Progress®
Kemp® LoadMaster®

Technical Note RADIUS Challenge Response

Generated on: 18 December 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 5

Intended Audience 5

Chapter 2: RADIUS Challenge/Response Authentication Flow 6

Chapter 3: References 8

1

Introduction

Introduction

As part of the 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.

The LoadMaster also supports RADIUS challenge/response authentication. RADIUS challenge/response is supported transparently – if the server sends a challenge, an additional form will be displayed and the user will be asked to enter the additional One Time Password (OTP).

An OTP is a password that is valid for only one login session. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication.

Related Links

- Document Purpose
- Intended Audience

Document Purpose

Document Purpose

The purpose of this document is to provide some further information on RADIUS challenge/response authentication.

For information on how to configure RADIUS ESP authentication in general, please refer to the RADIUS ESP Authentication, Feature Description.

Intended Audience

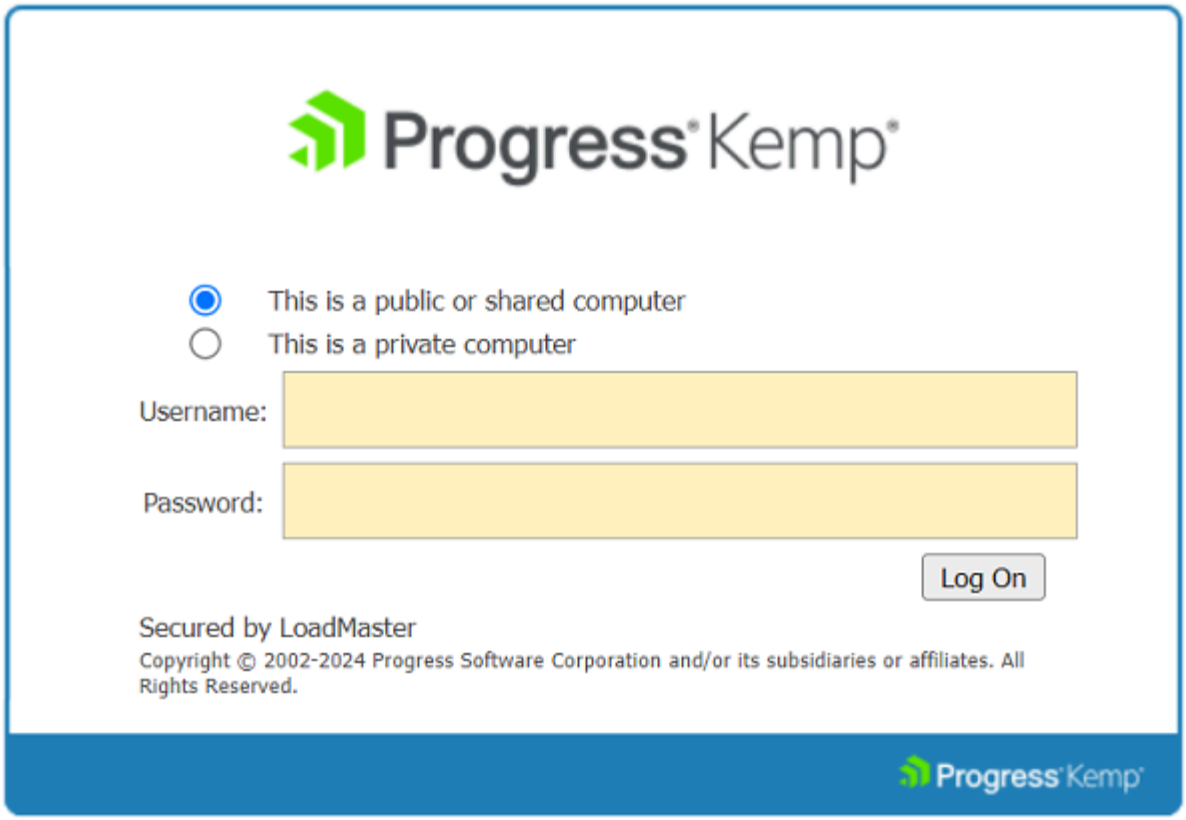
Intended Audience

This document is intended to be used by anyone interested in finding out more information about RADIUS challenge/response.

2

RADIUS Challenge/Response Authentication Flow

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 OTP is requested via 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.

3

References

References

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

RADIUS ESP Authentication, Feature Description