OpenID Connect SSO Solutions

Technical Guide

Version: Foundation EP4

Written by: Product Knowledge, R&D
Date: June 2021

Hyland

Copyright

Information in this document is subject to change without notice. The software described in this document is furnished only under a separate license agreement and may be used or copied only according to the terms of such agreement. It is against the law to copy the software except as specifically allowed in the license agreement. This document or accompanying materials contains certain information which is confidential information of Hyland Software, Inc. and its affiliates, and which is subject to the confidentiality provisions agreed to by you.

All data, names, and formats used in this document's examples are fictitious unless noted otherwise. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright law, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Hyland Software, Inc. or one of its affiliates.

Hyland® and Hyland Software®, as well as Hyland product names, are registered and/or unregistered trademarks of Hyland Software, Inc. and its affiliates in the United States and other countries. All other trademarks, service marks, trade names and products of other companies are the property of their respective owners.

© 2021 Hyland Software, Inc. and its affiliates. All rights reserved.

Table of Contents

Copyright **2**
OpenID Connect **4**
OpenID Connect Discovery **4**
Login profiles **4**
User claim mapping **4**
Setting up a solution **5**

OpenID Connect

OpenID Connect is an authentication protocol that is based on the OAuth 2.0 specification, but focuses on authentication rather than authorization. Through OpenID Connect, a client application can request and receive information from an OpenID Provider about end users that is narrowly scoped to what it needs. You can configure Perceptive Content and its client applications as OpenID clients that leverage OpenID Connect authentication.

You must register Perceptive Content clients with an OpenID Provider before you configure OpenID Connect authentication. Once registered and configured, Perceptive Content clients can leverage OpenID Providers for authentication. Perceptive Content supports the Authorization Code Flow and the Authorization Code Flow with Proof Key for Code Exchange (PKCE). OpenID Providers release claims about end-users based on scopes that are requested by the Perceptive Content clients. Perceptive Content uses identity claims to map authenticated end-users to Perceptive Content users.

OpenID Connect Discovery

If supported by the OpenID Provider, OpenID Connect Discovery can be used to simplify configuration of OpenID clients in Perceptive Content. To leverage OpenID Connect Discovery in Perceptive Content configure the openid-configuration endpoint for the OpenID Provider. Perceptive Content then uses the openid-configuration endpoint to discover OpenID Provider Metadata, such as additional endpoint URLs and token signing keys. If changes are made to the OpenID Provider configuration, Perceptive Content can use OpenID Connect Discovery to automatically reflect those changes. For example, if token signing keys are changed when using OpenID Connect Discovery, Perceptive Content automatically imports them and no additional client side changes are necessary.

Login profiles

In Perceptive Content, we provide the ability to utilize OpenID Connect through login profiles. Login profiles allow for multiple OpenID Connect configurations to be specified at the same time. Since multiple different clients can be registered with a given OpenID Provider, all with different secrets, permissions, and requirements, these login profiles allow for extremely flexible deployments. Any number of clients configured in any number of OpenID Providers may be used at any given time with Perceptive Content, so long as they have an associated login profile. We recommend that each login profile correspond to one client configured in an OpenID Provider.

User claim mapping

To make use of the claims returned by the OpenID Provider, Perceptive Content needs to know which claim returns values that are a one-to-one mapping to Perceptive Content usernames. Therefore, when configuring Perceptive Content Server for OpenID Connect, one of the required settings is the **user.claim** setting, from which Perceptive Content Server can map values of a claim to usernames in its database. The exact claim that should be chosen for this setting depends on which scopes and claims are supported by the OpenID Provider.

When integrating with the Hyland Identity Provider, the claim that works best for Perceptive Content is the **username** claim which is exposed when the **profile.onbase** scope is requested. In this configuration, the **profile** and **profile.onbase** scopes must be allowed by the client, and the scope setting in Integration Server must include both **openid** and **profile.onbase**. You can find more information about the Hyland Identity Provider on Hyland Community.

Setting up a solution

The high-level steps involved in setting up an OpenID Connect solution are as follows.

1. Set up your OpenID Provider.

   Note Configuration varies depending on the provider you are using. For more information, refer to the product documentation for the OpenID Provider.

2. Configure clients on your OpenID Provider. Ensure they support the authorization code flow and allow any necessary scopes.
3. Ensure Integration Server is configured for TLS and configure login profiles.
4. On the Perceptive Content Server, configure login profiles and ensure TLS trust is established with the OpenID Provider.