STRATIS ICO PLATFORM

Administrator Guide

Table of Contents

Introduction

The Stratis ICO (Initial Coin Offering) Platform allows you to run a secure and flexible web-based application that enables buyers to purchase your tokens before the point of initial allocation. Your tokens are purchased (or earned) by buyers when they contribute in either BTC or STRAT while the ICO is live. For more information on the workflow and the components involved with the ICO Platform, please refer to the *ICO Platform Overview* document.

The purpose of this guide is to detail how you can deploy the ICO Platform and then configure it for your ICO. This includes registering as an administrator on the ICO Platform Web Application and branding this application so it can be integrated with your own website.

> **Note**
> From now on in this document, the ICO Platform Web Application is simply referred to as the *Web Application*.

Buyers will also register on the Web Application so they can make contributions. How you configure the ICO Platform also decides which options the buyers have when making contributions and whether they must pass KYC requirements.

You will carry out the setup tasks detailed in this guide during what is referred to in the *ICO Platform Overview* document as the deployment phase.

Deployment phase tasks

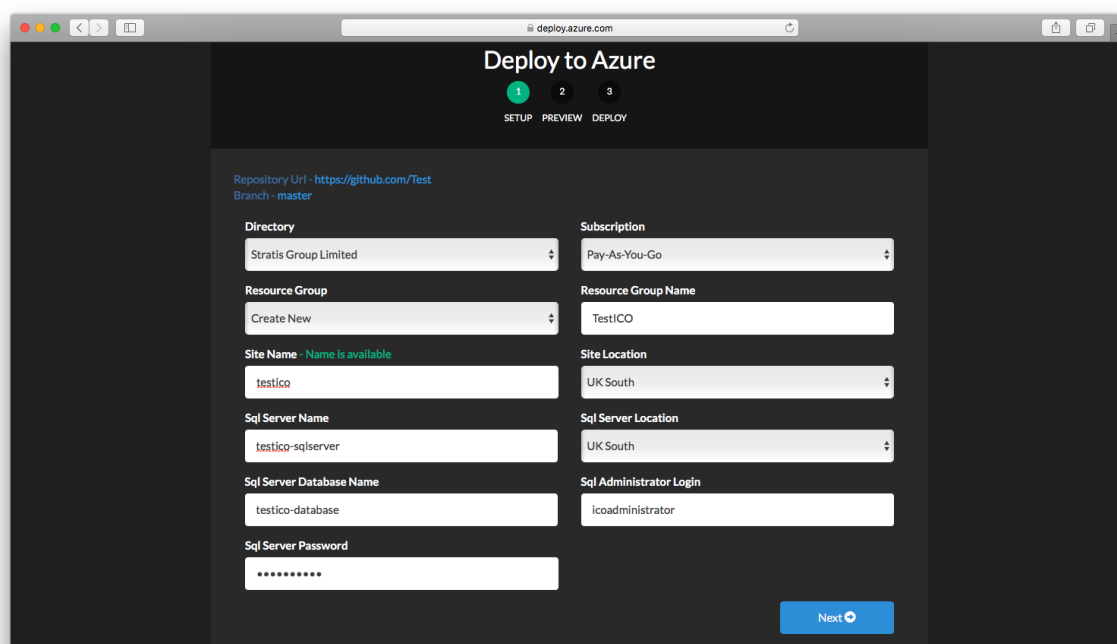The deployment phase involves five tasks which are your responsibility:

1. Deploy the Web Application and associated SQL Server database to Azure.
2. Launch the Web Application and register as an administrator.
3. Begin configuring the ICO Platform on the administration page of the Web Application. This includes: supplying the extended public keys for BTC and STRAT, branding the application so both the text and the look and feel are specific to your organization.
4. Finish configuring the ICO platform. This involves setting the period which the ICO will run and the prices for your tokens in BTC and STRAT. This task is affected by the cryptocurrency market, and depending on the situation, it can be delayed until the economic situation is most favourable.
5. Integrate the Web Application with your website. This involves creating DNS Records and setting a custom domain on the Web Application so buyers can reach the Web Application from one of your own domain names.

The following sections contain walkthroughs and advice on achieving these tasks:

Deploying the Web Application and associated SQL Server to Azure

Before beginning this task, you must set up an Azure subscription.
Once you have set up your subscription, navigate here and click the Deploy to Azure button. After logging in to Azure, you will see the first of the three deployment pages:

The following table describes what to specify for each field:

Field	Description
Directory	Always "Stratis Group Limited".
Subscription	Select which of your subscriptions to deploy the Web Application against.
Resource Group	Select which resource group you want to deploy the Web Application in or, alternatively, create a new resource group for the Web Application.
Resource Group Name	Specify a name for the resource group if you chose to create a new one.
Site Name	Specify a name for the site. The URL for the site will be: https://site_name.azurewebsites.net
Site Location	Specify a location for your site.
Sql Server Name	Specify a name for the SQL server the Web Application will use.
Sql Server Location	Specify a location for the SQL server.
Sql Server Database Name	Specify a name for the SQL server database the Web Application will use.
Sql Administrator Login	Specify a username for the SQL Server administrator.
Sql Server Password	Specify a password for the SQL Server administrator.

Click *Next* to proceed to the preview page:
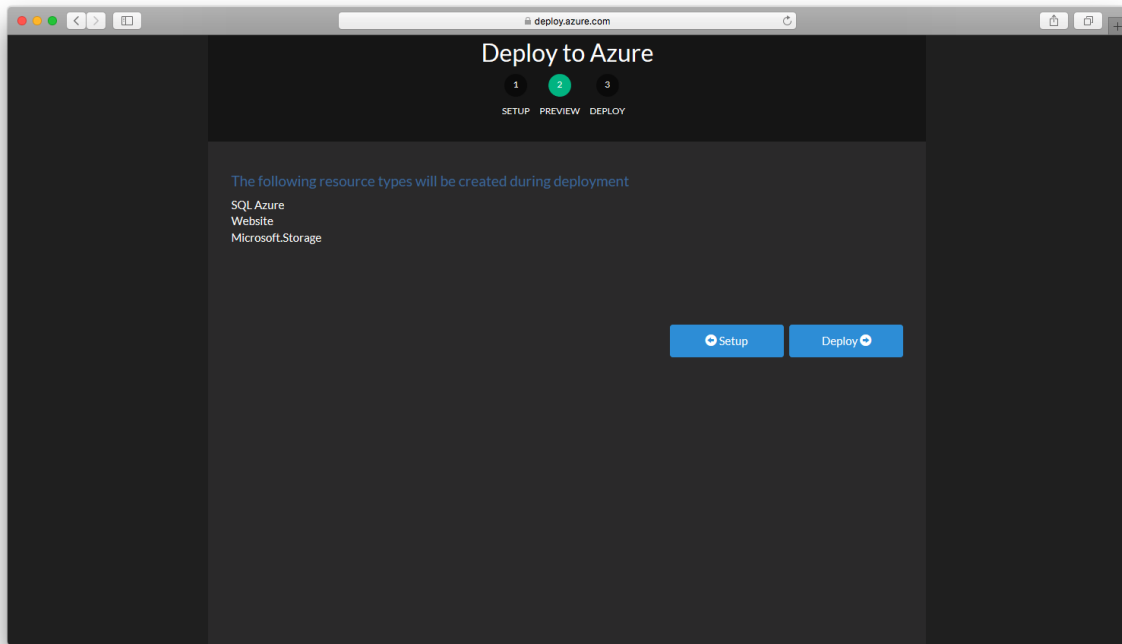
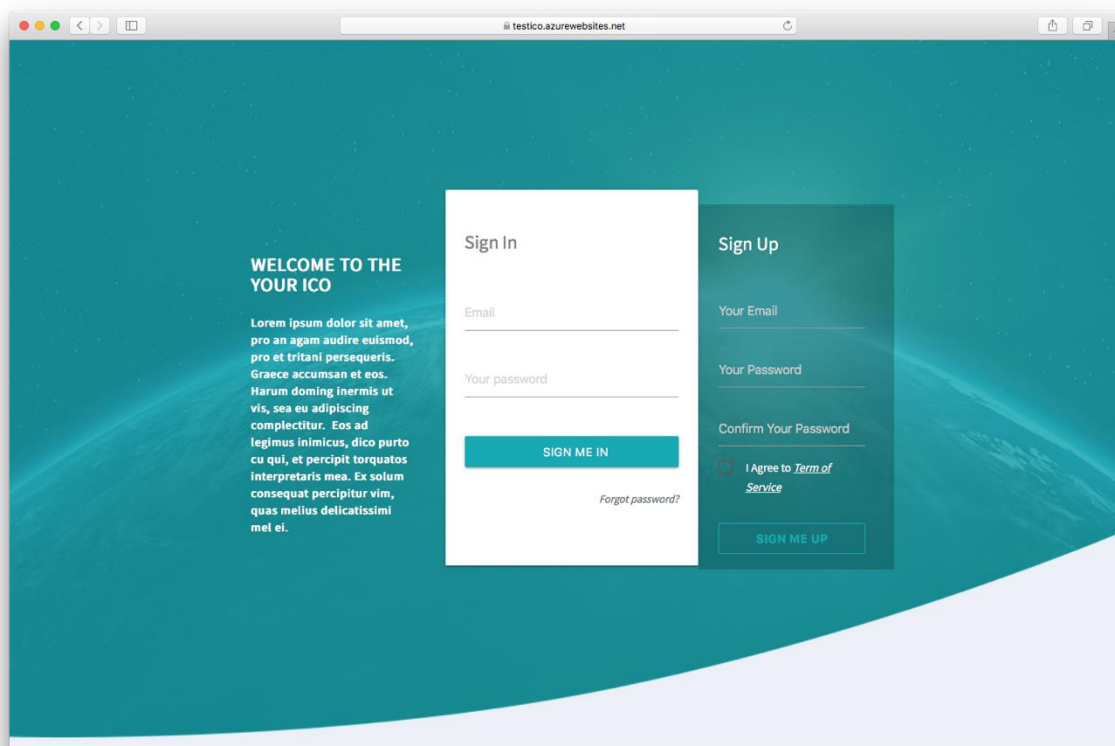Click *Deploy* to complete the deployment:
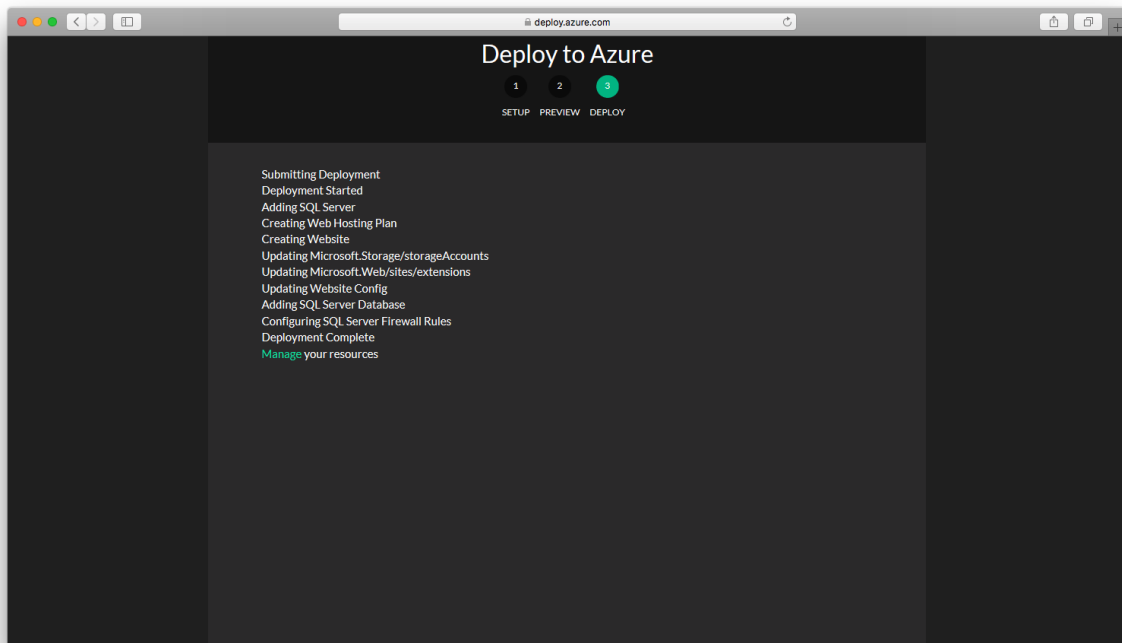
The *Manage* link takes you to the Azure Portal.

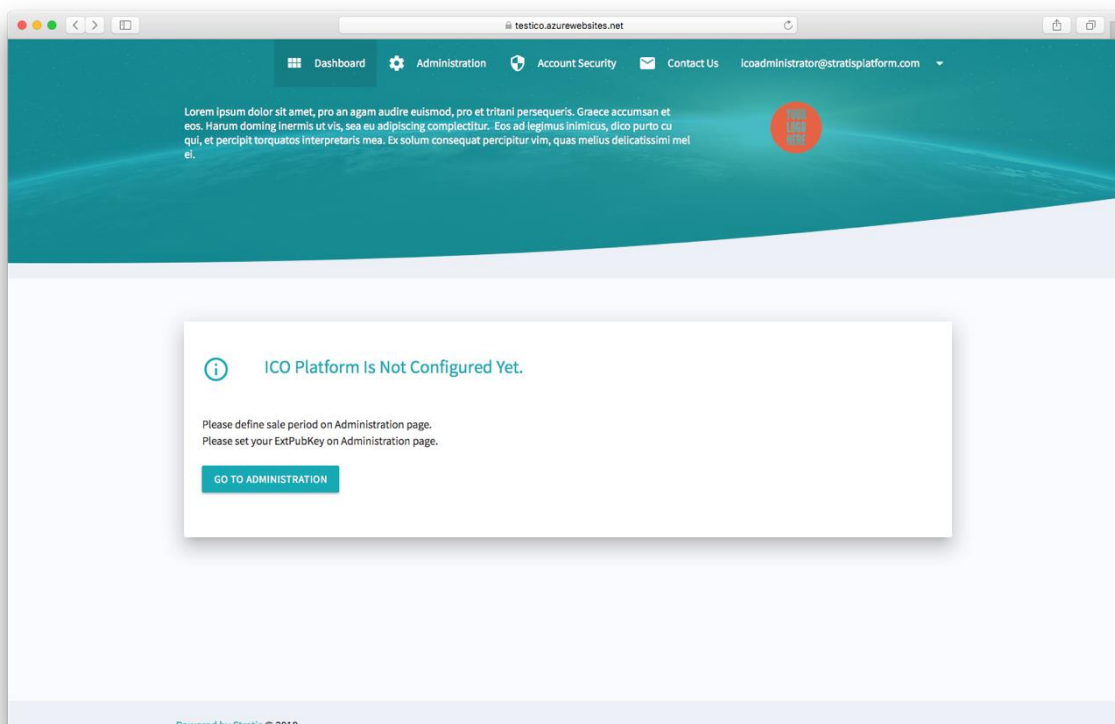## Registering as an administrator on the Web Application

The first user to register on the Web Application becomes the administrator. This means that the first user has access to the Administration page in addition to the Dashboard that "buyer" users see.

To register, navigate to the ICO Platform Login page, which appears unbranded at this stage:

Sign up to the platform by entering your email, a password, and a password confirmation. Once you have successfully signed up as the administrator, sign in using your email and password. The dashboard is displayed:

As mentioned previously, both you and the buyers see this dashboard. The contents of the dashboard vary according to the current point in the ICO process. In the previous figure, the Dashboard page is indicating that you, as the administrator, must supply an extended public key (ExtPubKey) and at least one sale period. Notice the link to the Administration page. It is here that you complete the next two tasks, which include supplying BTC and STRAT extended public keys and a sale period.

Configuring the Web Application Part 1

This task consists of six subtasks:

1. Setting the *Main Settings*.
2. Setting the *SendGrid Credentials*.
3. Branding the Web Application.
4. Setting the BTC and STRAT extended public keys.
5. Hooking into a third-party Know Your Customer (KYC) service.

These settings are all set in the Administration page of the Web Application:
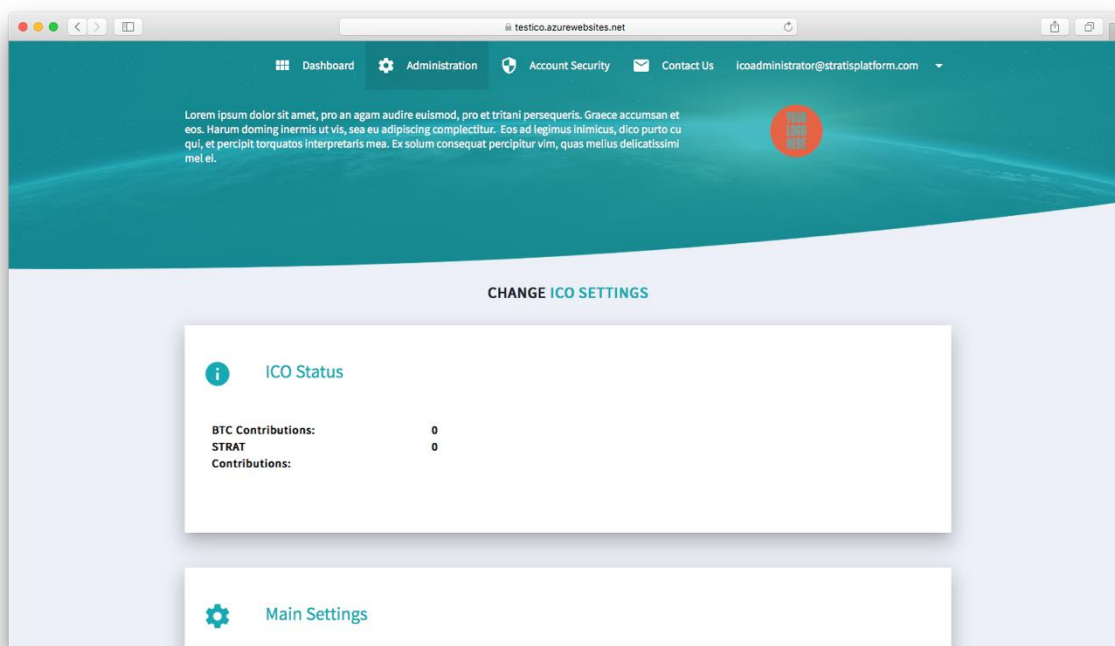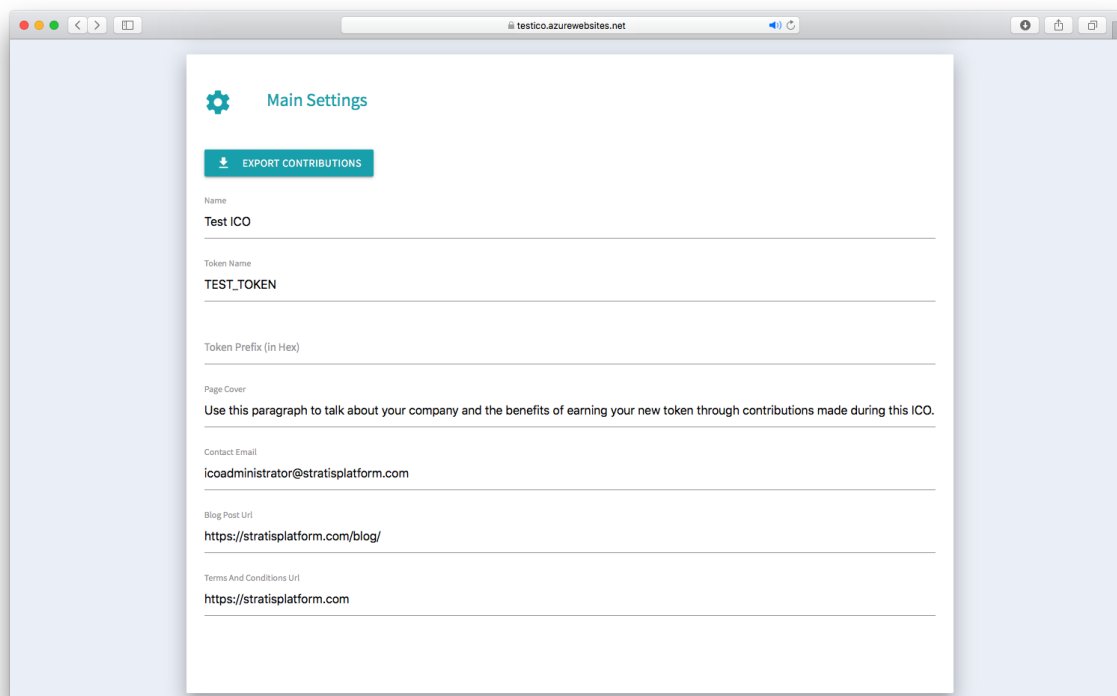
Note

On the Administration page, you can also see the contributions made in BTC and STRAT under *ICO Status*. You can choose to publish this information to increase interest in the ICO. For example, if the ICO is exceeding expectations a quarter of the way through, making this information public may boost contributions for the remainder of the ICO.

The following subsections provide a step-by step guide through each subtask:

Version 1.0

Setting the Main Settings

The following figure shows the *Main Settings* fields on the Administration page:

The following table describes what to specify for each setting and where the Web Application uses the settings:

| Field	Description
Name	Specify the name of the ICO. For example, "*Your_Organization ICO*". This setting is used on the Login page and in emails that the ICO Platform sends to users.
Token Name	Specify the name of your token. The name given here is used in the "YOUR CONTRIBUTIONS" boxes on the Dashboard page when referring to the amount of your tokens earned by a buyer.
Token Prefix	Specify the prefix value to use for validating your token addresses. The value must be added as 2 hexadecimal digits.
Contact Email	Specify the email address to use in correspondence from the ICO Platform to users. For example, the confirmation email sent when somebody signs up for the ICO is sent from this email address.
Blog Post Url	Specify a link to a blog post that you intend to put up when the ICO has ended. A non-configurable message is displayed on the Dashboard page at the end of the ICO, and this link is incorporated into the last four words of the message. The entire message reads: "The *ICO_Name* token crowdfund has finished successfully. We thank all participants for their contributions. Details on distribution can be found in our blog post."

Terms and Conditions	Specify a link to the page that lists the terms and conditions for your ICO. Used for a link on the Login page.

Note
As it refers to the branding and style of the Web Application, the *Page Cover* setting is discussed in Branding the Web Application.

Setting the SendGrid Credentials

The following figure shows the *SendGrid Credentials* fields on the Administration page:
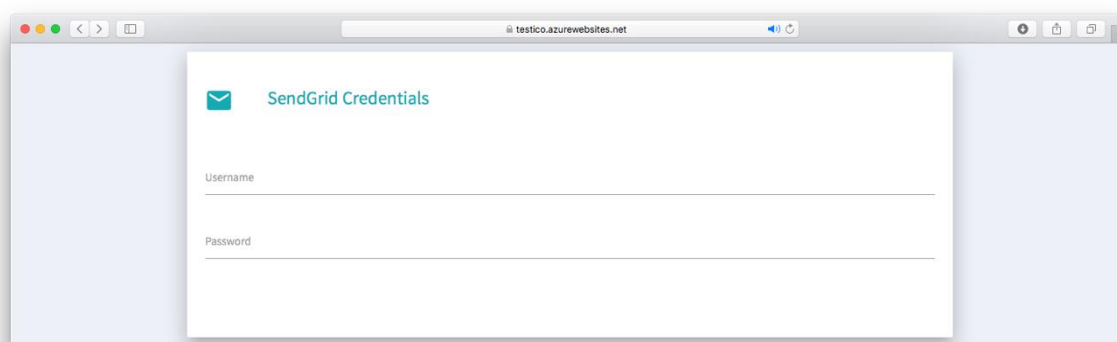
The Web Application uses the credentials in these fields when querying SendGrid services. If you do not have a SendGrid account, you can get one from here. The Web Application uses SendGrid to send a confirmation email when all users except for the administrator sign up to the platform. Refer to the following table for a description of the fields:
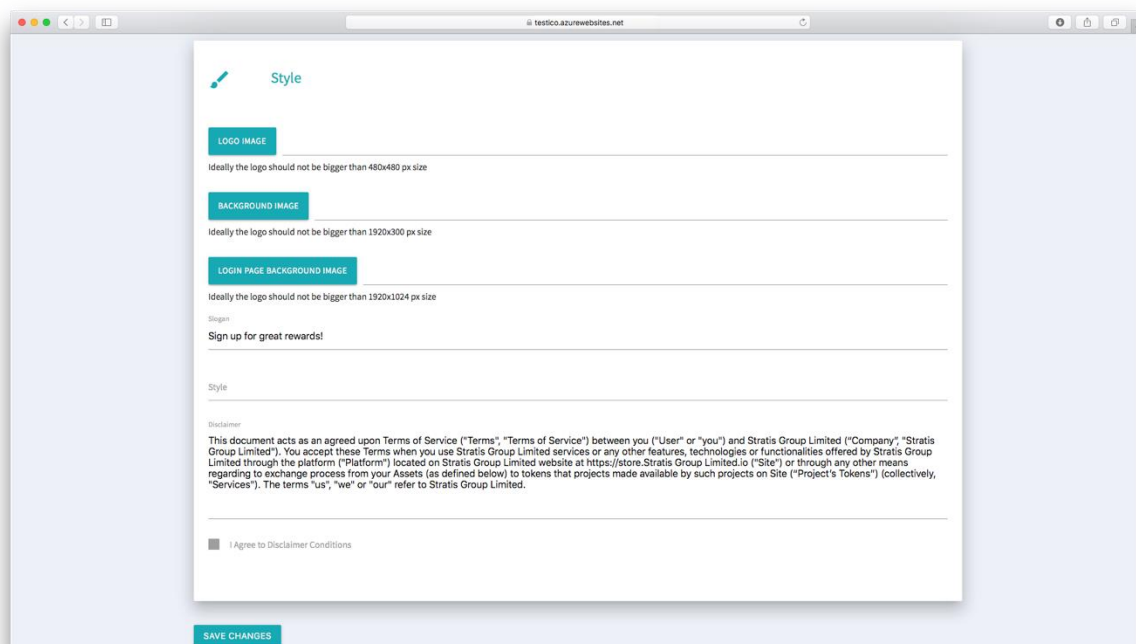
Field	Description
Username	Specify the username for the account you have with SendGrid.
Password	Specify the password for the account you have with SendGrid.

Important!
You must access your SendGrid account and ensure that emails sent from the ICO Platform pass SPF and DKIM email authentication checks. You can do this here. Failure to do this may result in emails generated by the ICO Platform going to users' junk email etc.

Branding the Web Application

The following figure shows the *Style* fields on the Administration page:

Version 1.0

Use the following table and the previous figure to explore what these fields offer in terms of branding:

Field	Description
Logo image	Upload a logo image for your organization, which is no greater than 480x480 pixels in size. Your logo replaces the red "YOUR LOGO HERE" placeholder image shown in this figure. In the *ICO Platform User Guide* default screenshots, the administrator has used this field to replace the placeholder image with a Stratis logo.
Background image	Upload a background image no greater than 1920x1024 pixels in size. Your background image replaces the green planet image shown on the Dashboard, Administration, and Account Security pages. In the *ICO Platform User Guide* default screenshots, the administrator has used this field to replace the planet image with a cityscape image.
Login page background image	Upload a background image no greater than 1920x1024 pixels in size. Your background image replaces the green planet image shown on the Login page. In the *ICO Platform User Guide* default screenshots, the administrator has used this field to replace the planet image with an image of balloons.
Slogan	Specify a slogan. Your slogan will appear in black text on the left hand side of the page. The slogan in this figure is "Sign up for great rewards!"
Style	Use this field to override the default CSS styling used for the Web Application. For example, to turn the settings panels to red specify:

Version 1.0

|	
	`.card-content{ background: #FF0000;}` In a more realistic situation, explore the HTML source of the Web Application to find out how the CSS classes are used. In the link elements at the top of the HTML files, you can find the location of the CSS stylesheets containing the default styles.
Disclaimer	***Read the entire disclaimer (scroll down to reveal the full text) and agree to the conditions contained within it by checking the checkbox.***

Note

Notice the white lorum ipsum text below the slogan. Use the *Page Cover* field from the *Main Settings* to define this text. You can see this text in the left-side box on the Login screen.

After setting the *Style* fields, click on the *Save Changes* button at the bottom of the Administration page. Use this button at any point to save your administrative settings.

Setting the BTC and STRAT extended public keys

The following figure shows the *ICO Settings* fields on the Administration page:
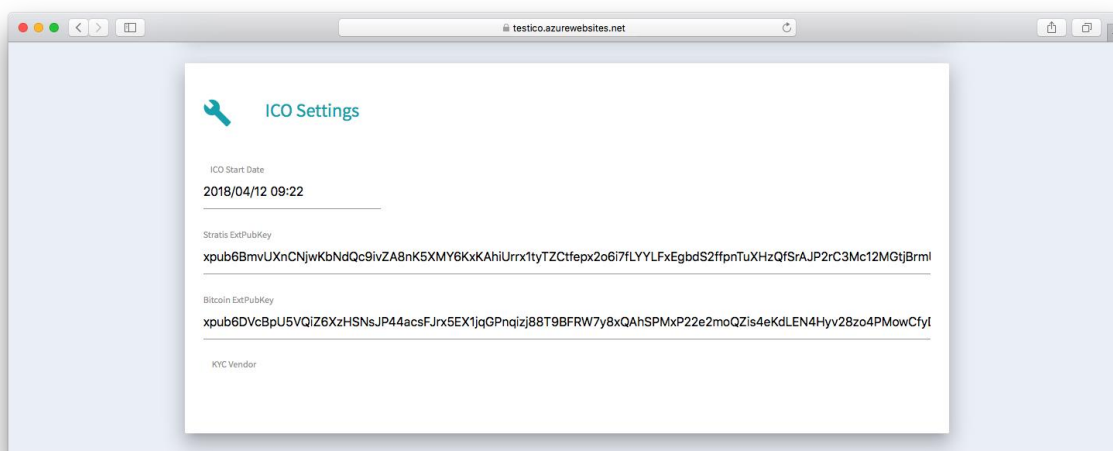
To receive contributions from buyers in BTC or STRAT, you must supply an extended public key for the respective cryptocurrencies. Obtain the BTC and STRAT extended public keys from a hierarchical deterministic wallet. In the previous figure, the administrator has provided an extended public key for BTC and STRAT. Now both the administrator and buyers can see their contributions in BTC and STRAT on the Dashboard.

Important!

Extended public keys can only be set once. Take care when setting these two fields.

The following figure shows the Dashboard page after an administrator has provided BTC and STRAT extended public keys, at least one sale period, and, if required, completed the KYC process:
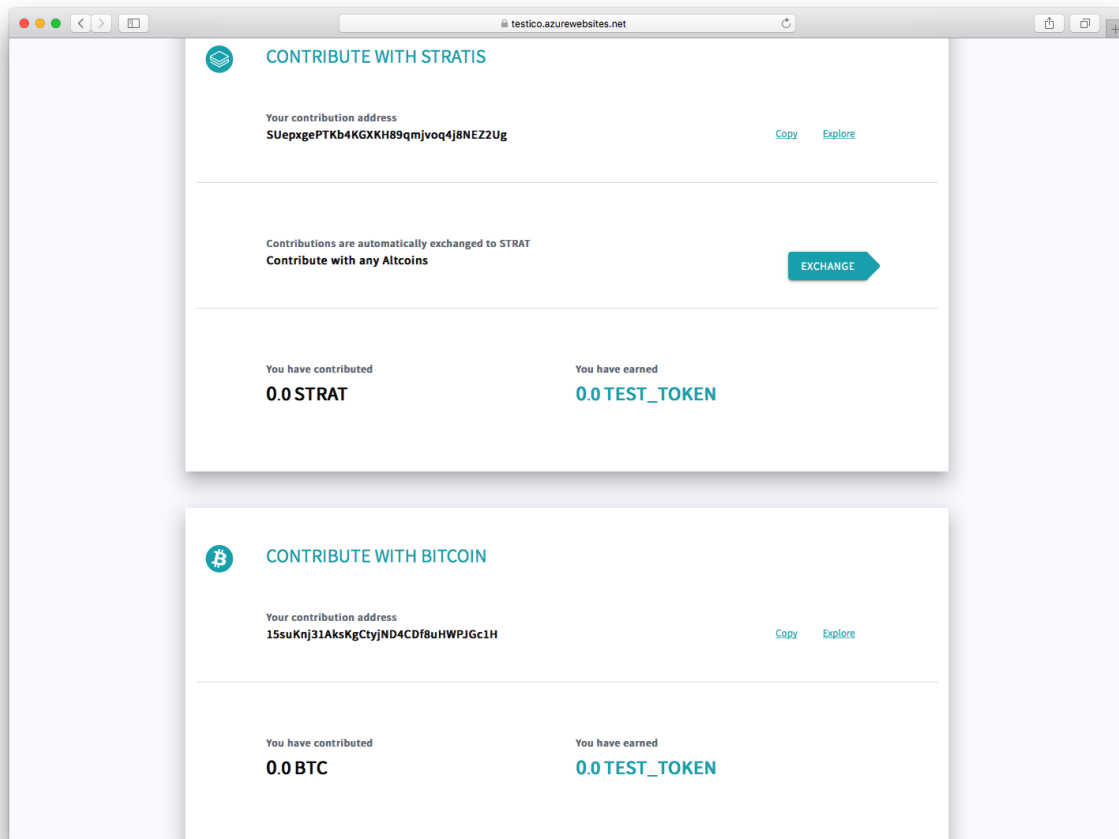

Hooking into a third-party Know Your Customer (KYC) service

The following steps describe how to set up a KYC service:

1. Set the *KYC vendor* field in the *ICO Settings*. Currently, the only vendor the Web Application supports is Onfido. After selecting Onfido, a *Settings* button appears.
2. Click the *Settings* button to display the options for the Onfido KYC service:
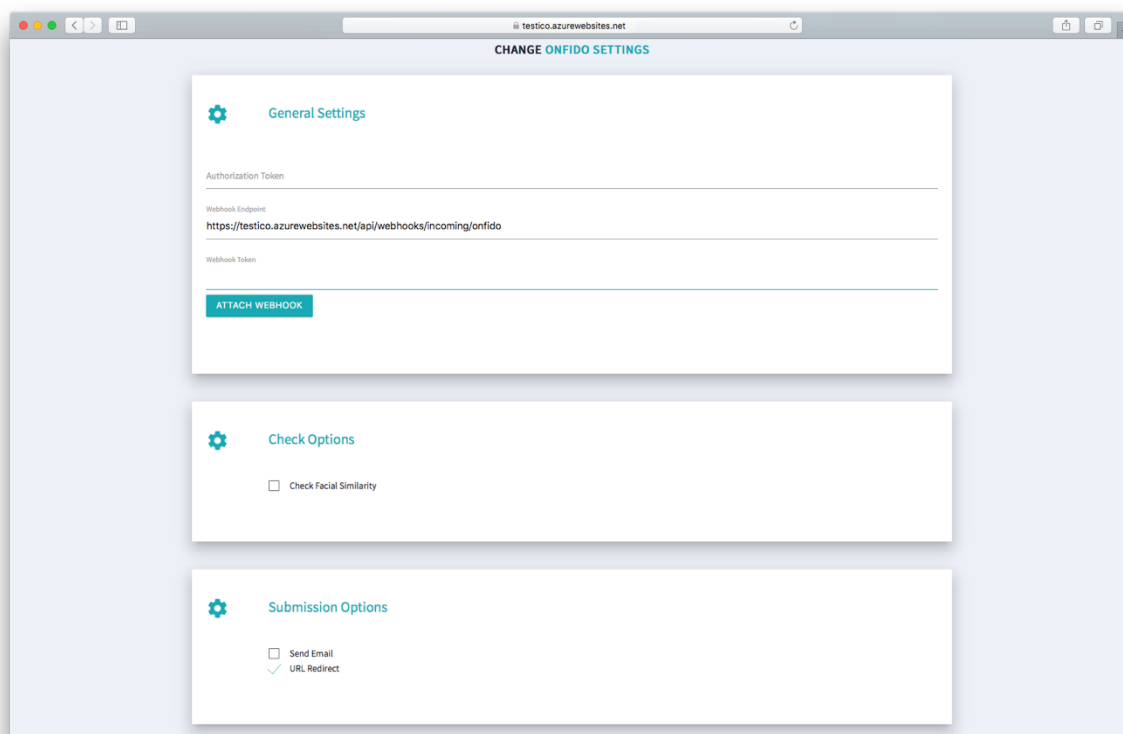
3. You must now obtain an Onfido authorization token. These are the API tokens found on the API -> Tokens page of the Onfido portal:
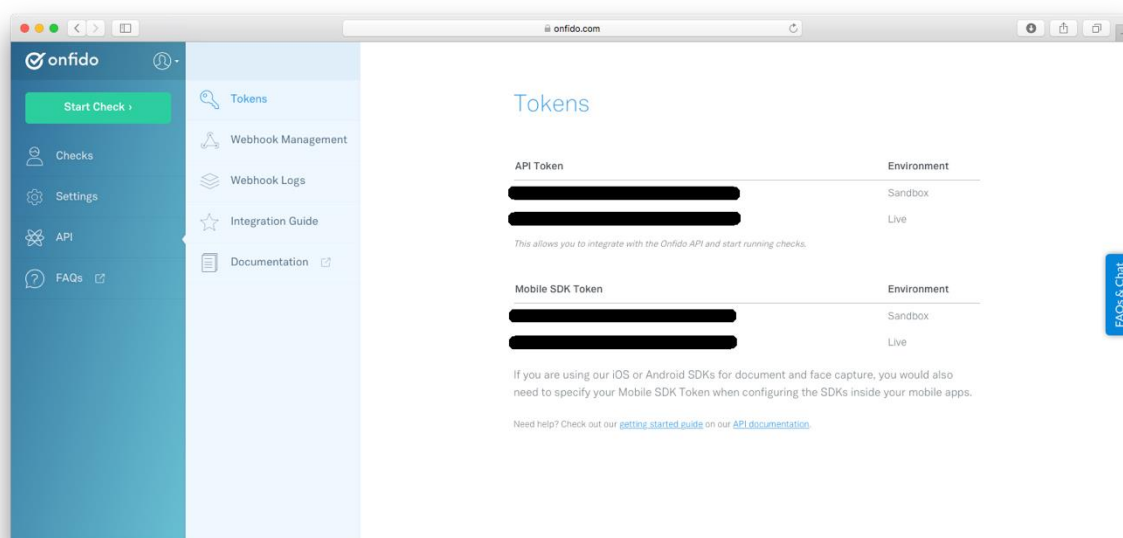

Copy the live authorization token to the *Authorization Token* field in the Web Application's *Onfido Settings*.

4. You must now supply the webhook for the ICO site to Onfido, which enables Onfido to be notified as a user progresses through the ICO site. Go to the API -> Webhook Management page on the Onfido site:
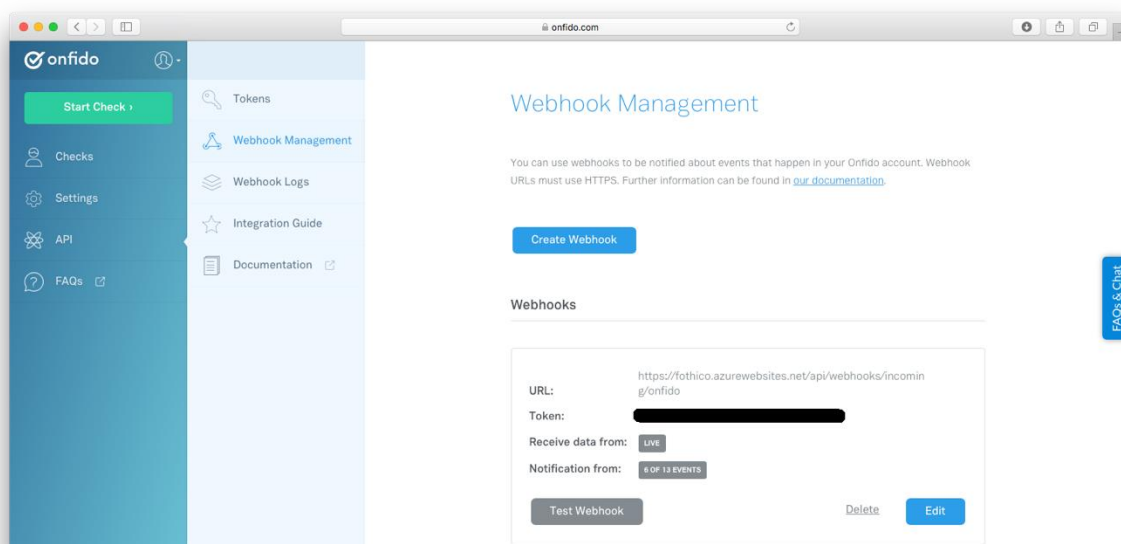
5. Hook your ICO site into Onfido's site using the *Create Webhook* button:
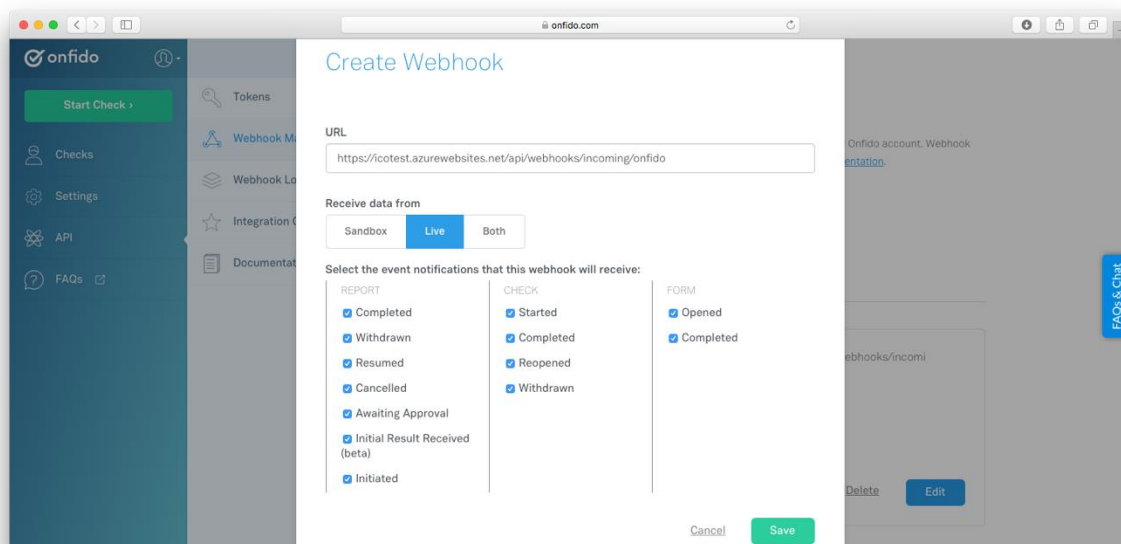
For the *URL* field, specify the URL of your ICO site with the following suffix:

api/webhooks/incoming/onfido

You can copy this URL directly from the *Webhook Endpoint* field in the Web Application *Onfido Settings*.

6. On returning to the API -> Webhook Management page, you should now see your newly generated webhook token:

Version 1.0 ©2018 Stratis Group Ltd. Proprietary and Confidential
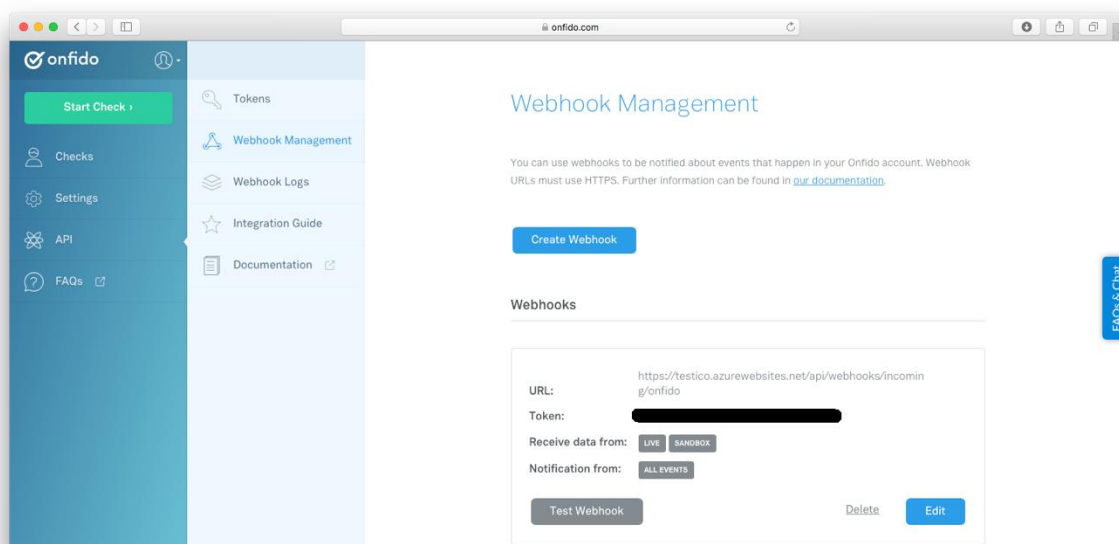
Copy this token to the *Webhook Token* field in the Web Application's *Onfido Settings*. Then click the *Save Changes* button.

7. On the Onfido site, you can now click the *Test Webhook* button to test that your ICO site is correctly linked into Onfido's site. If "Success" is returned, the Onfido site was able to successfully connect to your site.

8. Return to the *Onfido Settings on the Web Application*. The following table details the options provided by the fields there:

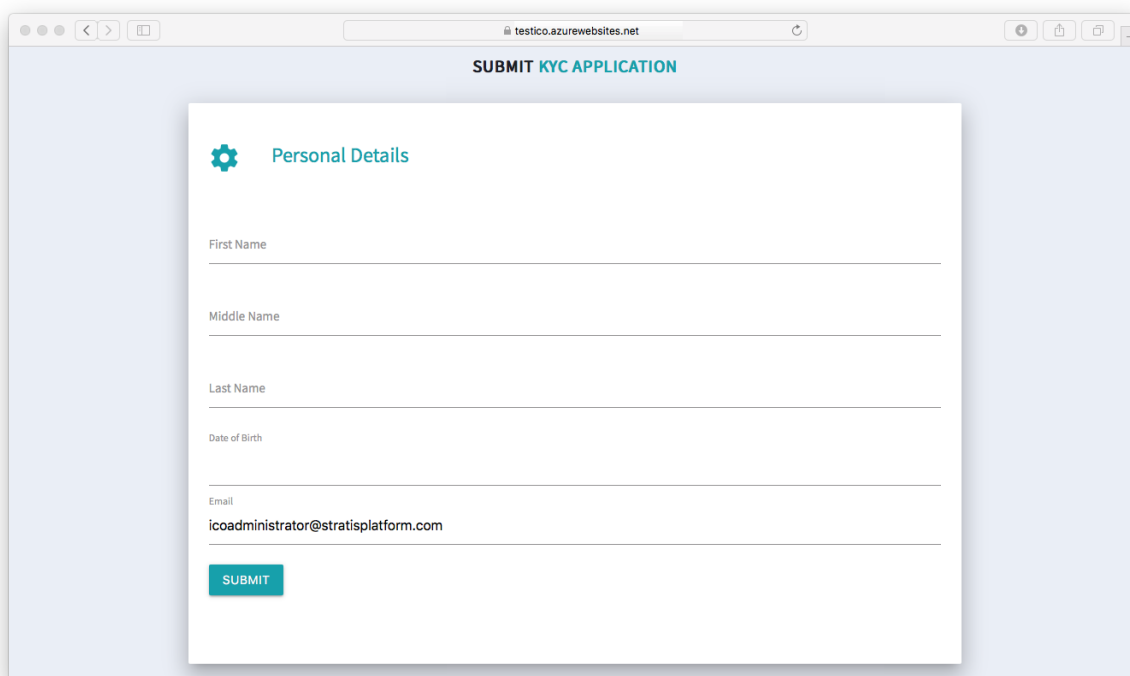| Field	Description
Check Facial Similarity	Check this box if you require Onfido to perform a facial similarity check in addition to the mandatory document and watchlist reports.
Send Email	Check this box if you require an email to be sent to users after they have submitted their applicant information on the ICO platform. This email has a link to a form on the Onfido site where the applicant can complete the verification process by entering the required KYC information.
Url Redirect	Check this box to automatically redirect the browser to the Onfido site after the applicant has submitted their applicant information. On the Onfido site, the applicant can complete the verification process by entering the required KYC information. After the user has completed this, the browser automatically redirects back to the Dashboard page of the Web Application.

Note
It is possible to check both the *Send Email* and *Url Redirect* fields.

9. Click on the *Save Changes* button to save the *Onfido Settings*.

Users will now see the following when they first go to the Dashboard page:
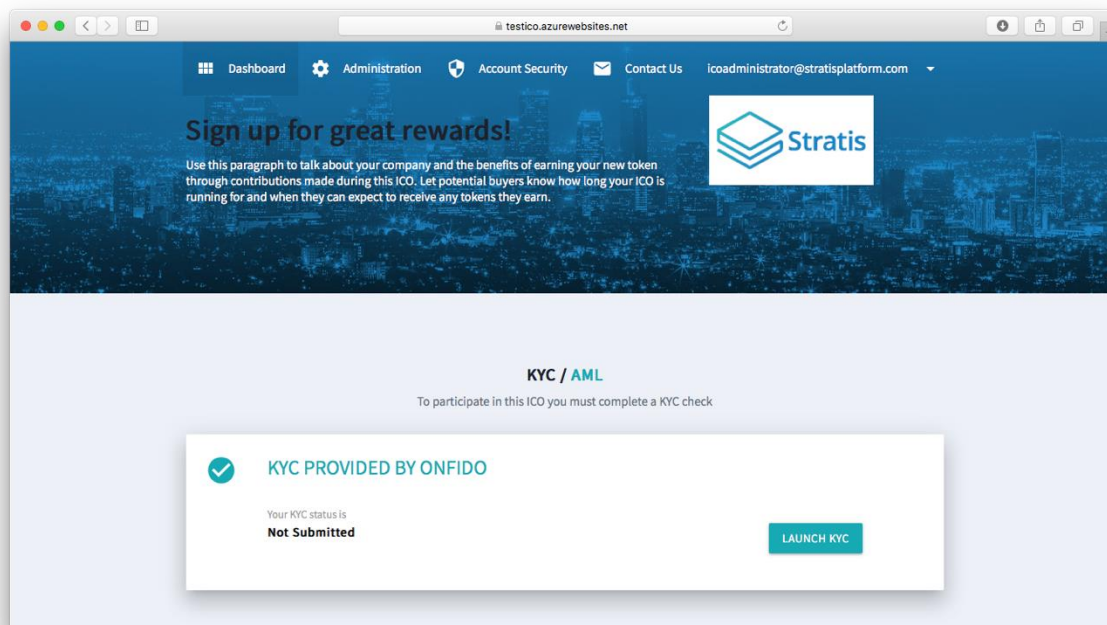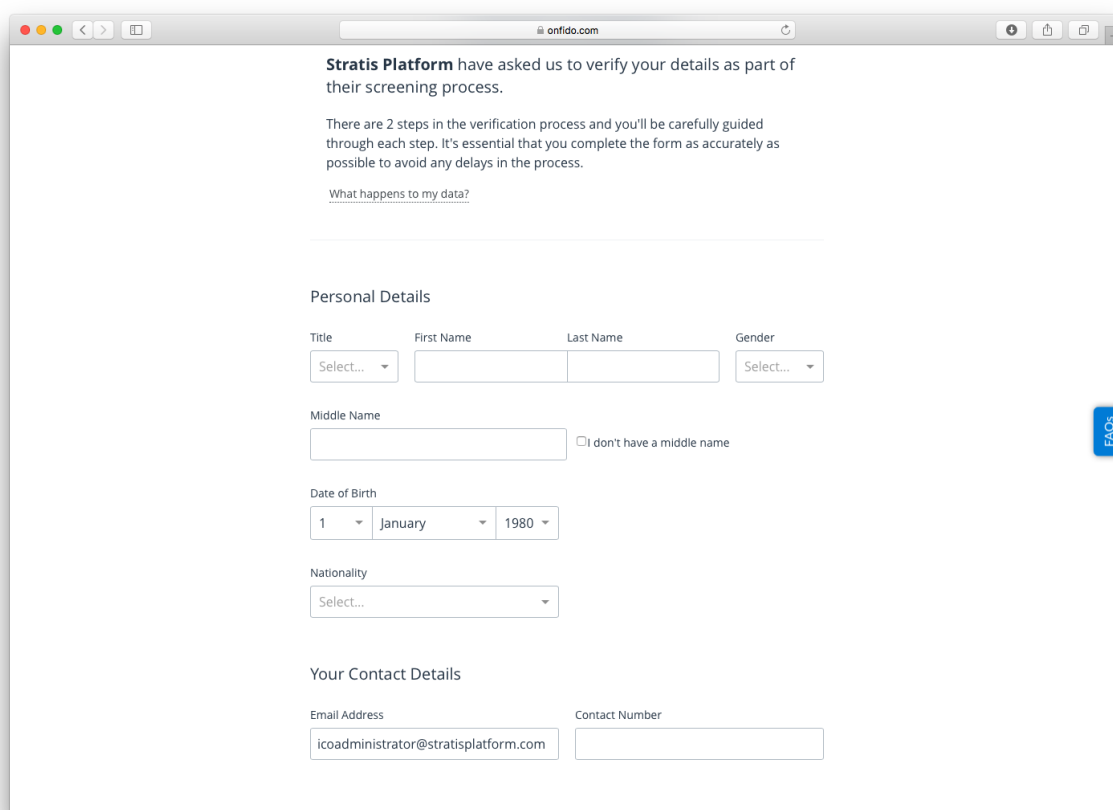

When users click on the *Launch KYC* button, they are prompted to enter their personal information:

On clicking the *Submit* button, users are either redirected to the Onfido site to complete the verification process and/or a link to the Onfido site is sent in an email.

This depends on how the *Submission Options* fields where set. The following figure shows the first page of the verification process on the Onfido site:

The next step involves submitting photographs of your passport or driving license. As the user moves through the Onfido verification process, the status of the KYC application is updated on the Dashboard page:

Clicking the *Check Id* hyperlink navigates to the Verification Process page on the Onfido site. Until verification has been completed, no other information is available on the Dashboard page. Upon verification, the user is free to make contributions on the Dashboard page. The *User Guide* document suggest users click the *ContactUs* link at the top of the Dashboard page if they encounter any difficulties in passing the verification process. These emails are sent to the email address specified by the *Contact Email* field in the *Main Settings*.

> **Note**
> As an administrator, you will also complete the KYC process once you have set it up. This enables you to see the Dashboard in the same way a buyer would.

Configuring the Web Application Part 2

The second stage of configuring the ICO Platform Application is to set:

1. The start date of the ICO.

2. The hard cap for BTC.
3. The hard cap for your own tokens.
4. The token sale periods.

Setting the start date of the ICO

The exact time you launch your ICO might depend on economic factors such as the price of BTC and STRAT. The configuration options detailed in this section allow you to set up the ICO in the way which is most beneficial to your company.

Use the *ICO Start Date* field from the *ICO Settings* to define the start date.

Setting the hard caps for the ICO

The hard cap for BTC is locked to 400 BTC. This means users can no longer contribute in BTC once 400 BTC have been contributed.

You can also set a hard cap for your own tokens. If the hard cap for your own token is reached, the ICO ends at that point regardless of the setting of the sale period/s. Specify a value of 0 to allow an unlimited amount of your own tokens to be earned via buyer contributions.

The following figure shows the fields for the Hard Caps on the Administration page:
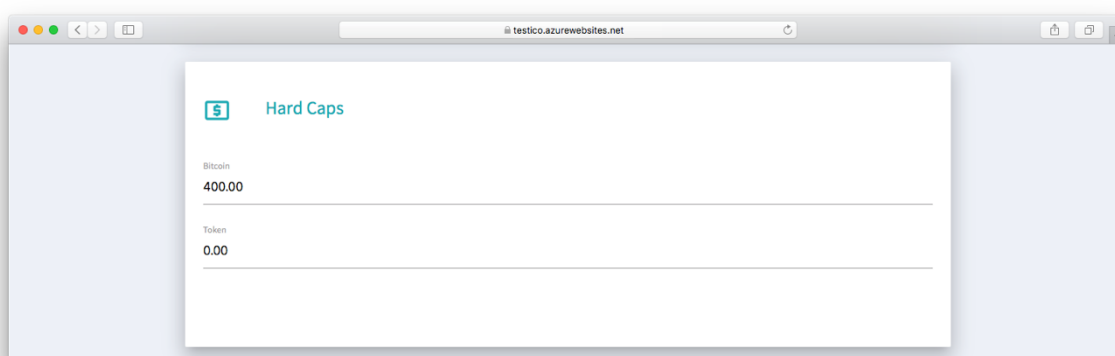
Setting the token sale periods

Token sale periods allow you to set different prices for your tokens during different periods in the ICO. The end date of the last token sale period marks the end of the ICO.

The following figure shows the fields for the Token Sale Periods on the Administration page:
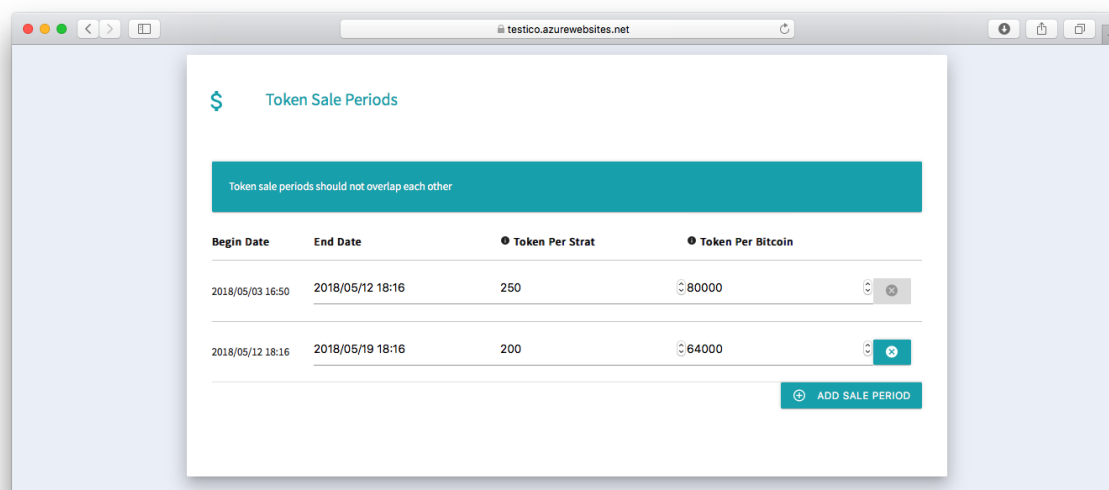
Use the buttons to add new token sale periods and to delete any that you no longer require.

Important!
Token sale periods should not overlap each other. The Web Application displays a warning if it detects that any sales period overlaps another.

In the previous figure two token sale periods have been defined. The price for tokens is more expensive in the second week than the first week, which should incentivise buyers to contribute as soon as possible.

Integrating the Web Application

To fully integrate the Web Application with your company website, you must access your domain registrar and create a new CNAME DNS record, which resolves to your deployment of the Web Application. More information on this is available [here](#) including information on how to validate the CNAME you provide.

Important!
Creating an A record is not recommended because these records resolve to an IP address. Azure may change the IP address of your Web Application at any time, and an A record becomes invalid in this situation.

The next step is to tell potential buyers where they can find the Web Application as part of your overall marketing strategy for your ICO. Your ICO will begin based on the start date you provided during [Configuring the Web Application Part 2](#).