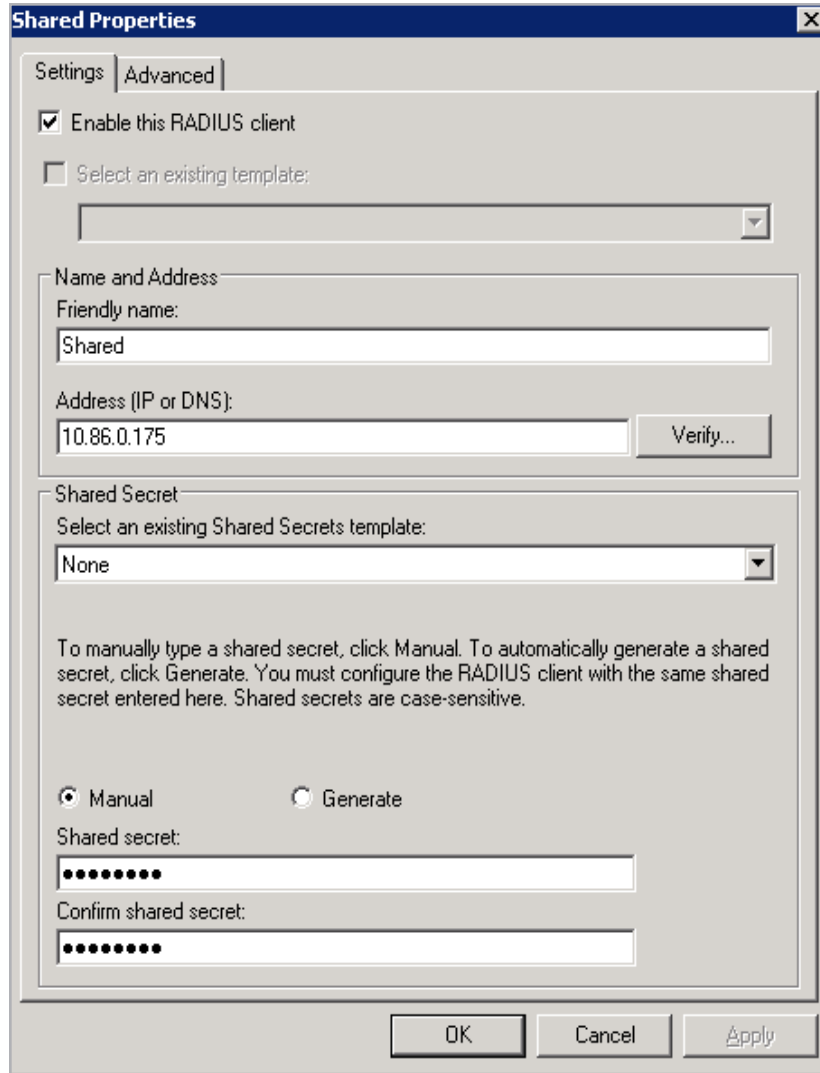
2 Prerequisites for Authentication and Authorization



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**.

2 Prerequisites for Authentication and Authorization

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

Add User

Password

Use RADIUS Server

User	Permissions	Operation
Administrator	Read Only	<div>ModifyDeletePassword</div>

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

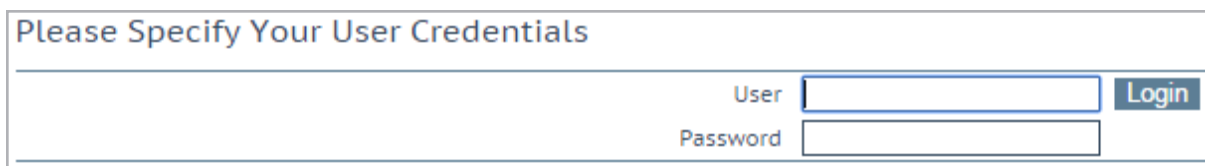
To use the RADIUS Authentication and Authorization method, **Session Management** must be enabled. To enable **Session Management**, follow the steps below:

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



WUI Session Management	
Enable Session Management	<input type="checkbox"/>

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



Please Specify Your User Credentials	
User	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

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

3 Configure Authentication and Authorization

WUI Session Management

Enable Session Management
☒

Require Basic Authentication
☒

Basic Authentication Password
Set Basic Password

Failed Login Attempts
Set Fail Limit (Valid values:1-999)

Idle Session Timeout
Set Idle Timeout (Valid values: 60-86400)

Limit Concurrent Logins

- 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:

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

Administrator Access

Allow Remote SSH Access
☒
Using: Port: Set Port

SSH Pre-Auth Banner
 Set Pre-Auth Message

Allow Web Administrative Access
☒
Using: Port:

Admin Default Gateway
 Set Administrative Access

Allow Multi Interface Access
☐

Enable API Interface
☒
Port: Set Port

Self-Signed Certificate Handling

Outbound Connection Cipher Set

Admin Login Method
 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
 Set GEO LoadMaster Port

GEO Update Interface

WUI Authorization Options

- Click **WUI Authorization Options**.

3 Configure Authentication and Authorization

WUI AAA Service Authentication Authorization Options			
RADIUS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div> RADIUS Server: <input type="text" value="10.154.11.80"/> Port: <input type="text" value="80"/> RADIUS Server </div> <div> Shared Secret: <input type="text" value="Please set passw"/> Set Secret </div> <div> Backup RADIUS Server: <input type="text"/> Port: <input type="text"/> Backup Server </div> <div> Backup Shared Secret: <input type="text"/> Set Backup Secret </div> <div> Revalidation Interval: <input type="text" value="60"/> Set Interval </div> <div> Send NAS Identifier: <input type="checkbox"/> </div>
LDAP	<input type="checkbox"/>		<div> LDAP Endpoint: <input type="text" value="EXAMPLE"/> Manage LDAP Configuration </div> <div> Remote User Groups: <input type="text" value="ExampleGroup2; ExampleRemoteUserGroup;"/> Select groups <input type="checkbox"/> Nested groups </div> <div> Domain: <input type="text"/> Set Domain </div>
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="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.

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

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 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 Kemp vendor ID is 12196.

3.2.2 Specifying RADIUS permissions for Groups and All Users

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

3 Configure Authentication and Authorization

- **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.

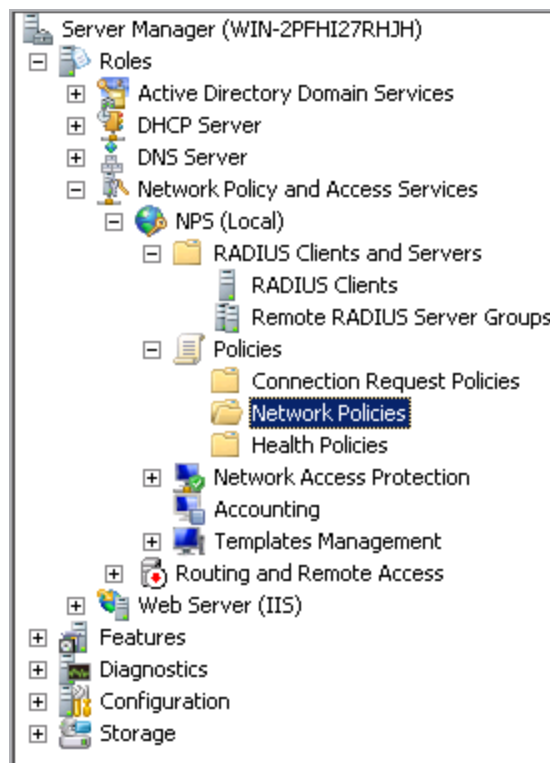
Connection request policies apply to all users. Network policies apply to groups.

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)

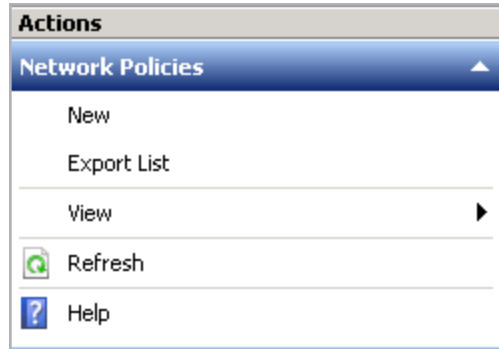
3.2.2.1.1 Specifying RADIUS Authentication for a Group

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

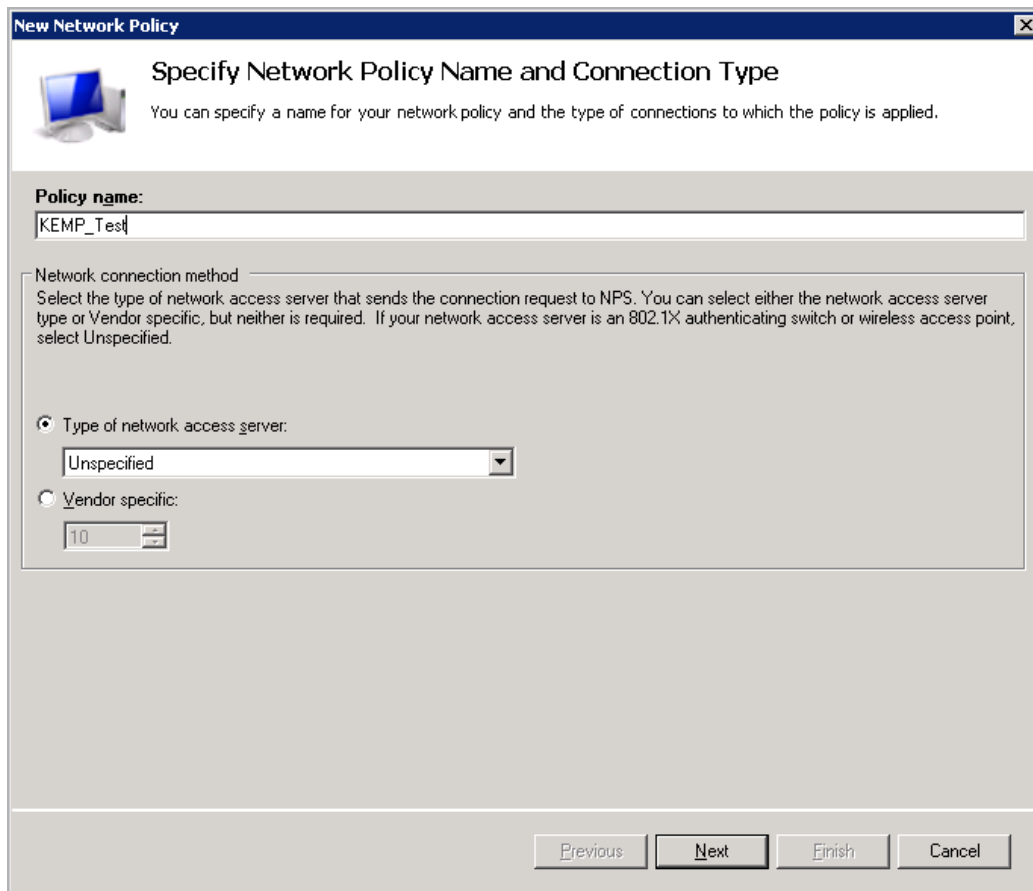


1. In the panel on the left, go to **Policies > Network Policies**.

3 Configure Authentication and Authorization



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:

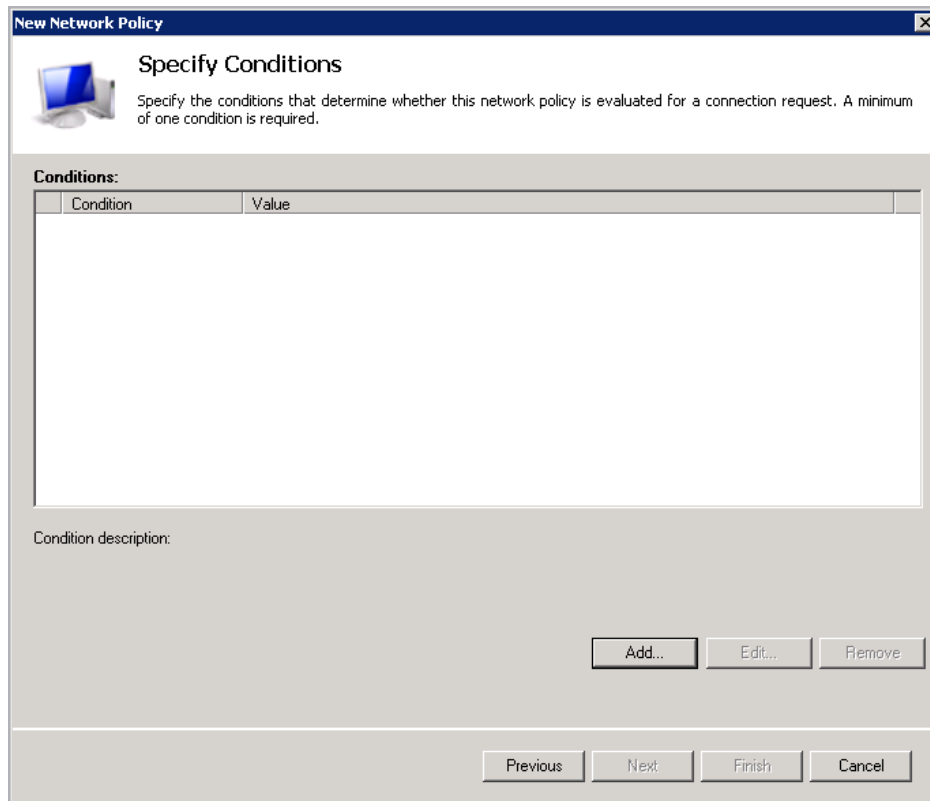
10

Previous Next Finish Cancel

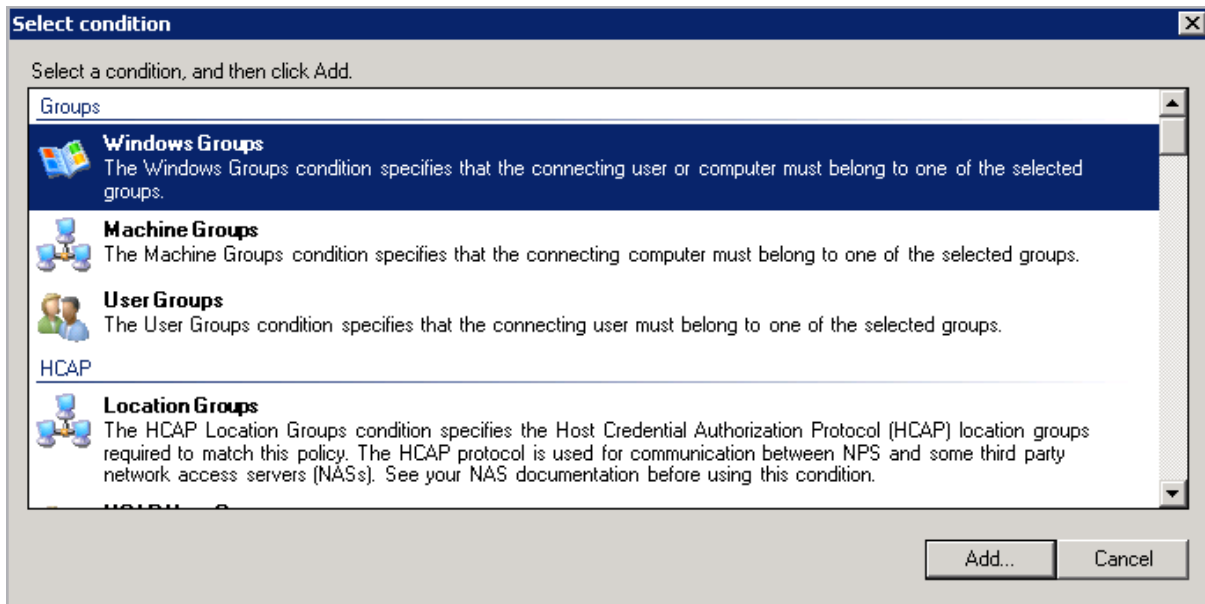
3. Enter a **Policy name**.

4. Click **Next**.

3 Configure Authentication and Authorization



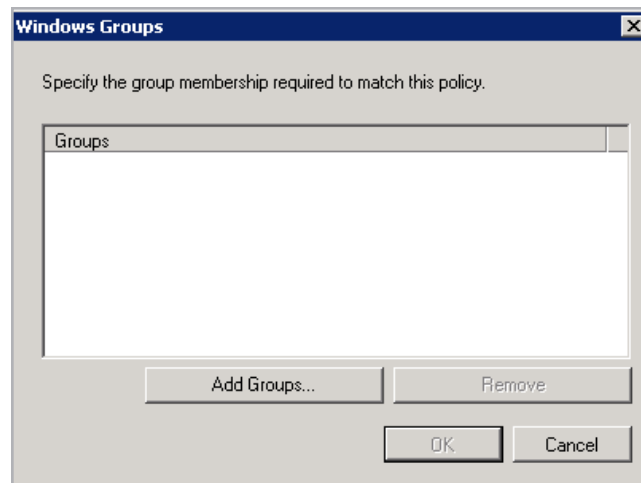
5. Click the **Add...** button.



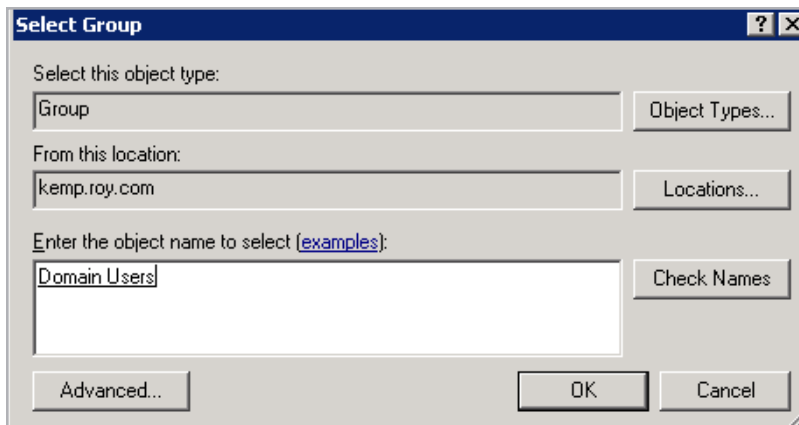
6. Select the relevant group type.

3 Configure Authentication and Authorization

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



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

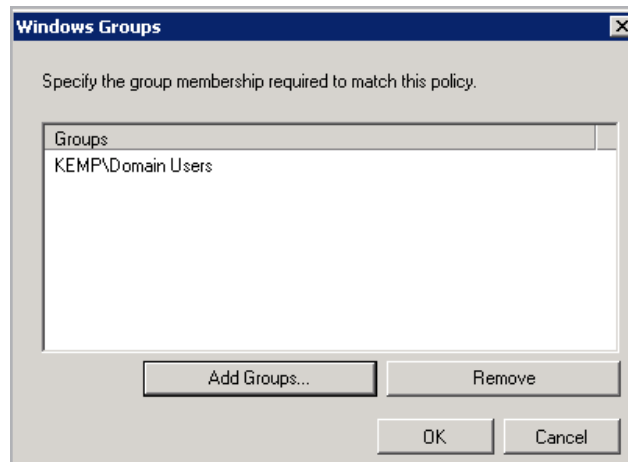


9. Enter the group name in the text area provided.

10. Click **Check Names**.

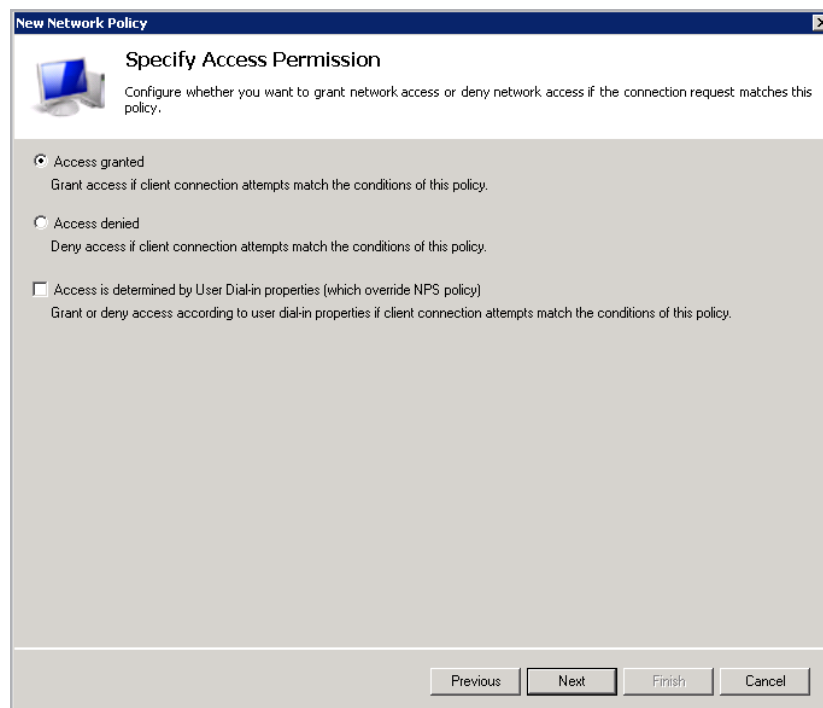
11. If the name is alright, click **OK**.

3 Configure Authentication and Authorization



12. Click **OK**.

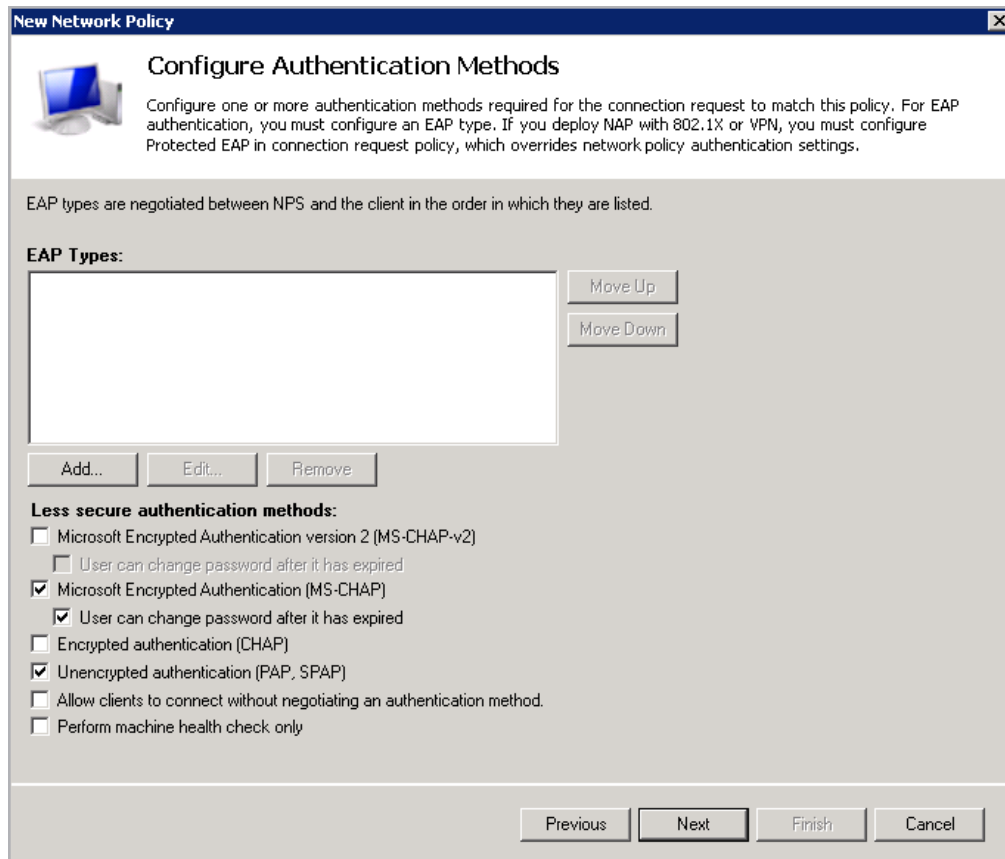
13. Click **Next**.



14. Select the relevant Access Permission option.

15. Click **Next**.

3 Configure Authentication and Authorization



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.

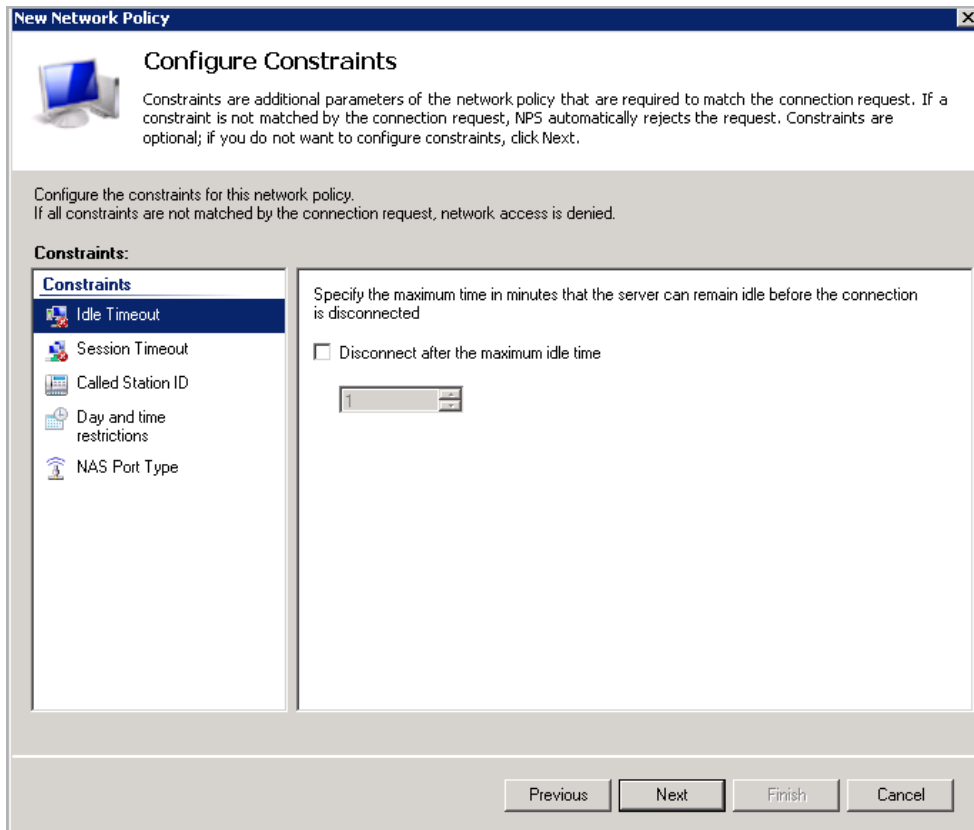
EAP Types:

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**.

3 Configure Authentication and Authorization



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

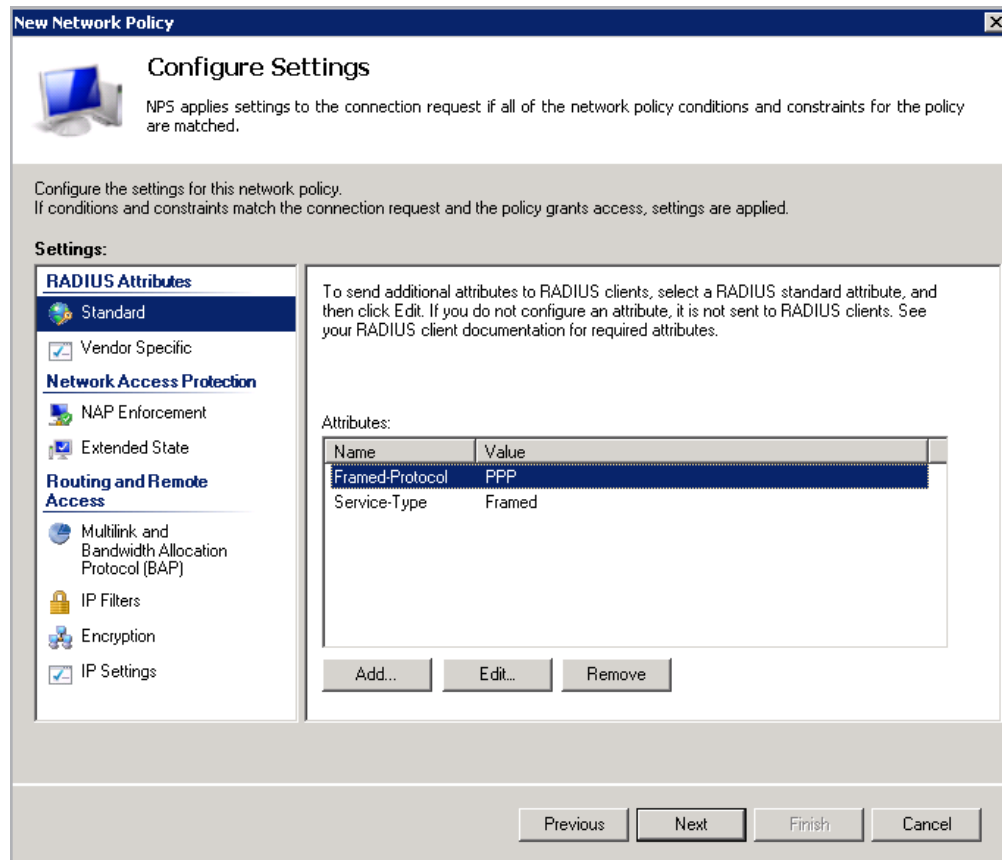
Previous Next Finish Cancel

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



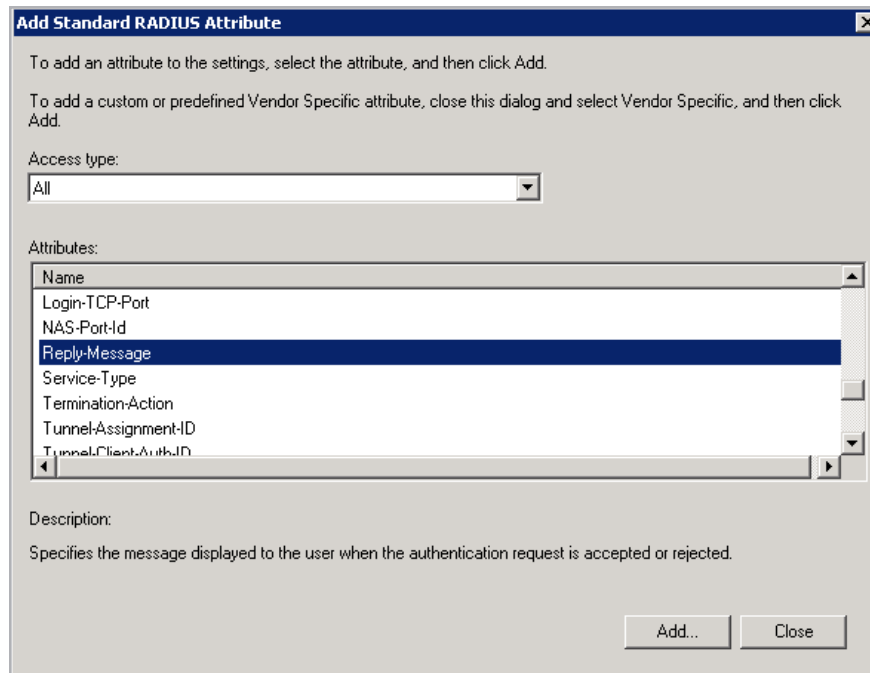
The **Attributes** on this screen need to be in a certain order for the settings to work correctly. The order is as follows:

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



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:

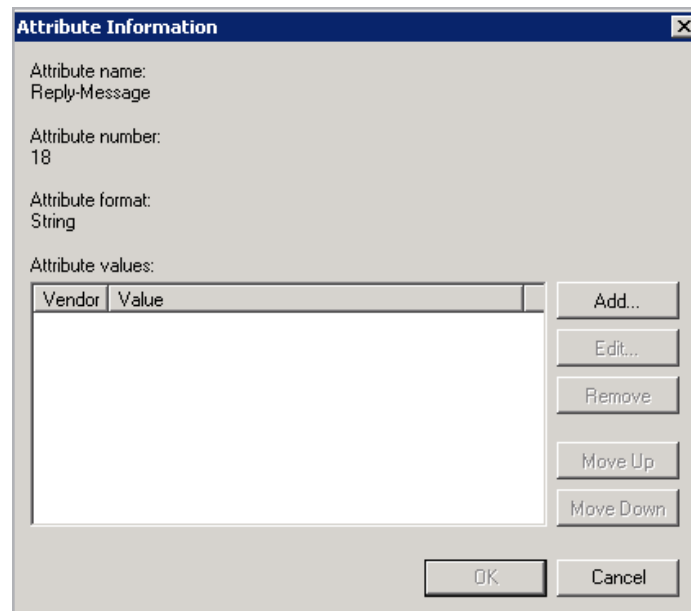
Name
Login-TCP-Port
NAS-Port-Id
Reply-Message
Service-Type
Termination-Action
Tunnel-Assignment-ID
Tunnel-Client-Auth-ID

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.



Attribute Information

Attribute name:
Reply-Message

Attribute number:
18

Attribute format:
String

Attribute values:

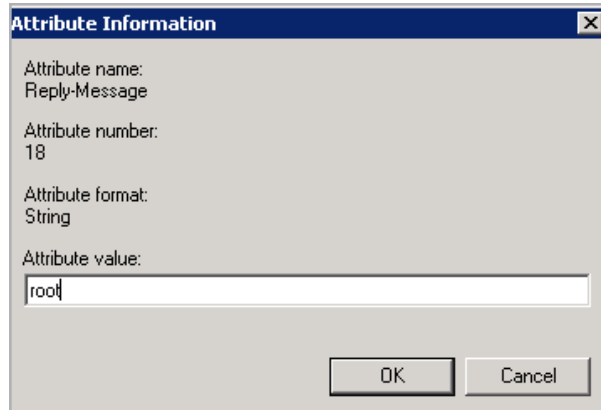
Vendor	Value

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

OK Cancel

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

3 Configure Authentication and Authorization

A screenshot of a Windows-style dialog box titled "Attribute Information". It contains four labeled text fields: "Attribute name:" with the value "Reply-Message", "Attribute number:" with the value "18", "Attribute format:" with the value "String", and "Attribute value:" with the value "root". At the bottom right are "OK" and "Cancel" buttons.

Attribute Information

Attribute name:
Reply-Message

Attribute number:
18

Attribute format:
String

Attribute value:
root

OK 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**

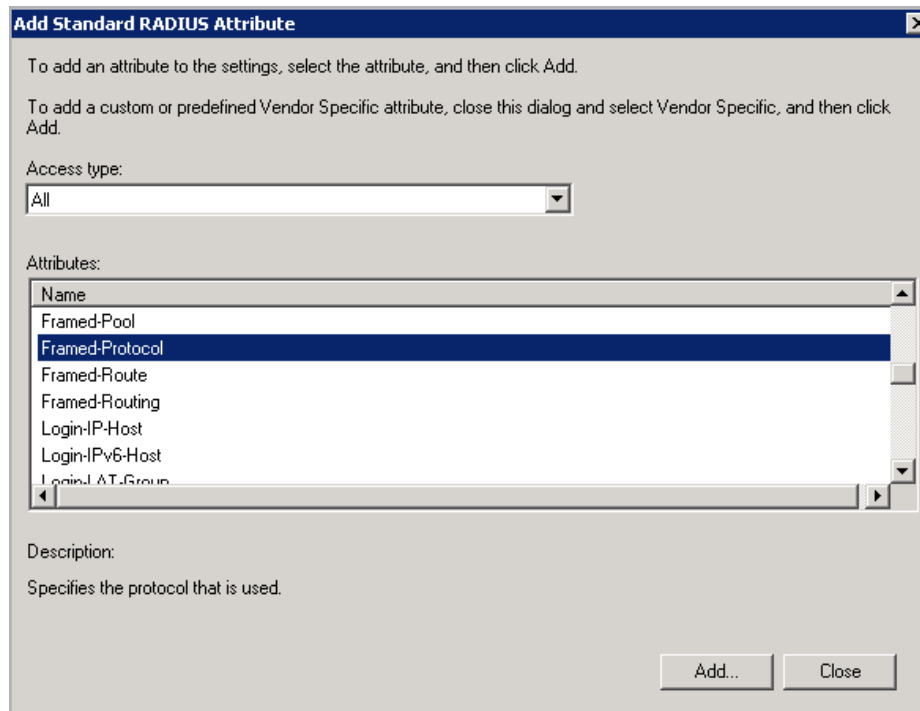
These correspond to the permission options in the LoadMaster Web User Interface (WUI).

The **root** permission grants all permissions.

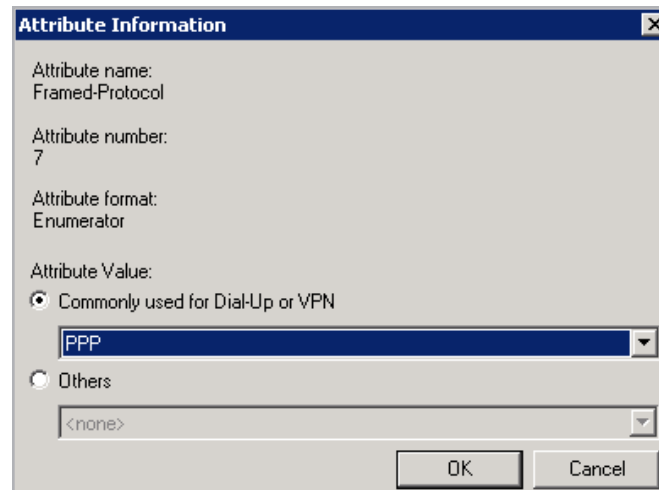
Multiple attributes can be specified here, but they must be separated by a comma (with no space).

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

3 Configure Authentication and Authorization



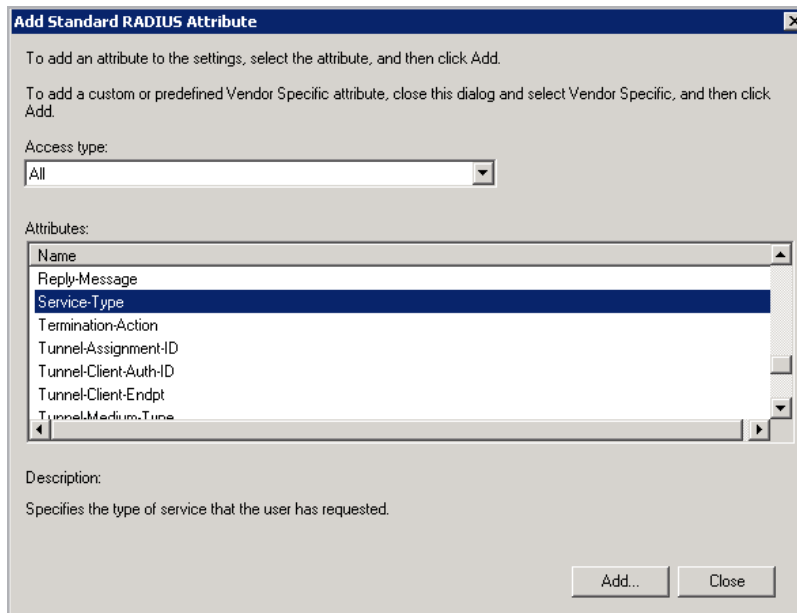
10. Click the **Add...** button.



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

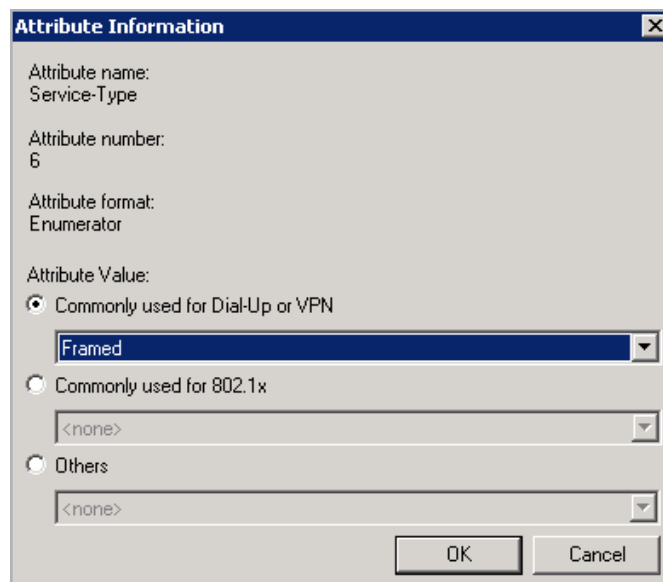
12. Click **OK**.

3 Configure Authentication and Authorization



13. Select **Service-Type**.

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

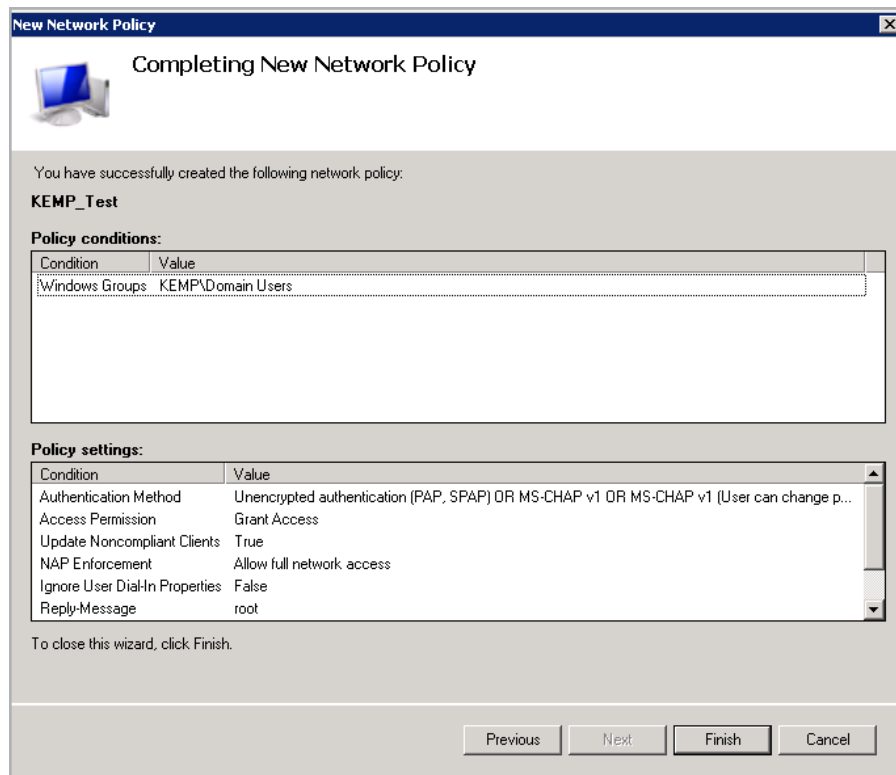


15. Select **Framed** from the **Commonly used for Dial-Up or VPN** drop-down list.

16. Click **OK**.

17. Click **Close**.

18. Click **Next**.



19. Click **Finish**.

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

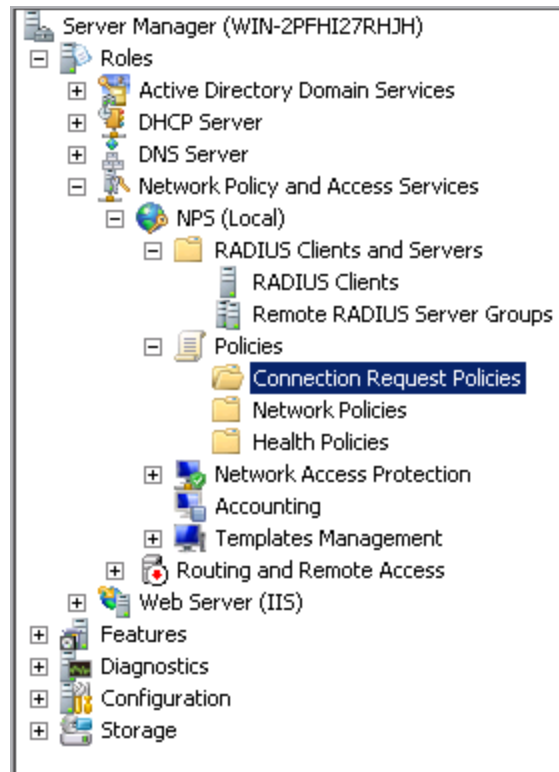
3.2.2.2 Specify RADIUS Authentication and Authorization for All Users

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.

3 Configure Authentication and Authorization

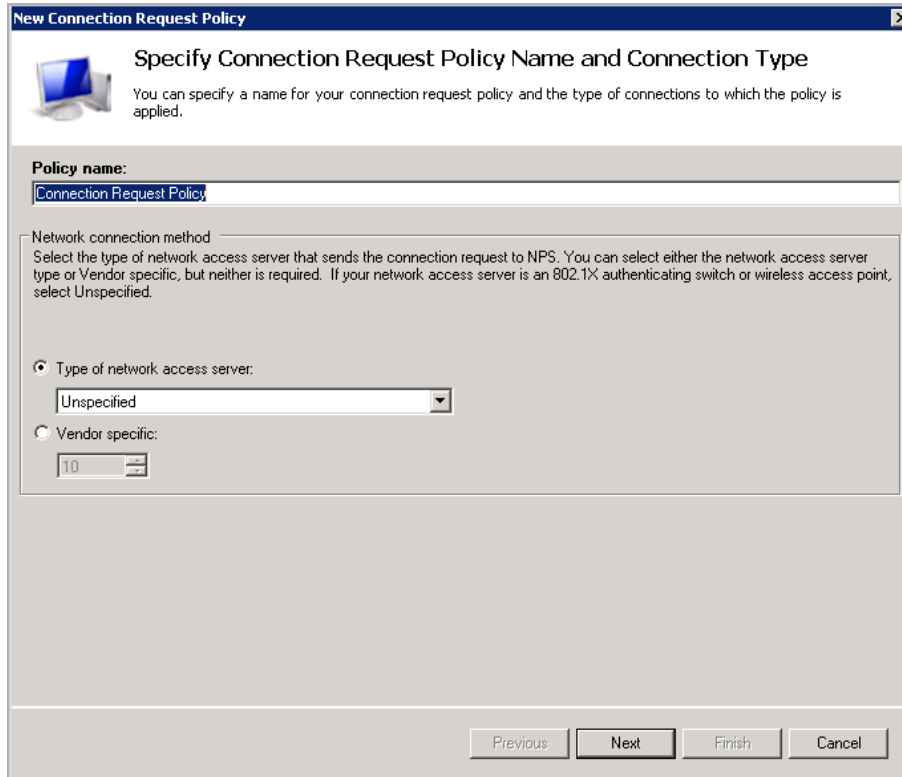


1. Navigate to **Roles > Network Policy and Access Services > Policies > Connection Request Policies**.



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

3 Configure Authentication and Authorization



The dialog box is titled "New Connection Request Policy". It contains a sub-header "Specify Connection Request Policy Name and Connection Type" with a small icon of a computer monitor. Below this is a text box for the "Policy name" containing the text "Connection Request Policy". Underneath is a section titled "Network connection method" with a descriptive paragraph. Two radio buttons are present: "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 box containing "10". At the bottom right are four buttons: "Previous", "Next", "Finish", and "Cancel".

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:

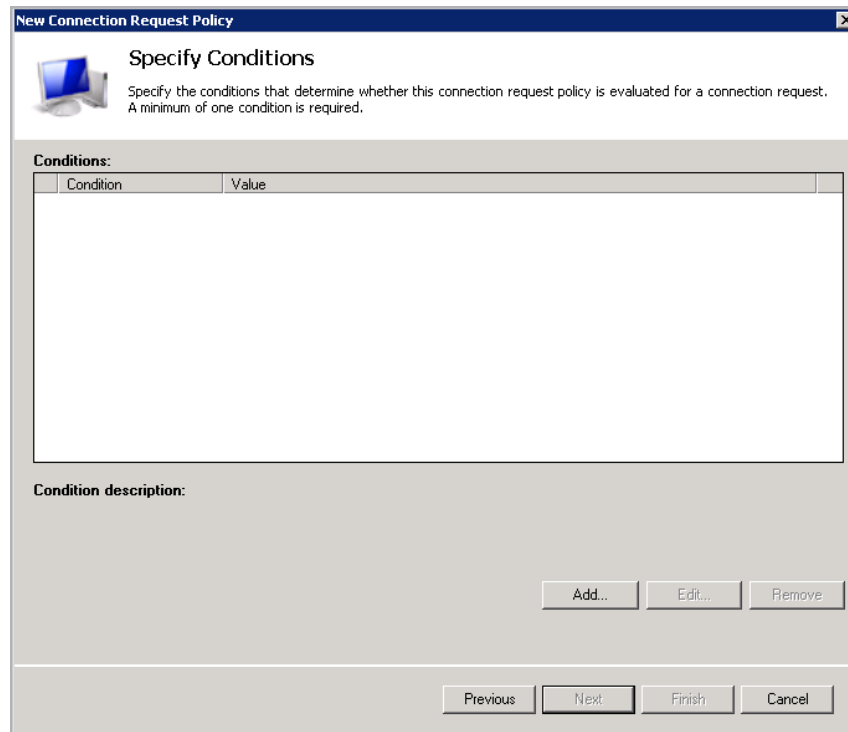
10

Previous Next Finish Cancel

3. Enter a **Policy name**.

4. Click **Next**.

3 Configure Authentication and Authorization



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:

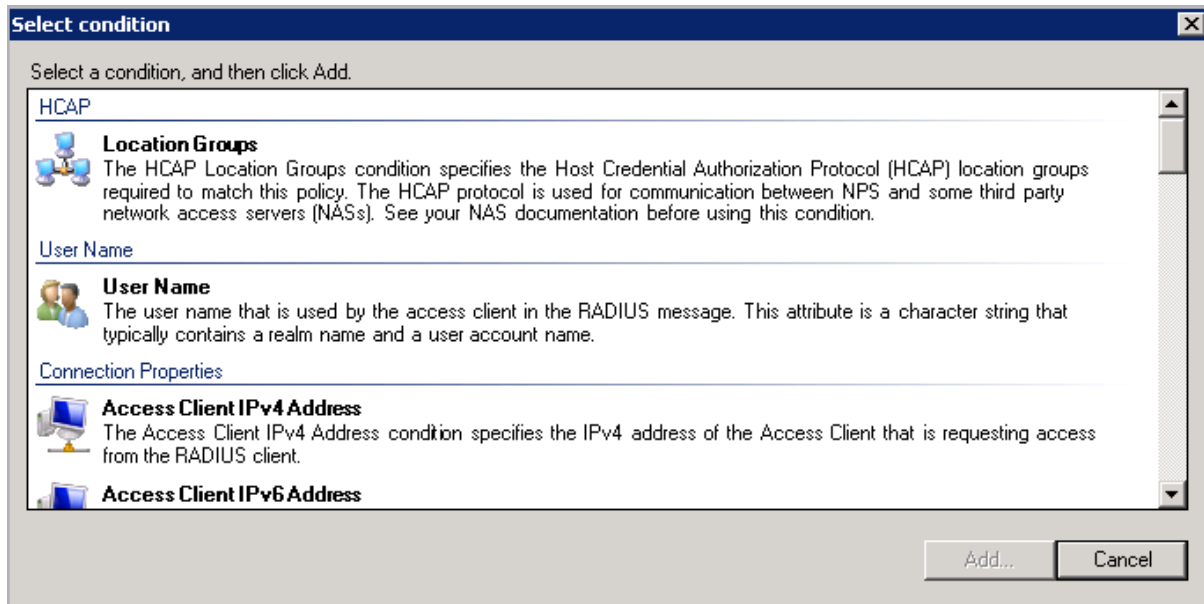
Condition	Value
-----------	-------

Condition description:

Add... Edit... Remove

Previous Next Finish Cancel

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



Select condition

Select a condition, and then click Add.

HCAP

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

User Name

User Name
The user name that is used by the access client in the RADIUS message. This attribute is a character string that typically contains a realm name and a user account name.

Connection Properties

Access Client IPv4 Address
The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access from the RADIUS client.

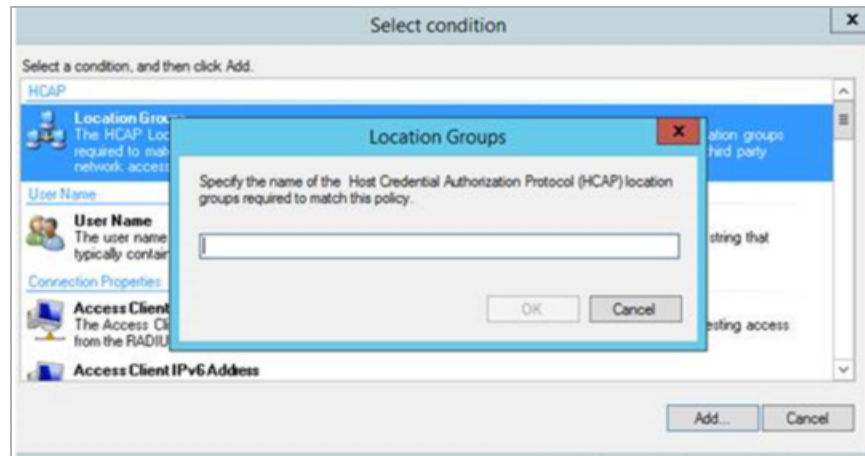
Access Client IPv6 Address

Add... Cancel

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

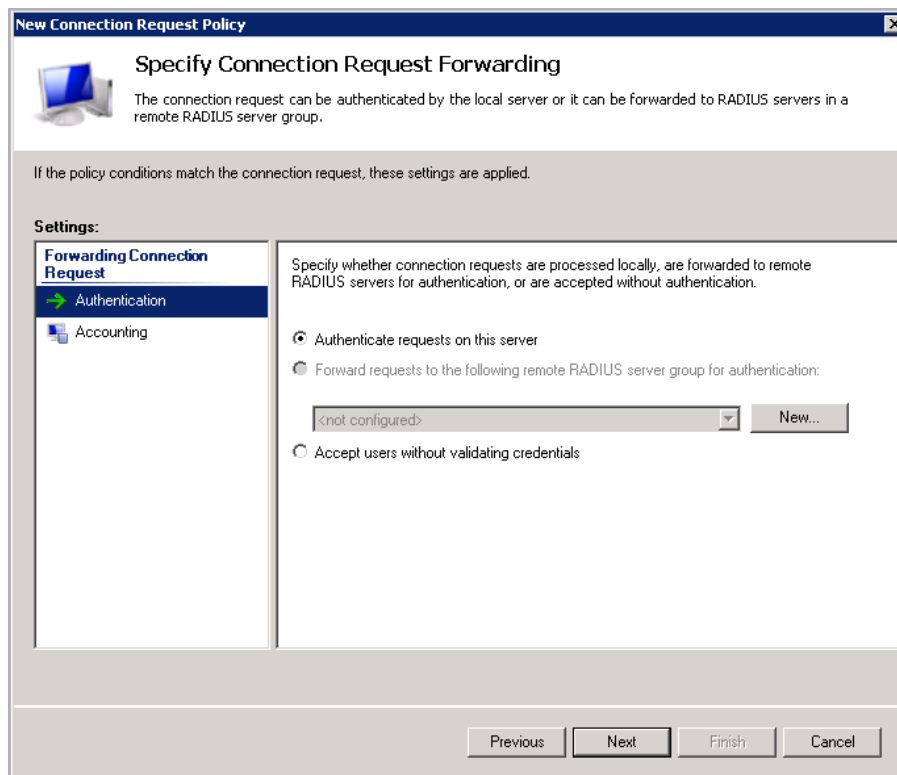
7. Click the **Add...** button.

3 Configure Authentication and Authorization



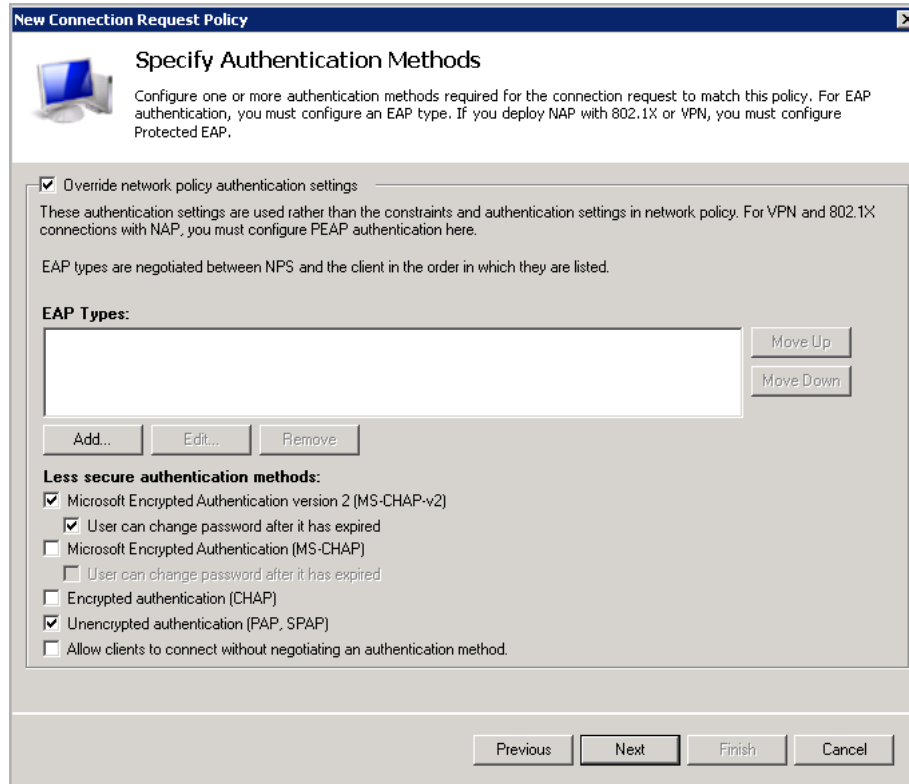
8. Type **Domain users** and click **OK**.

9. Click **Next**.



10. Click **Next**.

3 Configure Authentication and Authorization

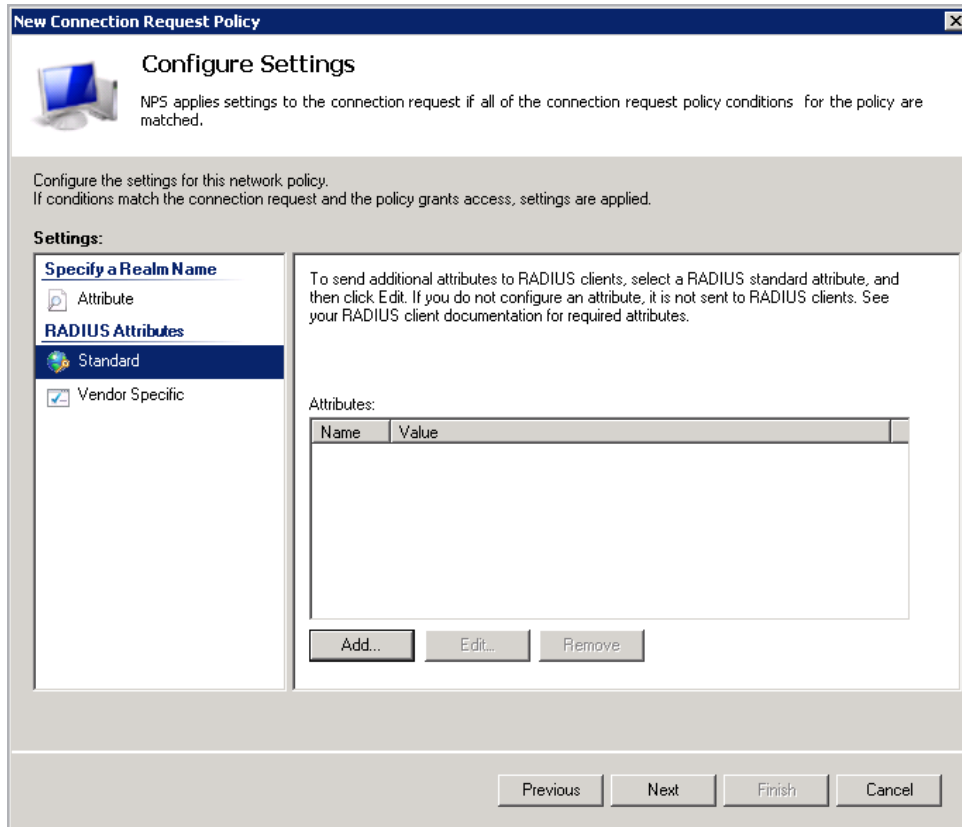


The screenshot shows the 'New Connection Request Policy' dialog box with the 'Specify Authentication Methods' tab selected. The dialog has a title bar with a close button. Below the title bar is a section with a computer icon and the title 'Specify Authentication Methods'. The text below the title reads: '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.' Below this text is a checkbox labeled 'Override network policy authentication settings' which is checked. Below the checkbox is a paragraph: '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.' Below this paragraph is another paragraph: 'EAP types are negotiated between NPS and the client in the order in which they are listed.' Below this paragraph is a section titled 'EAP Types:' with a list box containing no items. To the right of the list box are 'Move Up' and 'Move Down' buttons. Below the list box are 'Add...', 'Edit...', and 'Remove' buttons. Below these buttons is a section titled 'Less secure authentication methods:' with several checkboxes: 'Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)' (checked), 'User can change password after it has expired' (checked), 'Microsoft Encrypted Authentication (MS-CHAP)' (unchecked), 'User can change password after it has expired' (unchecked), 'Encrypted authentication (CHAP)' (unchecked), 'Unencrypted authentication (PAP, SPAP)' (checked), and 'Allow clients to connect without negotiating an authentication method.' (unchecked). At the bottom of the dialog are 'Previous', 'Next', 'Finish', and 'Cancel' buttons.

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 Configure Authentication and Authorization

3.2.2.2 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:

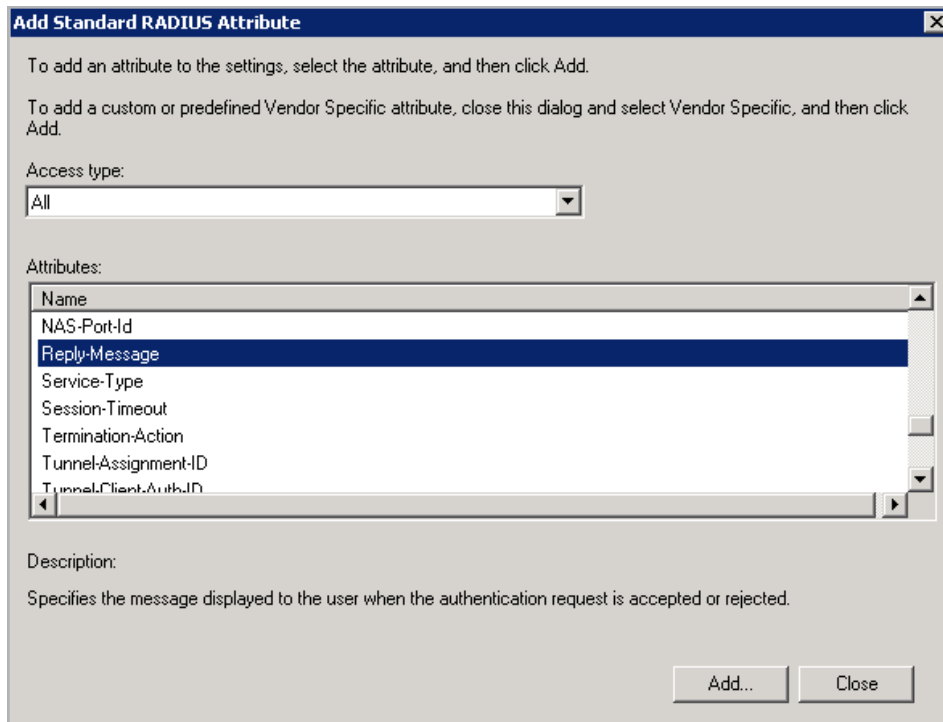
Name	Value
------	-------

Add... Edit... Remove

Previous Next Finish Cancel

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

3 Configure Authentication and Authorization



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:

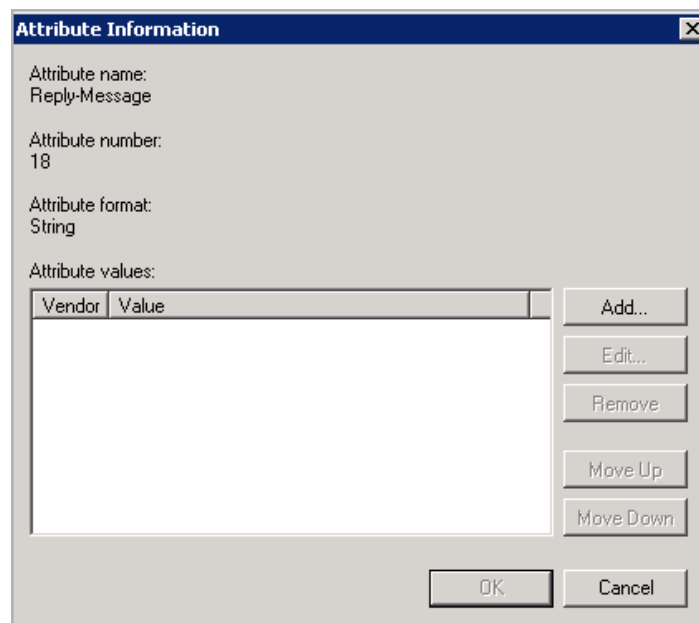
Attributes:

Name
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.

3. Select **Reply-Message**.

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



Attribute Information

Attribute name:
 Reply-Message

Attribute number:
 18

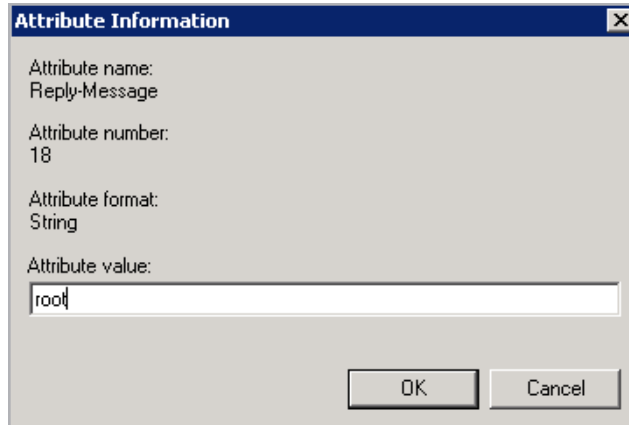
Attribute format:
 String

Attribute values:

Vendor	Value

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

3 Configure Authentication and Authorization

A screenshot of a Windows-style dialog box titled "Attribute Information". It contains four labels with corresponding values: "Attribute name:" with "Reply-Message", "Attribute number:" with "18", "Attribute format:" with "String", and "Attribute value:" with a text input field containing "root". At the bottom right are "OK" and "Cancel" buttons.

Attribute Information

Attribute name:
Reply-Message

Attribute number:
18

Attribute format:
String

Attribute value:
root

OK Cancel

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

The available permission options are as follows:

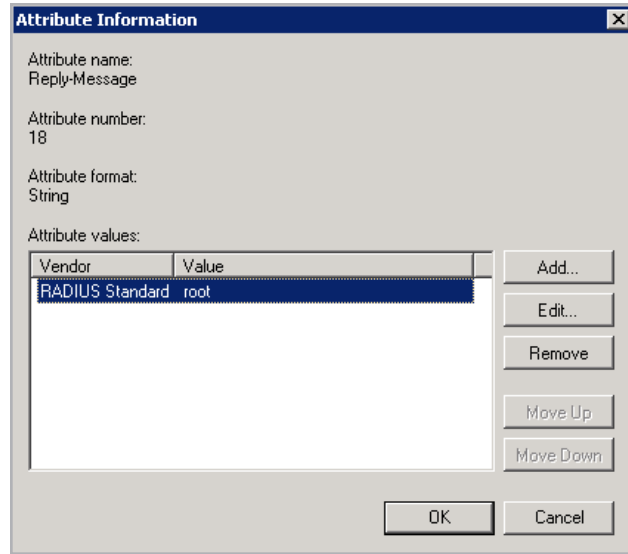
real,vs,rules,backup,certs,cert3,certbackup,users,root,geo

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



Attribute Information

Attribute name:
Reply-Message

Attribute number:
18

Attribute format:
String

Attribute values:

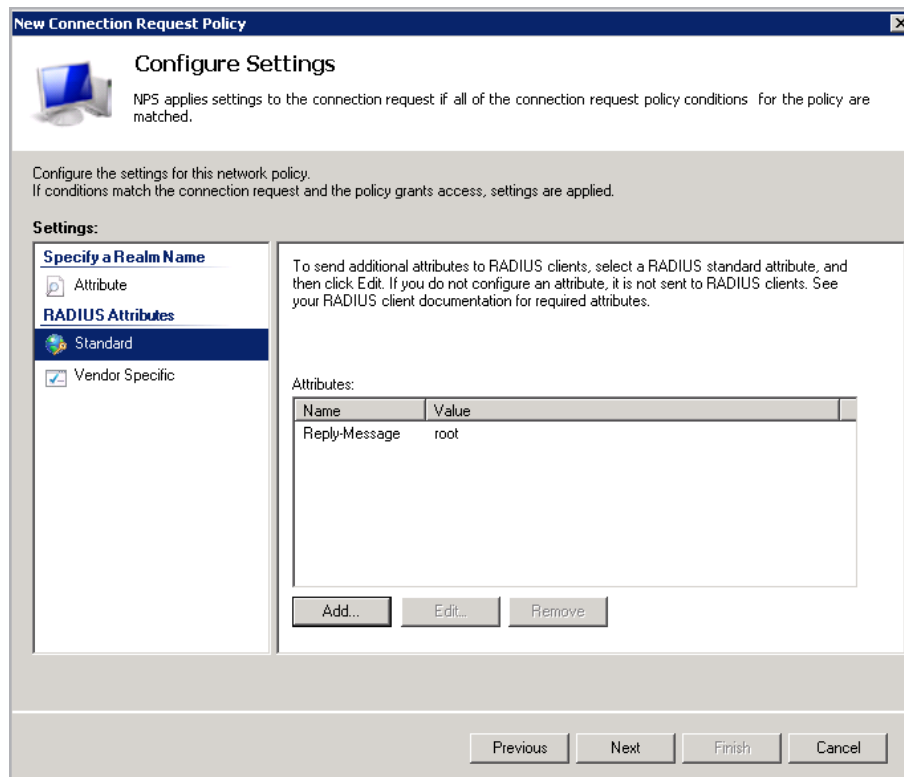
Vendor	Value
RADIUS Standard	root

Buttons: Add..., Edit..., Remove, Move Up, Move Down, OK, Cancel

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

Buttons: Add..., Edit..., Remove, Previous, Next, Finish, Cancel

10. Click **Next**.

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

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 28 July 2023.