Progress®
Kemp® LoadMaster®

Feature Description OIDC OAUTH ESP Authentication

Generated on: 16 September 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 7

Intended Audience 7

Chapter 2: Configure OIDC OAUTH ESP Authentication 8

Prerequisites 8

Create an SSO Domain. 9

Create a Virtual Service 10

Chapter 3: Redirect URI Logic. 12

1

Introduction

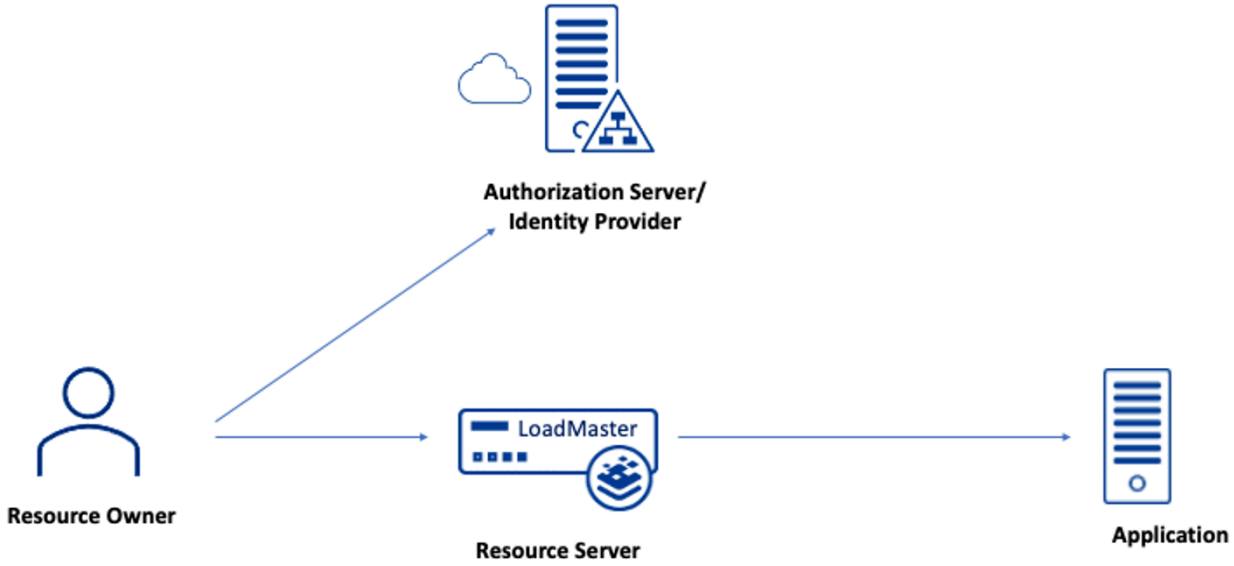
Introduction

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

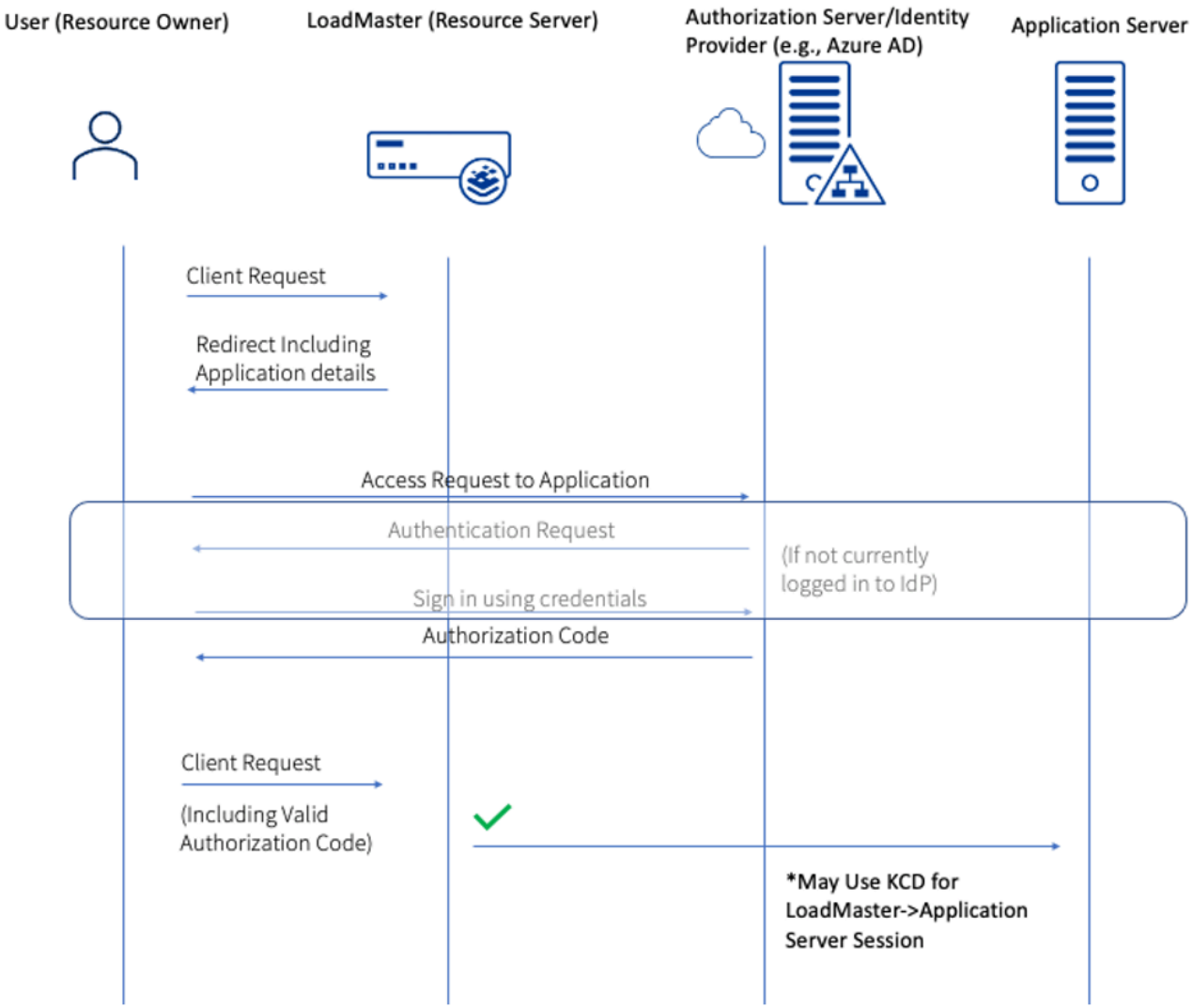
Open ID Connect (OIDC) is the preferred protocol from Microsoft for Azure AD/Identity Management OIDC is an authentication protocol based on the OAuth2 protocol (which is used for authorization). OIDC uses the standardized message flows from OAuth2 to provide identity services.

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.



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.

Related Links

- Document Purpose
- Intended Audience

Document Purpose

Document Purpose

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

Intended Audience

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 LoadMaster.

2

Configure OIDC OAUTH ESP Authentication

Configure OIDC OAUTH ESP Authentication

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

Related Links

- Prerequisites
- Create an SSO Domain
- Create a Virtual Service

Prerequisites

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.

Create an SSO Domain

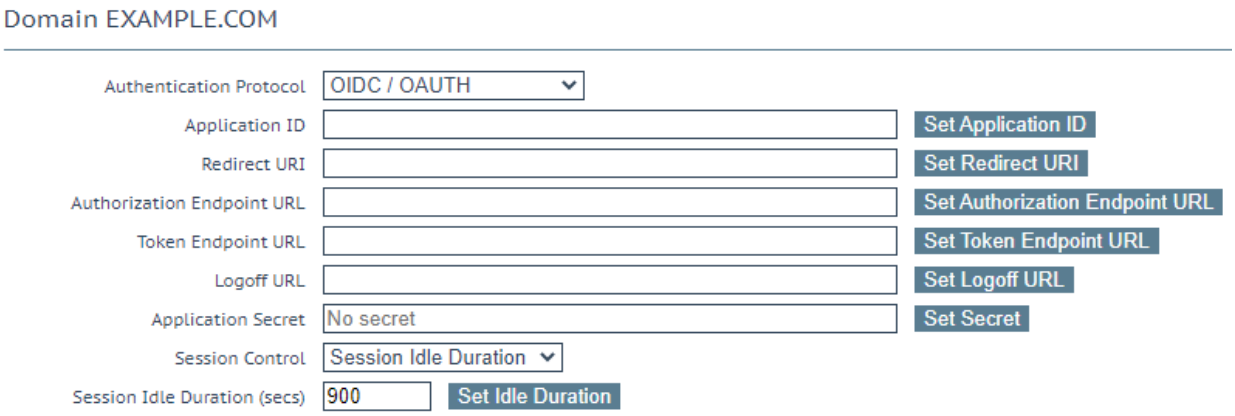
Create an SSO Domain

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**.



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**.

Note: 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**.

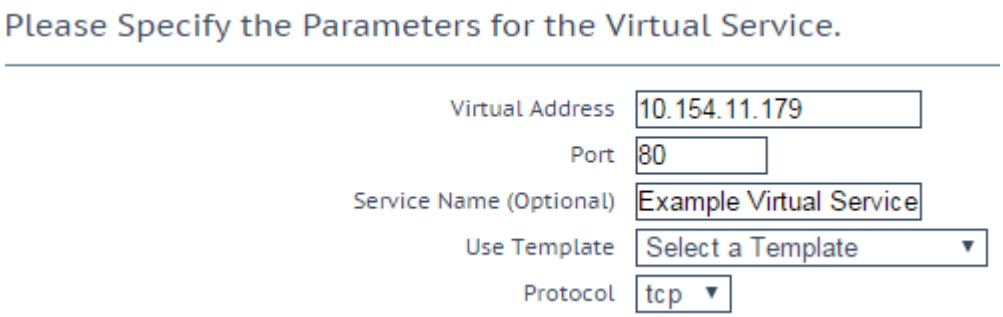
9. Enter the value of the Client Secret of the application in the **Application Secret** field and click **Set Secret**.
10. Select either **Session Idle Duration** or **Session Max Duration** in the **Session Control** drop-down list.
11. Specify the idle or maximum duration time (in seconds).

Create a Virtual Service

Create a Virtual Service

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

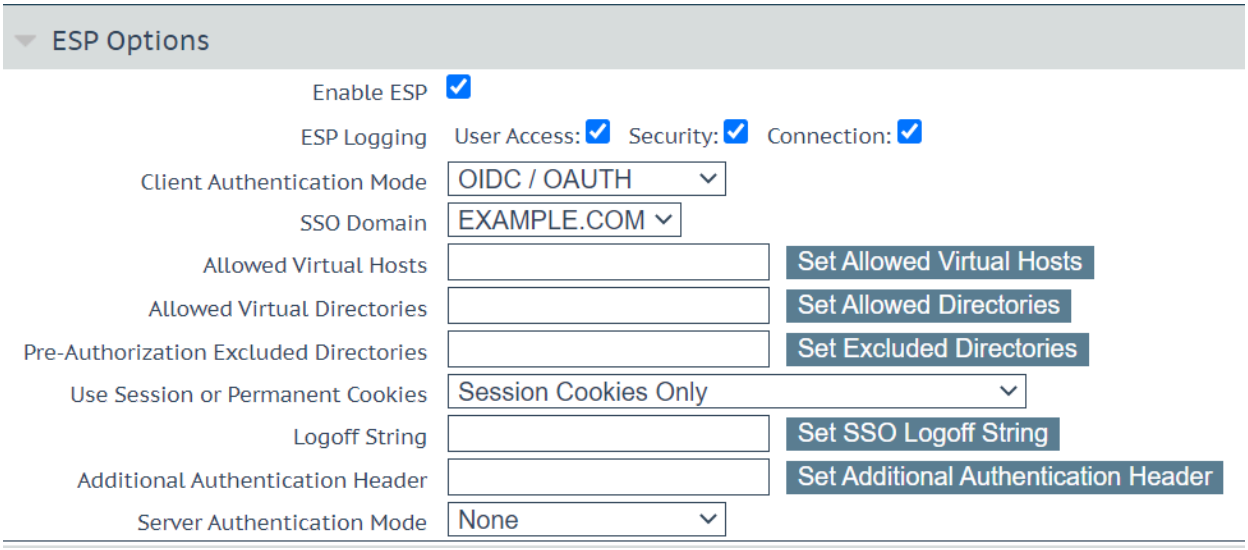
1. In the main menu of the LoadMaster WUI, navigate to **Virtual Services > Add New**.



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 **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. Set an **Additional Authentication Header**, if relevant.

Note:
When validating the token from the Identity Provider (IdP), the LoadMaster checks the claims (attributes) in the following sequence:

- preferred_username
- UPN
- unique_name
- email

For example, if the preferred_username is not available then the UPN is used. If the UPN is also not available, then unique_name or email is used for token validation.

---

10. Fill out any other fields, as needed.
11. Add any Real Servers, as needed.

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

Note: 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.

3

Redirect URI Logic

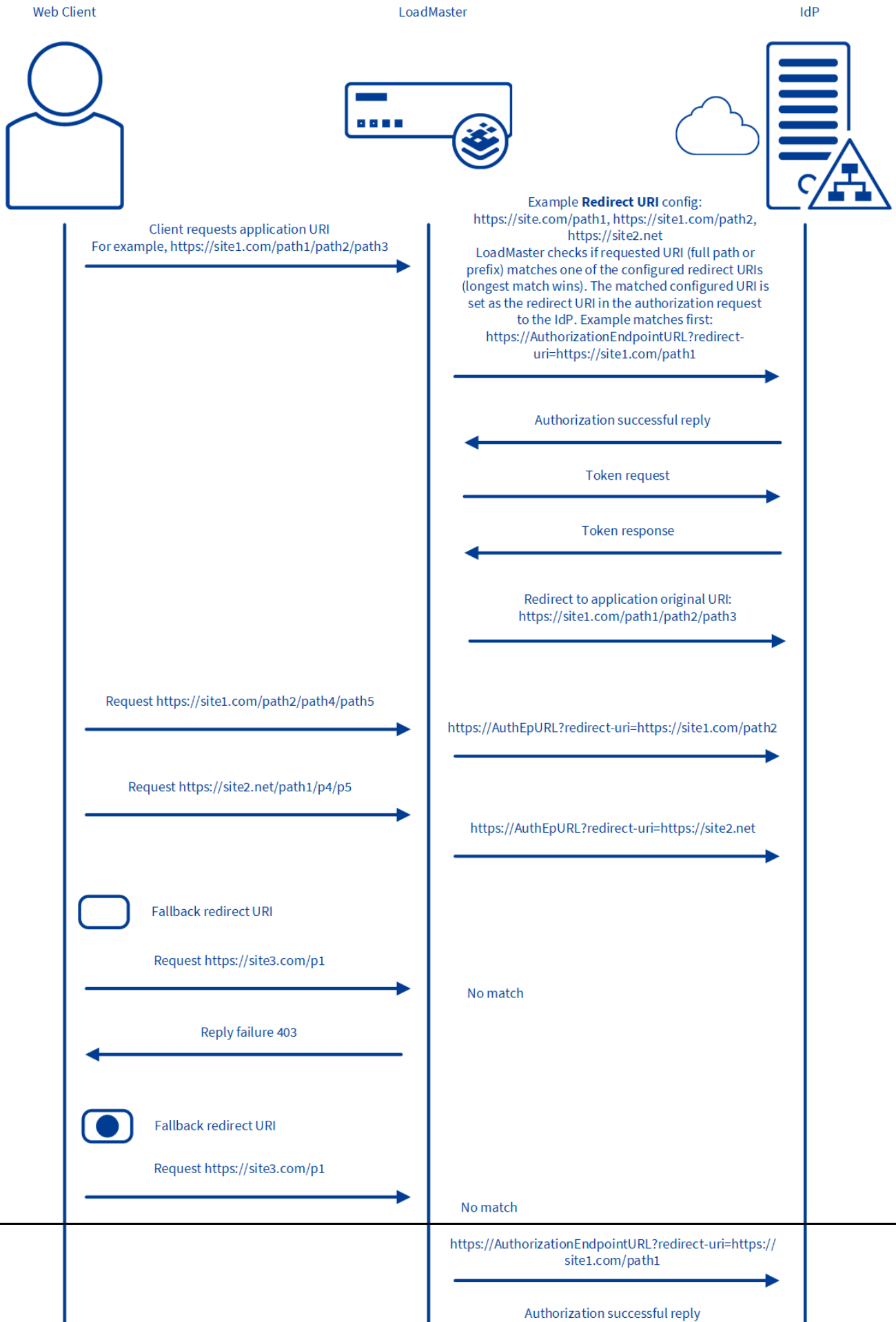
Redirect URI Logic

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:


Web Client
LoadMaster
IdP
Example **Redirect URI** config:
https://site.com/path1, https://site1.com/path2,
https://site2.net
LoadMaster checks if requested URI (full path or prefix) matches one of the configured redirect URIs (longest match wins). The matched configured URI is set as the redirect URI in the authorization request to the IdP. Example matches first:
https://AuthorizationEndpointURL?redirect-uri=https://site1.com/path1
Client requests application URI
For example, https://site1.com/path1/path2/path3
Authorization successful reply
Token request
Token response
Redirect to application original URI:
https://site1.com/path1/path2/path3
Request https://site1.com/path2/path4/path5
https://AuthEpURL?redirect-uri=https://site1.com/path2
Request https://site2.net/path1/p4/p5
https://AuthEpURL?redirect-uri=https://site2.net
Fallback redirect URI
Request https://site3.com/p1
No match
Reply failure 403
Fallback redirect URI
Request https://site3.com/p1
No match
https://AuthorizationEndpointURL?redirect-uri=https://site1.com/path1
Authorization successful reply