Web App

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Microsoft Defender for Cloud

Events (preview)

Log stream

Resource visualizer

> Deployment

∨ Settings

{x} Environment variables

Configuration

Instances

Authentication

Identity

Backups

Custom domains

Certificates

Networking

WebJobs

ⓘ Enable Application Insights for monitoring and profiling for your app.

Resource group (move)	: ASP-West	Default domain	nrh6h9agawb2.westcentralus-01.azurewebsites.net
Status	: Running	App Service Plan	: ASP-ASPWest-n
Location (move)	: West Central US	Operating System	: Windows
Subscription (move)	: OWO Cloud	Health Check	: Not Configured
Subscription ID	: d2cb6ac0-931e-4f9a-bb4f-816f854a49ef		

Tags (edit)   : Add tags

Properties   Monitoring   Logs   Capabilities   Notifications (1)   Recommendations

Web app

Name	standardspro
Publishing model	Code
Runtime Stack	Dotnet - v8.0

Domains

Default domain	.westcentralus-01.azurewebsites.net
Custom domain	Add custom domain

Hosting

Plan Type	App Service plan
Name	ASP-ASPWest-mmm58x9y4nz2r
Operating System	Windows

Deployment Center

Deployment logs	View logs
Last deployment	Loading deployments...
Deployment provider	None

Application Insights

Name	Enable Application Insights

Networking

Virtual IP address	
Outbound IP addresses	Dynamic
Additional Outbound IP addresses	Dynamic
Virtual network integration	Not configured

↻ Refresh

Platform settings

Platform

| 32 Bit | ⌄ |

Managed pipeline version

| Integrated | ⌄ |

SCM Basic Auth Publishing Credentials ⓘ   ☑

FTP Basic Auth Publishing Credentials ⓘ   ☑

FTP state ⓘ

| Disabled | ⌄ |

Inbound IP mode

| IPv4 | ⌄ |

HTTP version ⓘ

| 2.0 | ⌄ |

HTTP 2.0 Proxy ⓘ

| Off | ⌄ |

ⓘ The 'gRPC Only' option is only available for .NET and Java apps.

Web sockets   ☐

Always on ⓘ   ☑

Session affinity ⓘ   ☐

Session affinity proxy ⓘ   ☐

HTTPS only ⓘ   ☑

HTTPS only ⓘ

☑

Minimum Inbound TLS Version ⓘ

| 1.2 | ⌄ |

Minimum Inbound TLS Cipher Suite ⓘ   TLS_RSA_WITH_AES_128_CBC_SHA (Default) Change

End-to-end TLS encryption ⓘ

☑

Incoming client certificates

Client certificate mode ⓘ

○ Required
All requests must be authenticated through a client certificate.

○ Optional
Clients will be prompted for a certificate, if no certificate is provided fallback to SSO or other means of authentication. Unauthenticated requests will be blocked.

○ Optional Interactive User
Clients will not be prompted for a certificate by default. Unless the request can be authenticated through other means (like SSO), it will be blocked.

◉ Ignore
No client authentication is required. Unauthenticated requests will not be blocked.