



# RADIUS ESP Authentication

## Feature Description

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

---

<b>1 Introduction</b>	<b>4</b>
1.1 Document Purpose	4
1.2 Intended Audience	4
<b>2 Configure OIDC/OAUTH ESP Authentication</b>	<b>5</b>
2.1 Prerequisites	5
2.2 Create an SSO Domain	5
2.3 Create a Virtual Service	7
2.4 Set the L7 Client Token Timeout Value	10
2.5 Select the Send Vendor Specific Check Box	11
<b>3 RADIUS Challenge/Response</b>	<b>13</b>
<b>References</b>	<b>14</b>
RADIUS Authentication and Authorization, Technical Note	14
Web User Interface (WUI), Configuration Guide	14
<b>Last Updated Date</b>	<b>15</b>

# 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.

# 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).

---

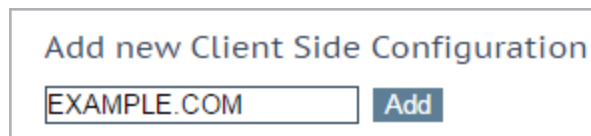
It is not possible to use RADIUS authentication if you are using a FIPS LoadMaster.

---

## 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**.

## 2 Configure OIDC/OAUTH ESP Authentication

Domain EXAMPLE.COM

Authentication Protocol
RADIUS

RADIUS Server(s)
Set RADIUS Server(s)

RADIUS Shared Secret
Please Set Password
Set Shared Secret

Send NAS Identifier
☒

RADIUS NAS Identifier
b100
Set NAS Identifier

Domain/Realm
Set Domain/Realm Name

Logon Format (Phase 1 RADIUS)
Principalname

Logon Format (Phase 2 Real Server)
Principalname

Logon Transcode
Disabled

Failed Login Attempts
0
Set Failed Login Attempts

Public - Untrusted Environment
900
Set Idle Time
1800
Set Max Duration

Private - Trusted Environment
900
Set Idle Time
28800
Set Max Duration

Use for Session Timeout:
idle time

Test User
Set Test User

Test User Password
Set Test User Password

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

For RADIUS authentication, the following are valid options:

- **RADIUS**
- **RADIUS and Unencrypted LDAP** (two factor 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 Configure OIDC/OAUTH ESP Authentication

Please Specify the Parameters for the Virtual Service.

Virtual Address	<input type="text" value="10.154.11.179"/>
Port	<input type="text" value="80"/>
Service Name (Optional)	<input type="text" value="Example Virtual Service"/>
Use Template	<input type="text" value="Select a Template"/>
Protocol	<input type="text" value="tcp"/>

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**.

ESP Options

Enable ESP ☐

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

## 2 Configure OIDC/OAUTH ESP Authentication

ESP Options

Enable ESP

☒

ESP Logging

User Access:

Security:

Connection:

☒
☒
☒

Client Authentication Mode

Form Based

SSO Domain

EXAMPLE.COM

Alternative SSO Domains

Available Domain(s)

SECOND.COM

THIRD.COM

Assigned Domain(s)

None Assigned

>

<

Set Alternative SSO Domains

Allowed Virtual Hosts

Set Allowed Virtual Hosts

Allowed Virtual Directories

/\*

Set Allowed Directories

Pre-Authorization Excluded Directories

Set Excluded Directories

Permitted Groups

Set Permitted Groups

Permitted Group SID(s)

Set Permitted Group SIDs

Include Nested Groups

☐

Steering Groups

Set Steering Groups

Verify Bearer Header

☐

SSO Image Set

Exchange

SSO Greeting Message

Set SSO Greeting Message

Logoff String

Set SSO Logoff String

Display Public/Private Option

☒

Disable Password Form

☐

Enable Captcha

☐

Use Session or Permanent Cookies

Session Cookies Only

User Password Change URL

https://serverlink

Set Password Change URL

User Password Change Dialog Message

You must change your

Set Dialog Message

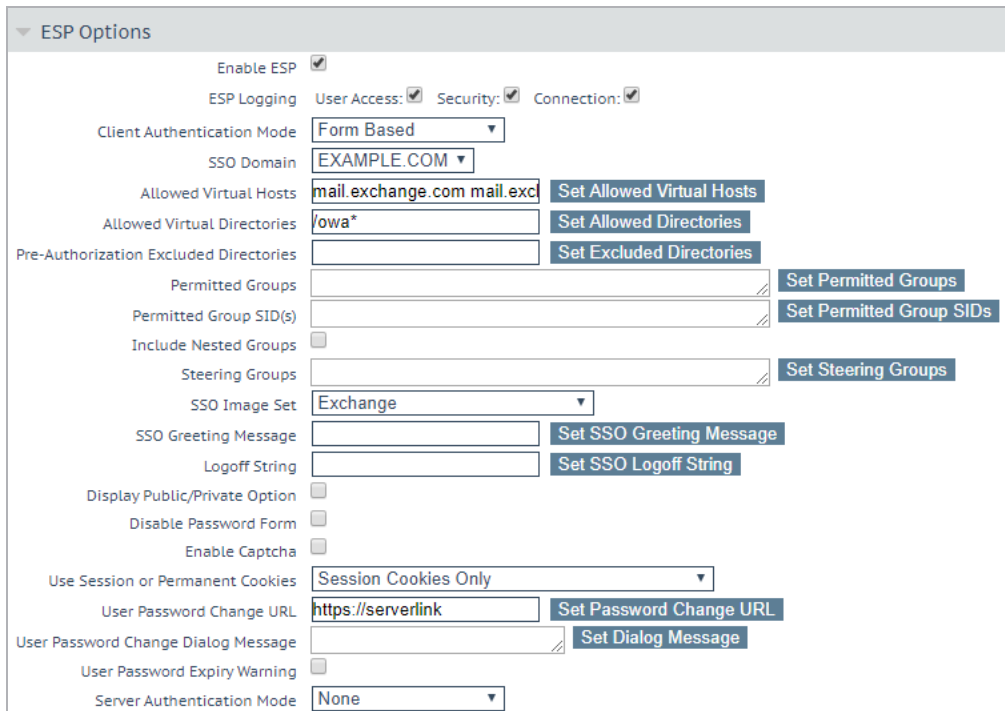
User Password Expiry Warning

☐

Server Authentication Mode

None

## 2 Configure OIDC/OAUTH ESP Authentication



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:

## 2 Configure OIDC/OAUTH ESP Authentication

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

Allow connection scaling over 64K Connections	<input type="checkbox"/>	
Always Check Persist	<input type="text" value="No"/>	
Add Port to Active Cookie	<input type="checkbox"/>	
Conform to RFC	<input checked="" type="checkbox"/>	
Close on Error	<input type="checkbox"/>	
Add Via Header In Cache Responses	<input type="checkbox"/>	
Real Servers are Local	<input type="checkbox"/>	
Drop Connections on RS failure	<input type="checkbox"/>	
Drop at Drain Time End	<input type="checkbox"/>	
L7 Connection Drain Time (secs)	<input type="text" value="300"/>	<b>Set Time</b> (Valid values:0, 60 - 86400)
L7 Authentication Timeout (secs)	<input type="text" value="30"/>	<b>Set Timeout</b> (Valid values:30 - 300)
L7 Wait after POST(ms)	<input type="text" value="2000"/>	<b>Set Post Wait</b> (Valid values:1 - 2000)
L7 Client Token Timeout (secs)	<input type="text" value="120"/>	<b>Set Timeout</b> (Valid values:60 - 300)
Additional L7 Header	<input type="text" value="X-Forwarded-For"/>	
100-Continue Handling	<input type="text" value="RFC-7231 Compliant"/>	
Allow Empty POSTs	<input type="checkbox"/>	
Allow Empty HTTP Headers	<input type="checkbox"/>	
Force Complete RS Match	<input type="checkbox"/>	
Least Connection Slow Start	<input type="text" value="0"/>	<b>Set Slow Start</b> (Valid values:0 - 600)
Share SubVS Persistence	<input type="checkbox"/>	
Log Insight Message Split Interval	<input type="text" value="10"/>	<b>Set Log Split Interval</b> (Valid values:1 - 100)
Include User Agent Header in User Logs	<input type="checkbox"/>	
Use CEF Log Format	<input type="checkbox"/>	
SSO Maximum Threads	<input type="text" value="128"/>	<b>Set SSO Max Threads</b> (Valid values:64 - 512)
NTLM Proxy Mode	<input checked="" type="checkbox"/>	

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

## 2.5 Select the Send Vendor Specific Check Box

In LoadMaster firmware version 7.2.51 and above, there is a check box called **Send Vendor Specific** in the User Interface (UI) when a **RADIUS Server** is set. When the **Send Vendor Specific** check box is enabled and a user is logging into the LoadMaster UI using RADIUS authentication with Cisco Access Control Server (ACS) or Identity Services Engine (ISE), the LoadMaster sends an Attribute Value Pair

## 2 Configure OIDC/OAUTH ESP Authentication

(AVP) to the server as part of the login request which contains Kemp's vendor ID (12196). 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.

To enable the **Send Vendor Specific** check box, follow the steps below:

1. In the main menu, go to **Certificates & Security > Remote Access**.
2. Click the **WUI Authorization Options** button on the **Remote Access** screen to display the **WUI Authentication and Authorization** screen.

The **WUI Authorization Options** button is only available when Session Management is enabled.

WUI AAA Service		Authentication	Authorization	Options
RADIUS	<input type="checkbox"/>	<input type="checkbox"/>		<div> RADIUS Server <input type="text"/> Port <input type="text"/> <a href="#">RADIUS Server</a>  Shared Secret <input type="text"/> <a href="#">Set Secret</a>  Backup RADIUS Server <input type="text"/> Port <input type="text"/> <a href="#">Backup Server</a>  Backup Shared Secret <input type="text"/> <a href="#">Set Backup Secret</a>  Revalidation Interval <input type="text" value="60"/> <a href="#">Set Interval</a>  Send NAS Identifier <input checked="" type="checkbox"/>  RADIUS NAS Identifier <input type="text" value="Kemp_2"/> <a href="#">Set NAS Identifier</a>  Send Vendor Specific <input type="checkbox"/> </div>
LDAP	<input checked="" type="checkbox"/>			<div> LDAP Endpoint <input type="text" value="LDAP_TEST.COM"/> <a href="#">Manage LDAP Configuration</a>  Remote User Groups <input type="text" value="ldaptestgroup;ldaptestgroup2;"/> <a href="#">Select groups</a> <input type="checkbox"/> Nested groups  Domain <input type="text" value="aktest.com"/> <a href="#">Set Domain</a>  Server Certificate Validation <input type="checkbox"/> </div>
Local Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Use ONLY if other AAA services fail <input checked="" type="checkbox"/>
Test AAA for User				
<div> Username <input type="text"/>  Password <input type="password"/> <a href="#">Test User</a> </div>				

3. Click the **Send Vendor Specific** check box.

# 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 28 July 2023.