



Identity-as-a-Service

Nomidio Connect Quick Start Guide

Version 1.6

Versions

Version	Authors	Approved	Date	Notes
1.0	tc, aks, mj	mj, pb, cjt	22 April 2020	Initial version
1.1	tc, aks, mj	mj	19 May 2020	Softphone high challenge
1.2	tc	mj	16 July 2020	Update architecture diagrams and images
1.3	tc, sa	aks, mj	13 August 2020	Chat/Lex integration
1.4	tc	mj	1 September 2020	Add new Contact Attribute Outputs
1.5	tc, aks	mj	21 October 2020	New webchat authentication and agent quick connects
1.6	tc	aks	20 January 2021	Auto deployment of Connect Contact Flows

Contents

Versions	2
Contents	3
About this Guide	4
Overview	4
Prerequisites	5
Architectural Overview	5
What is Covered	6
Setting up a Nomidio Connect Subscription	8
Nomidio Connect Onboarding Portal	8
Enterprise And Connect Region Details	9
Administrator Account Creation	10
Email Verification	10
Administrator Password	11
Two Factor Authentication	11
Nomidio Admin Service	12
Creating Nomidio Connect Credentials	13
Installing Nomidio Connect Resources	14
CloudFormation	14
AWS Resources	14
Parameters	16
Executing the CloudFormation Template	18
Updating the CloudFormation Stack	18
Configuring the Amazon Connect Contact Centre	19
Enable Live Media Streaming	19
Add Lex bots	19
Manually Importing Custom Amazon Connect Contact Flows	19
Manual Amazon Connect Flow Import	20
Configure Agent Challenge Quick Connect	21
Assigning a Phone Number	21
Testing the Contact Flow	22
Customising the Contact Flows	22
Customising the Customer Experience prior to Nomidio Authentication	22
Contact Attribute Inputs	22
Customising the User Experience after Nomidio Authentication	23

Contact Attribute Outputs	23
Accessing and using the Standalone Softphone	24
Whitelisting the Standalone Softphone	24
Accessing the Softphone	24
Using the Softphone	24
User Enrolment	24
Agent Requested Challenge	25
Blocking User	26
Setting Fraud Flag	27
Definition of Terms	28
Challenge Authentication Level	28
Challenge Status	28
Nomidio Status	29
No Authentication	29
Authenticated	29
Fraud Flag Status	30
Appendices	30
Appendix A	30

About this Guide

This implementation guide discusses the architecture, setup and configuration steps required to successfully deploy the Nomidio integration for Amazon Connect.

This guide is intended for customers interested in installing and configuring the Nomidio integration for Amazon Connect.

Overview

The Nomidio integration for Amazon Connect provides a seamless integration between Amazon Connect contact centres and the Nomidio identity platform. The integration manages the entire lifecycle of users from initial on-boarding and registration through to ensuring data compliance and managing the user opt-out process. It also allows for custom contact handling based on authentication results and the ability to extend your existing contact flows with authentication. The authentication process happens prior to connecting to an agent, reducing agent contact time and streamlining the security process.

The integration uses lambda functions that consume the customer's audio samples in real time during the authentication process and validate the authenticity of the inbound user. This result is available to your contact flow, allowing for intelligent contact routing.

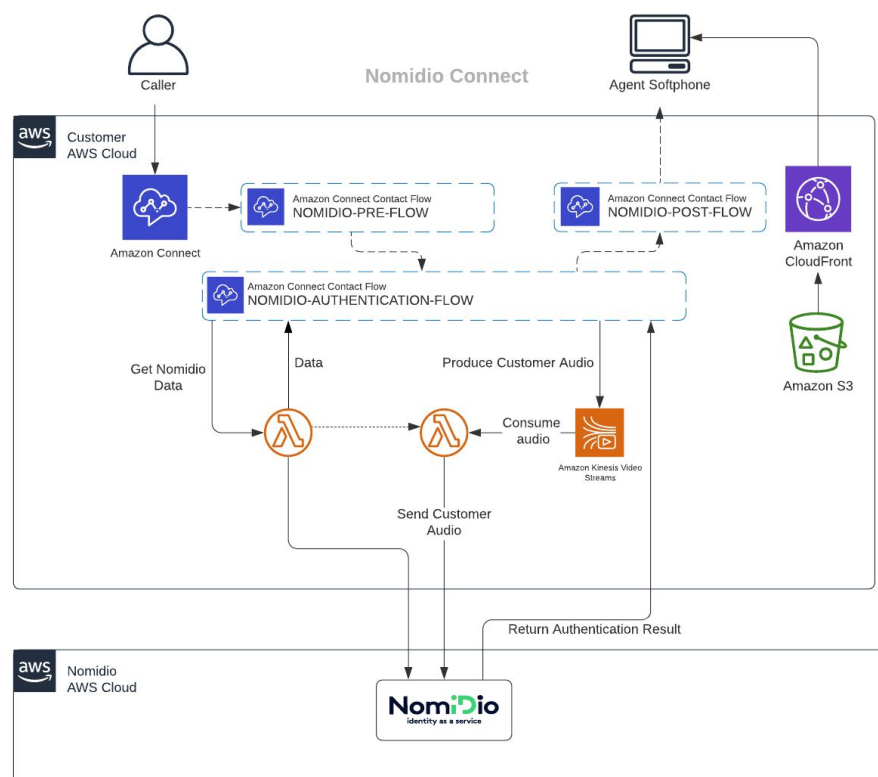
Prerequisites

Before using this integration, you will need to have a deployed instance of Amazon Connect. If you have not yet done this, follow the [Get Started with Amazon Connect](#) guide before returning to this guide.

If you intend to use the chat feature, you need to embed Amazon Connect Chat on your website. If you have not done this yet, see [Enabling your app for chat](#) in the Amazon Connect Guide.

Nomidio Connect makes use of Kinesis Video Stream (KVS) to capture audio samples as part of the voice contact flow, in order to authenticate the caller. AWS allocates a default limit of 50 concurrent KVS streams per account, therefore if you use KVS for other purposes or anticipate inbound call rates higher than 10 calls per second then you will need to raise a support case with AWS support to update the limit (see [Plan for Live Media Streaming](#) for more details).

Architectural Overview



The Nomidio Connect integration consists of three stages, pre-authentication, authentication and post-authentication. The integration provides six contact flows to configure these stages:

- Customisable PRE flow: anything done prior to authentication
- The AUTHENTICATION flow: identity management and authentication verification*
- The LEX AUTHENTICATION flow: identity management and authentication verification, performed using Amazon Lex*
- The AGENT CHALLENGE QUEUE flow: a 'transfer to queue' flow used to deliver the contact challenge experience during agent created challenges.
- The CHALLENGE flow: a common flow used to handle a contacts journey during an authentication challenge
- Customisable POST flow: anything done after authentication

* based on the customer interaction configuration these flows may not be deployed.

The authentication, challenge and lex authentication flows use lambda functions (*nomidioAction* and *nomidioLex*) to query Nomidio for information on the connecting customer's registration status. If the customer is registered with Nomidio then a challenge is created and (in the case of a voice contact) the *nomidioAction* lambda function calls the *sampleUpload* lambda, consuming the Kinesis Video Stream (KVS) and sending it to Nomidio for verification. The *nomidioAction* lambda function then polls for the result and stores it in a [contact attribute](#), ready to be presented to the agent or used to inform routing decisions.

What is Covered

The procedure for setting up and deploying the Nomidio Connect integration consists of the following steps. For detailed instructions, follow the links for each step.

[Step 1. Subscribing to Nomidio and onboarding the enterprise](#)

First step of integrating Nomidio Connect is subscribing through AWS Marketplace.

- Subscribe to [Nomidio product](#) through AWS Marketplace
- Follow the enterprise onboarding process

[Step 2. Creating Nomidio Connect credentials](#)

In order to use the Nomidio Connect integration, you will require a set of client credentials to authenticate your enterprise with Nomidio.

- Login to the [Nomidio Admin Service](#)
- Generate a set of client credentials

Step 3. Launching the stack

There is a CloudFormation template available to deploy the resources required to use the Nomidio Connect integration.

- Login to the [Nomidio Admin Service](#)
- Click on the deploy stack button
- Enter the required parameters
- Launch the stack

Step 4. Configure the Connect instance

The Nomidio Connect integration relies on live media streaming of the customer's voice during the Nomidio authentication process on the voice channel. And Amazon Lex for webchat and/or voice command customer interactions. These services need to be configured on your AWS Connect instance.

- Login to the Amazon Connect Console
- Select the Connect instance
- Enable Live Media Streaming
- Add the bots prefixed with 'Nomidio'*

* Only if chosen Customer Interaction Configuration requires Chat/Lex

Step 4a. Manual importing the Amazon Connect contact flows

Note: Only required if the CloudFormation auto importing ('Deploy Contact Flows to Connect instance' setting) has been disabled.

The CloudFormation template will have published five contact flows to the S3 bucket defined in the S3 Setup Bucket parameter of the CloudFormation template.

- Download the contact flows from the S3 Bucket
- Import them into your Amazon Connect instance in the following order:
NOMIDIO-POST-FLOW, NOMIDIO-CHALLENGE-FLOW,
NOMIDIO-AUTHENTICATION-FLOW and/or
NOMIDIO-LEX-AUTHENTICATION-FLOW, NOMIDIO-PRE-FLOW,
NOMIDIO-AGENT-CHALLENGE-QUEUE

Warning: the order of import is the reverse order of the flows and it is important to follow this order for successful contact flow creation. In case of having both NOMIDIO-AUTHENTICATION-FLOW and NOMIDIO-LEX-AUTHENTICATION-FLOW flows, NOMIDIO-AUTHENTICATION-FLOW must be imported first.

[Step 5. Configure agent challenge quick connect](#)

Create a quick connect to facilitate audio capture during challenges created by agents while connected to a contact.

- Login to your Amazon Connect instance
- Create a 'Nomidio Agent Challenge Flow'
- Assign it to your active queue
- Direct it to the 'NOMIDIO-AGENT-CHALLENGE-QUEUE' flow

Note: This step is not required if you are only interested in chat.

[Step 6. Assign a phone number](#)

Assign a phone number to the flow.

- Login to your Amazon Connect instance
- Claim a phone number
- Direct it to the NOMIDIO-PRE-FLOW

Note: This step is not required if you are only interested in chat.

[Step 7. Testing the Flow](#)

- Call your assigned phone number - you should complete the Nomidio authentication process and then be transferred to the AWS softphone

[Step 8. Accessing and using the standalone softphone \(if deployed\)](#)

- The URL to access the softphone (if deployed) can be found by looking at the "SoftphoneUrl" value of the CloudFormation stack.
- Whitelist the standalone softphone URL in Amazon Connect Approved Origins
- Access the softphone


Setting up a Nomidio Connect Subscription

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

Nomidio Connect 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 Connect integration.

Enterprise And Connect Region Details



NomidioConnect | 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 NomidioConnect


Get started



Copyright © PQ Solutions Limited.
All rights reserved.

The first step of the onboarding process is to input the company name. Select the 'Yes, we are using Amazon Connect' option and the region where your Nomidio Connect integration will be deployed. This should be the same region as your Amazon Connect instance.

Note: The Nomidio Identity-as-a-Service is currently only hosted in AWS region eu-west-2 (London). It is recommended that the Amazon Connect instance and Nomidio Connect integration be deployed in this region. This should be considered in conjunction with the Amazon Connect guidelines for [region selection](#). As Nomidio expands its hosting to more regions, any existing integrations will be directed to the best available region.



NomidioConnect | Register

Let's get started

Please enter company details to create an account

Company Name (required)

The Test Company

Please enter the company name you use with your customers

Will you be using Nomidio with Amazon Connect?

☒ Yes, we are using Amazon Connect

☐ No, we will integrate Nomidio with a different contact centre

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


Europe (London) eu-west-2 Recommended ★


North America (N. Virginia) us-east-1


North America (Oregon) us-west-2


Europe (Frankfurt) eu-central-1


Europe (London) eu-west-2 Recommended ★


 Enter company details

 Create admin account

 Confirm email address

 Set account password

 Enable 2FA



Copyright © PQ Solutions Limited.
All rights reserved.

page 9 of 32

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
identity as a service

NomidioConnect | Register

Create Administrator Account

Please enter the administrator's details to create an account

Email address (required)
test@test.com
You'll need access to this email address to verify your account

First name (required)
Admin

Last name (required)
Name

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

Next

☒ 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.

Email Verification

NomiDio
identity as a service

NomidioConnect | Register

Administration email confirmation

A PIN has been sent to the administrator's email at **test@test.com**

Please enter the PIN from the email (required)
7 5 2 6 2 4

Confirm PIN

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

Entered the wrong email? If **test@test.com** is the wrong email, you can [change your email](#).

☒ Enter company details

☒ Create admin account

☒ Confirm email address

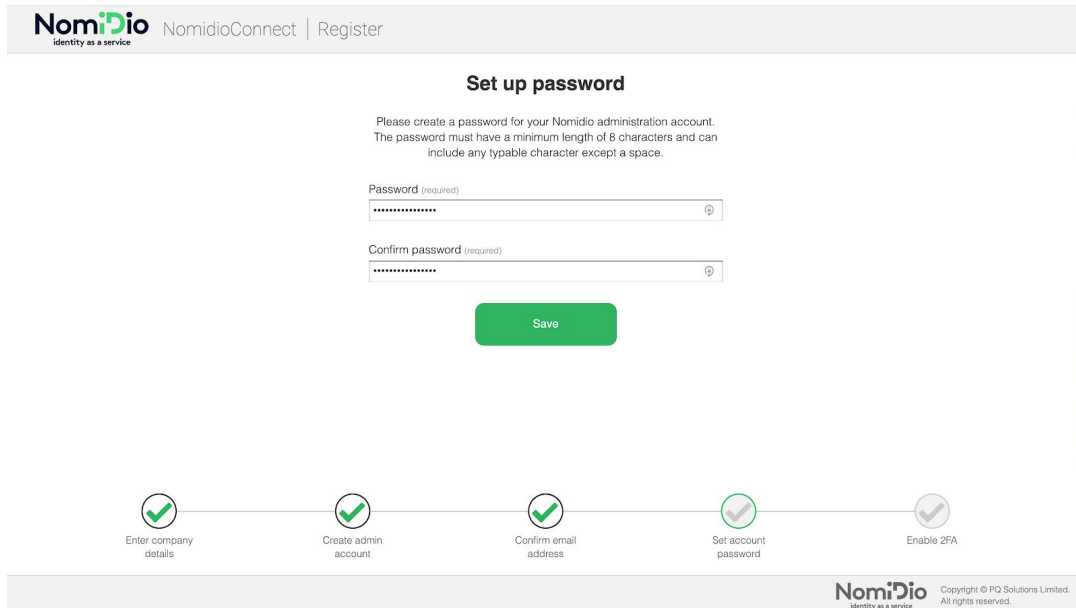
☐ Set account password

☐ Enable 2FA

NomiDio
identity as a service

Copyright © PQ Solutions Limited.
All rights reserved.

Administrator Password



NomiDio NomidioConnect | 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

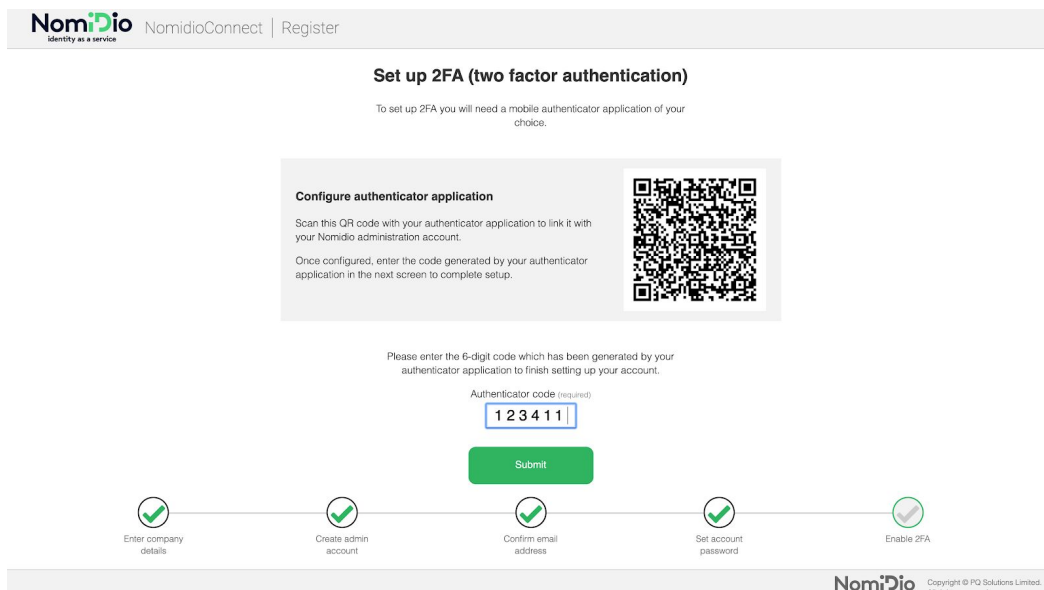
Progress bar: Enter company details (checked), Create admin account (checked), Confirm email address (checked), Set account password (checked), Enable 2FA (unchecked)

NomiDio 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 NomidioConnect | 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)

Submit


Progress bar: Enter company details (checked), Create admin account (checked), Confirm email address (checked), Set account password (checked), Enable 2FA (checked)

NomiDio Copyright © PQ Solutions Limited. All rights reserved.

Once the administrator account is successfully created the user is prompted to login to the Nomidio Admin Service where they can launch the CloudFormation template and generate credentials required to integrate with Nomidio Connect.

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. After entering a valid email and password the user is taken to the two factor authentication page as shown below. Using the authenticator app on their mobile phone to get an authentication code.



identity as a service


Enter authentication code.

Please enter the 6 digit code which has been generated by your authenticator app to complete two-factor authentication.

Authentication code

823145

Submit



Identity as a service

Once logged in the administrator is able to:

- Update the enterprise name (click “Edit” button).
- Launch the CloudFormation template (click “>” in CloudFormation box).
- Create new client credentials (click Client Credentials tab and “+” button).
- Add enterprise IP addresses to allowlist* (click Allowlist tab and “+” button)
- Add, edit and disable Enterprise Admins (click Admins tab)
- View enterprise usage for the current and previous month
- Upgrade from free trial limits

*Note: Nomidio allowlist is NOT required for integrations with Amazon Connect

Creating Nomidio Connect Credentials

To integrate with Nomidio Connect, credentials need to be generated. The credentials are automatically created and presented to the user. The secret can only be viewed/copied at time of creation, thus it is recommended to wait until needed during setup via the CloudFormation.

Create New IDAAS Client Credentials

This is the only time the IDAAS Key Secret can be viewed or downloaded. You cannot recover it later. However, you can create a new key at any time.

IDAAS Key ID

9ODO5FL9B50A5V9Y0Q6Q

Copy

IDAAS Key Secret

.....

Show Secret

Copy

Download CSV file

Done

Note: If a secret is lost it can not be recovered and a new one must be generated. A maximum of five active client credentials are permitted at any time.

Installing Nomidio Connect Resources

CloudFormation

In order to use the Nomidio Connect AWS Integration, some infrastructure must be deployed within the customer AWS account. This is deployed via AWS CloudFormation. The CloudFormation template can be launched via the Nomidio Admin Service and the resources that will be deployed, plus the steps required to deploy them, are described in the following sections.

AWS Resources

The CloudFormation template deploys the following resources:

Name	Type	Purpose
nomidioAction	Lambda Function	Used by the Amazon Connect contact flow to communicate with the Nomidio service
	Lambda Permission	Permission granted to Amazon Connect to trigger and consume this Lambda Function
nomidioActionIAMRole	IAM Role	Assumed by the nomidioAction Lambda function to: <ul style="list-style-type: none"> - invoke the sampleUpload Lambda function - decryptNomidioConnectSecretPolicy
deploymentHelper	Lambda Function	Used during the CloudFormation deployment process to perform the following functions: <ul style="list-style-type: none"> - generate and deploy contact flows - encrypt the Nomidio access key secret - generate and deploy the softphone files (if deployed) - deploy the Lex bots (when applicable)
deploymentHelperIAMRole	IAM Role	Assumed by the deploymentHelper Lambda function to: <ul style="list-style-type: none"> - encrypt using the KMS key (encryptionKey) - put/list/delete on the s3Bucket - decryptNomidioConnectSecretPolicy - get/put/delete nomidio lex resources

		<ul style="list-style-type: none"> - Connect permissions required for importing contact flows
deployLambdaPackagesIAMRole	IAM Role	Used by deployLambdaPackagesFunction: <ul style="list-style-type: none"> - put/delete objects in s3Bucket
deployLambdaPackagesFunction	Lambda Function	Used to: <ul style="list-style-type: none"> - copy lambda packages to s3Bucket
s3Bucket	S3 Bucket	Used to store: <ul style="list-style-type: none"> - Custom Amazon Connect contact flows - Lambda function deployment packages - standalone softphone source (if deployed)
encryptionKey	KMS Key + KMS Alias	A KMS key that is used to encrypt/decrypt the Nomidio access key secret
decryptNomidioConnectSecretPolicy	IAM Managed Policy	Used to provide decrypt access to the created AWS KMS key in order to decrypt the ciphertext
kvsStreamIAMRole	IAM Role	Assumed by the uploadSample Lambda function to: <ul style="list-style-type: none"> - list, describe and get Kinesis Video streams (used to consume the Amazon Connect call audio) - decryptNomidioConnectSecretPolicy
sampleUpload	Lambda Function	Used to consume the caller's authentication attempt audio and send it to Nomidio for processing
cloudFrontDistribution*	CloudFront Distribution	Used to cache and serve the softphone from the s3Bucket
cloudFrontOriginAccessIdentity*	CloudFront Origin Access Identity	Used to identify the CloudFormation distribution in the cloudFrontReadPolicy
cloudFrontReadPolicy*	S3 Bucket Policy	Applied to s3Bucket to allow read access only from the cloudFrontDistribution using the cloudFrontOriginAccessIdentity
nomidioLexIAMRole**	IAM Role	Assumed by the nomidioLex Lambda function to: <ul style="list-style-type: none"> - decryptNomidioConnectSecretPolicy
nomidioLex**	Lambda Function	Used by Amazon Lex to communicate with the Nomidio service and provide the relevant prompts

*Note: Only deployed when `deployStandaloneSoftphone` is true

**Note: Only deployed when Customer Interaction Configuration requires Chat/Lex

Parameters

You will then be presented with a screen to set the following Parameters:

Parameter	Default Value	Description
KMS Configuration		
KMS Key Administrator	<REQUIRED>	The ARN of the user/role (which can be found in the IAM console) that should obtain permissions to manage the generated KMS key. Format: arn:aws:iam:...
S3 Configuration		
Bucket Name	<REQUIRED>	The base name for the S3 bucket to be created to hold the Nomidio Connect resources. Use lower case letters and numbers only. A unique number is appended to your name to make sure it is unique.
Nomidio Configuration		
Supplier Code	<REQUIRED>	Your supplier code, retrieved by logging in to the Nomidio admin panel. This field should be prefilled if you used the Nomidio Admin Service to launch the template and should not be altered unless explicitly told to do so by a Nomidio technical support team member.
Enterprise Code	<REQUIRED>	Your enterprise code, retrieved by logging in to the Nomidio admin panel. This field should be prefilled if you used the Nomidio Admin Service to launch the template and should not be altered unless explicitly told to do so by a Nomidio technical support team member.
Enterprise Name	<REQUIRED>	The friendly name of the enterprise - this should be prefilled if you used the Nomidio Admin Service to launch the template
IDaaS Connect Gateway URL	<REQUIRED>	Do not alter this unless explicitly told to do so by a Nomidio technical support team member
Access Key Id*	<REQUIRED>	Enter the Access Key Id generated via Nomidio Admin Service

Access Key Secret*	<REQUIRED>	Enter the Access Key Secret generated via Nomidio Admin Service
Connect Instance Configuration		
Connect Instance Id	<REQUIRED>	The Amazon Connect instance id or instance ARN (this can be found through Amazon console selecting Amazon Connect)
Connect Instance URL	<REQUIRED>	The Amazon Connect instance URL (this can be found through Amazon console selecting Amazon Connect) and is the address used to interact with your instance
Customer Interaction Configuration	<REQUIRED>	<p>Determines how your customers interact with Nomidio Connect:</p> <ul style="list-style-type: none"> - Standard Voice Only: Customers use their phone keypad to select menu options (note: this option does not support chat communications) - Standard Voice + Chat: In addition to the support for standard voice, this option allows customer interaction via chat using an Amazon Lex chatbot. - Lex Voice + Chat: Amazon Lex is used in both chat and voice channels, allowing customers to verbally speak their menu selections when on the phone, in addition to using their phone keypad.
Deploy Contact Flows to Connect Instance?	true	Determines whether the deployment should deploy the required Nomidio Contact Flows to the Connect instance automatically (recommended). If set to 'false', the 'manual' import steps below should be followed
Standalone Softphone Configuration		
Deploy Standalone Softphone?	true	Determines whether the standalone softphone gets deployed (recommended for testing)
Default Country Code	GB	The country that phone numbers should be assumed to be coming from when the phone number is ambiguous

*See section [Creating Nomidio Connect Credentials](#)

Executing the CloudFormation Template

In order to launch the CloudFormation deployment, login to the AWS Console and then click on the launch stack button in the Nomidio Admin Service:

- Choose a region to launch the stack in, using the region selector in the console navigation bar¹.
- Provide a name for the stack and enter the parameter values (as described in [Parameters](#)).
- Check the checkbox acknowledging that CloudFormation will be deploying IAM resources (as described in [AWS Resources](#)).
- Click on the “Create Stack” button

Updating the CloudFormation Stack

Updating the CloudFormation stack allows the user to update certain parameters that were previously selected. Examples of changes that user may want to make are:

- Updating the credentials generated through the Nomidio Admin Service
- Adding/removing the standalone softphone
- Adjusting of enterprise name used in the contact flow (see [Testing the Contact Flow](#))
- Changing the Customer Interaction Configuration

In order to update the stack:

- Login to AWS Console
- Navigate to CloudFormation
- Click on ‘View Stacks’ and select the stack which needs updating
- Click on ‘Update’ and select ‘Use current template’ option
- Update parameters as required
- Proceed to update the stack by pressing ‘Next’
- Wait for the update to complete

Note: if the enterprise name was changed as part of the stack update, the NOMIDIO-PRE-FLOW (Contact Contact Flow) will need re-importing (see [Importing the Custom Amazon Contact Flows](#)).

¹ This region should match the region that Amazon Connect is deployed.

Configuring the Amazon Connect Contact Centre

Enable Live Media Streaming

This integration requires live media streaming in order to collect the callers voice sample and use it for authentication. This feature therefore must be enabled on your Amazon Connect instance (see Amazon Connect guide [Enable Live Media Streaming in Your Instance](#) for instructions).

The default service KMS Key (aws/kinesisvideo) can be used as the “KMS master key” and the “Data retention period” can be set to “No Data Retention”.

Add Lex bots

All bots prefixed with ‘Nomidio’ should be added to the connect instance (see [Add the Lex bot to an Amazon Connect Instance](#) for more details).

Manually Importing Custom Amazon Connect Contact Flows

Note: This step is only required if *Deploy Contact Flows to Connect Instance* was disabled during deployment.

During the CloudFormation deployment process, three Amazon Connect Contact Flows will have been generated and placed into the ‘contact-flows/’ folder of the new S3 bucket (as named by the user deploying the integration). The contact flows consist of:

- NOMIDIO-PRE-FLOW: a simple flow that sets the active queue and welcomes the contact to your company using the previously set Enterprise Name parameter
- NOMIDIO-AUTHENTICATION-FLOW: a complex flow that handles the authentication pipeline (note: this flow should not be altered in any way)
- NOMIDIO-LEX-AUTHENTICATION-FLOW: a complex flow that handles the authentication pipeline using Amazon Lex to receive user input (note: this flow should not be altered in any way)
- NOMIDIO-CHALLENGE-FLOW: a common flow that handles the user experience of fulfilling a security challenge (note: this flow should not be altered in any way)
- NOMIDIO-POST-FLOW: a simple flow that routes the contact to the active queue (as set in the pre flow)
- NOMIDIO-AGENT-CHALLENGE-QUEUE: a ‘transfer to queue’ flow that is triggered by the agent creating an authentication challenge while connected to a

contact and redirects to the NOMIDIO-CHALLENGE-FLOW (note: this flow should not be altered in any way)

Download the generated Contact Flows (“NOMIDIO-PRE-FLOW“, “NOMIDIO-LEX-AUTHENTICATION-FLOW” and/or “NOMIDIO-AUTHENTICATION-FLOW”, NOMIDIO-CHALLENGE-FLOW, “NOMIDIO-POST-FLOW” and “NOMIDIO-AGENT-CHALLENGE-QUEUE”) from the S3 bucket generated as part of the CloudFormation process (for more details on downloading from S3 see the AWS [user guide](#)). A link to the bucket can be located in the Output tab of the CloudFormation stack.

After downloading the required files, complete the following steps for each of the flow templates in the following order:



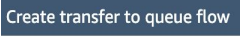
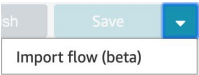

1. NOMIDIO-POST-FLOW
2. NOMIDIO-CHALLENGE-FLOW
3. NOMIDIO-AUTHENTICATION-FLOW*
4. NOMIDIO-LEX-AUTHENTICATION-FLOW*
5. NOMIDIO-PRE-FLOW
6. NOMIDIO-AGENT-CHALLENGE-QUEUE

* depending on selected Customer Interaction Configuration.

Warning: The import order is the reverse of the flow order and must be followed for correct integration between the flows.

Manual Amazon Connect Flow Import

Note: Amazon Connect UI may have changed and can differ depending on AWS region. For more details on importing, see [Amazon Connect - Import/Export Contact Flows](#).

- Login to your connect instance dashboard
- Using the right-hand menu, open the  menu and select “Contact Flows”
- Click on the  button above the table on the right-hand side - In the case of “NOMIDIO-AGENT-CHALLENGE-QUEUE”, the dropdown menu should be expanded and  selected
- Once the page loads, click on the blue dropdown arrow in the top right of the  button screen and click on the  button and browse for the flow (downloaded from S3) and click “Open”

- Click on the **Import** button - note: this process may take some time and may cause the browser to appear unresponsive.



- Select **Save & publish** from the dropdown in the top right hand corner of the page and then click the **Publish** button that appears in the confirmation dialog
- Repeat for all flows.

Configure Agent Challenge Quick Connect

- Login to your Amazon Connect instance
- Access the **Routing** menu and select **Quick connects**
- Click on **Add new**
- For the name input, input 'Nomidio Agent Challenge Flow' (note this must match exactly), for type, select 'Queue', for destination, select the name of the active queue and for contact flow select 'NOMIDIO-AGENT-CHALLENGE-QUEUE'
- Click on **Save**
- Access the **Routing** menu and select **Queues**
- Click on the name of the active queue
- For the Quick connects input, enter 'Nomidio Agent Challenge Flow'
- Click on **Save**

Assigning a Phone Number

- Login to your connect instance dashboard
- Using the right-hand menu, open the **Routing** menu and select **Phone numbers**
- Either select an existing number or click on the **Claim a number** button at the top-right of the table
- If claiming a new number, select a number type (Toll free/Direct Inward Dialing), pick a country and optional prefix and select a phone number from the given options and optionally enter a description for the purpose of the phone number

Contact flow / IVR

- Using the **Sample inbound flow (first contact experience)** select the "NOMIDIO-PRE-FLOW"

For more details on claiming a phone number, see [Amazon Connect - Claim a Phone Number](#).

Testing the Contact Flow

- If a standalone softphone was deployed, access the softphone (see [Using the Standalone Softphone](#))
- Dial the previously assigned phone number which is pointing to the NOMIDIO-PRE-FLOW
- The NOMIDIO-PRE-FLOW will then say “Welcome to <Your Company Name>” where the company name is previously inputted Enterprise Name
- The contact is then routed to the NOMIDIO-AUTHENTICATION-FLOW or the NOMIDIO-LEX-AUTHENTICATION-FLOW - these flows handles all of the Nomidio integration logic and prompts (note: these flows should not be altered)
- The call is then routed to the NOMIDIO-POST-FLOW where it is transferred to an agent queue

Customising the Contact Flows

Customising the Customer Experience prior to Nomidio Authentication

- On an inbound contact entering the connect instance, it is currently set to execute the “NOMIDIO-PRE-FLOW” (as described in [The Contact Flow](#)) .
- If you wish to alter the customer experience prior to the authentication flow, create a contact flow with the desired customer experience and ensure it ends with a “Transfer to flow” block pointing to the *AuthenticationFlowName* output from the CloudFormation stack, to perform the authentication. And set your custom pre-flow as the “Contact flow / IVR” assigned to your phone number.
- Within your prior flow, you can optionally set the “nomidio_auth_level” (see below) which can be used to set the challenge authentication level. This could be useful if you have gathered that the customer wishes to discuss a sensitive subject by pre authenticating them at a high level.
- Note: the default “NOMIDIO-POST-FLOW” expects a working queue to have been set and therefore this should be included in your prior flow if you intend to use the default post flow.

Contact Attribute Inputs

Contact Key	Attribute	Possible Values/Format	Default Value	Description
nomidio_post_flow_id		arn:aws:connect:<region>:<aws_account_number>:<instance_id>/contact-flow/<contact_flow_id>	<ARN of NOMIDIO-POST-FLOW>	The ARN of the contact flow that the contact should be routed to after completing the

			Nomidio flow.
nomidio_auth_level	STANDARD/HIGH	STANDARD	The authentication level the challenge will be created at (see Challenge Authentication Level)

Customising the User Experience after Nomidio Authentication

- On an inbound contact completing authentication, it is currently set to execute the “NOMIDIO-POST-FLOW” (as described in [The Contact Flow](#)).
- If you wish to change this behaviour, you may create your own flow to handle the contact after authentication. When using your own flow, you should click on the “Show additional flow information” dropdown in the left hand sidebar of the flow editor and take note of the ARN associated with the flow.
- You should then ensure that in your prior flow, you set the “nomidio_post_flow_id” contact attribute value to this ARN.
- Within your post authentication flow, you also have access to the authentication data specified below. This can be useful in order to change routing behaviour based on the authentication result or customer status.

Contact Attribute Outputs

Contact Attribute Key	Type	Description
nomidio_status	Nomidio Status	The current status of the customer's Nomidio ID
nomidio_fraud_flag	Fraud Flag Status	Details any fraud flag that is attached to the customer (empty string if none).
nomidio_challenge_auth*	Auth Level	When a challenge is completed, this attribute contains the authentication level of the challenge that was fulfilled.
nomidio_challenge_result*	Challenge Status	When a challenge is completed, this attribute contains the customer's challenge result.
nomidio_authenticated_enrolled*	Boolean	This attribute indicates if the user is enrolled and has passed a challenge.

*Only available if a challenge has taken place

Accessing and using the Standalone Softphone

The built-in standalone softphone is a simple way to get up and running with the Nomidio Connect integration.

Whitelisting the Standalone Softphone

If the standalone softphone deployment was selected, the CloudFront origin needs to get whitelisted in the Amazon Connect instance.

In order to whitelist the standalone softphone:

- Login to the AWS Console:
- Navigate to the Amazon Connect and select your instance
- Click on Application Integration from the menu
- Click on Add Origin and input the “SoftphoneUrl” value copied from the CloudFormation output

Accessing the Softphone

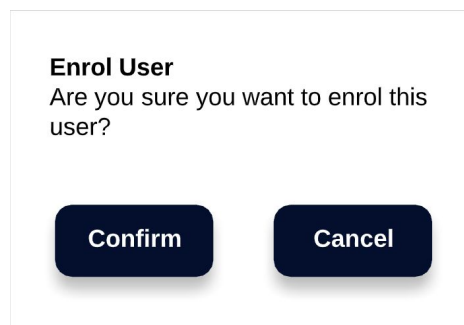
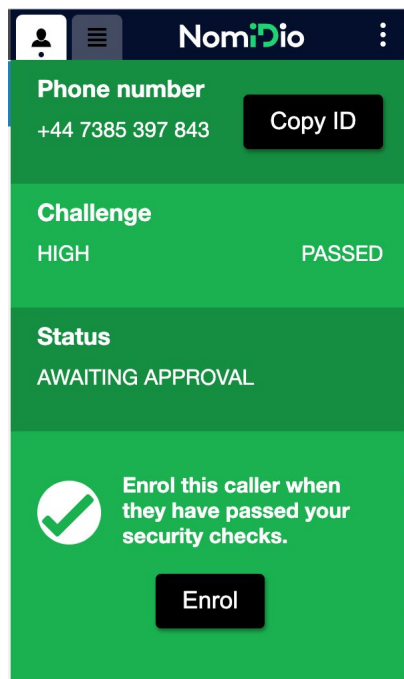
- Go to the CloudFormation stack and select the Outputs tab
- Click on the URL displayed as the “SoftphoneUrl”
- Follow the prompt to login to your Amazon Connect instance

Using the Softphone

There are several actions that can be done by agents through the softphone.

User Enrolment

Users can only be enrolled when their current Nomidio status is ‘AWAITING APPROVAL’ (for further information on Nomidio statuses, see [Nomidio Status](#)). Another requirement for a user to be enrolled is passing a high authentication level challenge (for more information on challenges, see [Challenge Authentication Level](#)). Agent will be shown with following screen when user passes the challenge:

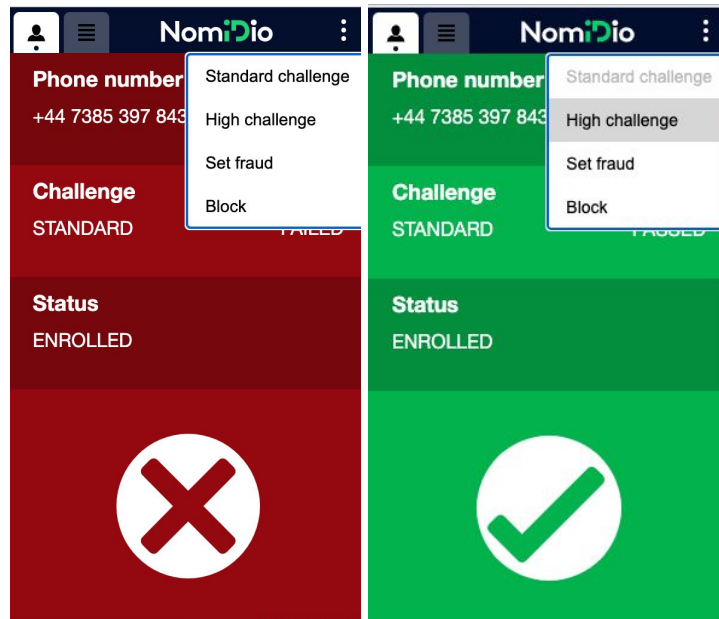


To enrol an inbound contact, an agent clicks on the 'Enrol' button which triggers a confirmation pop up to appear. Clicking the 'Confirm' button copies the user's unique Nomidio ID to the clipboard so the agent can update the user's CRM record by adding the Nomidio ID. The Nomidio ID can then be used to reference the user in the future.

Agent Requested Challenge

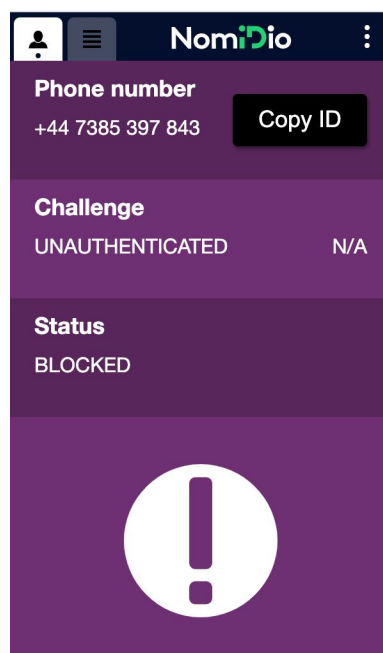
Once a user has been enrolled they can be authenticated on the IVR or through a web app with a standard level challenge. If the contact has passed the standard challenge then it is possible for the agent to request the user perform additional checks for a high authentication level challenge. If the contact has failed the standard challenge then it is possible for the agent to request the user perform another standard challenge or a high challenge.

To request another challenge an agent selects *High challenge* or *Standard Challenge* on the top menu shown below:



Blocking User

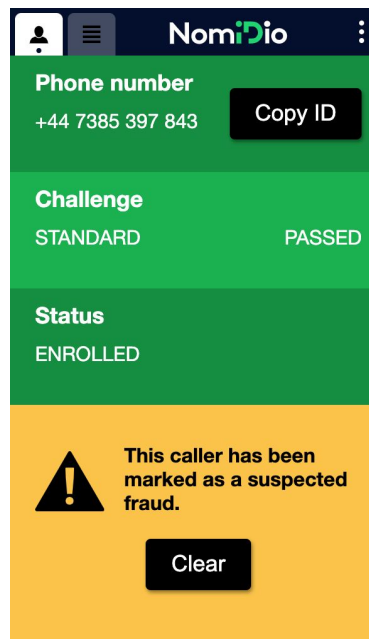
Agents can block a calling user with any Nomidio status (for further information on Nomidio statuses, see [Nomidio Status](#)) and regardless of whether they have completed a challenge. To block the user an agent selects *Block* from the top menu (see image in previous section). Blocked users will be connected to the agent without completing any Nomidio authentication, the agent will then see the following screen:



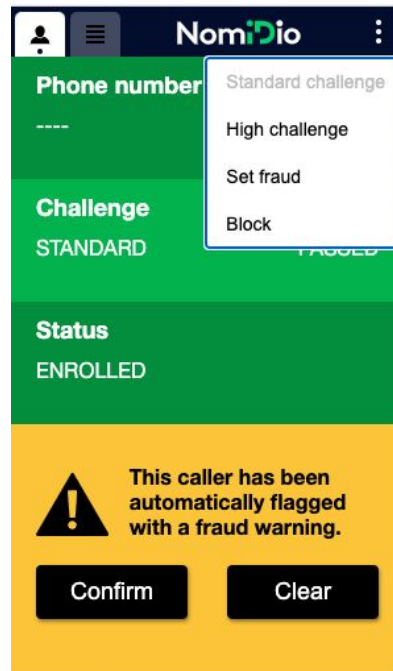
From this screen the agent is able to unblock the user through the same menu.

Setting Fraud Flag

Agents have the option of setting a fraud flag for a contact by selecting *Set fraud* from the top menu (see image in section [High Security Challenge](#)). Setting the fraud flag updates the contact's fraud flag to 'SUSPECTED_FRAUD' (for more information on fraud flags, see [Fraud Flag Status](#)). A warning screen is shown when the contact initiates future inbound communications. From this screen an agent can also clear the users fraud flag.



Some users may have a fraud flag set to 'FRAUD_WARNING' by Nomidio (for more information on fraud flags, see [Fraud Flag Status](#)), as shown below:



Agents can either clear the fraud flag set by Nomidio, or press 'Confirm' which would set the fraud flag to 'SUSPECTED_FRAUD'.

Definition of Terms

Challenge Authentication Level

Value	Description
STANDARD	A challenge that requires the user to verify their identity using their voice only.
HIGH	A challenge that requires the user to verify their identity using their voice and face.

Challenge Status

Value	Description
PASSED	The contact was able to satisfy all the checks included in the challenge.
FAILED	The contact was unable to satisfy some/all of the checks included in the challenge.
TIMEOUT	The contact did not complete the challenge within a reasonable period of time.

Nomidio Status

No Authentication

Value	Description
IDENTIFICATION_FAILED	The user (using chat) failed to identify themselves during authentication..
WITHHELD_NUMBER	The contact has withheld their phone number.
NOT_FOUND	The contact does not have a Nomidio ID and has chosen not to register at this time.
ERROR	A technical error has occurred during the authentication process.
NOMIDIO_UNAVAILABLE	A technical error occurred when communicating with Nomidio and therefore the authentication process has been skipped.
INVITED	The contact has an invitation to register for a Nomidio ID.
PENDING	The contact has started registration for a Nomidio ID but has not completed it yet.
INVITATION_SENT	The contact has been sent an invitation SMS.
OPTED_OUT	The contact has opted out of using their Nomidio ID with this enterprise.
EXISTS	The contact has an existing Nomidio ID but has neither opted in or out of enrolling with the enterprise. i.e. may still choose to enrol at a later date.
BLOCKED	The contact has been blocked by this enterprise.
TAC_EXPIRED	The contact has been enrolled with the enterprise, but has not accepted the latest Nomidio terms and conditions. The contact is required to accept the new terms and conditions in order to use their Nomidio ID.
FREE_TRIAL_LIMIT	The enterprise has exceeded the trial quota - Upgrade via the Nomidio Admin Service to remove free trial period restrictions.

Authenticated

Value	Description
AWAITING_APPROVAL	The contact has given consent to use their Nomidio ID with the enterprise and is awaiting enrollment approval.
ENROLLED	The contact has been enrolled with the enterprise.

TAC_WARN	The contact has been enrolled with the enterprise, and has not accepted the latest Nomidio terms and conditions. However the terms and conditions that the contact has accepted are still valid for performing authentication.
----------	--

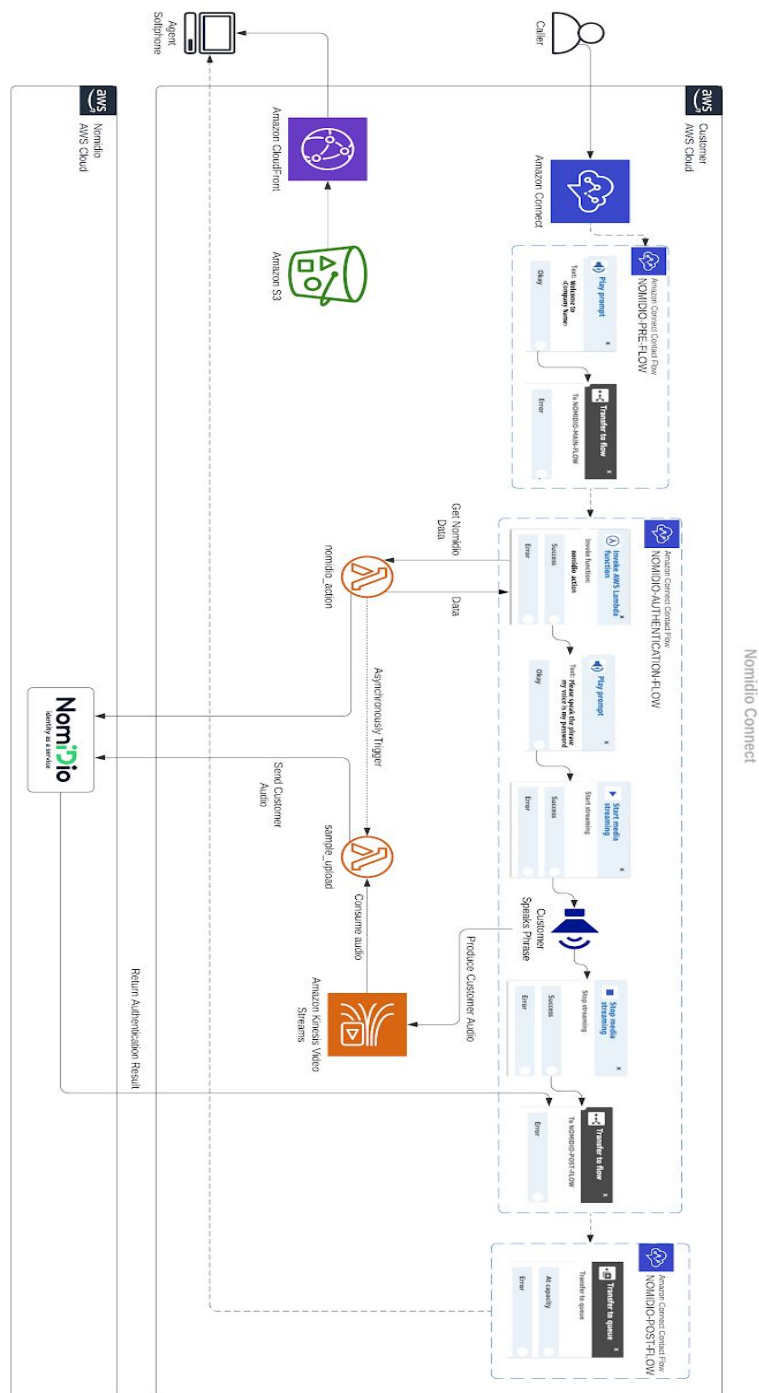
Fraud Flag Status

Value	Description
FRAUD_WARNING	Nomidio has placed a fraud warning flag on this contact.
SUSPECTED_FRAUD	This enterprise has marked the contact as suspected fraud.

Appendices

Appendix A

Nomidio Connect Voice



Nomidio Connect Chat

