Privilege Management Cloud
authID Verified Integration

TC:2/13/2024

Set Up AuthID for EPM

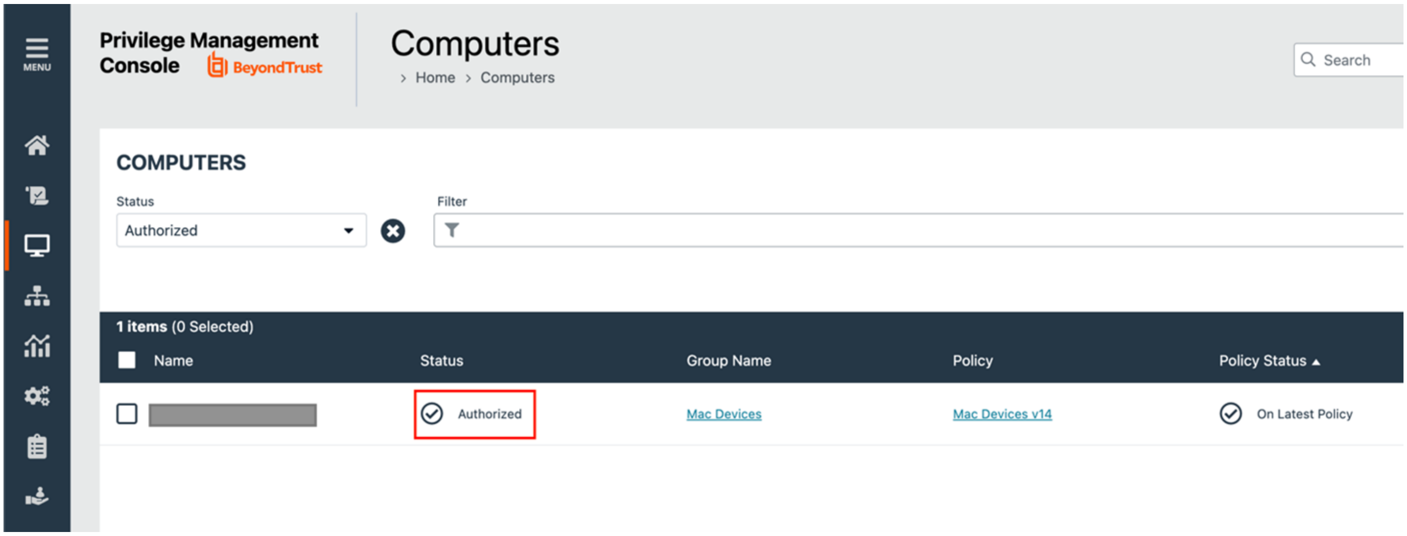
The following steps show how to set up an OIDC connection in BeyondTrust EPM to leverage authID's biometric authentication platform.

The authID Verified platform delivers human factor authentication (HFA) that combines secure FIDO2 passkeys with strong cloud biometric identity assurance to verify the human behind the device.

HFA fortifies *something the user has* with *something the user is* to protect work platforms from unauthorized access and lateral movement of bad actors with truly portable NIST and FIDO2 compliant authentication. Deploy unphishable, passwordless authentication on any desktop or mobile device and everywhere your employees, contractors, and partners work.

Install Endpoint Privilege Management

Using the appropriate installation guide for Windows or Mac, ensure Endpoint Privilege Management software is installed to computers and the computers are synchronized in the EPM console:



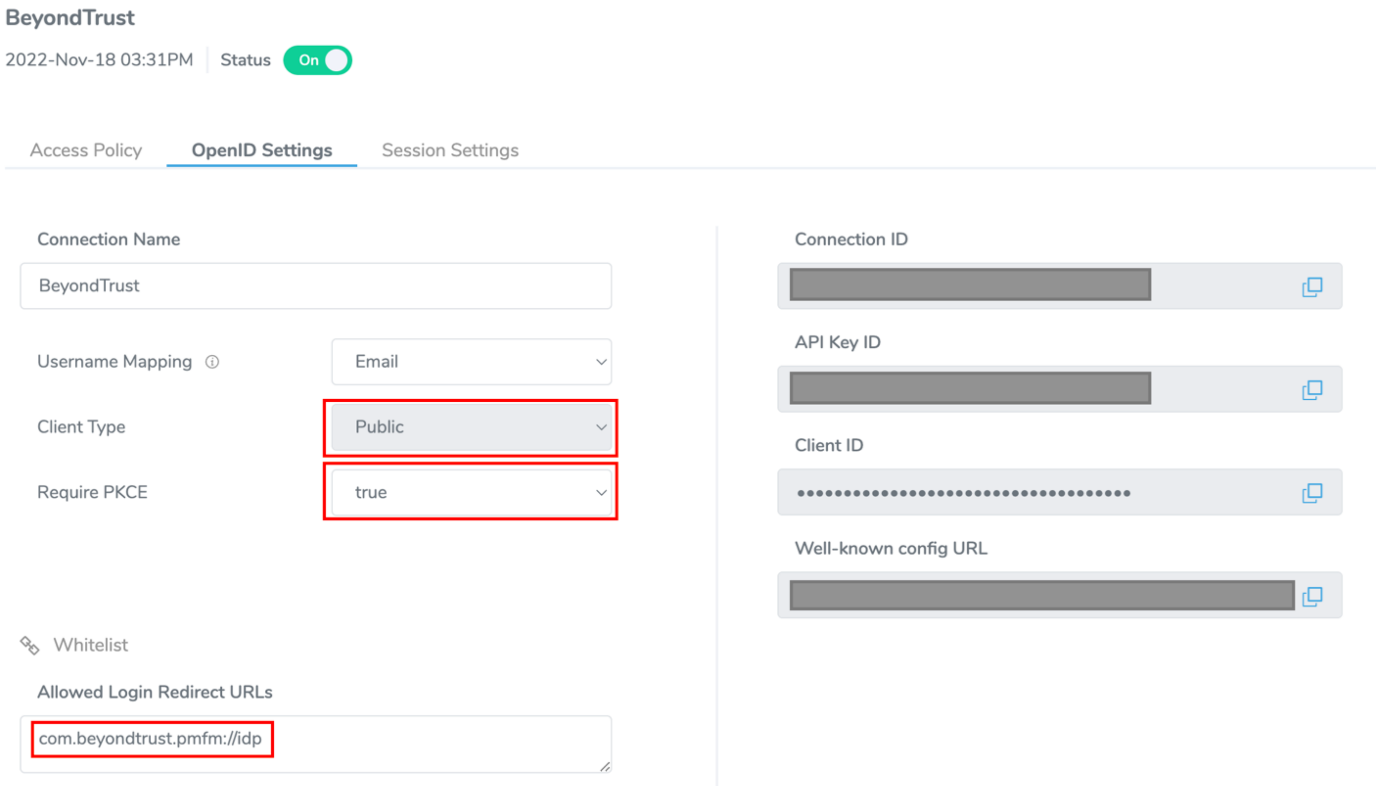
For more information about installing Windows or Mac, please see:

- *Install Endpoint Privilege Management for Windows at https://www.beyondtrust.com/docs/privilege-management/windows/admin/install-upgrade/install-pm-windows.htm.*
- *Install the Endpoint Privilege Management for Mac Client at https://www.beyondtrust.com/docs/privilege-management/mac/admin/install-mac-client.htm.*

Create authID Integration

1. Follow the steps in the authID integration guide to create an identity provider.
2. Set the **Client Type** to **Public** and **Require PKCE** to **true**. This will not generate a client secret but ensures that the integration remains secure using PKCE.
3. Set the login redirect URL to *com.beyondtrust.pmfm://idp*.

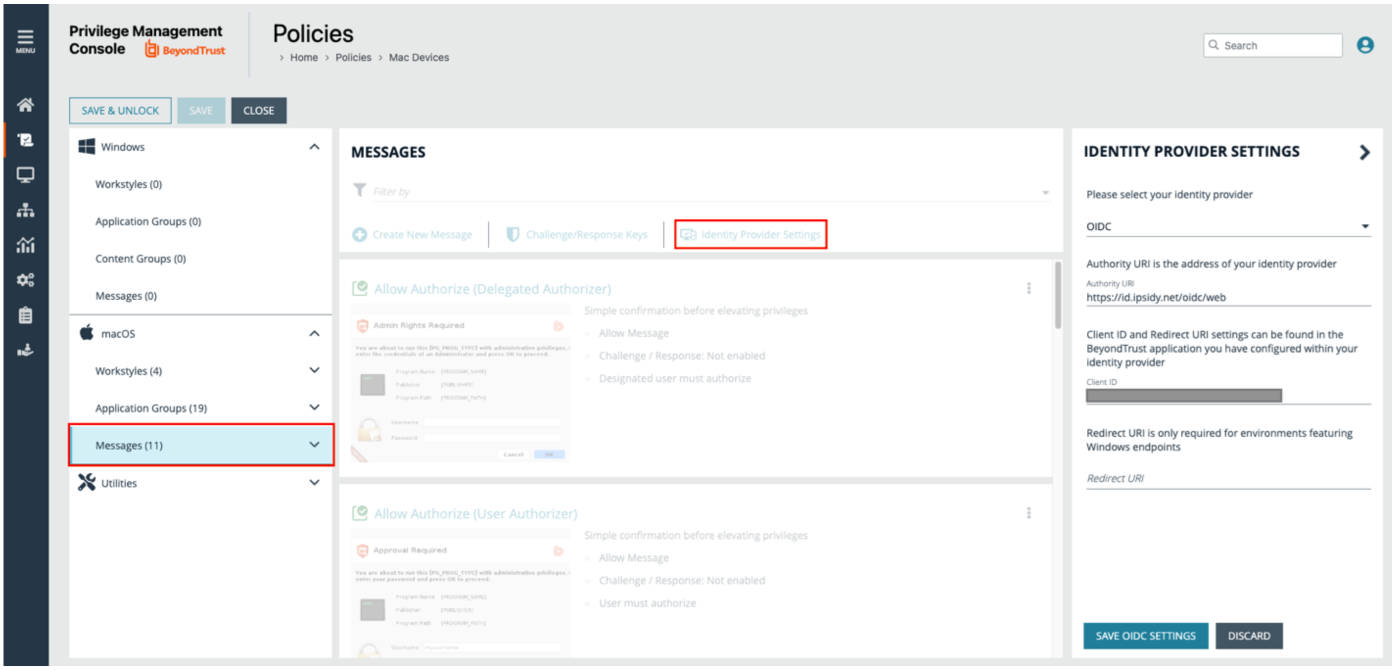
For more information, please see [authID Integration](https://developer.authid.ai/docs/verified/cloud-connect/oidc/authid-integration) at https://developer.authid.ai/docs/verified/cloud-connect/oidc/authid-integration.



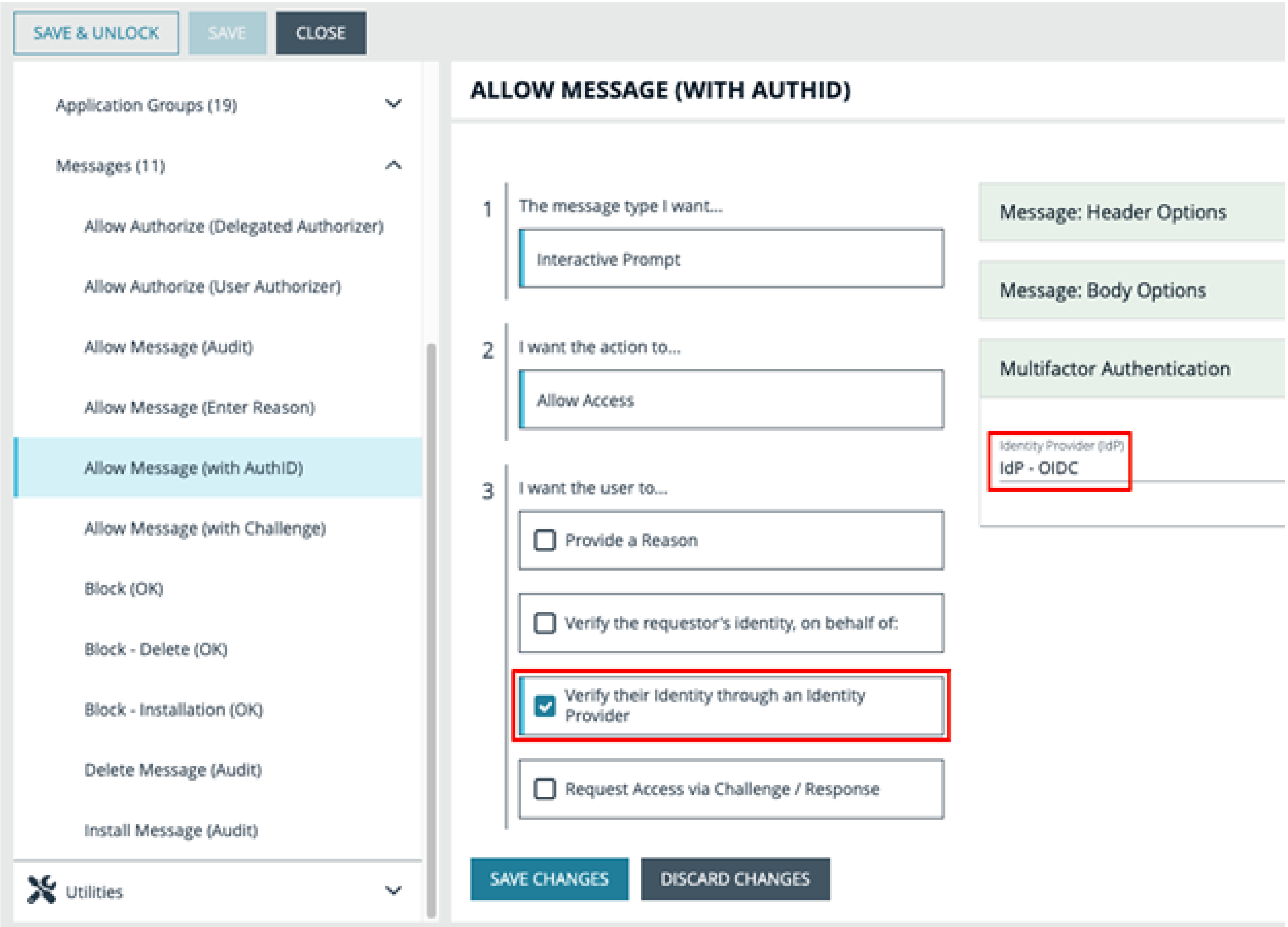
Update Policy

If you correctly configured and deployed a policy for Windows or macOS, update the policy to use the authID identity provider you created in the previous section.

1. Edit and unlock the relevant policy in the policy list, and then navigate to **Messages** for either Windows or macOS.
2. Click the **Identity Provider Settings** button to enter the following details for the integration:
    - **Identity provider**: Select **OIDC** from the menu.
    - **Authority URI**: Enter *https://id.ipsidy.net/oidc/web*
    - **Client ID**: Enter the value from the previous step.
    - **Redirect URI**: Enter the redirect URI used for Windows endpoints.

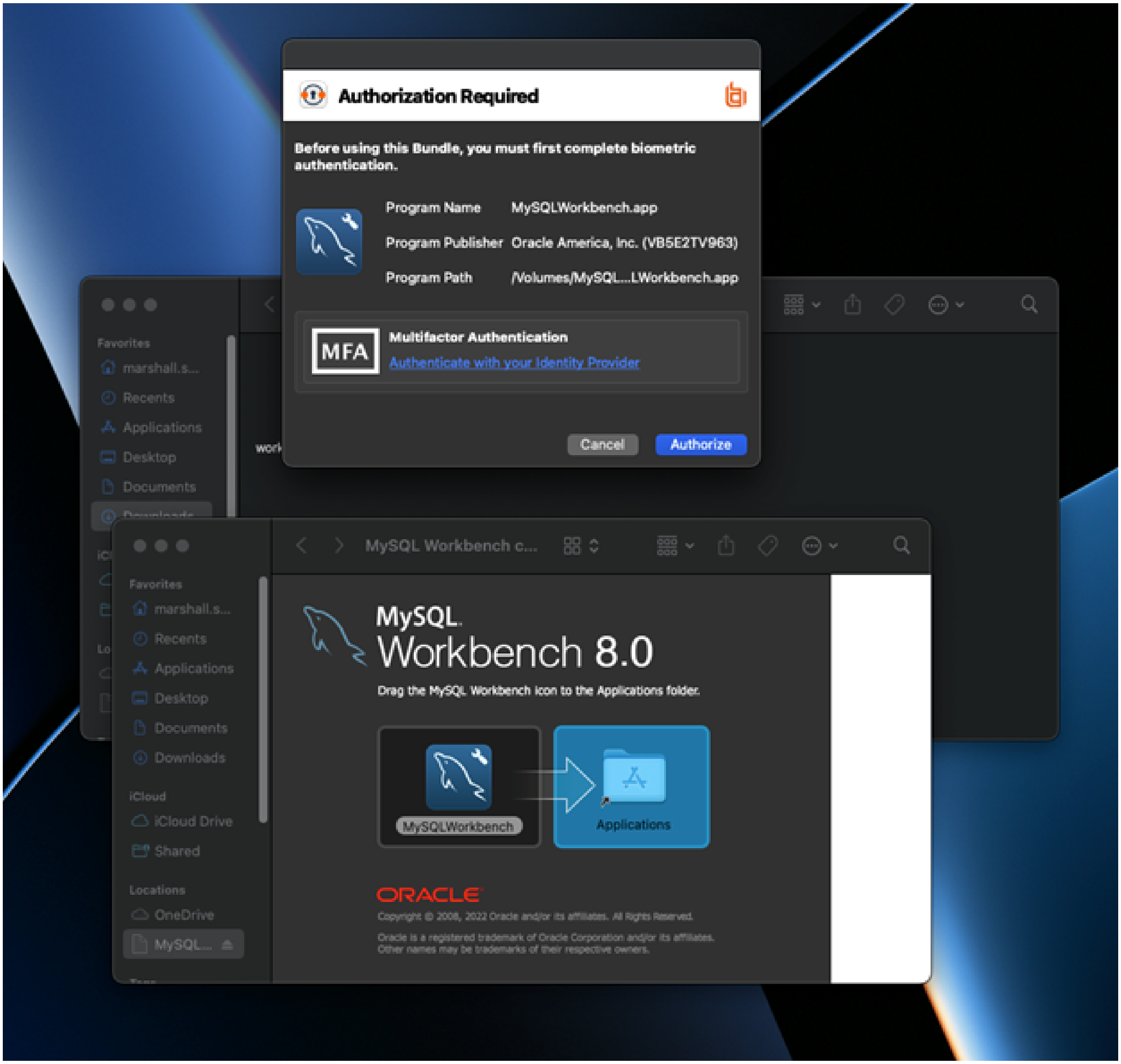


3. (Optional). Create a new message type or modify an existing one to activate the IdP authentication.
4. In the third section, check the box **Verify their Identity through an Identity Provider**.
5. Select **Idp - OIDC** from the **Multifactor Authentication** dropdown.

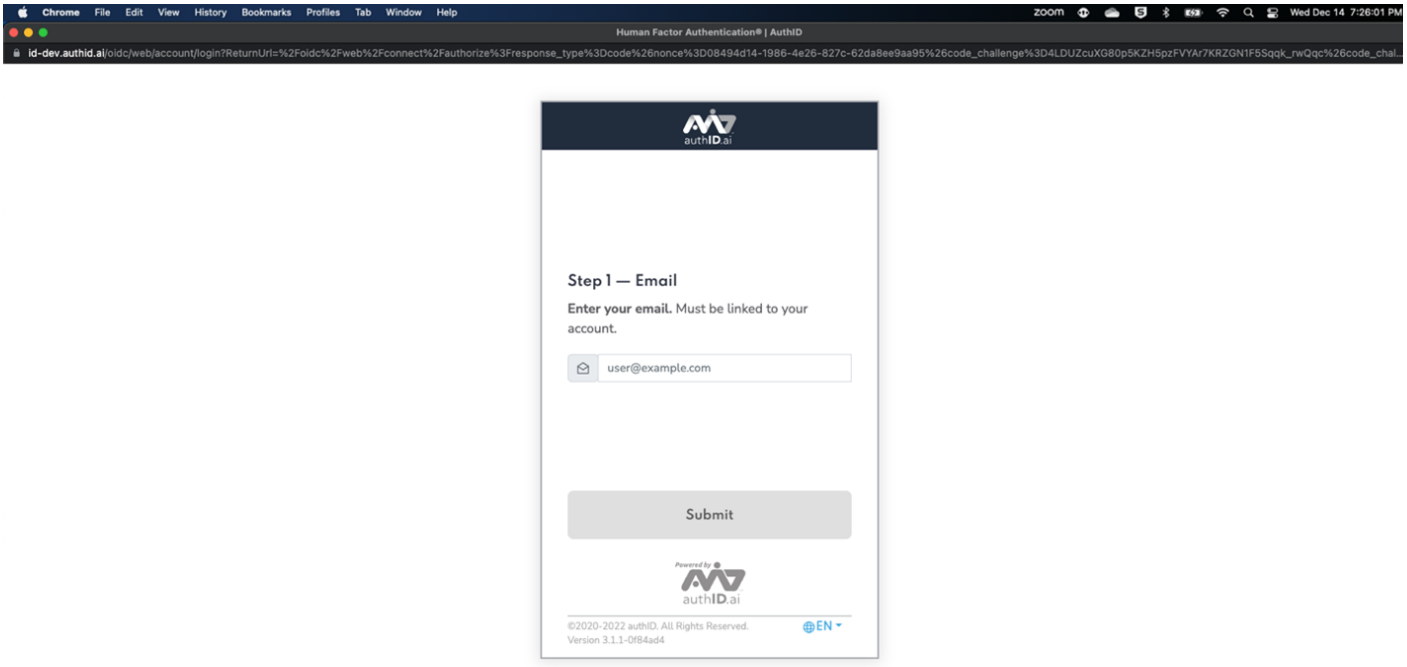


Test Policy (Optional)

You can test that the policy works correctly by having a user engage in an activity that activates the message you created. A dialog box displays where the user enters their details in the authID system to complete the authentication.



From here, the default browser appears. The user is prompted to continue their authentication with authID:


Human Factor Authentication® | AuthID
Step 1 — Email
Enter your email. Must be linked to your account.
user@example.com
Submit
authID.ai
©2020-2022 authID. All Rights Reserved.
Version 3.1.1-0f84ad4
EN