RADIUS ESP Authentication

Feature Description

UPDATED: 20 March 2021

Copyright Notices

Table of Contents

1 Introduction

As part of the Kemp Edge Security Pack (ESP), the LoadMaster supports a number of authentication protocols, including Remote Authentication Dial-In User Service (RADIUS).

RADIUS is a widely deployed protocol enabling centralized authentication, authorization and accounting for network access. Originally developed for dial-up remote access, RADIUS is now supported by Virtual Private Network (VPN) servers, wireless access points, authenticating Ethernet switches, Digital Subscriber Line (DSL) access, and other network access types.

A RADIUS client (typically an access server such as a dial-up server, VPN server, or wireless access point) sends user credentials and connection parameter information in the form of a RADIUS message to a RADIUS server. The RADIUS server authenticates and authorizes the RADIUS client request, and sends back a RADIUS message response. RADIUS clients also send RADIUS accounting messages to RADIUS servers. Additionally, the RADIUS standards support the use of RADIUS proxies. A RADIUS proxy is a computer that forwards RADIUS messages between RADIUS clients, RADIUS servers and other RADIUS proxies. RADIUS messages are never sent between the access client and the access server.

1.1 Document Purpose

This document provides step-by-step instructions on how to configure authentication and Single Sign On (SSO) using RADIUS in the LoadMaster.

For instructions on how to use RADIUS authentication for LoadMaster Web User Interface (WUI) access, refer to the **RADIUS Authentication and Authorization, Technical Note**.

1.2 Intended Audience

This document is intended to be used by anyone who is interested in finding out how to configure RADIUS ESP authentication in the Kemp 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 Configure OIDC/OAUTH ESP Authentication

Follow the steps in the sections below to configure the LoadMaster to use Radius ESP authentication.

2.1 Prerequisites

Before configuring the LoadMaster, please ensure that there is a RADIUS authentication server in place and that it is configured with the client details (the IP address of the LoadMaster and the shared secret which is used for password encryption).

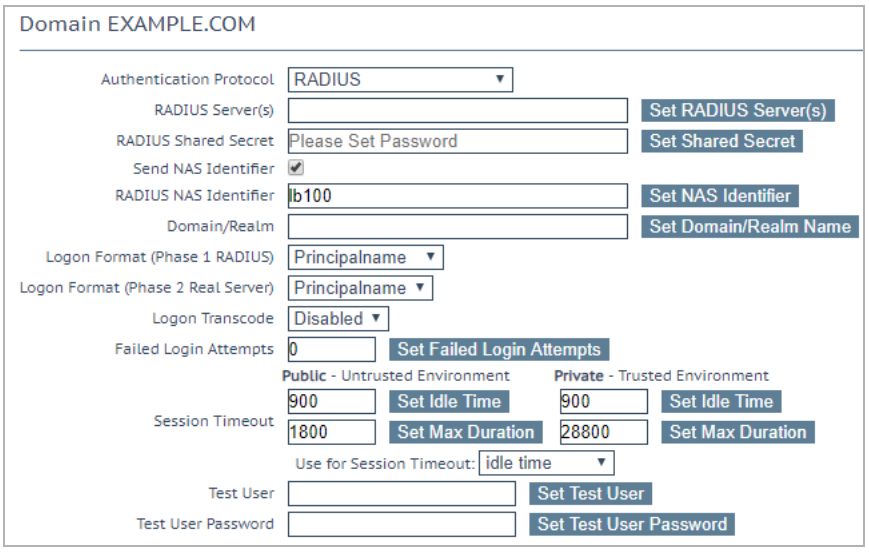
> It is not possible to use RADIUS authentication if you are using a FIPS LoadMaster.

2.2 Create an SSO Domain

Follow the steps below to create an SSO domain in the LoadMaster:

1. In the LoadMaster WUI, navigate to **Virtual Services > Manage SSO**.

2. Enter the name of the SSO configuration in the **Add new Client Side Configuration** field and click **Add**.



3. Select the relevant **Authentication Protocol**.

> **RADIUS** and **RADIUS and Unencrypted LDAP** (two factor authentication) are the valid options for RADIUS authentication.

> As of LoadMaster firmware version 7.2.52, RADIUS two-factor and LDAP authentication is supported. For further details, refer to the following article: RADIUS Two-Factor and LDAP Authentication.

4. Select the relevant **LDAP Endpoint**, if using two factor authentication.

5. Enter the address(es) of the **RADIUS Server(s)** to be used to authenticate this domain and click **Set RADIUS Server(s)**.

> Multiple addresses can be entered using a space-separated list.

> IPv6 is not supported for RADIUS authentication.

6. Enter the **RADIUS Shared Secret** that is to be used between the RADIUS server and the LoadMaster and click **Set Shared Secret**.

> The Shared Secret is a text string that serves as a password between the LoadMaster and the RADIUS server.

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

> If this check box is disabled (default), a Network Access Server (NAS) identifier is not sent to the RADIUS server. If it is enabled, a 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.

8. 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.

9. Enter the **Domain/Realm** and click **Set Domain/Realm Name**.

> This is also used with the logon format to construct the normalized username, for example:
> - **Principalname:** <Username>@<Domain>
> - **Username:** <Domain>\<Username>

10. Select the relevant logon string format in the **Logon Format (Phase 1)** drop-down list.

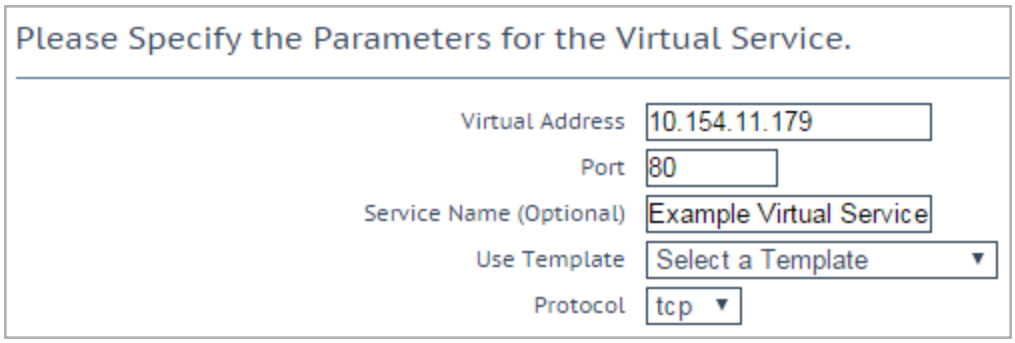
11. Select the relevant logon string format in the **Logon Format (Phase 2)** drop-down list.

12. Fill out the remaining fields as needed.

2.3 Create a Virtual Service

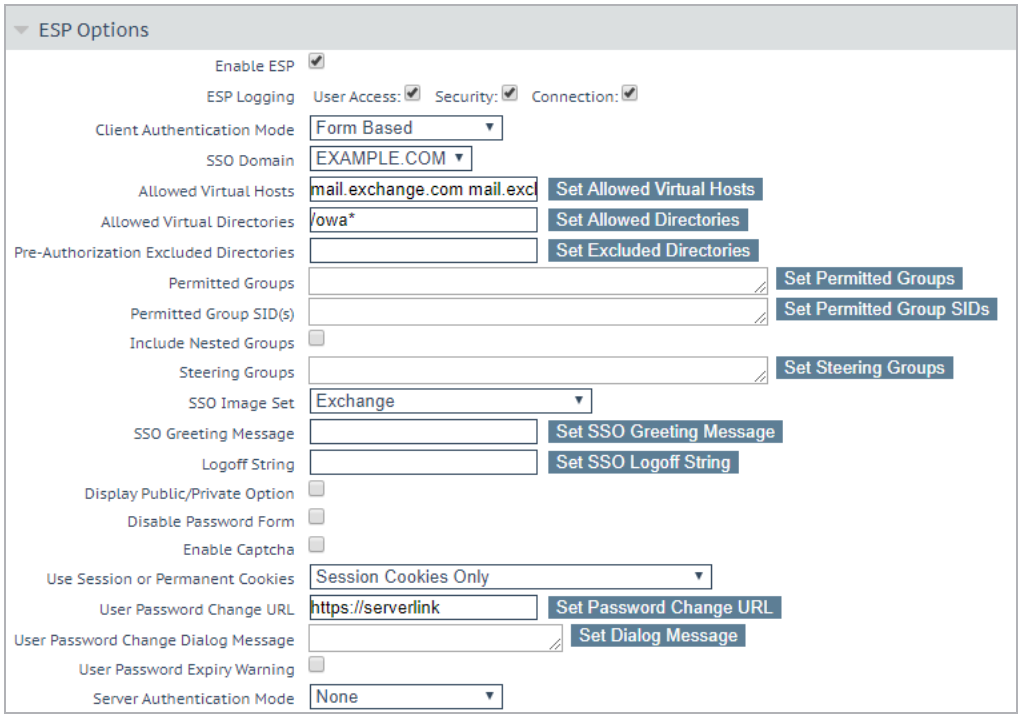
Follow the steps below to create a Virtual Service and configure the ESP Options:

1. In the main menu of the LoadMaster WUI, navigate to **Virtual Services > Add New**.



2. Enter a valid IP address in the **Virtual Address** text box.
3. Fill out the other fields as needed.
4. Click **Add this Virtual Service**.

5. Expand the **ESP Options** section.
6. Tick the **Enable ESP** check box.



7. Select the relevant **Client Authentication Mode**.

> The RADIUS **SSO Domain** will not be available if the **Client Authentication Mode** is set to **Delegate to Server** – please select a different mode.

8. Select the RADIUS SSO domain, which was previously configured, from the **SSO Domain** drop-down list.

9. Fill out any other fields, as needed.

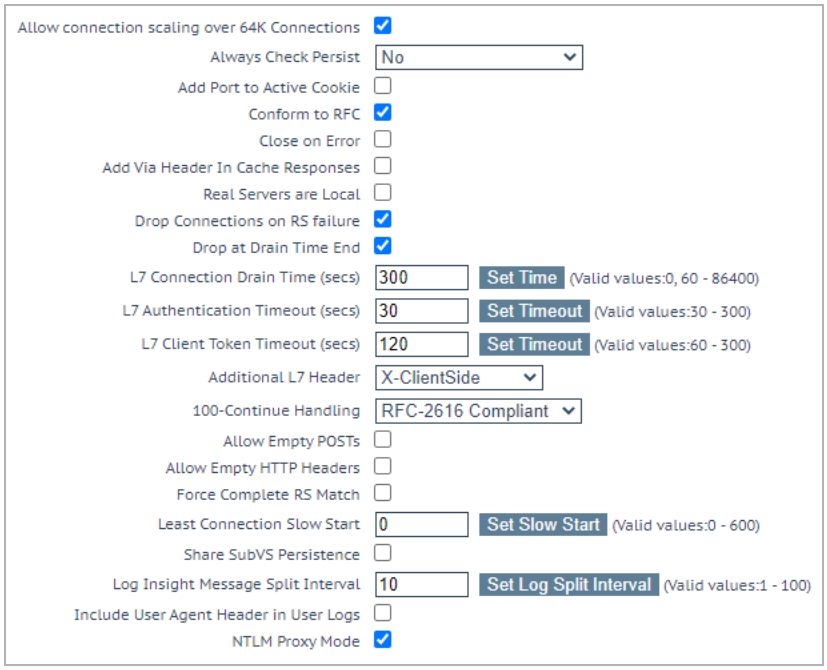
10. Add any Real Servers, as needed.

For an explanation of all of the WUI fields, refer to the **Web User Interface (WUI), Configuration Guide**.

2.4 Set the L7 Client Token Timeout Value

The L7 Client Token Timeout is the duration of time (in seconds) to wait for the client token while the process of authentication is ongoing. The default L7 client token timeout is set to 120 seconds. This can be modified as needed in the LoadMaster WUI. The range of valid values is 60 to 300. To configure the timeout value, follow the steps below:

1. In the main menu, go to **System Configuration > Miscellaneous Options > L7 Configuration**.



2. Enter the new value in the **L7 Client Token Timeout** text box and click **Set Timeout**.

3 RADIUS Challenge/Response

The LoadMaster supports RADIUS challenge/response authentication. RADIUS challenge/response is supported transparently – if the server sends a challenge, an additional form is displayed and the user is asked to enter the additional token/password.

The authentication flow is as follows:

1. The end user is prompted to enter a username and password.
2. If the username and password credentials have authenticated successfully, the One Time Password (OTP) is requested using a server challenge. An additional form is displayed and the end user needs to enter the additional token/password.
3. The username and OTP details are then submitted to the server for authentication.

Regarding the methods used during the authentication flow – an Access Request is sent from the LoadMaster to the server (which includes the username and password), the server responds with an Access Challenge (if the credentials have authenticated successfully) which will result in a subsequent form to collect the OTP. The LoadMaster then sends another Access Request (with the State and OTP included) and the server then responds with either an Access Accept or Access Reject, depending on whether the authentication was successful or not.

References

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

RADIUS Authentication and Authorization, Technical Note

Web User Interface (WUI), Configuration Guide

Last Updated Date

This document was last updated on 20 March 2021.