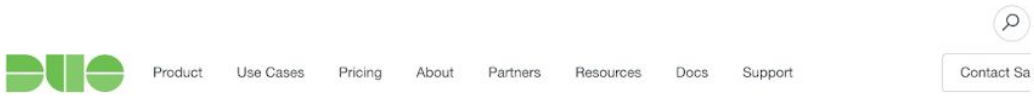
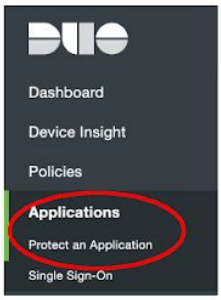
### Duo Multi-Factor Authentication

In order to set up **Duo Multi-Factor Authentication** with the rXg, you will need to login to your Duo account, or create a new account at https://duo.com/

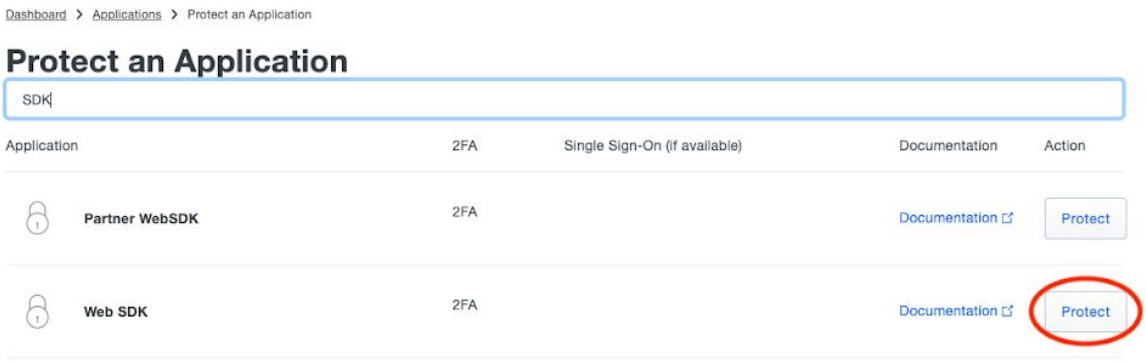



Once you are logged into the admin panel (https://admin.duosecurity.com/), you will need create a new Application to protect, and retreive your Integration Key, Secret Key and API Hostname to be entered into the corresponding fields in the rXg.

To do so, click on the applications link on the Duo Dashboard, and then on "Protect an Application".




Next, search for the term "SDK" and click the **Protect** button for the **Web SDK** Application.




Copy the fields in the Application details to the appropriate fields in the rXg


Select the admin roles for which Multi-Factor Authentication should be enforced.

Multi-Factor Authentication may optionally be applied to SSH access. If **MFA for SSH** is enabled in the admin role, the admin may log into the rXg via SSH by providing a public key OR providing a valid username and password combination. When providing a username and password, a push notification will be sent to the mobile device, or the admin may register by visiting a generated URL (if the Duo application policy allows it).

To configure Duo for SSH navigate to System-->Admins and edit the Administrative Role for which you would like to enable MFA for SSH.