

OIDC OAUTH ESP Authentication

Feature Description

UPDATED: 27 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.

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

Table of Contents

1 Introduction **4**

1.1 Document Purpose 6

1.2 Intended Audience 6

2 Configure OIDC OAUTH ESP Authentication **7**

2.1 Prerequisites 7

2.2 Create an SSO Domain 7

2.3 Create a Virtual Service 8

3 Redirect URI Logic **11**

Last Updated Date **13**

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

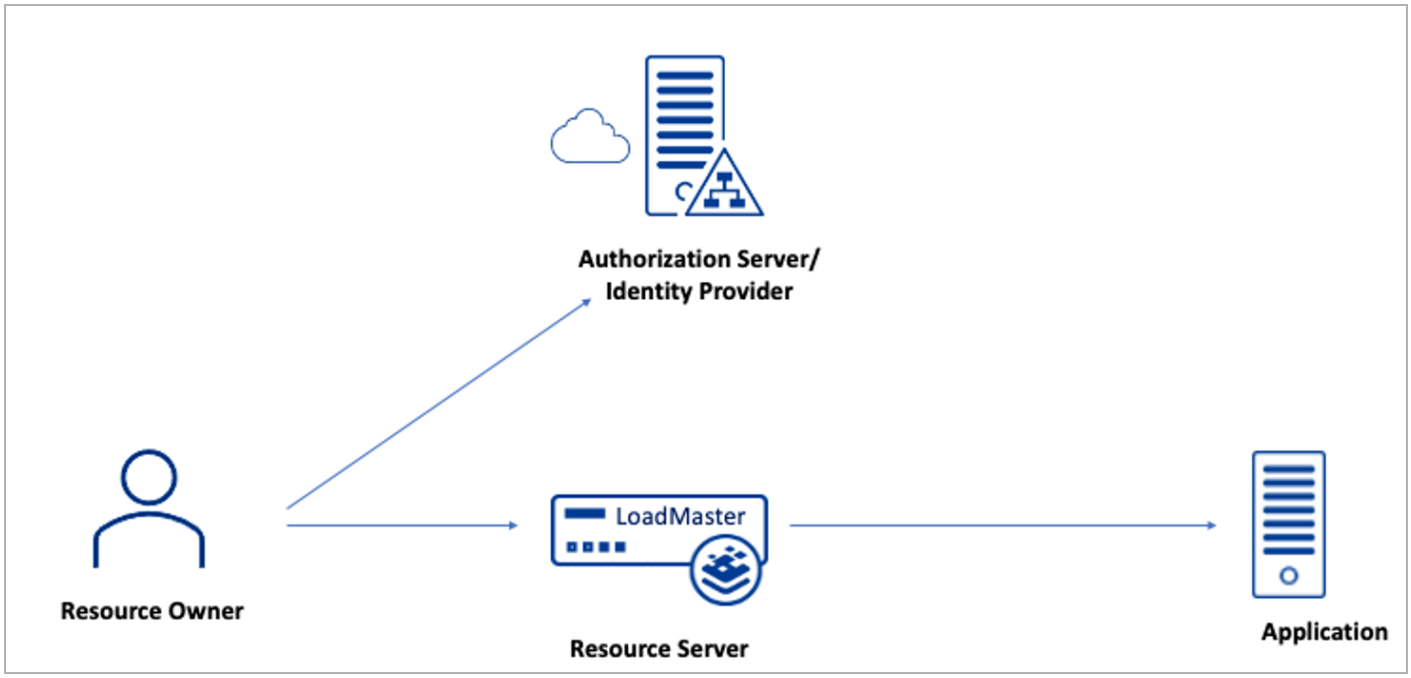
1 Introduction

As part of the Kemp Edge Security Pack (ESP), the LoadMaster supports a number of authentication protocols, including OIDC/OAUTH authentication.

Open ID Connect (OIDC) is the preferred protocol from Microsoft for Azure AD/Identity Management OIDC is an authentication protocol based on the OAuth2 protocol (which is used for authorization). OIDC uses the standardized message flows from OAuth2 to provide identity services.

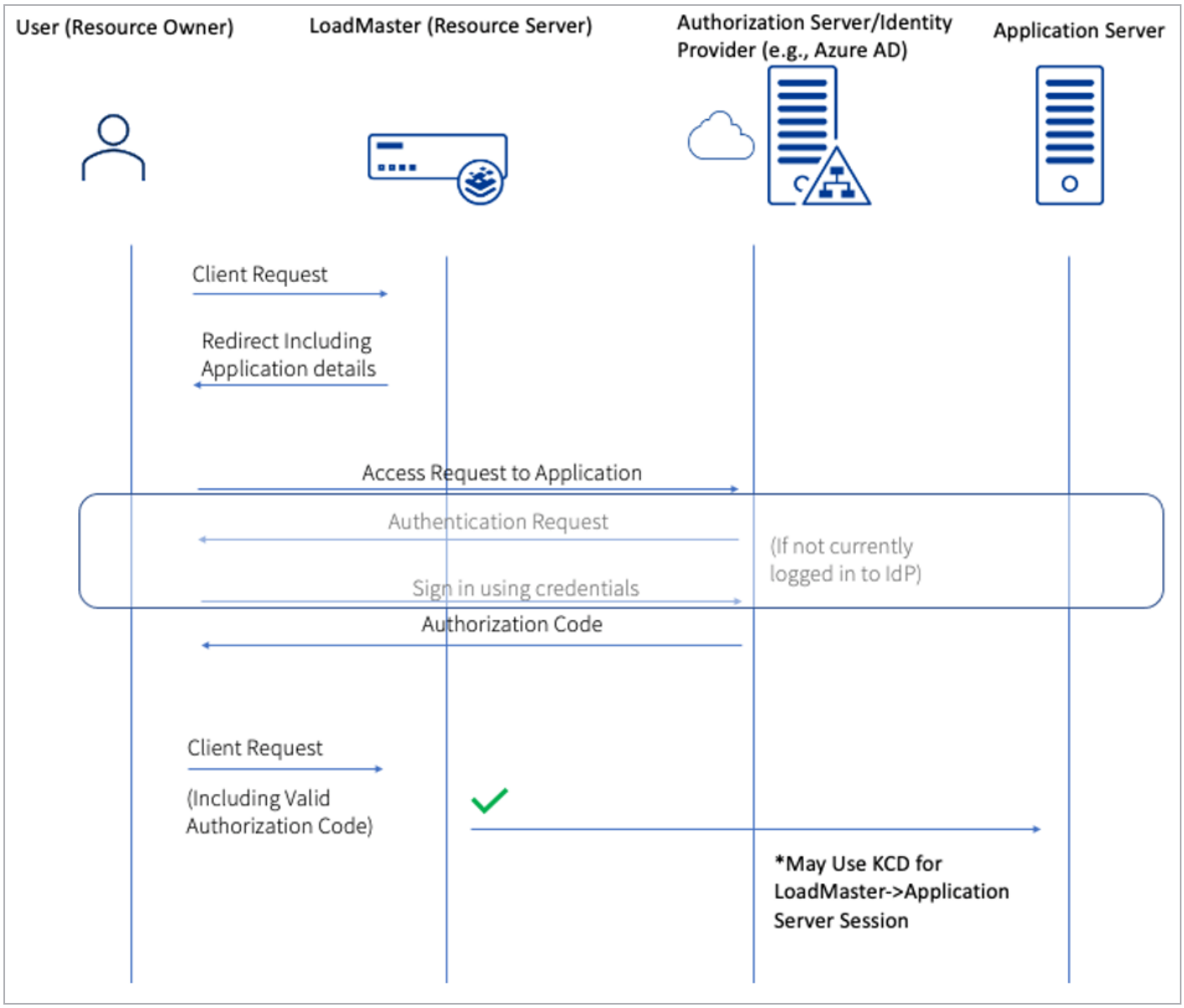
Open ID Connect (OIDC) is an identity layer added to the OAuth2.0 Protocol that enables authentication of users via tokens provided by an Identity Provider(IdP) (Referred to as the Authorisation Server role in Oauth). OIDC is commonly used to enabled Single Sign On of users across multiple applications via a single Identity Provider. OIDC uses the standardized message flows from OAuth2 to provide identity services.

When using OIDC on the LoadMaster, the loadmaster performs the Resource Server role, granting or denying access to an application via authorisation tokens. This requires an Identity Provider to be utilised for actually authenticating the users for example Microsoft Azure AD Identity Management.



Below is a brief outline of the flow when using OIDC to authenticate users on LoadMaster. Some details of the OIDC/Oauth protocol have been left out for simplicity.

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



As can be seen the LoadMaster doesn't process user credentials but instead access is granted via the authorization token that is provided by the Identity Provider. Where Single Sign on is enabled the user does not need to sign in to subsequent applications and the flow shown can occur 'silently' without user input.

For details on the logic used when the **Redirect URI** field is configured, refer to the **Redirect URI Logic** section.

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

1.1 Document Purpose

This document provides step-by-step instructions on how to configure authentication using OIDC/OAUTH in the LoadMaster.

1.2 Intended Audience

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

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

2 Configure OIDC OAUTH ESP Authentication

Follow the steps in the sections below to configure the LoadMaster to use OIDC/OAUTH ESP authentication.

2.1 Prerequisites

Before configuring the LoadMaster, please ensure that you have obtained the following information from the application configuration on your Identity Provider:

1. The Application (client) ID
2. The OAuth 2.0 authorization endpoint URL
3. The OAuth 2.0 Token Endpoint URL
4. The Logoff URL
5. The Client Secret

This information will be used to configure the Client-Side Single Sign On (SSO) configuration settings.

2.2 Create an SSO Domain

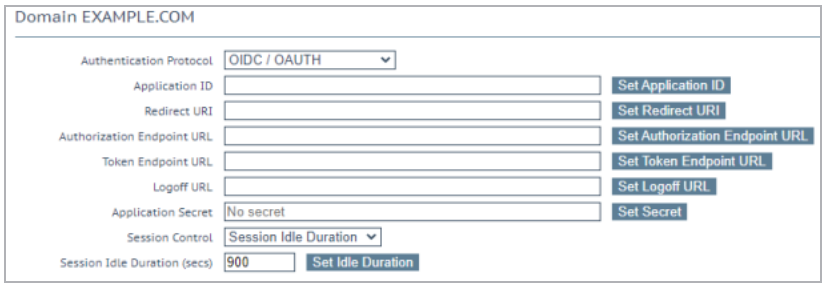
Follow the steps below to create an SSO domain in the LoadMaster:

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



2. Enter a name for the SSO domain in the **Add new Client Side Configuration** text box and click **Add**.

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



3. Select **OIDC / OAUTH** as the **Authentication Protocol**.

4. Enter the Application (client) ID of the application in the **Application ID** field and click **Set Application ID**.

5. Specify the redirect Uniform Resource Identifier (URI) or URIs (reply URLs) in the **Redirect URI** text box and click **Set Redirect URI**.

> You can enter multiple URIs separated by a space. A maximum of 255 characters can be specified in the **Redirect URI** text box. Once a value is set for this field, you cannot unset it. For further details about the logic used when the **Redirect URI** field is set, refer to the **Redirect URI Logic** section.

6. Enter the OAuth 2.0 authorization endpoint URL of the application in the **Authorization Endpoint URL** field and click **Set Authorization Endpoint URL**.

7. Enter the OAuth 2.0 Token Endpoint URL of the application in the **Token Endpoint URL** field and click **Set Authorization Endpoint URL**.

8. Enter the logout URL of the application in the **Logoff URL** field and click **Set Logoff URL**.

9. Enter the value of the Client Secret of the application in the **Application Secret** field and click **Set Secret**.

10. Select either **Session Idle Duration** or **Session Max Duration** in the **Session Control** drop-down list.

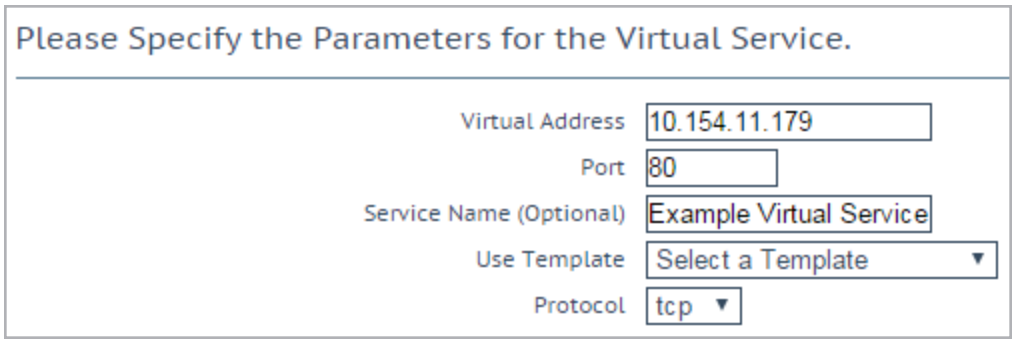
11. Specify the idle or maximum duration time (in seconds).

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**.

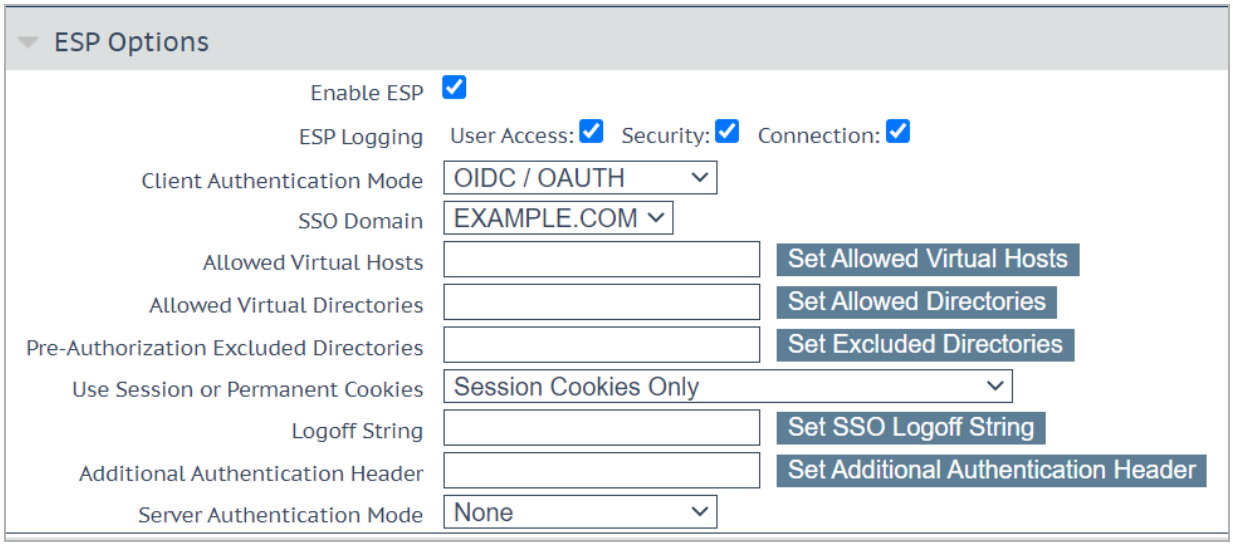
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



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 **OIDC/OAUTH** as the Client Authentication Mode.
8. Select the OIDC/OAUTH SSO domain, which was previously configured, from the **SSO Domain** drop-down list.



9. Fill out any other fields, as needed.

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

10. Add any Real Servers, as needed.

> When using the OIDC/OAUTH Client Authentication Mode, the only available Server Authentication Modes are **None** and **KCD**

> If the **Logoff String** is configured but the **Logoff URL** field in the **Manage SSO** options is left blank, when the **Logoff String** is used the user's session on the LoadMaster will be closed but they will not be logged out of their session with the Identity Provider. If a logoff URL is provided, any request that matches the logoff string will end the session on the LoadMaster and trigger a logout of the session with the Identity Provider.

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

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

3 Redirect URI Logic

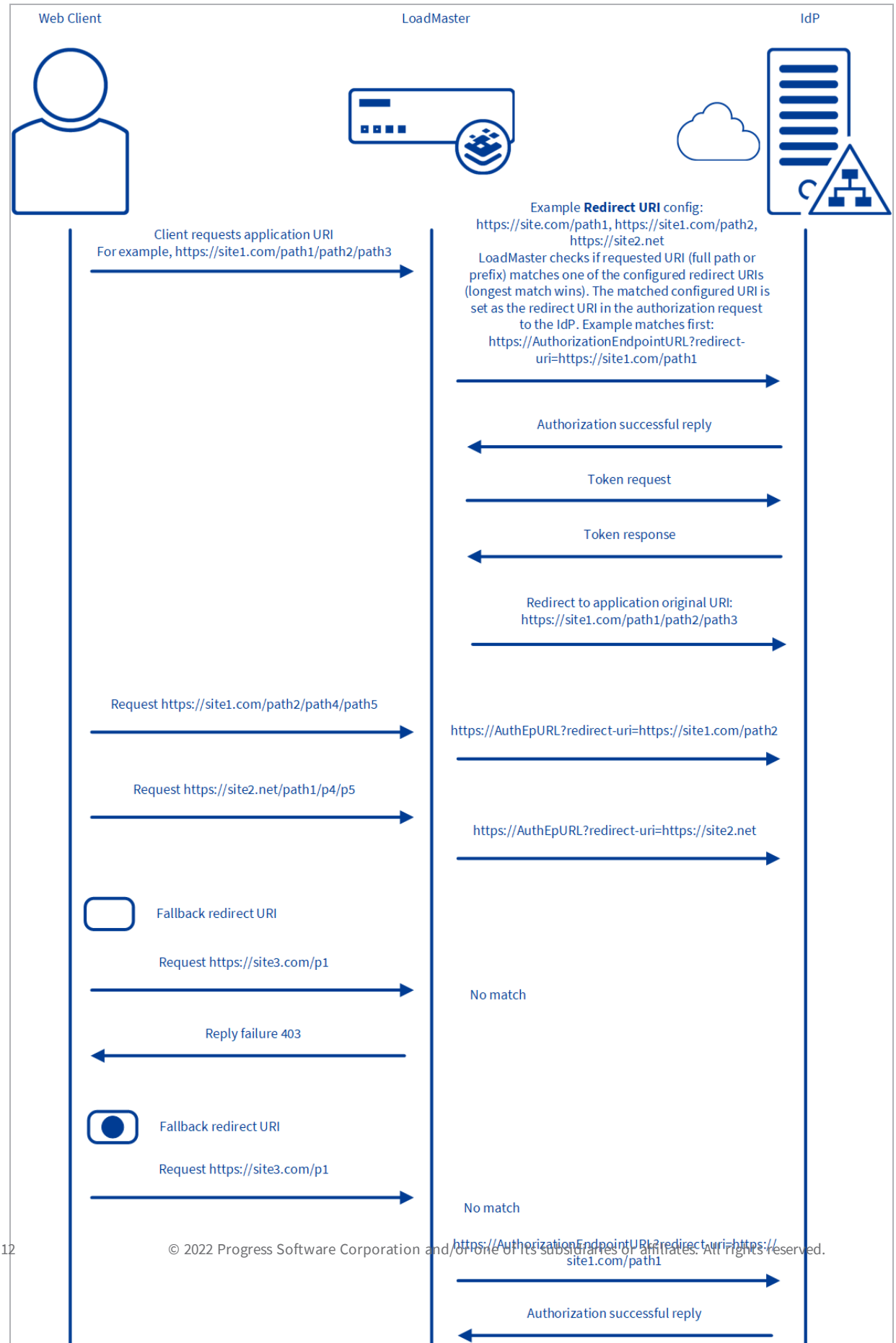
You can specify one or more redirect URIs using a space-separated list in the **Redirect URI** text box in the modify SSO domain screen (**Virtual Services > Manage SSO > Modify**).

A maximum of 255 characters can be specified in the **Redirect URI** text box. Once a value is set for this field, you cannot unset it. When set, the LoadMaster compares the requested URL with the configured list of redirect URIs. If the requested URL prefix matches, the redirect URI is used in the OIDC authorize and token messages.

If there is no match, the first configured redirect URI is used for authorize and token requests.

The logic of checking the request URL against the configured redirect URI is explained in the following diagram:

© 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.

Last Updated Date

This document was last updated on 27 July 2023.

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