

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

1 Introduction	5
1.1 Document Purpose	5
1.2 Intended Audience	5
1.3 Related Firmware Version	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	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 Specifying RADIUS Authorization for All Users	35



References	40
Last Updated Date	41

1 Introduction



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



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.

Actions
RADIUS Clients
New
Export List
View 🕨
Q Refresh
🕜 Help

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

2 Prerequisites for Authentication and Authorization



ed Properties		
ttings Advanced		
Enable this RADIUS client		
Select an existing template:		
		~
) Nama and Address		
Friendly name:		
Shared		
Address (IP or DNS):		
10.86.0.175		Verify
Shared Secret		
Select an existing Shared Secrets tem	plate:	
None	- -	•
To manually type a shared secret, click secret, click Generate. You must confi secret entered here. Shared secrets ar Manual C Genera	k Manual. To automatically gr gure the RADIUS client with re case-sensitive. ate	enerate a shared the same shared
Shared secret:		
•••••		
Confirm shared secret:		
•••••		
		. 1
	UK Cance	Apply

- 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.

kemp.ax



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 nonalphanumeric or other characters are used that require multibyte 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	Modify Delete 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			
Virtual Services	-		
Rules			
System Backup			
Certificate Creation			
Intermediate Certificates			
Certificate Backup			
User Administration			
All Permissions			
Geo Control			

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.



User		Login
Password		
	User Password	User Password

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

WUI Session Management	
Enable Session Management	 Image: A start of the start of
Require Basic Authentication	
Basic Authentication Password	••••• Set Basic Password
Failed Login Attempts	3 Set Fail Limit (Valid values:1-999)
Idle Session Timeout	600 Set Idle Timeout (Valid values: 60-86400)
Limit Concurrent Logins	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 V 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 Server	10.154.11.80 Por	RADIUS Server
			Shared Secret	Please set passv Set Secret	
RADIUS		a	Backup RADIUS Server	Port Back	ckup Server
1010105			Backup Shared Secret	Set Backup Secret	
			Revalidation Interval	60 Set Interval	
			Send NAS Identifier		
			LDAP Endpoint	EXAMPLE Manage LDAP Configuration	1
LDAP			Remote User Groups	ExampleGroup2;Example RemoteUserGroup;	Nested groups
			Domain	Set Domain	
Local Users		•	Use ONLY if other AAA service	fail	
Test AAA for Us	ser				
Username Password		Test User			

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

IPv6 is not supported for RADIUS authentication.

8. Select the **Radius Authentication** check box.

kemp.ax



- 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

3 Configure Authentication and Authorization



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: <u>Send Kemp</u> <u>Vendor Specific Attribute In RADIUS Requests</u>.

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**.

3 Configure Authentication and Authorization





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

Actions
Network Policies
New
Export List
View
Q Refresh
👔 Help

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

3 Configure Authentication and Authorization



New Network P	olicy X
	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	
Type of ne Unspecifie Unspecifie Unspecifie Unspecifie Unspecifie Unspecifie	ection method a of network access server that sends the connection request to NPS. You can select either the network access server specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, ified. twork access server: ad ecific:
	<u>Previous</u> <u>Next</u> <u>Finish</u>

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





New Network P	olicy					×
	Specify Co Specify the cond of one condition	DINCRITIONS ditions that determine whether the is required.	nis network policy	is evaluated for	a connection requ	uest. A minimum
Conditions:						
Condition	1	Value				
Condition desc	ription:			Add	Edit	Hemove
			Previous	Next	Finish	Cancel

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

Groups		
1	Windows Groups The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.	
	Machine Groups The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.	
<u>88</u>	UserGroups The User Groups condition specifies that the connecting user must belong to one of the selected groups.	
HCAP		
2 4 2	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.	-
.	The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location gro required to match this policy. The HCAP protocol is used for communication between NPS and some third part network access servers (NASs). See your NAS documentation before using this condition.	iups y

6. Select the relevant group type.

kem	p.ax
I.C.I.I.	prun



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

Windows Grou	ps	×
Specify the g	roup membership required to ma	atch this policy.
Groups		
	Add Groups	Remove
		OK Cancel
		OK Cancel

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

Select Group		? ×
Select this object type:		
Group		Object Types
From this location:		
kemp.roy.com		Locations
Enter the object name to select (<u>examples</u>):		
Domain Users		Check Names
		-
Advanced	OK	Cancel

- 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

Specify the c	i ps	atch this policy	E
Groups			
KEMP\Dor	nain Users		
		-	
	Add Groups	R	emove
			1

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

New Network F	Policy X
	Specify Access Permission
	Configure whether you want to grant network access or deny network access if the connection request matches this policy.
 Access gradient access 	anted sss if client connection attempts match the conditions of this policy.
C Access de	mied
Deny acce	iss if client connection attempts match the conditions of this policy.
Access is	determined by User Dial-in properties (which override NPS policy)
Grant or de	my 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.

3 Configure Authentication and Authorization



New Network P	olicy X
	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 r	negotiated between NPS and the client in the order in which they are listed. Move Up Move Down
Add Less secure Microsoft E User ca Kirosoft E User ca Encrypted Allow client Perform ma	Edit Remove authentication methods:
	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.

3 Configure Authentication and Authorization



New Network P	Polic y	×
	Configure Co Constraints are additi constraint is not matc optional; if you do not	nstraints onal parameters of the network policy that are required to match the connection request. If a hed by the connection request, NP5 automatically rejects the request. Constraints are want to configure constraints, click Next.
Configure the d If all constraints Constraints Constraints Constraints Constraints Constraints Constraints Called S Called S Call	constraints for this netwo is are not matched by the eout Timeout tation ID d time ins it Type	rk policy. a connection request, network access is denied. Specify the maximum time in minutes that the server can remain idle before the connection is disconnected Disconnect after the maximum idle time I
		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

New Network P	olicy	X			
	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 s If conditions and Settings: RADIUS AT Standard Vendor Network Ad Southers And NAP Er Restander Routing an Access Bandwin Protocc Bandwin Protocc Pritter Restin Der Settin	settings for this network nd constraints match the tributes rd Specific ccess Protection aforcement ad State dth Allocation i (BAP) s ion ngs	policy. connection request and the policy grants access, settings are applied. 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			
		Previous Next Finish Cancel			

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



dd Standard RADIUS Attribute	×
Fo 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 V Add.	ndor Specific, and then click
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:	
n na serie de la composition de la composition de la contra	Laure to deal
Specifies the message displayed to the user when the authentication request is accept	a or rejectea.
	Add Class

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

Attribute Information	X
Attribute name: Reply-Message	
Attribute number: 18	
Attribute format: String	
Attribute values:	
Vendor Value	Add
	E dit
	Remove
	Move Up
	Move Down
OK	Cancel

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



3 Configure Authentication and Authorization

Attribute Information	×
Attribute name: Reply-Message	
Attribute number: 18	
Attribute format: String	
Attribute value:	
1004	
	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,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.

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]
Framed-Pool	
Framed-Protocol	
Framed-Route	
Framed-Routing	
Login-IP-Host	
Login-IPv6-Host	
	-
Description: Specifies the protocol that is used.	
Add Close	

10. 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		
PPP		•
C Others		
<none></none>		7
	OK	Cancel

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

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 selected. Add, $% \left({{{\rm{A}}_{\rm{A}}}} \right)$	ect Vendor Specific, and then click
Access type:	
All	
Attributes:	
Name	
Reply-Message	
Service-Type	
Termination-Action	
Tunnel-Assignment-ID	
Tunnel-Client-Auth-ID	
Tunnel-Client-Endpt	
Tunnel-Medium-Tune	
Description:	
Specifies the type of service that the user has requested.	
	Add Close

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

Attribute Information		×
Attribute name: Service-Type		
Attribute number: 6		
Attribute format: Enumerator		
Attribute Value:		
Commonly used for Dial-Up or VPN		
Framed		•
C Commonly used for 802.1x		
<none></none>		7
C Others		
<none></none>		v
	OK	Cancel

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



18. Click Next.

You have successfully created the following network KEMP_Test Policy conditions:	vork Policy
You have successfully created the following network KEMP_Test	policy:
KEMP_Test	
Policy conditions:	
oncy conditions.	
Condition Value	
D-1:]
Policy settings:	
Policy settings: Condition Value Authentication Method Unencrypted authen Access Permission Grant Access Update Noncompliant Clients True NAP Enforcement Allow full network ac	tication (PAP, SPAP) OR MS-CHAP v1 OR MS-CHAP v1 (User can change p

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.

Connection Request Policies
New
Export List
View
🖪 Refresh
👔 Help

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

3 Configure Authentication and Authorization



New Connectio	n 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 R	equest Policy
Network comm Select the type type or Vendor select Unspec Type of ne Unspecifie Vendor spe	ection method e of network access server that sends the connection request to NPS. You can select either the network access server specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, fied. twork access server: ed
10	
	Previous Next Finish Cancel

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





New Connection	n Request Polic	Ŷ				×
	Specify Co Specify the cond A minimum of on	onditions ditions that determine whether the ne condition is required.	nis connection reque	est policy is evalu	ated for a connec	tion request.
Conditions:						
Condition		Value				
Condition de	scription:			Add	Edit	Remove
			Previous	Next	Finish	Cancel

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

Selec	ct condition	×
Sele	ect a condition, and then click Add.	
HC	CAP	
3	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.	
<u>Us</u>	ser Name	
8	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.	
Co	onnection 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.	
	Ccess Client IPv6 Address	-
	Add Cano	el

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



3 Configure Authentication and Authorization

ect a condition, and the	n click Add.		
CAP			-
Location Group The HCAP Loc required to mate	Location Groups	ation groups hird party	
network access er Name	Specify the name of the Host Credential Authorization Protocol (HCAP) location groups required to match this policy.		
User Name The user name typically contain		string that	
nnection Properties			
Access Client The Access Cli from the RADIU	OK Cancel	esting access	
Access Client IF	Pv6Address		
from the RADIU	∿6Address		

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

New Connection R	equest Policy pecify Connection Request Forwarding te connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a mote RADIUS server group. tions match the connection request, these settings are applied.	X
Settings: Forwarding Co Request	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: Interconfigured> New Accept users without validating credentials	
	Previous Next Finish Cance	

10. Click Next.

3 Configure Authentication and Authorization



New Connectio	n 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.	
These auther connections of EAP types ar	network policy authentication settings ntication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X with NAP, you must configure PEAP authentication here. e negotiated between NPS and the client in the order in which they are listed.	
Add Add Less secur Microsoft User of User of	Edit Remove Edit Remove e authentication methods: Encrypted Authentication version 2 (MS-CHAP-v2) can change password after it has expired Encrypted Authentication (MS-CHAP) can change password after it has expired d authentication (CHAP) coted authentication (PAP, SPAP) ints 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

New Connectio	n Request Policy		×
	Configure Se NPS applies settings t matched.	ttings o the connection request if all of the connection request policy conditions for the policy are	
Configure the s If conditions ma	settings for this network atch the connection req	policy. uest and the policy grants access, settings are applied.	
Settings: Specify a R Attribute RADIUS Att Standar Vendor	ealm Name tributes d 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	
		Previous Next Finish Cancel	J

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

3 Configure Authentication and Authorization



dd 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.

Attribute Information	×
Attribute name: Reply-Message	
Attribute number: 18	
Attribute format: String	
Attribute values:	
Vendor Value	Add
	E dit
	Remove
	Move Up
	Move Down
OK	Cancel

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



3 Configure Authentication and Authorization

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 Informat	ion		X
Attribute name: Reply-Message			
Attribute number: 18			
Attribute format: String			
Attribute values:			
Vendor	Value		Add
RADIUS Standard	root		E dit
			Remove
			Move Up
			Move Down
		ОК	Cancel

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

New Connection Request Po	licy	×
Configu NPS applies s matched.	re Settings settings to the connection request if all of the connection request policy conditions for the policy are	
Configure the settings for this If conditions match the conne	network policy. ction request and the policy grants access, settings are applied.	
Settings: Specify a Realm Name Attribute RADIUS Attributes Standard	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.	
Z Vendor Specific	Attributes: Name Value Reply-Message root	
	Add Edit Remove	
	Previous Next Finish Cancel	



10. Click Next.

w Connection Reques	Policy X
Comp	leting Connection Request Policy Wizard
You have successfully cr	eated the following connection request policy:
Connection Request	Policy
Policy conditions:	
Condition Value	
Location Groups Doma	in 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 place white missed which	
To close this wizard, click	Finish.
To close this wizard, click	. Finish.

11. Click Finish.

References





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

Web User Interface, Configuration Guide

kemp.ax

Last Updated Date



Last Updated Date

This document was last updated on 19 March 2021.

kemp.ax