Hyland Preferences Service

Technical Specifications

Version: 3.0.x

Written by: Documentation Team, R&D
Date: August 2023

Hyland™

Documentation Notice

Table of Contents

Overview

Hyland Preferences Service is a micro-service used to store user preferences for applications. Although the service can be used directly, its recommended use is by services that authenticate a user prior to making requests to the preferences service. For example, Perceptive Content uses the service through Integration Server to store preferences for a Perceptive Content user.

System requirements

Specification	Description
Operating Systems	We recommend that you upgrade to the latest operating system patch of the following supported operating system versions. • Microsoft Windows Server 2016 or 2019 • RedHat Linux x86_64 version 7 • Oracle linux version 7
Framework	.NET Core is distributed as part of the service bundle, and does not need to be installed separately. ASP.NET Core Runtime 6.0 Windows Hosting Bundle is required if running the service as an IIS service. .NET Core runtime dependencies may be required on Linux. Refer to Microsoft's documentation to determine what prerequisities, if any, are required.
Internet Information Services (IIS)	A minimum of IIS 7.5 is required if running the service as an IIS service.

Service database

Specification	Description
DBMS	We recommend that you upgrade to the latest DBMS patch of the following supported versions. • Microsoft SQL Server 2016, 2017 and 2019 • Oracle 12c R1 (12.1), 12c R2 (12.2.0.1), 18c and 19c • PostgreSQL 13, 14, and 15
Memory	Database size varies by implementation and use of the product.
Disk Space	Database size varies by implementation and use of the product.

Authentication

A trust relationship is established between the Hyland Preferences Service and the service using it through an asymmetrically signed JSON Web Token (JWT). The service creating and signing the JWT

provides a public key to the preferences service so the service can validate the JWT's signature with every request.

Note The public key must be an X509 certificate, PKCS8 encoded key or a PKCS7 object. The JWT is required to contain the following headers and claims.

Name	Location	Options	Description
kid	Header	Any valid string	A configuration entry should exist in the Hyland Preferences Service configuration.
alg	Header	RS256 RS384 RS512 ES256 ES384 ES512	Hash algorithm used when creating the key-pair used to sign and validate the JWT. Should match the preferences service configuration.
typ	Header	hsi.pref.svc.jwt.v1	
sys	Claims	Any valid string	Identifies the external system the user ID comes from.
uid	Claims	Any valid string	Used in combination with **sys** to uniquely identify a user.
exp	Claims	A valid number	The expiration time of the JWT. The current date/time must be before the expiration date/time for the JWT to be considered valid.