



Nomidio OpenID

AWS Quick Start Guide

Version 1.2



Versions

Version	Authors	Approved	Date	Notes
1.0	mj, aks, jk	pb, cjt, mj	23 October 2020	Initial version
1.1	mj, aks	mj, cjt	10 December 2020	Adding SAML
1.2	aks, mj	mj	20 January 2021	Updated admin screens

Contents

Versions	2
Contents	3
About this Guide	5
Certification	5
Overview	5
Prerequisites	5
What is Covered	5
Architectural Overview	6
Terminology	6
Setting up a Nomidio OpenID Subscription	8
Nomidio OpenID Onboarding Portal	8
Enterprise And Connect Region Details	8
Administrator Account Creation	9
Email Verification	9
Administrator Password	10
Two Factor Authentication	10
Identity Provider Setup	11
OpenID Connect	11
SAML 2.0	11
Sign in Button	12
Nomidio OpenID Access Management	12
Nomidio Admin Service	12
Enterprise Privacy Policy	13
OpenID Admin Permissions	13
OpenID Client Management	13
OpenID Access Management	14
Applications	14
Creating an Application	14
Application Management	15
Editing the Application Details	16
Registering a Client	17
Create OpenID Connect Client	18
Signature Algorithm	18
Scopes	19

Redirect URIs	19
Client ID and Secret	19
Create SAML Client	20
SAML Name Identifier Format	21
Attribute Profile	21
Basic	21
LDAP	21
SOAP	22
Service Provider Entity ID	22
Assertion Consumer Service URL	22
Service Provider's Signing Certificate	22
Signature Algorithm	22
IdP Entity Id, Certificate and Metadata	22
Editing Client Details	24
Application Access Policies	24
Adding an Application Access Policy	24
Nomidio OpenID Access Groups	25
Adding an Access Group	25
Group Types	26
Anyone	26
Enrolled	26
Restricted	26
Blocked	27
Access Rules	27
Rule Types	28
Adding an Access Rule	28
Assigning Applications to an Access Group	29
Managing Application Access	29
Authentication Level	30
Standard Security Authentication	30
High Security Authentication	30
Multiple Access Groups	30
Creating a Nomidio ID	30
Nomidio ID Registration Link	31
Create Registration Link	31
Share Registration Link	31
Registration on Login	31
Sign in with Nomidio OpenID	32

Single Sign-On with Nomidio OpenID	34
Appendices	35
Nomidio ID Account Registration	35
Key Recovery Login	42

About this Guide

This implementation guide discusses the architecture, setup and configuration steps required to successfully integrate applications, which support OpenID Connect, OAuth 2, or SAML 2.0 sign-on, with the Nomidio OpenID Identity Provider.

Certification

Nomidio is a [member](#) of the OpenID Foundation and has certified that Nomidio OpenID conforms to the *Basic OpenID Provider* profile of the OpenID Connect™ protocol. For more information about the OpenID Foundation and the certification see [OpenID Certification](#).

Overview

Nomidio OpenID provides secure multi-factor biometric user authentication via a user's web browser, without the need for any additional applications or passwords.

Prerequisites

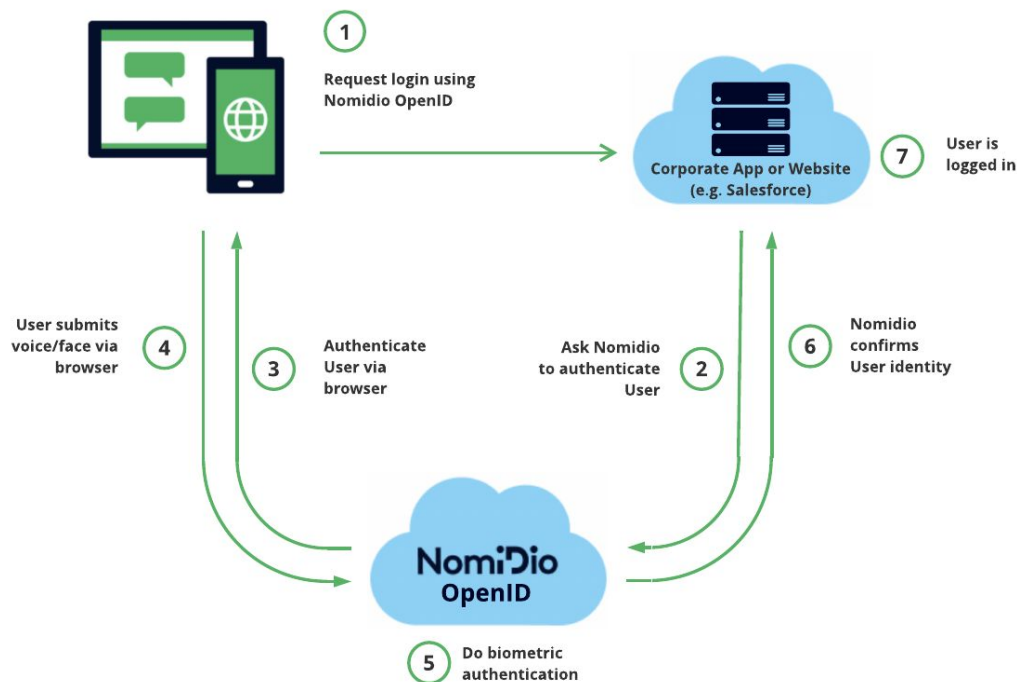
Nomidio OpenID is a cloud hosted Software-as-a-Service, so the only prerequisite for using Nomidio OpenID is that your applications or websites support the OpenID Connect, OAuth 2.0, or SAML 2.0 standards for user authentication.

What is Covered

This guide will take you through the process of enabling sign-on with Nomidio OpenID for your enterprise applications. This requires the following steps:

- Subscribe to the Nomidio OpenID product in [AWS marketplace](#)
- Register your company details and create your Nomidio administrator account
- Create OpenID Connect and/or SAML credentials for your applications
- Setup the user access group for your application
- Create a Nomidio ID account and sign-in using Nomidio OpenID

Architectural Overview



Terminology

OpenID Connect and SAML are both open standards for user authentication and each has a slightly different set of terminology. The terminology listed here covers both terms that appear in this document and some which are not used here but may appear in the relevant application documentation for identity provider integration.

- **Nomidio OpenID** - The Nomidio Identity Provider SaaS product which enables enterprises to use Nomidio IDaaS for user authentication with the OpenID Connect and SAML 2.0 authentication standards.
- **Nomidio ID** - The user's digital identity.
- **Nomidio IDaaS** - A cloud based Identity-as-a-Service which enables users to create a secure digital identity and enterprise to authenticate users with biometric checks either via the web with open standard authentication protocols (OpenID Connect and SAML), or through direct server integrations via the Nomidio IDaaS API for services like over the phone (IVR) call centre authentication, authenticate web-chat, ...
- **OpenID Connect** (or OIDC) - An open standard for internet based user authentication built on top of the OAuth2 standard and maintained by OpenID Foundation. For more details visit <https://openid.net>

- **OpenID** - Generally refers to the OpenID Connect standard rather than the Nomidio OpenID product. There are some cases where this term is referring to the Nomidio OpenID product, i.e. administrator permissions in the Nomidio Admin Service use the term for permission associated with the product, but in such cases it should be clear by the context.
- **OAuth 2.0** (or OAuth2) - An internet standard protocol for authorisation, providing standardised flows for resource owners to authorise 3rd-party access to their resources. In the case of OIDC the resource owner is the user and the resource they are authorising with the 3rd-party (application) to access is their identity information. For more details visit <https://oauth.net/2>
- **SAML 2.0** (or SAML) - An XML-based protocol for the exchange of authentication, authorisation, and attestations securely between two entities, namely the Identity Provider and Service Provider. The standard was ratified by OASIS and for more information visit <https://wiki.oasis-open.org/security/FrontPage>
- **Identity Provider** (or IdP) - A service which maintains the identity of a subject (user) and can provide authentication of that subject to a Relying Party. The Nomidio OpenID server is the IdP.
- **Authorization Server** - The server within the OAuth2 flow which provides the Relying Party with the access token to the requested resource, usually involving authentication and approval from the Resource Owner. The Nomidio OpenID server is the Authorization Server.
- **Relying Party** (or RP) - The service (often referred to as the client) in the OAuth2 flow requesting access to the Resource Owner's resource. The enterprise website or application is the RP.
- **Service Provider** (or SP)- The service in the SAML exchange for which the user needs to be authenticated. The enterprise application is the SP.
- **User Agent** - Usually refers to the user's web browser, and sometimes the user.
- **Resource Owner** - This is the user who can authorise the resource access granted to the RP in the OAuth2 flow.
- **Resource Server** - The service which holds the resources that the RP will be able to access with the token provided by the Authorization Server. In the context of OIDC this is the user info endpoint from which the RP can get the user's profile details. The Nomidio OpenID server is the Resource Server.
- **Issuer** - In OIDC this is the IdP, but with SAML it is both the Service Provider for the SAML request and the IdP for the SAML response.
- **Audience** - The intended recipient of the authentication assertion (i.e. RP in OIDC and SP in SAML.)
- **Entity** - either the IdP or SP depending on the context.

Setting up a Nomidio OpenID Subscription

In order to use Nomidio OpenID you will need to subscribe to [the Nomidio OpenID product](#) in the AWS Marketplace and enrol your company. On subscribing to the product you will be redirected to the Nomidio OpenID onboarding portal.

Nomidio OpenID Onboarding Portal

The onboarding portal allows you to enter enterprise details and create a Nomidio administrator account for the setup and management of the Nomidio OpenID integration.

Enterprise And Connect Region Details

NomiDio
identity as a service

Nomidio OpenID | Register

Welcome to Nomidio

To complete your subscription to the Nomidio service you will now:

- Enter your company details
- Create a Nomidio administration account
- Confirm access to the administration account
- Secure your account with a password
- Configure two factor authentication for the account

You will then be ready to log in and set up Nomidio OpenID

Get started

NomiDio
identity as a service

Copyright © PQ Solutions Limited.
All rights reserved.

The first step of the onboarding process is to input the company name and select a region for your enterprise.

NomiDio
identity as a service

Nomidio OpenID | Register

Let's get started

Please enter company details to create an account

Company Name (required)

Bravo Finance

Please enter the company name you use with your customers

Please select the region where you will use Nomidio (required)

Select a region

- North America (US West)
- North America (US Midwest)
- North America (US Northeast)
- North America (US Southeast)
- North America (US Southwest)
- North America (Canada)
- Europe (Central)
- Europe (West)**
- Europe (UK & Ireland)
- Europe (East)
- Europe (Scandinavia)

Enter company details

Create admin account

Confirm email address

Set account password


Enable 2FA

NomiDio
identity as a service

Copyright © PQ Solutions Limited.
All rights reserved.

Administrator Account Creation

The next step of the process is to create a Nomidio administrator account. Upon creation of the account, a verification email, containing a one time pin, is sent to the provided email address. The account setup requires the email verification pin, setting a strong password, as well as activation of two factor authentication.


Nomidio OpenID | Register

Create Administrator Account

Please enter the administrator's details to create an account

Email address (required)

You'll need access to this email address to verify your account

First name (required)

Last name (required)

☒ I accept the [Terms of Service](#) and have read the [Services Privacy Notice](#)

[Next](#)


☒
Enter company details

☒
Create admin account


☐
Confirm email address

☐
Set account password

☐
Enable 2FA


Copyright © PQ Solutions Limited. All rights reserved.

Email Verification


Nomidio OpenID | Register

Administration email confirmation

A PIN has been sent to the administrator's email at jean.grey@bravo-finance.com

Please enter the PIN from the email (required)

[Confirm PIN](#)

Didn't get the PIN email? [Request another](#)

Entered the wrong email? If jean.grey@bravo-finance.com is the wrong email, you can [change your email](#)


☒
Enter company details

☒
Create admin account


☒
Confirm email address

☐
Set account password

☐
Enable 2FA


Copyright © PQ Solutions Limited. All rights reserved.

Administrator Password

 Nomidio OpenID | Register

Set up password

Please create a password for your Nomidio administration account. The password must have a minimum length of 8 characters and can include any typable character except a space.

Password (required)

Confirm password (required)

Save


Enter company details

Create admin account

Confirm email address

Set account password


Enable 2FA

 Copyright © PQ Solutions Limited. All rights reserved.

Two Factor Authentication

Two factor authentication (2FA) requires using a mobile authenticator app. Examples of such apps are Google Authenticator, LastPass Authenticator, Sophos Authenticator and many more.

A QR code is presented on the screen, after setting the account password. Scan the displayed QR code using the authenticator app on the user's mobile device and enter the 6-digit code generated to activate 2FA.

 Nomidio OpenID | Register


Set up 2FA (two factor authentication)

To set up 2FA you will need a mobile authenticator application of your choice.

Configure authenticator application

Scan this QR code with your authenticator application to link it with your Nomidio administration account.

Once configured, enter the code generated by your authenticator application in the next screen to complete setup.



Please enter the 6-digit code which has been generated by your authenticator application to finish setting up your account.

Authenticator code (required)

1 2 3 4 5 6

Submit

Enter company details

Create admin account

Confirm email address

Set account password

Enable 2FA

Once the administrator account is created the user is redirected to the [Nomidio Admin Service](#) where they can create the OpenID client credentials required to integrate with Nomidio OpenID authentication. The administrator should also receive a welcome email which will include a link to the Admin Service.

page 10 of 42

Identity Provider Setup

In order to use Nomidio OpenID as an Identity Provider for your enterprise websites or applications, follow the steps described by the relevant application. This will require registering your applications details in Nomidio OpenID and configuring the identity provider setting in the application.

OpenID Connect

The OpenID Connect Relying Party (client) configuration will require a client id and secret which are obtained when an OpenID Connect client is created via the Nomidio Admin Service (see [Registering an OpenID Connect Client](#).)

If the application supports OpenID Connect Discovery configuration then that can be done by providing the Nomidio discovery URL:

<https://api.aws.idp.nomidio.idaas.io/.well-known/openid-configuration>

In the case of static configuration, use the following endpoint details as required:

Authorization	https://api.aws.idp.nomidio.idaas.io/oauth/authorize
Token	https://api.aws.idp.nomidio.idaas.io/oauth/token
Issuer	https://api.aws.idp.nomidio.idaas.io
Jwks	https://api.aws.idp..nomidio.idaas.io/.well-known/jwks.json
User info	https://api.aws.idp.nomidio.idaas.io/openid/userinfo

SAML 2.0

The Nomidio OpenID SAML IdP issuer (entity id), certificate and metadata are unique per Service Provider (client) and can be obtained when creating the SAML client via the Nomidio Admin Service (see [Registering SAML Client Details](#).)

The Service Provider should be configured to use HTTP-Redirect binding for making a SAML request and the Nomidio OpenID Single Sign-On URL is:

<https://api.aws.idp.nomidio.idaas.io/saml2/sso>

The Service Provider may also require configuration of the user info attribute mappings (see [SAML Attribute Profiles](#) for more details.)

Sign in Button

The application sign in button should include the Nomidio ID logo and text should be either “Nomidio ID” or “Sign in with Nomidio ID”.

The Nomidio ID icon can be obtained from the links below:

https://marketplace.aws.nomidio.io/assets/logo/nomidio_id.png

https://marketplace.aws.nomidio.io/assets/logo/nomidio_id.svg

Nomidio OpenID Access Management

Nomidio OpenID access management is configured via the Nomidio Admin Service screen and is needed to provision Nomidio OpenID as an Identity Provider for applications which support the OpenID Connect or SAML protocol for user login and single sign-on.

Nomidio Admin Service

Nomidio Admin Service can be accessed via login at the end of account creation during onboarding or later via the link sent in the welcome email on successful registration.

The screenshot shows the Nomidio Admin Service interface. At the top, there's a header with the Nomidio logo and a navigation bar. Below the header, a banner indicates the trial status: "Your OpenID product is currently in trial mode, which will expire at midnight (UTC) at the end of January 28, 2021. There are 20 free users and 50 credits remaining. The trial will automatically be lifted after the expiry date or after all credits are used." The main content area is titled "Bravo Finance Management" and includes an "Edit" button. Below this, there are two sections: "Enterprise Code" (F24F7245-3ED5-494C-8DCE-D25776688D2E) and "Supplier Code" (NOMIDIO-QA). The "Enterprise Resources" section contains a table with "OpenID Usage Data" and "Admins" tabs. The "OpenID Usage Data" tab is active, showing a table with columns for "Type", "Dec 2020", "This Month", and "Remaining Quota". The table lists "Standard challenges", "High challenges", and "Credit" under "Challenges", and "Total users" under "Enrolments".

Type	Dec 2020	This Month	Remaining Quota
Standard challenges	0	0	----
High challenges	0	0	----
Credit			50
Enrolments			
Type	Dec 2020	This Month	Remaining Quota
Total users	0	0	20

Once logged in the administrator is able to:

- Update the enterprise name and privacy policy URL (click “Edit” button)
- Create the OpenID Connect and/or SAML clients needed for your applications
- Create and manage access groups for your users

- Assign access groups and manage security requirement for your applications
- Add, edit and disable Enterprise Admins (click Admins tab)
- View enterprise usage for the current and previous month

Enterprise Privacy Policy

A URL to enterprise's privacy policy should be added by clicking the Edit option at the top right of the enterprise screen. This is used when the user logs in via Nomidio ID and approves their data being shared with an application (see [Sign in with Nomidio OpenID.](#)) This helps provide the user with more details of how their personal data will be used by the enterprise.

The screenshot shows the Nomidio Enterprise Management interface. At the top, there's a header with the Nomidio logo and a trial notice: "Your OpenID product is currently in trial mode, which will expire at midnight (UTC) at the end of January 28, 2021. There are 20 free users and 50 credits remaining. The trial will automatically be lifted after the expiry date or after all credits are used." Below this, the "Bravo Finance Management" screen is visible. It includes fields for "Enterprise Code" (F24F7245-3ED5-494C-8DCE-D25776688D2E) and "Supplier Code" (NOMIDIO-QA). An "Edit" link is in the top right. A modal titled "Edit Enterprise" is open in the center. It has two input fields: "Enterprise Name" with the value "Bravo Finance" and "Privacy policy URL" with the value "https://bravo-finance.com/privacypolicy". Both fields have green checkmarks indicating they are valid. At the bottom of the modal are "Cancel" and "Save" buttons. In the background, the "Enterprise Resources" section is partially visible, showing a table for "OpenID Usage Data" with columns for "Type", "Dec 2020", "This Month", and "Remaining Quota". The table lists "Standard challenges", "High challenges", "Credit", and "Enrolments".

OpenID Admin Permissions

Nomidio OpenID administration is divided into two aspects, namely OpenID Connect client management and Application access management.

Note: The initial admin user created during onboarding will be granted both of these permissions.

OpenID Client Management

The OpenID Client Management permission allows the administrator to create and manage the OpenID Connect and SAML client details which are required for the application which will be using Nomidio OpenID as an Identity Provider.

OpenID Access Management

The OpenID Access Management permission allows the administrator to create and manage the access groups for applications.

Applications

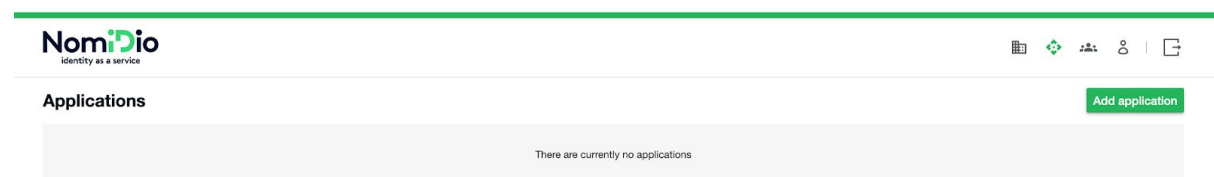
In order to create the OpenID Connect or SAML client and the access management groups for an application, an application listing needs to be created in Nomidio. An application listing can be created by an administrator with either of the OpenID management permissions. Applications are created and managed on the Application admin screen which can be accessed by clicking on the application icon in the navigation bar (top right) on the admin screen.



Note: Applications listed in Nomidio do not need to be a one-to-one list of applications using Nomidio OpenID as an Identity Provider. It could also be a single Application entry in Nomidio to represent a group of 3rd-party applications. This is to allow flexibility between minimal access management setup when using Nomidio OpenID as an Identity Provider to an existing IAM system or a more complex setup with individual application access managed using Nomido. However, it is recommended that each application is created separately as the application name is used when obtaining the user's consent to sharing their data for sign-in with their Nomidio ID.

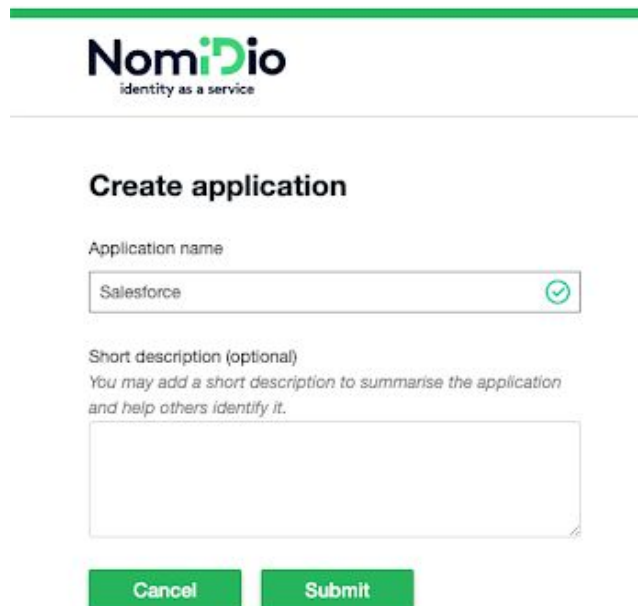
Creating an Application

To add a new application click the *Add application* button in the top right corner of the application management page.



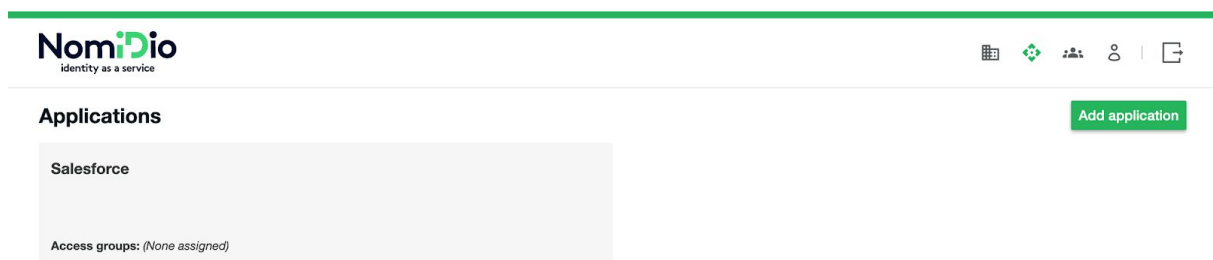
This will present the administrator with the *Create application* form (see below), which requires providing the application name and an optional description of the application. The application name will be used during the sign-in process to provide details to the user of which application their data is being shared with (see [Sign-in with Nomidio](#)

[OpenID](#)). The description is only displayed within the admin screens and can be used to help other administrators when an application entry is being used to manage access to a range of applications.



The screenshot shows the 'Create application' form in the NomiDio admin interface. At the top is the NomiDio logo and tagline. Below the title 'Create application', there is a text input field for 'Application name' containing the word 'Salesforce', followed by a green checkmark icon. Below this is a text area for 'Short description (optional)' with a placeholder text: 'You may add a short description to summarise the application and help others identify it.' At the bottom of the form are two green buttons: 'Cancel' and 'Submit'.

Once an application has been created it will appear in the list of applications in the application management screens.



The screenshot shows the 'Applications' management screen. At the top left is the NomiDio logo. To the right of the logo is a navigation bar with several icons. Below the logo, the word 'Applications' is displayed in bold. To the right of this is a green button labeled 'Add application'. Below the 'Applications' header, there is a list of applications. The first application listed is 'Salesforce'. Below the application name, it says 'Access groups: (None assigned)'.

Application Management

Managing the application is done by clicking on the application entry in the Applications list. The application page (see below) provides a number of options related to the application but different options will be available depending on the administrator's permissions.

The screenshot shows the Nomidio application management interface. At the top, there's a header with the Nomidio logo and navigation icons. Below the header, the 'Application' section is highlighted. It contains a form with two fields: 'Name' (Salesforce) and 'Description' (none). A green 'Disable application' button is visible. Below the application details, there's a tabbed interface with 'Clients', 'Access Policies', and 'Users' tabs. The 'Clients' tab is selected, and it shows 'No data to display.'

Editing the Application Details

Applications details can be updated by clicking on the *Edit* option on the right side of the application details section on the application management page. This will allow the administrator to update the application name and description, which can then be saved or cancelled by clicking the relevant option.

This screenshot shows the 'Application' details form in edit mode. The 'Name' field contains 'Salesforce' and the 'Description' field is empty. At the top right of the form, there are 'Save' and 'Cancel' buttons. A green 'Disable application' button is located at the bottom left of the form.

Disabling an application can be done by clicking the *Disable application* button. This will prevent all users from being able to login to that application using their Nomidio ID and so a confirmation popup will be displayed to verify the application should be disabled.

The screenshot shows a confirmation popup with a red exclamation mark icon. The text reads: 'Are you sure you want to disable this application?'. At the bottom, there are two buttons: a dark blue 'Cancel' button and a green 'Disable application' button.

A disabled application can be re-enabled by clicking the *Enable application* button.

Application

Name

Salesforce

Description

(none)

This application is disabled.

Enable application

Registering a Client

OAuth2 (OpenID Connect) Relying Parties and SAML Service Providers are registered with Nomidio OpenID by creating the relevant client in the application management screen. From the application page, an administrator with the *OpenID Client Management* permission, will be able to create the OpenID Connect or SAML client required to configure the application's identity provider. This is done by clicking the + button on the Clients tab. This will load the *Create Client* page where the administrator selects what type of client they would like to create (see below for more details on the creation of the two types of clients.)

Create a Client

1

2

3

Choose Type

Setup Client

Complete Setup

Please select a client type from the list below create.

OAuth2 (OpenID Connect)

☒

SAML 2

☐

Cancel


Create

Create OpenID Connect Client

After selecting the OAuth2 client type the administrator is taken to the Setup Client step, where client's signature algorithm, scopes, and redirect URIs are entered and submitted to create the client.

Note: with some integrations the application may require the client details before providing the redirect URI, in which case the redirect URI does not need to be added in this step and can be done in the Complete Setup step.

Create a Client



The diagram shows a three-step process for creating a client. Step 1, 'Choose Type', is highlighted with a green circle. Step 2, 'Setup Client', is also highlighted with a green circle. Step 3, 'Complete Setup', is shown with a grey circle. The steps are connected by a horizontal line.

Algorithm

ES512

Scopes

OpenId ☒

Profile ☒

Email ☒

Redirect URIs

https://bravo-finance.my.salesforce.com/services/auth/sso/nomidio ☒

https://...

Return **Submit**

Signature Algorithm

The cryptographic algorithm which Nomidio will use when signing the `id_token` for the application (see [OpenID Connect Core 1.0 section 2](#) for more details). Nomidio recommends the use of ES512 where possible. However, not all applications will support this algorithm, in which case RS256 should be used.

Note: details of what algorithms are supported may not be included in the application's documentation but clients which comply with the OpenID Connect standard should support RS256, and so when unsure, or if a client setup with ES512 returns an error, then client registration can be updated to use RS256.

Scopes

Scopes are used to limit what user data can be requested by the client. The `openid` scope is required for OpenID Connect integrations but if using Nomidio ID with just standard OAuth 2.0 sign-in flow then this scope is not needed. The `profile` scope will allow the client to request the user's first and last name, while the `email` scope will allow the client to request the user's email address. For more information about scopes and the associated claims see [OpenID Connect Core 1.0 section 5.4](#).


Redirect URIs

The redirect URI which the application uses will need to be provided. Details of this will likely be found in the application's documentation for OpenID Connect Identity Provider setup or may be created by the application after the client details have been provided. The URI can be left as blank when creating a client and then updated later for the case where the application only provides the redirect URIs after client details are added. Multiple redirect URI can be added to a client but this will depend on the application requirements.

Client ID and Secret

After submitting the data in step 2, the client id and client secret will be created and presented in the Complete Setup step. They can be copied to the clipboard for pasting in the application's setup screens or downloaded in a CSV file to be saved by the administrator.

Create a Client



The diagram shows a three-step process for creating a client. Step 1 is 'Choose Type', Step 2 is 'Setup Client', and Step 3 is 'Complete Setup'. Each step is represented by a green circle with a white number inside, connected by a horizontal line.

Client ID

81e311a9-a2c0-4ea9-9385-40e84234c078 **Copy**

Client Secret [Show Secret](#)

..... **Copy**

Download CSV file **Done**

Note: after clicking on the Done button the client secret can no longer be viewed and a new secret will need to be created (which can be done at any time via the Edit OpenID client screen.)

Create SAML Client

For SAML integrations select the SAML 2 client type in the step 1. The Service Provider details, attribute profile and signature algorithm can then be set in the Setup Client step. Along with the Service Provider Entity ID and Assertion Consumer Service URL (ACS).

Note: if the Entity ID and ACS URL are only generated by the Service Provider after providing the IdP details then these can be skipped in step 2 to be added in step 3.

Create a Client

1

2

3

Choose Type

Setup Client

Complete Setup

Algorithm

RS256

SAML Name Identifier Format

Persistent Unique Identifier

Attribute Profile

Basic

Service Provider Entity ID

Assertion Consumer Service URL

https://...

Service Provider's Signing Certificate

-----BEGIN CERTIFICATE-----
...

Upload from File

Return

Submit

SAML Name Identifier Format

This refers to the type of identifier used as the NameID of the SAML Subject (i.e. the identifier of the authenticated user). For more details about SAML Name Identifier see Section 8.3 in the [SAML 2.0 Core](#) Specifications.

It is highly recommended to use the “Persistent Unique Identifier” which will be the user’s unique Nomidio UUID for the given enterprise and has the SAML NameIDType of `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.

Some Service Provider may require the NameID to be the user’s email address, this can be done by selecting “Email” as the Name Identifier Format will set the Subject NameID of the SAML attestation to the user’s email address with NameIDType `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.

Attribute Profile

The attribute profile determines what naming convention is used for the user attributes in the SAML authentication response. For more details about SAML Attribute Profiles see Section 8 of the [SAML 2.0 Profiles](#) Specification. The options are “Basic” and “LDAP” which correspond to the SAML 2.0 attribute profiles in sections 8.1 and 8.2 respectively. The third option “SOAP” is not in the specifications but uses the XML Schema URIs for the attribute names, which are used by a number of Service Providers.

Basic

User Attribute	SAML Attribute Name
User Id	uid
Common Name	cn
First Name	givenName
Last Name	surname
Email Address	email

LDAP

User Attribute	SAML Attribute Name
User Id	urn:oid:0.9.2342.19200300.100.1.1
Common Name	urn:oid:2.5.4.3
First Name	urn:oid:2.5.4.42
Last Name	urn:oid:2.5.4.4
Email Address	urn:oid:1.2.840.113549.1.9.1

SOAP

User Attribute	SAML Attribute Name
User Id	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
Common Name	http://schemas.xmlsoap.org/claims/CommonName
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Email Address	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Service Provider Entity ID

This is the Service Provider URI which is used as the issuer of the SAML request coming from the SP to the IdP and will be used as the Audience URI in the SAML response sent from the IdP to the SP. This information should be provided by the application the client is being configured for. In some cases the application may only generate the SP entity ID after the necessary data from the IdP has been provided, thus this field can be left empty when creating the client but will need to be added before the client can be set to active.

Assertion Consumer Service URL

The Assertion Consumer Service (ACS) URL is the Service Provider endpoint to which the SAML authentication response must be sent. The client can list multiple ACS URLs as any response will always be sent to the URL designated in the request (which will need to be one of the registered ACS endpoints.) As with SP entity ID this can be left empty on creation for case that SP only provides URL after IdP details are set.

Service Provider's Signing Certificate

It is recommended that the SAML request is signed if supported by the Service Provider, in which case the SP X.509 certificate (in PEM format) should be uploaded. Either by pasting the certificate data in the place provided or using the "Upload from File" button.

Signature Algorithm

The cryptographic algorithm which Nomidio will use when signing the SAML assertion and response. Nomidio recommends the use of ES512 where possible. However, not all applications will support this algorithm, in which case RS256 should be used.

Note: The IdP certificate is needed to verify a signature, thus a new IdP certificate will be generated if the signature algorithm is changed.

IdP Entity Id, Certificate and Metadata

Once the Setup Client step has been submitted, the necessary data for the Service Provider configuration will be generated and displayed. Nomidio OpenID uses a different

certificate for each Service Provider and thus has a unique IdP Entity ID and metadata URL per client. If the Service Provider supports configuration via metadata, it can either be downloaded or the URL copied depending on SP requirements.

For manual setup requiring the IdP Entity ID, this is the same as the metadata URL and thus the copied metadata URL can be used. The Service Provider setup will also require the IdP certificate (which can be copied or downloaded) or its fingerprint, which can be generated with the necessary hashing algorithm.

Create a Client

1

Choose Type

2

Setup Client

3

Complete Setup

IdP Entity ID [Copy Metadata URL](#)

https://api.aws.idp.qa.nomidio.io/saml2/metadata

Download Metadata

IdP Certificate [Copy Certificate](#)

```
-----BEGIN CERTIFICATE-----
MIIFJDCCAwygAwIBAgIUeiZTa9NTDPkQzg7YF8Qw4XOyR1MwDQYJKoZIhvcNAQEL
BQAwHjEcmBoGA1UEAwTcWEubm9taWRpby5pZGFhcy5pbzAeFw0yMTAxMjAw
MDAwMDAwMDBaFw0yMzAxMjAwMDAwMDBaMB4xHDAaBgNVBAMME3FhLm5vbWlkaW8ua
-----END CERTIFICATE-----
```

Download Certificate

Certificate Fingerprint [Copy Fingerprint](#)

A0:94:3C:B5:CA:0B:68:59:17:D2:80:74:57:0A

SHA-256

Service Provider Entity ID

https://www.okta.com/saml2/service-provider/spbaofkqivdgydlbyimr
✓

Assertion Consumer Service URL


https://nomidio-6115170.okta.com/sso/saml2/0aa405dlyZDdLvi8y5d6
✓

Skip

Activate

In the case that the Service Provider ID and/or ACS URL were not provided in step 2, they can be added in step 3 in order to activate the client.

To view this data again select the client from the SAML client list to download or copy the necessary IdP data.



Nomidio
Identity as a service

[Grid](#) |
 [Settings](#) |
 [Users](#) |
 [Groups](#) |
 [Logout](#)

SAML Client Details Edit

Client Status
ACTIVE
Algorithm
RS256
SAML Name Identifier Format
UID
Attribute Profile
BASIC
Service Provider Entity ID
https://www.okta.com/saml2/service-provider/shdbofkqvdydlbyimr
Assertion Consumer Service URI
<ul style="list-style-type: none"> https://nomidio-6115170.okta.com/sso/saml2/0oa405dlyZDD...

Disable Client

Identity Provider Details

IdP Entity ID Copy Metadata URL

Download Metadata

```
https://api.aws.idp.qa.nomidio.io/saml2/metadata/6d3f8823-46f5-432e-82a0-f135da11f374
```

IdP Certificate Copy Certificate

Download Certificate

```
-----BEGIN CERTIFICATE-----
MIIFJDCCAwgAwIBAgIUZo8O3Y2kW3qGXJxOVtHK7xlf2
wwDQYJKoZIhvcNAQEL
BQAQHjEcmBoGA1UEAwwTcWUubm9taWRpbypzGZFhcys
pbXAeFw0yMTAxMjAwMDAwMDBaMB4xHDAaBgNVBAMM
E3FhlLm5vbWikaW8uaWRlRnYXMu
aW8wgglMAAGCSqGSIb3DQEBAQUAA4ICDwAwggIKApIC
AQQCNgq+kGZVFLZGWVTtz
```

Certificate Fingerprint Copy Fingerprint

SHA-256 ▾

```
86:75:C4:96:9E:EF:72:6E:C0:14:58:FF:2A:DA:8A:60:60:29:2D:...
```

Editing Client Details

The client details can be accessed by clicking on the entry in the Clients list, which will display the View Client Details screen. To edit the client details click on the “Edit” button within the View Client screen which will then allow the relevant client details to be updated.

Application Access Policies

The access policies on the application screen can only be viewed and edited by an administrator with the OpenID Access Management permission, and requires access groups to have been created via the Access Groups admin screen (see [Nomidio OpenID Access Groups](#) for more details.)

Adding an Application Access Policy

In order to add an access policy to the application click the (“+”) button on the Access Policies tab. This will present the *Add access policy* dialog (see below) where the administrator can select the relevant Access group and set the access policy *Authentication level* of the application for the selected group. The Authentication level determines what checks will be performed to authenticate the user when they login using Nomidio OpenID (see [Authentication Level](#) for more details.)

Add access policy

Authentication level

☐ Standard
☒ High

Access Group

Sales Team ▼

Cancel

Submit

Nomidio OpenID Access Groups

In order to be able to sign-in to an application using Nomidio OpenID, a user needs to be approved by the enterprise. This is done via Access Groups, which are setup via the Nomidio Admin service using the Access Groups management screens. These screens require the administrator to have the *OpenID Access Management* permission and can be found by clicking the Access Groups icon in the navigation bar (top right.)



Adding an Access Group

To add a new Access Group click the *Create a group* button in the Access Groups management screens.

NomiDio
identity as a service

Access Group Management

Active registration links

Share existing link

Create registration link

0 out of 5 registration links active.

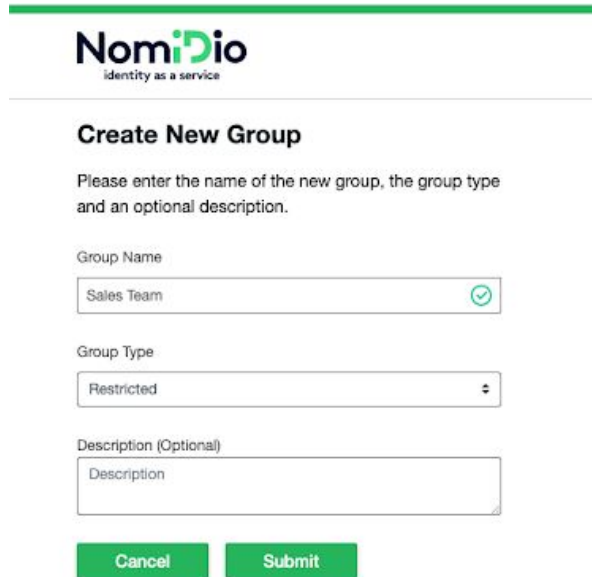
Code	Expires on
No active registration links	

Access Groups

Create a group

There are currently no groups

This will display the *Create New Group* screen (see below) which requires setting the group name and type, as well as an optional description of the group.



NomiDio
identity as a service

Create New Group

Please enter the name of the new group, the group type and an optional description.

Group Name
 ✓

Group Type

Description (Optional)

Group Types

An access group is not a fixed group of users but rather a set of rules which get applied to determine if a user is allowed. This is done based on the group type and a set of access rules (see [Access Rules](#)) added to the group.

Anyone

The *Anyone* group type will allow any user to login to an application associated with the group. Specific users or domains can be excluded from an *Anyone* group by adding the relevant exclusion rule.

Enrolled

The *Enrolled* group type is only applicable to enterprises which also use the [Nomidio IDaaS product](#), and will allow access to users that have been enrolled with the enterprise via Nomidio IDaaS.

Note: Exclusion rules can be added to the *Enrolled* group, but this exclusion would only apply to the user's access to Nomidio OpenID and it does not change their IDaaS user status.

Restricted

The *Restricted* group type determines user access based on the group's access rules.

Blocked

The *Blocked* group type is used to prevent user access to an application.

Note: this is different from adding an exclusion rule in another group type, as the exclusion rule only applies to the given group and so in the case that multiple groups are linked to a given application and a user is excluded from one group but included in another, then that user would have access to the application. This is where the Blocked group can be used as it will override a user's access from all other access groups linked to the application.

Access Rules

Access rules are added to a group by selecting the group from the Access Groups screen.

NomiDio
identity as a service

Access Group Management

Active registration links

0 out of 5 registration links active.

Share existing link Create registration link

Code	Expires on
No active registration links	

Access Groups

Salesteam
Type: Restricted

Create a group

And then clicking on the add (“+”) button in the *Rules* section on the Access Group page.

NomiDio
identity as a service

Access Groups

Type: Restricted

Group Name
Sales Team

Description (optional)
(none)

Rules Access Policies Users

Type	Email/Domain
No data to display.	

+

Rule Types

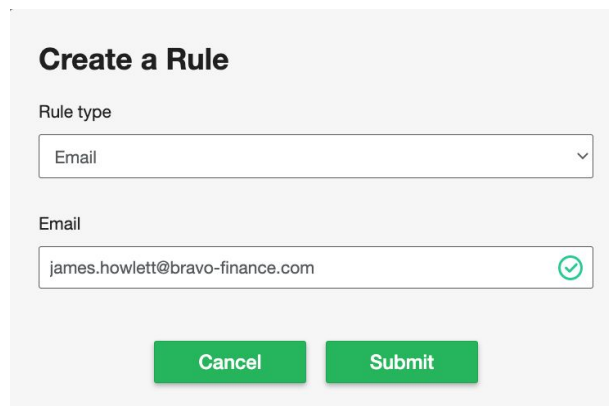
An access rule has one of the following three types:

- Email - this allows the user access based on the exact email address
- Domain - this allows the user access based on the user's email domain
- Exclusion - this can be either an individual email address or an email domain and will exclude the user if their email address matches

Note: the *Email* and *Domain* rule types only apply to the *Restricted* group type whereas the *Exclusion* rule type can be added to any group type. The *Blocked* group type uses the *Exclusion* rule type to block the given email address or domain. i.e. the *Exclusion* rule in the *Blocked* group gets applied as an exclusion from all groups linked to the application.

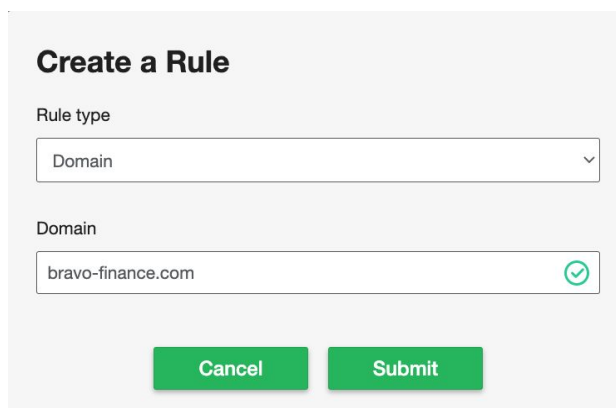
Adding an Access Rule

After clicking the add rule button the *Create a Rule* dialog (see below) will be displayed, where the rule type needs to be selected and the appropriate valid rule value (email address or domain) is entered.



The 'Create a Rule' dialog shows the 'Rule type' dropdown set to 'Email'. The 'Email' input field contains 'james.howlett@bravo-finance.com' and has a green checkmark icon on the right. At the bottom are 'Cancel' and 'Submit' buttons.

For the email domain rule this must not include the "@" symbol.



The 'Create a Rule' dialog shows the 'Rule type' dropdown set to 'Domain'. The 'Domain' input field contains 'bravo-finance.com' and has a green checkmark icon on the right. At the bottom are 'Cancel' and 'Submit' buttons.

Assigning Applications to an Access Group

An Access Group can be applied to an Application either by adding the Access policy via the Application page, or by connecting the Application to the Access Group on the Access Group page. For the latter click on the add (“+”) button in the Access Policies tab on the Access Group page. This will display the Add access policy dialog box (see below), where the administrator can select the desired Application and appropriate Type (see [Authentication Level](#)) and click the Submit button.

Add access policy

Authentication level

☐ Standard
 ☒ High

Application

Salesforce

Cancel
Submit

The Access Policies and Rules section should appear in the relevant sections on the Access Group page, and can be removed by clicking the delete icon at the right.

Access Groups

Type: Restricted

Edit

Group Name

Salesteam

Description (optional)

(none)

Rules

Access Policies

Users

Application

Authentication Level

Last Modified At

Salesforce

HIGH

20 January 2021, 2:29 PM

<<

Page 1 of 1 (1 elements total)

>>

Managing Application Access

As described in the previous section, access is managed by associating Applications and Access Groups. This can be done either from the Application page or the Access Group and is an n-to-n relationship. i.e. an Access Group can be assigned to multiple Applications and an Application can be connected to multiple Access Groups.

Authentication Level

When an *Access Group* and an *Application* are linked the Authentication level for that assignment will be set. This determines what check a user who matches the access group rules will need to pass in order to access the given application, and can be either Standard or High.

Standard Security Authentication

Standard security includes a device key and voice biometric authentication.

Note: The device key is the private key of a key pair generated by the user's device during registration. While the public key of this key-pair is stored in the user's Nomidio account, the private key however never leaves the device. When the user attempts to login from a device without a private key, either having cleared the device storage, or login from another device, then they will need to do a key recovery in order to create (and store) a new key pair (see [Key Recovery Login](#)).

High Security Authentication

High security includes the device key and voice biometric authentication, as per standard, as well as a face biometric authentication.

Multiple Access Groups

The Authentication Level is set per *Application* and *Access Group* link. This allows setting a different authentication level per application for a given group, as well as a different level per *Access Group* for a given application. When a user is included in multiple access groups that are associated with an application at different levels (High and Standard) the user will be required to perform the High security authentication.

Creating a Nomidio ID

In order for users to access an application using Nomidio OpenID, the user will require a Nomidio ID account with a verified email address that matches the application access rules. Users who are within an application access group will be able to complete the registration via the Nomidio ID web application when they first attempt to login using Nomidio OpenID, or via a registration link which can be sent to them in an email.

Note: users can also be registered if invited by an enterprise using the Nomidio IDaaS product.

Nomidio ID Registration Link

A Nomidio ID registration link has a unique code which will allow users to register for the given enterprise.

Note: registration links will only work if the user registers with an email address which is approved for an application. i.e. must be included in an access group which has been linked to an application.

Create Registration Link

Registration links are created via the Group Management page by clicking on the *Create Registration link* button.

The screenshot shows the 'Access Group Management' page in the Nomidio interface. At the top, there's a header with the Nomidio logo and navigation icons. Below the header, the page title 'Access Group Management' is displayed. Underneath, there's a section for 'Active registration links' with two buttons: 'Share existing link' and 'Create registration link'. A message indicates '1 out of 5 registration links active.' Below this is a table with two columns: 'Code' and 'Expires on'. The table contains one entry with the code 'MVXvo1cd' and an expiration date of '6 March 2021, 11:59 PM'. To the right of the table are icons for navigation and deletion. Below the table is a section for 'Access Groups' with a 'Create a group' button. A single group named 'Salesteam' is listed with the type 'Restricted'.

Code	Expires on
MVXvo1cd	6 March 2021, 11:59 PM

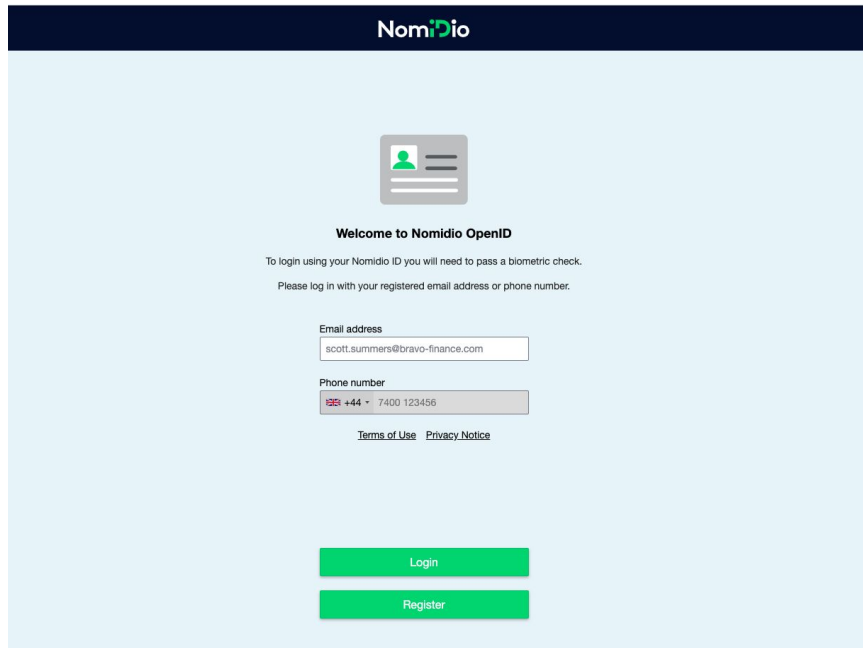
Access Groups
Salesteam Type: Restricted

Share Registration Link

Clicking on the registration code will display the relevant URL with the option to copy, if the administrator wants to share the link themselves, alternatively by clicking the *Share existing link* button the administrator can provide a list of email addresses and Nomidio will send an email containing the link.

Registration on Login

When a user without a Nomidio ID account is redirected to Nomidio OpenID for the first time on attempting to login to an application, their device will not be recognised and they will be presented with a Welcome screen (see below) allowing them to create an account by clicking the 'Register' button.

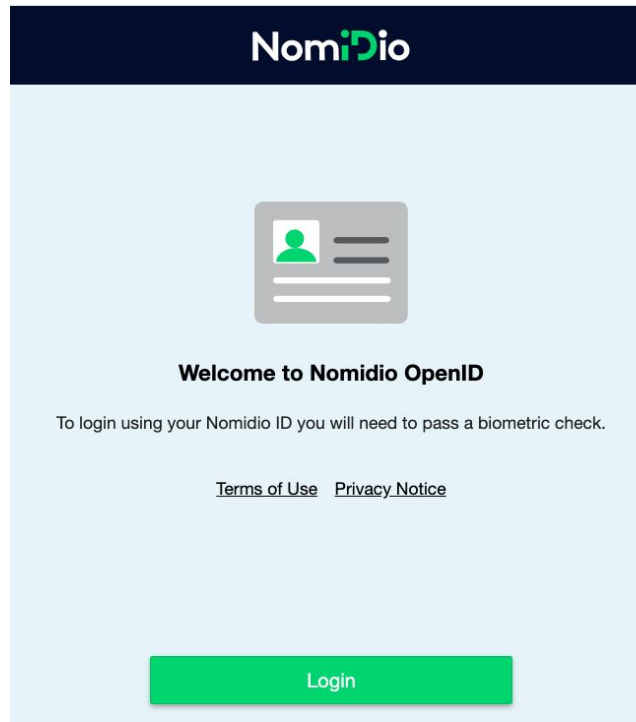


For further information on the registration process see the appendix [Nomidio Account Registration](#).

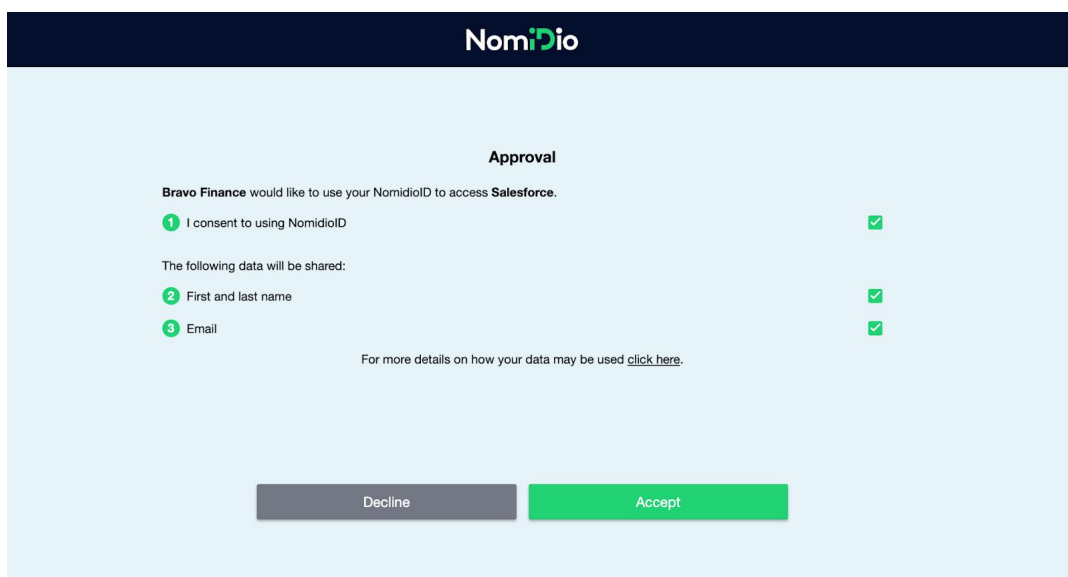
Note: when a user who is already registered attempts to login with Nomidio ID on a new device (i.e. without their device private key), they will also be presented with the same Welcome screen from which they can enter their email address and click the Login button to recover their device key (see appendix [Key Recovery Login](#)) and complete authentication.

Sign in with Nomidio OpenID

Once a new user has registered for a Nomidio ID account they can login to an application using Nomidio OpenID, and will be redirected to the Welcome page (see below). They will only need to click on the 'Login' button, without any need for a username or password, and complete their login using the necessary biometric checks based on the required authentication level for their access group associated with the application. i.e. voice for Standard and both voice and face for High.



After completing the biometric checks on the first login to an application, the user will be prompted to approve the use of their Nomidio ID and consent to any data sharing that has been requested by the application. The approval screen will include the enterprise name and the name of the *Application* that was created via the Nomidio Admin screens. It will also provide a link to the enterprise's privacy policy.



Single Sign-On with Nomidio OpenID

Once a Nomidio ID user has successfully authenticated themselves to login to an enterprise's application, the device will retain an authentication session for 24 hours allowing the user to be automatically logged in to other enterprise applications using Nomidio OpenID as an enterprise SSO. This does not apply if the user authentication level of the initial login was Standard and the user then attempts to access an application requiring High authentication. In this case the user will need to be re-authenticated with a High security check.

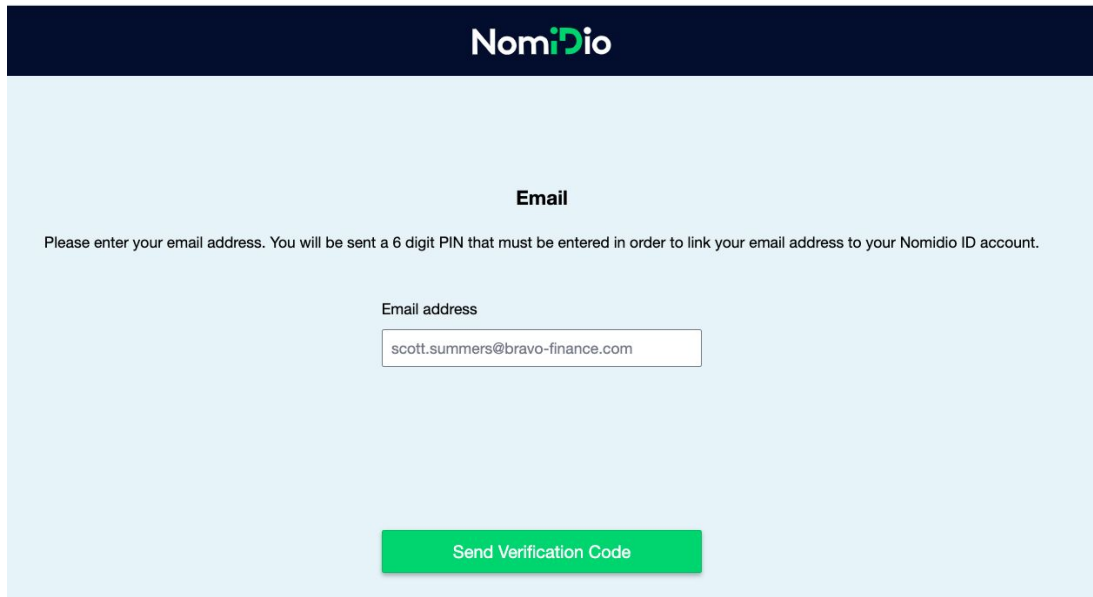
Appendices

Nomidio ID Account Registration

Having selected to Register from the Nomido OpenID Welcome page, the user will be taken through account registration, starting with accepting the Nomidio Terms of Use and Privacy Notice documents.

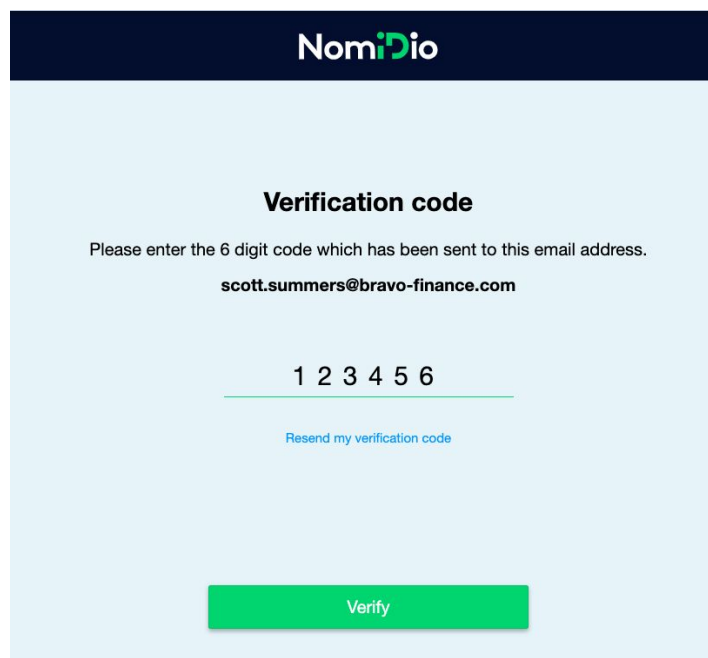
The screenshot shows a web interface for Nomidio. At the top is a dark blue header with the 'Nomidio' logo. Below the header, the main content area has a light blue background. The title 'We need your consent' is centered. Below the title, there is a paragraph explaining that to create a Nomidio ID, personal information (name, email, biometric data) will be collected and used for verification. It also states that biometric data will not be shared unless required by law. A second paragraph mentions that once a phone number is linked, an SMS message will be sent for a face check. A third paragraph states that consent can be withdrawn at any time. Below this, a section titled 'You need to agree to the following:' lists three items, each with a green checkmark to its right: 1. 'I consent to my personal information being used to create my Nomidio ID.' 2. 'I confirm that I have reviewed and accept the Terms of Use.' with a link to 'Terms of Use' below it. 3. 'I confirm that I have reviewed the Privacy Notice.' with a link to 'Privacy Notice' below it. At the bottom of the form are two buttons: 'Decline' (grey) and 'Accept' (green).

Next step of the registration process is to verify the user's email address and phone number. No personal or biometric data will be gathered unless the user is able to verify their email address, which is approved for use via the applications access groups.



The screenshot shows the 'Email' verification screen. At the top is a dark blue header with the 'NomiDio' logo. Below the header, the title 'Email' is centered. A message states: 'Please enter your email address. You will be sent a 6 digit PIN that must be entered in order to link your email address to your Nomidio ID account.' Below this is a text input field labeled 'Email address' containing the email 'scott.summers@bravo-finance.com'. At the bottom is a green button labeled 'Send Verification Code'.

Clicking on the 'Send Verification Code' button requests an email containing verification code to be sent to the provided email address, which will need to be entered on the next screen.



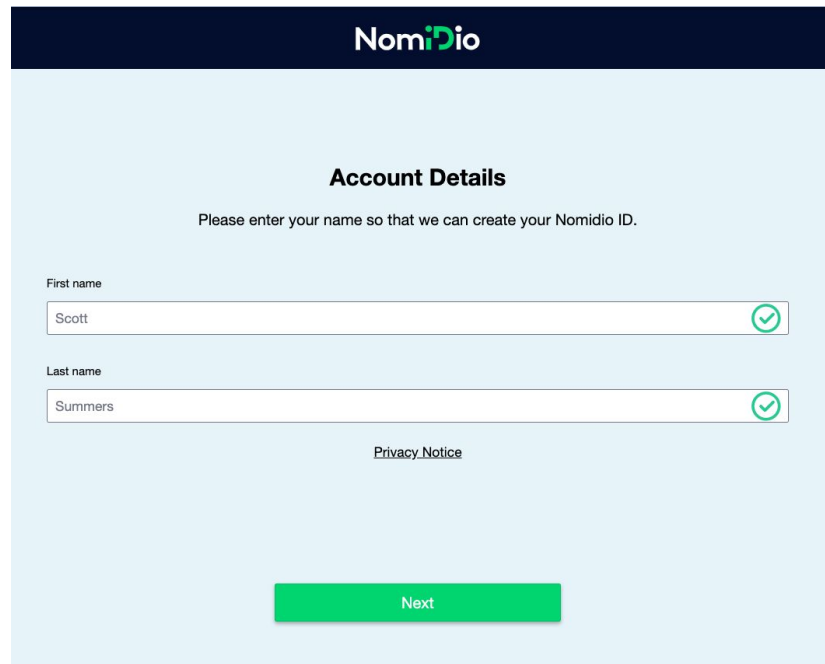
The screenshot shows the 'Verification code' screen. At the top is a dark blue header with the 'NomiDio' logo. Below the header, the title 'Verification code' is centered. A message states: 'Please enter the 6 digit code which has been sent to this email address.' Below this is the email address 'scott.summers@bravo-finance.com'. Underneath is a row of six input fields, each with a number (1 through 6) above it. Below the input fields is a blue link that says 'Resend my verification code'. At the bottom is a green button labeled 'Verify'.

Once their email is successfully verified, the user is required to verify their mobile phone number.

The screenshot shows the NomiDio 'Phone Number' verification screen. At the top is the NomiDio logo. Below it, the title 'Phone Number' is centered. A message states: 'Please enter your mobile number. You will be sent a 6 digit PIN that must be entered in order to link your phone number to your account.' There is a text input field labeled 'Phone number' containing a dropdown menu with a UK flag and '+44', followed by the number '7401234567'. At the bottom is a green button labeled 'Send Verification Code'.

Pressing 'Send Verification Code' button requests an SMS text message containing the verification code to be sent to the user's mobile number, which will also then need to be entered to complete the verification.

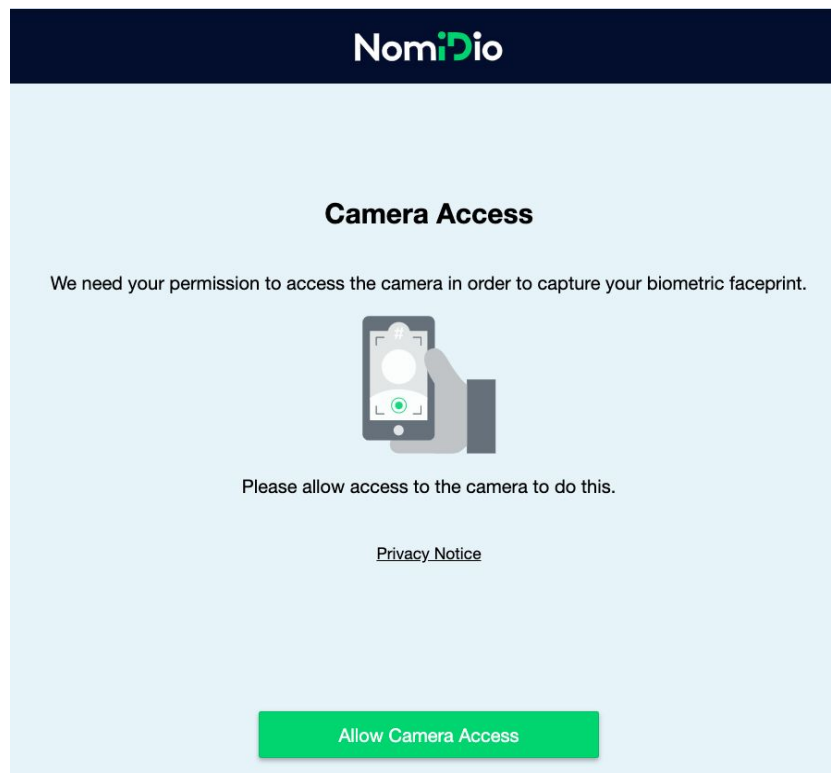
The screenshot shows the NomiDio 'Phone verification code' screen. At the top is the NomiDio logo. Below it, the title 'Phone verification code' is centered. A message states: 'Please enter the 6 digit code which has been texted to this phone number.' Below this, the phone number '+447401234567' is displayed. Underneath the number, the digits '7 7 9 1 8 3' are shown in a large font, with a green underline beneath them. Below the digits is a blue link that says 'Resend my verification code'. At the bottom is a green button labeled 'Verify'.



The screenshot shows the 'Account Details' registration screen. At the top is a dark blue header with the 'NomiDio' logo. Below the header, the title 'Account Details' is centered. A message states: 'Please enter your name so that we can create your Nomidio ID.' There are two input fields: 'First name' with the value 'Scott' and 'Last name' with the value 'Summers'. Both fields have a green checkmark icon to their right. Below the fields is a link for 'Privacy Notice'. At the bottom is a green button labeled 'Next'.

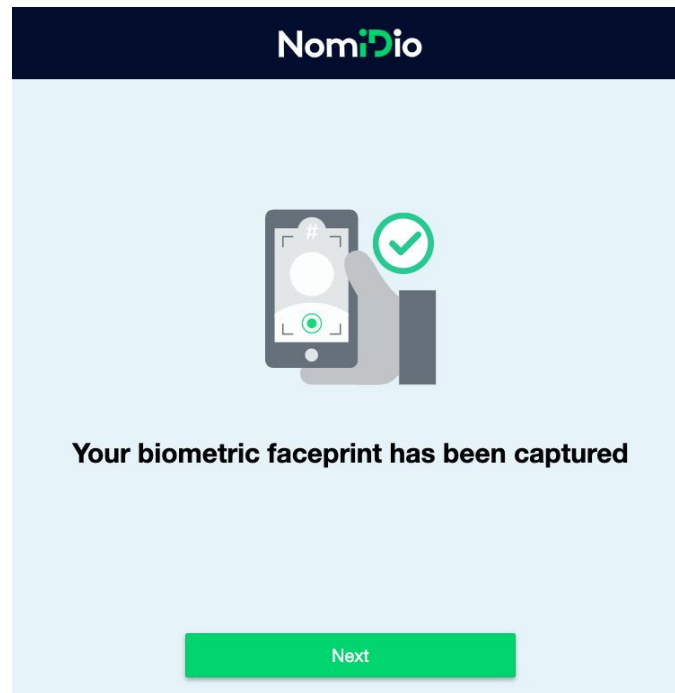
With the user's email address and phone number both verified they will then be able to complete the registration by providing their name and registering their biometrics.

The first biometric data to be captured will be the user's faceprint. To proceed, the user is required to allow camera access permission.

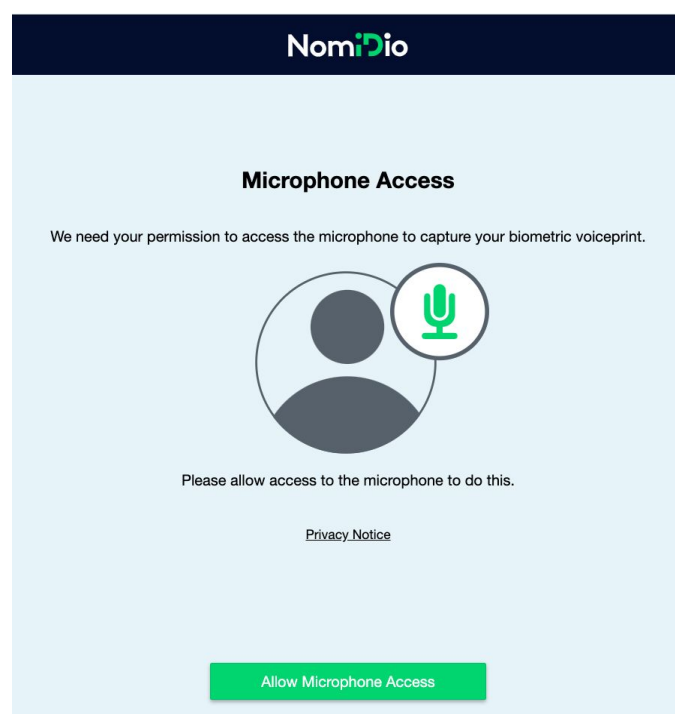


The screenshot shows the 'Camera Access' screen. At the top is a dark blue header with the 'NomiDio' logo. Below the header, the title 'Camera Access' is centered. A message states: 'We need your permission to access the camera in order to capture your biometric faceprint.' Below the message is an illustration of a hand holding a smartphone with a camera icon on the screen. Below the illustration is the text: 'Please allow access to the camera to do this.' Below this text is a link for 'Privacy Notice'. At the bottom is a green button labeled 'Allow Camera Access'.

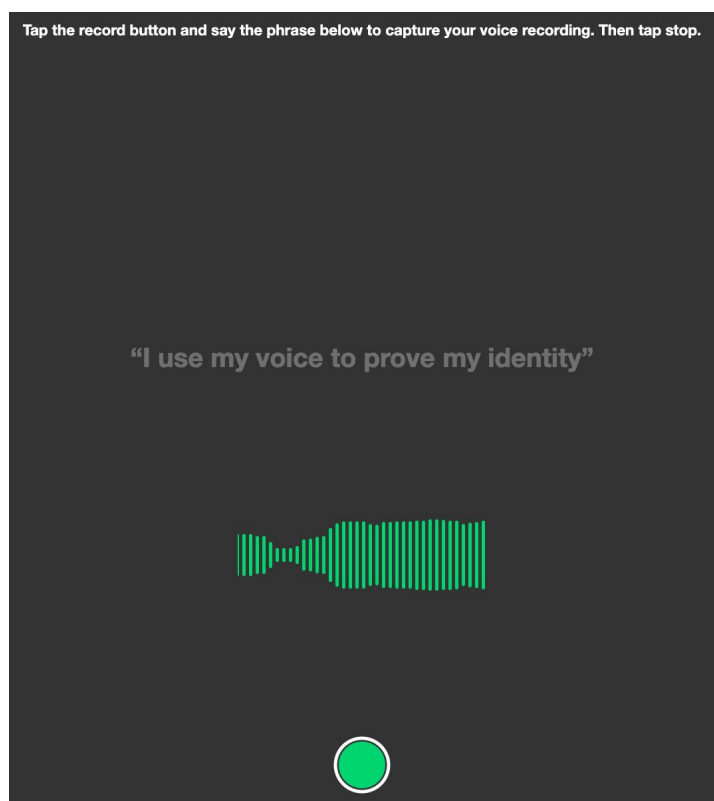
After following the instruction in the web application to complete the faceprint registration



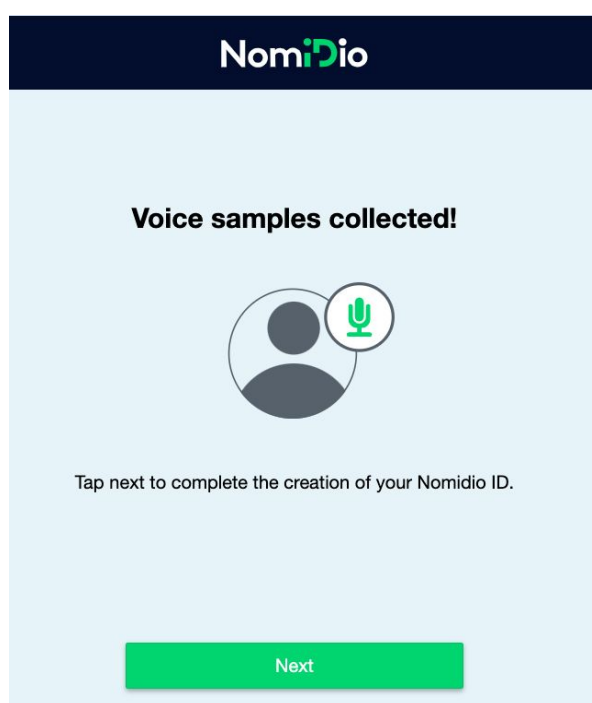
To proceed with capturing the voiceprint, the user is required to allow microphone access permission.



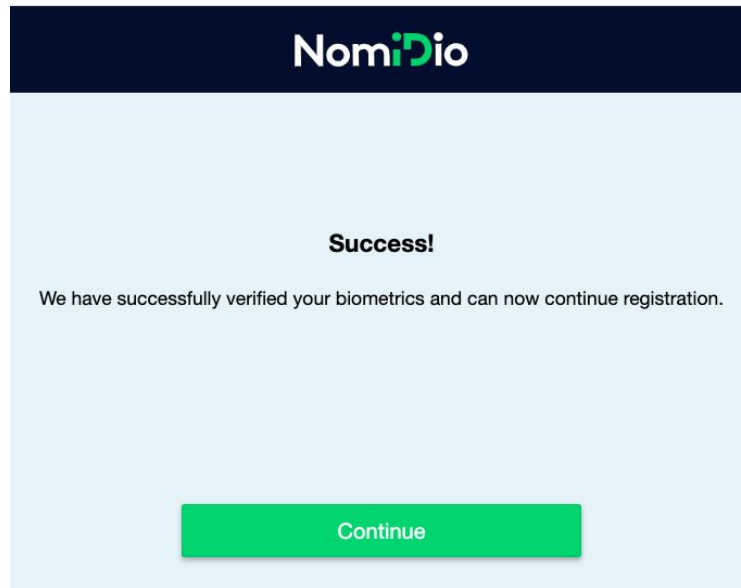
Users are requested to provide voice samples by recording a phrase displayed on screen.



Once all required voice samples are collected, users can proceed with the registration process.



At this point, users are required to verify their biometric samples by providing additional face and voice samples.



The final step of the process allows users to verify their details and complete the registration.

A screenshot of a web interface with a dark blue header containing the 'NomiDio' logo. The main content area is light blue and features a grey icon of a person's head and shoulders. Below the icon, the heading 'Verify Personal Data' is displayed in bold. The form contains three input fields, each with a green checkmark on the right side. The first field contains 'Scott Summers' and has an 'Edit' link to its right. The second field contains '+447401234567'. The third field contains 'scott.summers@bravo-finance.com'. At the bottom center, there is a green rectangular button with the text 'Submit' in white.

Key Recovery Login

When a registered Nomidio ID user attempts to login to an application using Nomidio OpenID on a new device (or after clearing the browser data on an existing device), they will need to create a new device private key as well as recover their encryption keys which are used to secure their PII data stored in the Nomidio PII cloud. This is mostly hidden from the user in order to provide them with a simple user experience but is achieved by using a number of quorum key fragments which were created for the user during registration. Unlocking these fragments requires the user to pass an email multi-factor authentication (MFA) check as well as both voice and face biometric checks.

Thus when a user attempts to login on the unknown device they will need to enter their email address (or phone number) which will trigger the email MFA to be sent to the registered user, and after entering the sent MFA code the user will continue with the biometric check as per a High security authentication.