OpenID Connect Settings for Entrust

Last Modified on 04/08/2025 12:54 pm EDT

This article describes settings that have been successfully used within OnGuard and Entrust IntelliTrust in order to use IntelliTrust as a third-party 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 for other differences. The following settings are not guaranteed to work in all situations. Contact your third-party provider to see their documentation for details on using their service.

Procedure Steps

Entrust IntelliTrust Settings:

1. When adding OnGuard as an application resource, select **Generic OIDC Application**.
2. Under **Response Types**, select **code (Basic Flow)**.
3. Set **User Info Signing Algorithm** to **None**.
4. Redirect URI(s) must include the URI for Lenel Console for the specific OnGuard installation. A trailing "/" may be required.

   Note: Entrust does not allow entering IP addresses as redirect URIs. To use Entrust as an identity provider with OnGuard, the OnGuard server must have a non-IP URL that can be found by Entrust via DNS.
5. For **Token Endpoint Client Authentication Method**, select either **Client Secret Basic** or **Client Secret Post**.

OnGuard Settings:

1. On the IntelliTrust Application Settings page, in the General Settings section, fill in the **Client ID** and **Client Secret** fields.
2. On the Advanced sub-tab, uncheck the **Require Access Token Hash** check box.
3. On the Advanced sub-tab, confirm that the setting for **Token Authentication Style** matches the setting made in Step 5 above (Entrust IntelliTrust settings).

Applies To

OnGuard 7.5 (and above)

Additional Information