OpenID Connect Settings for Okta

Last Modified on 02/18/2022 4:06 pm EST

OpenID Connect Settings for Okta

This article describes settings that have been used successfully with OnGuard and Okta in order to use Okta 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 are not guaranteed to work in all situations. Contact your third-party provider or refer to their documentation for details on using their service.

Procedure Steps

Okta Settings:

1. The application must be added as the "Native iOS, Android" type.
2. Allowed grant types must include the Authorization Code.
3. Login redirect URIs must include the URI for Lenel Console for the specific OnGuard installation.
4. Client authentication should be set to -- **Use Client Authentication**.

OnGuard Settings:

1. Set the Base URL to **https:///oauth2/default**.
2. Fill in the Client ID from the Client Credentials section in the Okta settings.
3. If using Client authentication mode User Client authentication, fill in the Client Secret from the Client Credentials section in the Okta settings.
4. Set Advanced > Additional Endpoints to **https:///oauth2/v1/client**, or uncheck **Validate Endpoints**.

Applies To

OnGuard 7.5 (and above)

Additional Information