

RADIUS Challenge Response

Technical Note

UPDATED: 28 July 2023

Table of Contents

1 Introduction **4**

1.1 Document Purpose 4

1.2 Intended Audience 4

2 RADIUS Challenge/Response Authentication Flow **5**

References **6**

Last Updated Date **7**

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

© 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.

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

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.

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.

1.1 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.

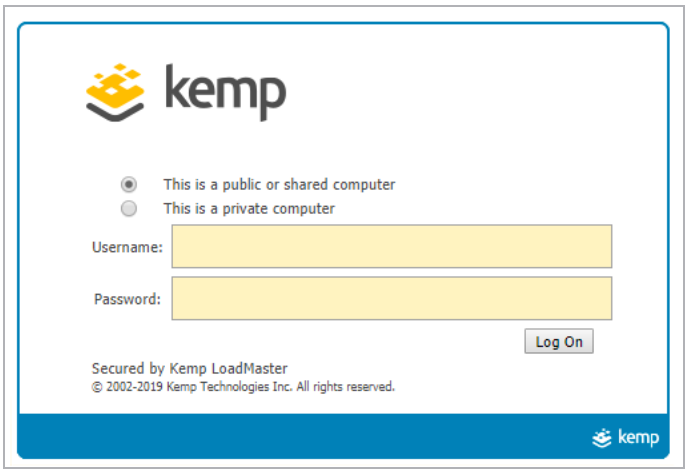
1.2 Intended Audience

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

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

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.

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

References

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

RADIUS ESP Authentication, Feature Description

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

Last Updated Date

This document was last updated on 28 July 2023.

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