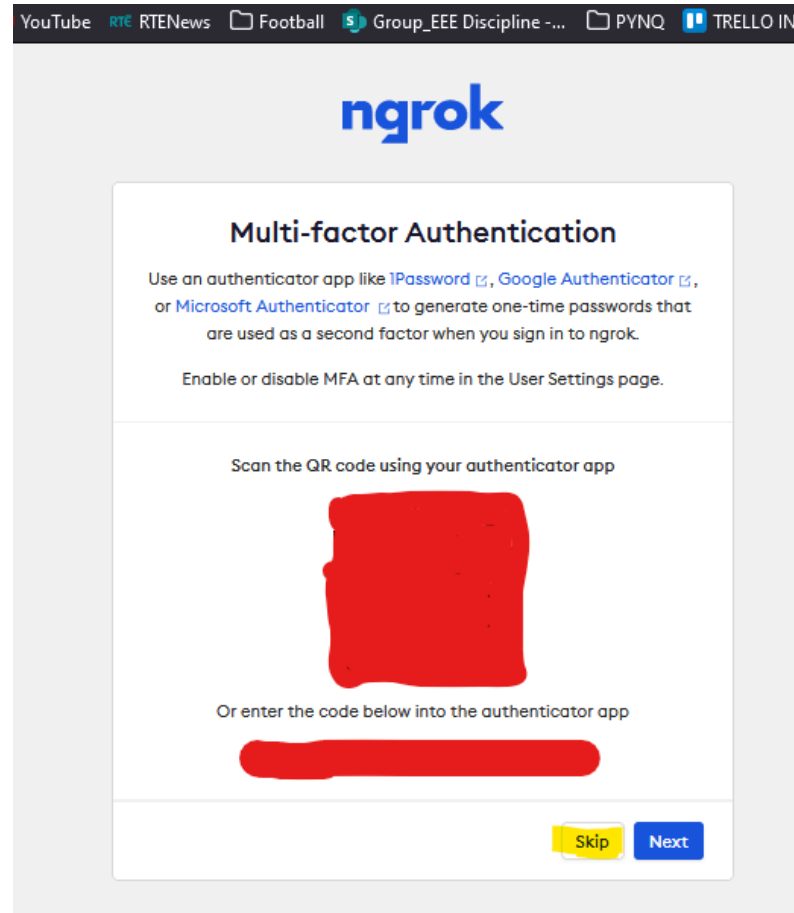
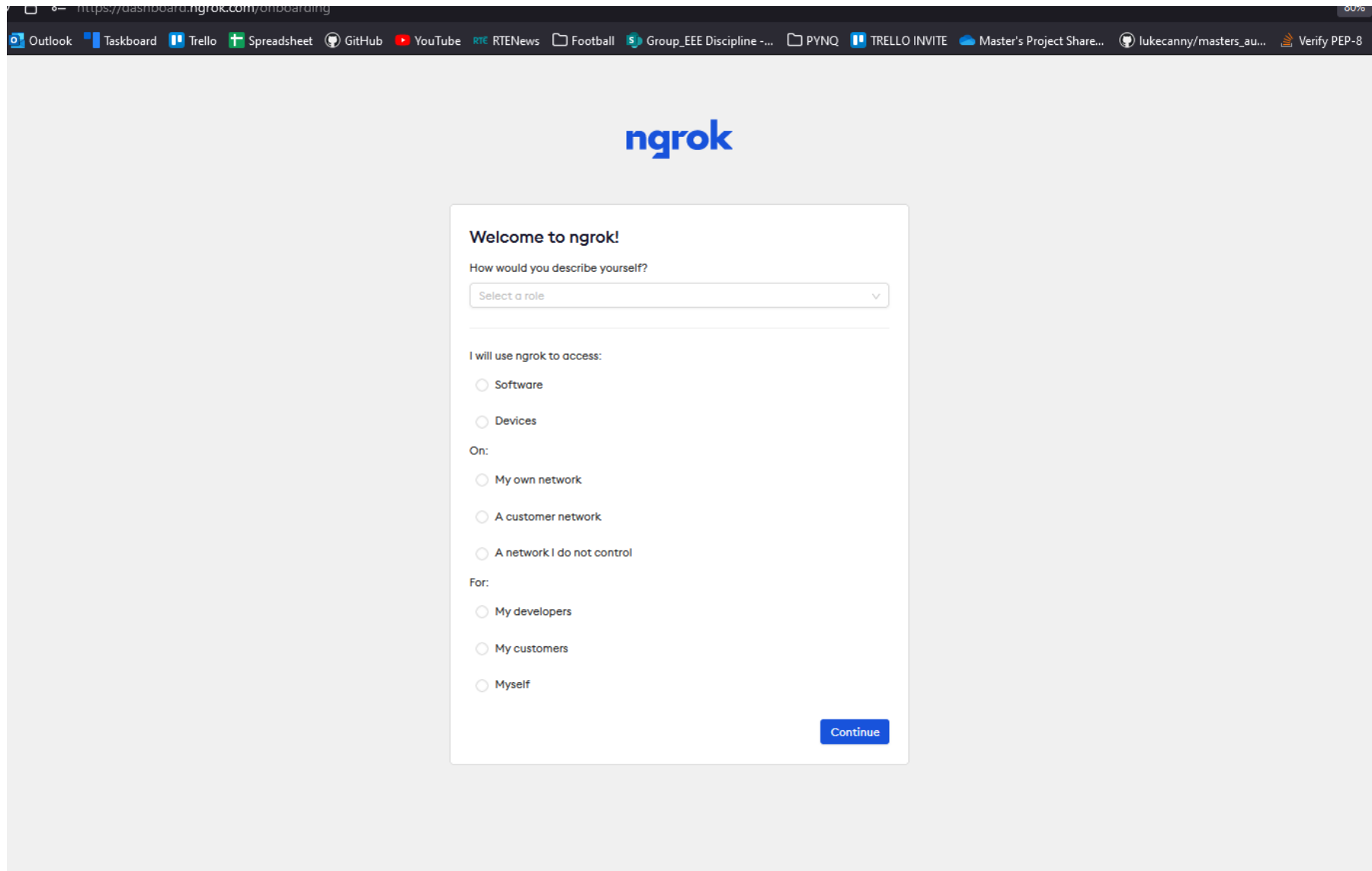


# Creating and Configuring an Account at [ngrok.com](https://ngrok.com)

# Create account – Click link sent by email- Skip 2FA



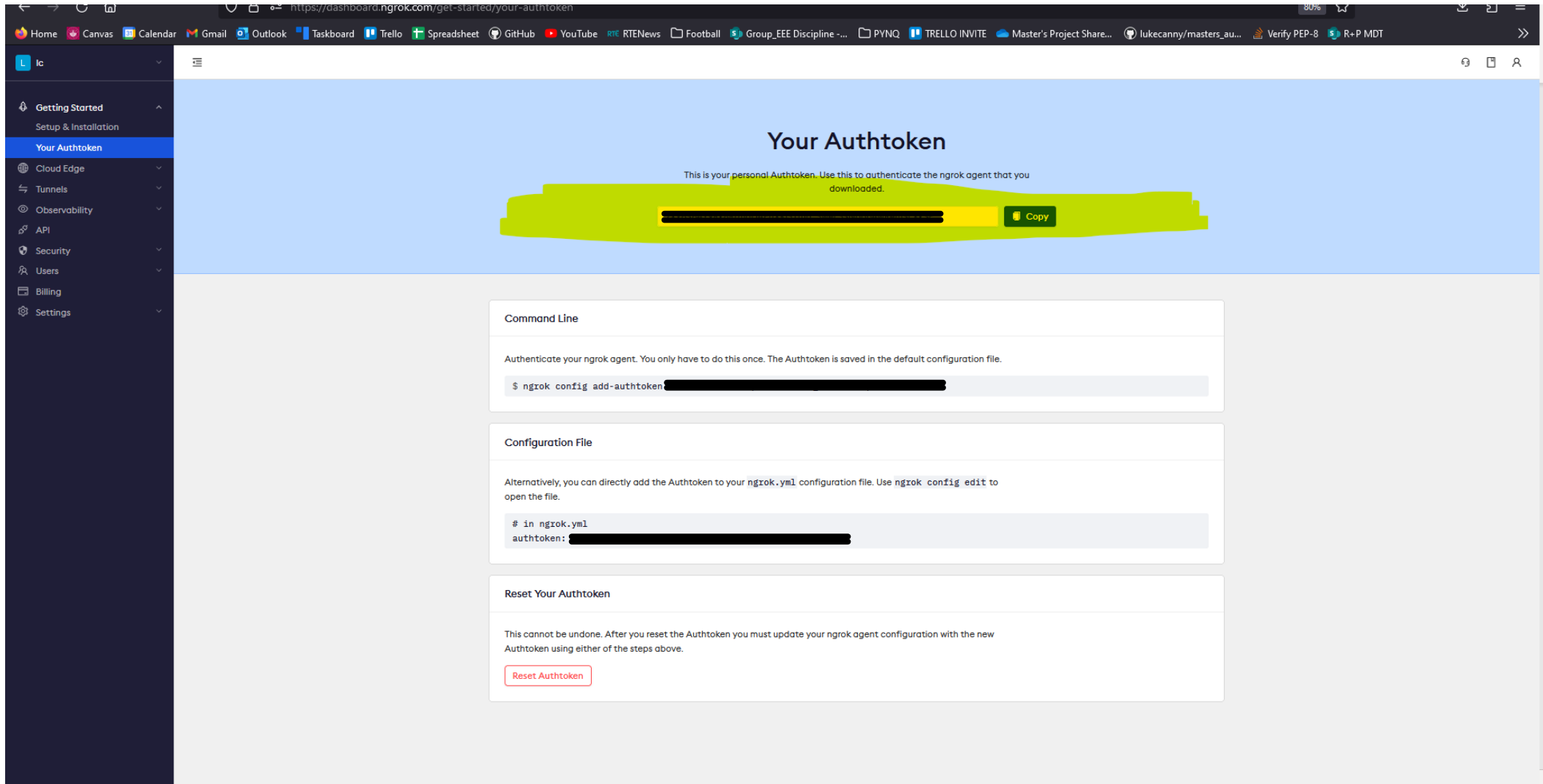
# Doesn't need to be filled out, just continue



The screenshot shows a web browser window with the URL `https://dashboard.ngrok.com/onboarding`. The browser's tab bar includes Outlook, Taskboard, Trello, Spreadsheet, GitHub, YouTube, RTE RTENews, Football, Group\_EEE Discipline ~..., PYNQ, TRELLO INVITE, Master's Project Share..., lukecanny/masters\_au..., and Verify PEP-8. The main content area features the Ngrok logo at the top. Below the logo is a white onboarding form titled "Welcome to ngrok!". The form contains the following sections:

- How would you describe yourself?**: A dropdown menu with the placeholder text "Select a role".
- I will use ngrok to access:**: Two radio button options: "Software" and "Devices".
- On:**: Three radio button options: "My own network", "A customer network", and "A network I do not control".
- For:**: Three radio button options: "My developers", "My customers", and "Myself".
- Continue**: A blue button at the bottom right of the form.

# Click on “Your Authtoken” on top left and make note of auth token



The screenshot shows the Ngrok dashboard at the URL `https://dashboard.ngrok.com/get-started/your-authtoken`. The left sidebar contains a navigation menu with the following items: Home, Canvas, Calendar, Gmail, Outlook, Taskboard, Trello, Spreadsheet, GitHub, YouTube, RTN News, Football, Group\_EEE Discipline, PYNQ, TRELLO INVITE, Master's Project Share, lukecanny/masters\_au..., Verify PEP-8, and R+P MDT. The main content area has a light blue header with the title "Your Authtoken". Below the header, a message states: "This is your personal Authtoken. Use this to authenticate the ngrok agent that you downloaded." A large, redacted auth token is displayed, followed by a green "Copy" button. Below this, there are three sections: "Command Line" with instructions to authenticate the ngrok agent and a code block showing `$ ngrok config add-authtoken` followed by the redacted token; "Configuration File" with instructions to add the token to the `ngrok.yml` file and a code block showing `# in ngrok.yml` and `authtoken:` followed by the redacted token; and "Reset Your Authtoken" with a warning that this action cannot be undone and a red "Reset Authtoken" button.

**Your Authtoken**

This is your personal Authtoken. Use this to authenticate the ngrok agent that you downloaded.

`[Redacted Authtoken]` [Copy](#)

**Command Line**

Authenticate your ngrok agent. You only have to do this once. The Authtoken is saved in the default configuration file.

```
$ ngrok config add-authtoken [Redacted Authtoken]
```

**Configuration File**

Alternatively, you can directly add the Authtoken to your `ngrok.yml` configuration file. Use `ngrok config edit` to open the file.

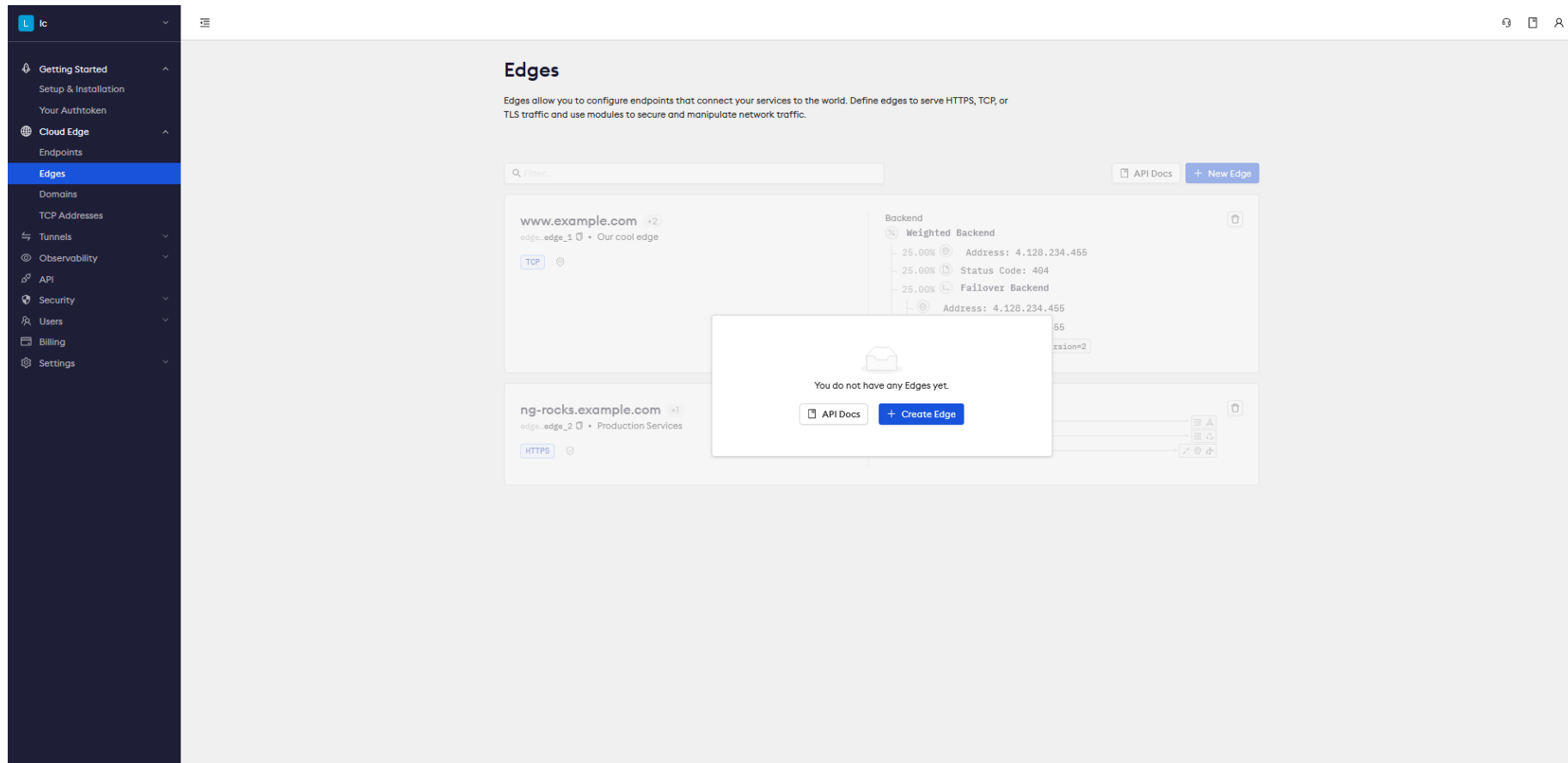
```
# in ngrok.yml
authtoken: [Redacted Authtoken]
```

**Reset Your Authtoken**

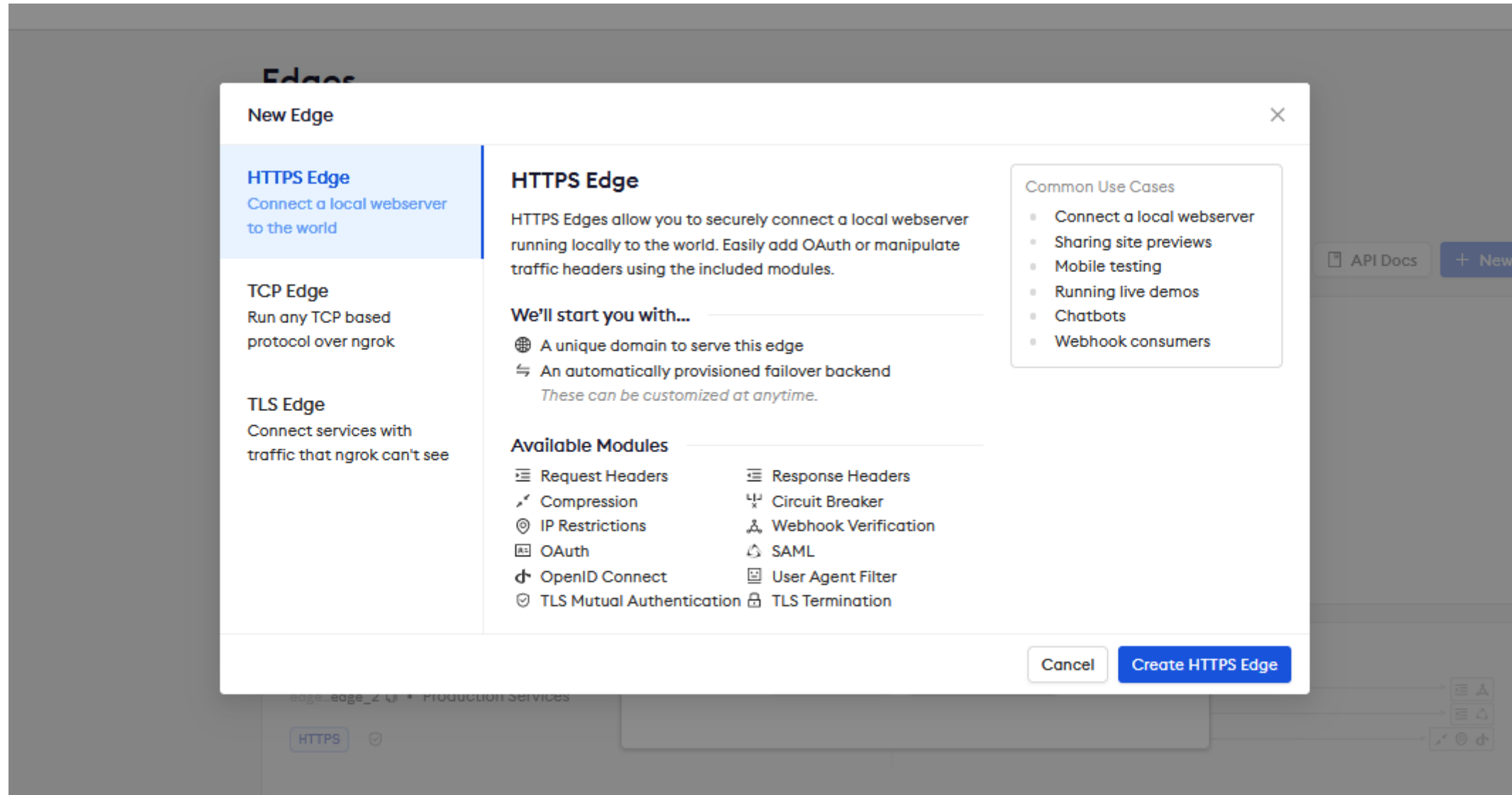
This cannot be undone. After you reset the Authtoken you must update your ngrok agent configuration with the new Authtoken using either of the steps above.

[Reset Authtoken](#)

# Next under “Cloud Edge” select “Edges” – Click “Create Edge”



# Choose HTTPS Edge



# Take note of the edge label AND the endpoint web address

The screenshot displays the Ngrok dashboard interface. At the top, a navigation bar shows a back arrow, the protocol 'HTTPS', a link to 'no description', and a 'Save' button. Below this, a status bar indicates 'edgths\_ZPKnS7' was created less than a minute ago with 0 bytes of metadata.

A yellow banner at the top of the main content area reads: 'Congrats! You've got a spot on the internet. Start a Tunnel to serve your web app at the primary URL: capable-outgoing-sloth.ngrok-free.app'. A 'Start a Tunnel' button is located on the right of this banner.

The 'Endpoints' section shows a single endpoint: 'https://capable-outgoing-sloth.ngrok-free.app'. A 'Manage Endpoints' link is on the right.

The 'Routes' section is active, showing a list of modules on the left: Overview, Selector, Backend, Mutual TLS, TLS, Circuit Breaker, Compression, IP Restrictions, OAuth, OIDC, Request Headers, Response Headers, SAML, and Webhook Verification.

The 'Traffic' tab is selected, displaying the following configuration:

- Status:** No tunnels with labels matching 'edge=edgths\_2XsByGdzAidHFBjk4aRnbZPKnS7' are online. Buttons for 'Start a Tunnel' and 'Refresh' are present.
- Selector:** '/'
- Backend:** 'Failover Backend' with a single backend entry 'edge=edgths\_2XsByGdzAidHFBjk4aRnbZPKnS7' and a status code of 404.

The 'Add Modules' section is expanded, showing two categories:

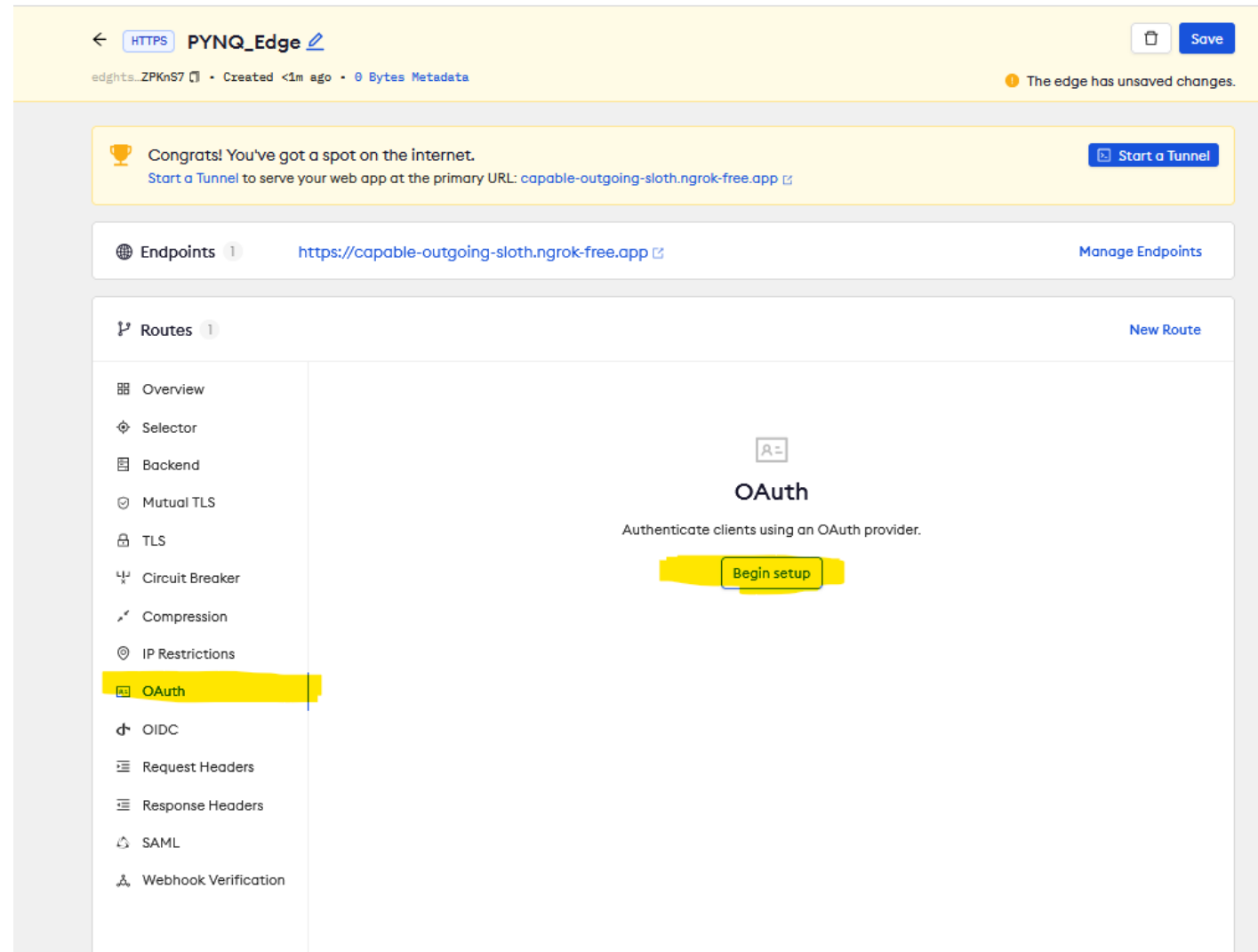
- Security:** Secure traffic through your Edge by adding these modules. Options include 'Add Mutual TLS', 'Add IP Restrictions', and 'Add Webhook Verification'.
- SSO:** Ensure only authenticated users can access your Edge. Options include 'Add OAuth', 'Add OIDC', and 'Add SAML'.

# Rename edge to “PYNQ\_Edge” and hit save

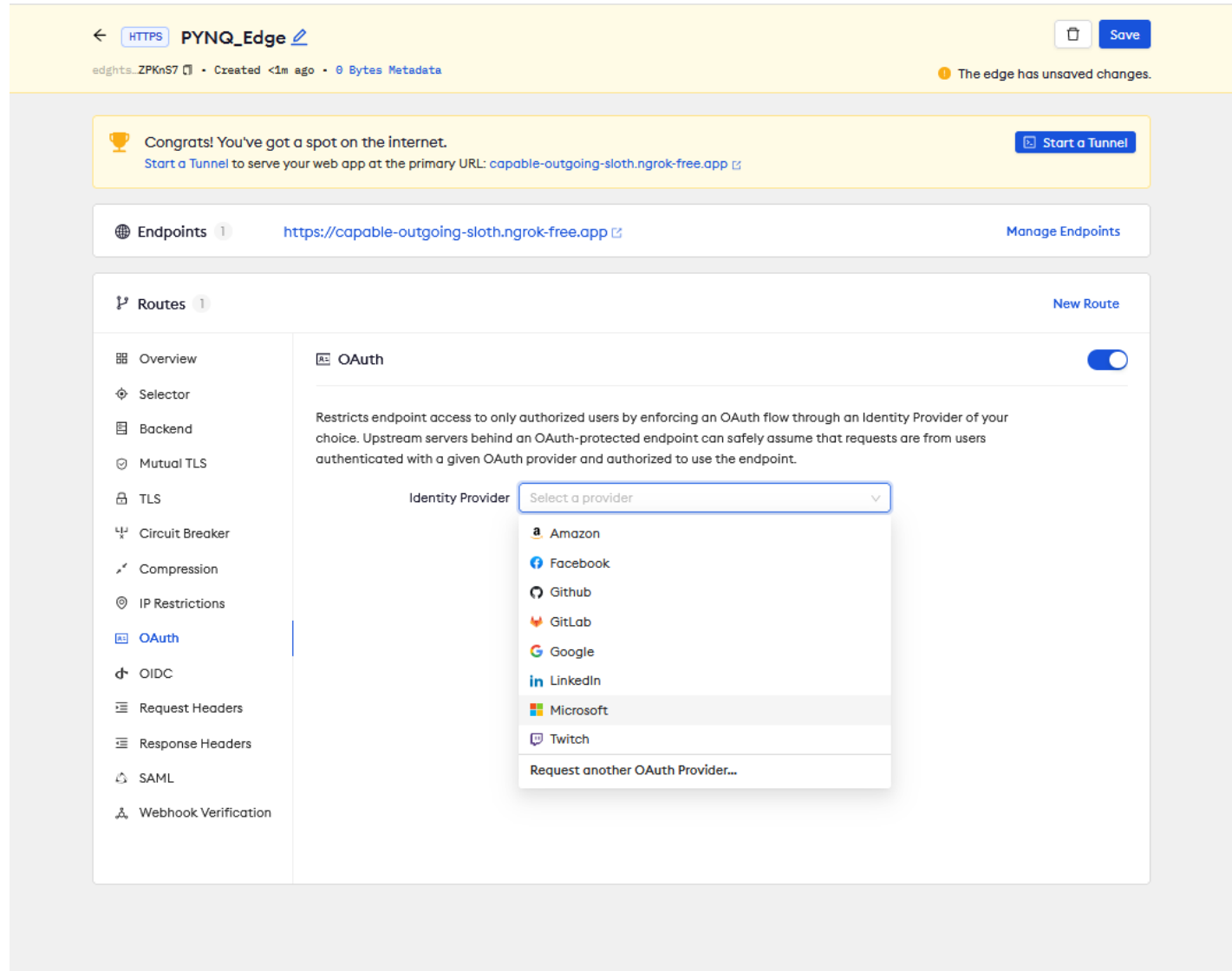
The screenshot shows the Ngrok dashboard interface. At the top, the breadcrumb navigation shows 'HTTPS' and 'PYNQ\_Edge' with an edit icon. Below this, it says 'edghts\_ZPKnS7' and 'Created <1m ago • 0 Bytes Metadata'. A notification on the right states 'The edge has unsaved changes.' with a 'Save' button. A yellow banner at the top says 'Congrats! You've got a spot on the internet. Start a Tunnel to serve your web app at the primary URL: capable-outgoing-sloth.ngrok-free.app'. Below this, the 'Endpoints' section shows a single endpoint 'https://capable-outgoing-sloth.ngrok-free.app' with a 'Manage Endpoints' link. The 'Routes' section shows a single route with a 'New Route' link. On the left, a sidebar lists various configuration options: Overview, Selector, Backend, Mutual TLS, TLS, Circuit Breaker, Compression, IP Restrictions, OAuth, OIDC, Request Headers, Response Headers, SAML, and Webhook Verification. The main content area is divided into three sections: 'Traffic', 'Add Modules', and 'Security'. The 'Traffic' section shows the status 'No tunnels with labels matching edge=edghts\_2XcByGDzAidHFBjk4wRNbZPKnS7 are online.' with 'Start a Tunnel' and 'Refresh' buttons. It also shows the selector '/' and the backend 'Failover Backend' with a status code of 404. The 'Add Modules' section is currently empty. The 'Security' section provides instructions on how to secure traffic and lists modules to add: Add Mutual TLS, Add IP Restrictions, Add Webhook Verification, Add OAuth, Add OIDC, and Add SAML.



# To set up OAuth – Click OAuth on LHS and click begin set up



Select the provider (I will choose Microsoft, although you can decide. This is how users will authenticate. Same as how Microsoft login used on Canvas/Blackboard)



Set either the specific email addresses OR email domain that is allowed to access your board. The college's domain should suffice – i.e. only logins with @universityofgalway.ie are allowed. – remember to click save

The screenshot shows the PYNQ\_Edge configuration interface. The top bar includes a back arrow, the URL 'HTTPS PYNQ\_Edge', a 'Save' button, and a notification 'The edge has unsaved changes.' The left sidebar lists various configuration options: Selector, Backend, Mutual TLS, TLS, Circuit Breaker, Compression, IP Restrictions, OAuth (selected), OIDC, Request Headers, Response Headers, SAML, and Webhook Verification. The main content area is divided into sections: 'Restricts endpoint access to only authorized users by enforcing an OAuth flow through an Identity Provider of your choice. Upstream servers behind an OAuth-protected endpoint can safely assume that requests are from users authenticated with a given OAuth provider and authorized to use the endpoint.' The 'Identity Provider' is set to 'Microsoft'. The 'Application' section has 'OAuth Application' set to 'Use an ngrok-managed OAuth application.' The 'Authorization' section has 'Authorization Rules' set to 'Restrict access to users that both authenticate and match a given set of rules'. Under 'Email Addresses', the value 'l.canny3@universityofgalway.ie' is entered. Under 'Email Domains', the value 'universityofgalway.ie' is entered. The 'Scopes' section has 'User.Read' selected. The 'Session' section is currently empty.

edgths.ZPKnS7 [i] • Created <1m ago • 0 Bytes Metadata

The edge has unsaved changes.

Selector

Backend

Mutual TLS

TLS

Circuit Breaker

Compression

IP Restrictions

**OAuth**

OIDC

Request Headers

Response Headers

SAML

Webhook Verification

Restricts endpoint access to only authorized users by enforcing an OAuth flow through an Identity Provider of your choice. Upstream servers behind an OAuth-protected endpoint can safely assume that requests are from users authenticated with a given OAuth provider and authorized to use the endpoint.

Identity Provider Microsoft

Application

OAuth Application ☒ Use an ngrok-managed OAuth application.  
☐ Use my own OAuth application  
ngrok managed OAuth applications have [restrictions](#) to prevent abuse

Authorization

Authorization Rules ☐ Any user who successfully logs in with Microsoft will be allowed  
☒ Restrict access to users that both authenticate and match a given set of rules  
ngrok managed OAuth requires that you specify at least 1 email address or 1 email domain

Email Addresses l.canny3@universityofgalway.ie

Each email address listed here is allowed access. Adds the `User.Read` scope.

Email Domains universityofgalway.ie

Every user whose email address ends with one of the domains listed here are allowed access. Adds the `User.Read` scope.

[Advanced Options](#)

Scopes

Scopes User.Read

The requested set of permissions you'd like to ask for from the identity provider. You can find the available scopes for Microsoft [here](#).

Session

# That is all!

- You should now have your
  - Authtoken
  - Edge Label (edge=abcdef123456)
  - Ngrok URL

All of which will be needed by the PYNQ board

# Additional Information/Understanding

- The authtoken is used by the ngrok client on the PYNQ board to authenticate the user (i.e. login to your ngrok account on the PYNQ)
- The edge label is used to tell ngrok what endpoint will be used by the ngrok client, the endpoint means the URL that will become active and available online.
- Finally, the ngrok URL is what you will use in your browser to access the pynq board remotely (more specifically the JNB web interface)