OpenID Connect Settings for Microsoft Azure AD

Last Modified on 01/11/2022 4:51 pm EST

OpenID Connect Settings for Microsoft Azure AD

This article describes settings that have been used successfully within OnGuard and Microsoft Azure AD in order to use Azure AD as a third-party identity provider for OnGuard via the OpenID Connect protocol.

Note: Third-party settings may be different from those discussed here based on the specific third-party product or version in use or other differences. The following settings and directions on where to find settings in the Azure administration portal are not guaranteed to work in all situations. For details on using their service, contact your third-party provider, or refer to their documentation.

Procedure Steps

Azure AD Settings:

1. When adding OnGuard to your application registrations, select **Native** as the Application Type.
2. The Redirect URI must be the URI for Lenel Console for the specific OnGuard installation.
3. The redirect URIs may be edited, if necessary, by editing the Manifest at ***Home > Azure > Active Directory > App Registrations >*** .

OnGuard Settings:

1. Set the Base URL to **https://login.microsoftonline.com/**. You can find your Directory ID in the Azure administration page at ***Home > Azure Active Directory > Properties***.
2. Use the Application ID listed for the application for the Client ID in OnGuard. You can find the Application ID in the Azure administration page at ***Home > Azure Active Directory > Properties > App Registrations.***
3. Uncheck ***Advanced > Require Access Token Hash***.
4. Uncheck ***Advanced > Validate Issuer Name***.
5. Set ***Advanced > Additional Endpoints*** to **https://login.microsoftonline.com/common/discovery/keys**, or uncheck **Validate Endpoints**.

Applies To

OnGuard 7.5 (and above)

Additional Information