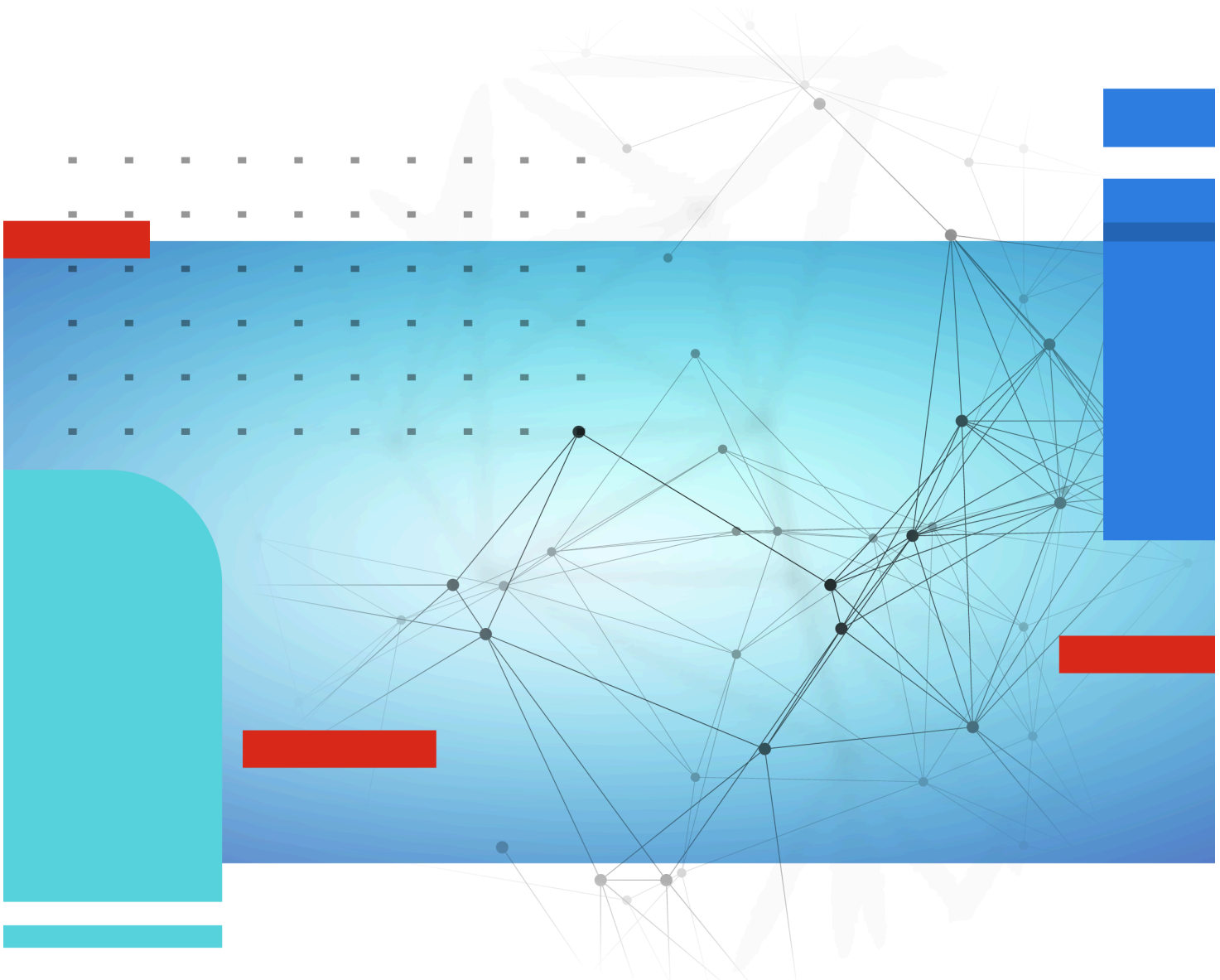
FortiCASB-SSPM Application Connector

Duo Security Connector



Duo Security Connector

Category

- IAM

Connection Method

- API Token
- Service Account

Supported SSOs for connection

- Okta
- Azure
- OneLogin
- Google
- JumpCloud

Data Collected

- Misconfigurations
- 3rd Party Applications
- Identities

Integration Guide

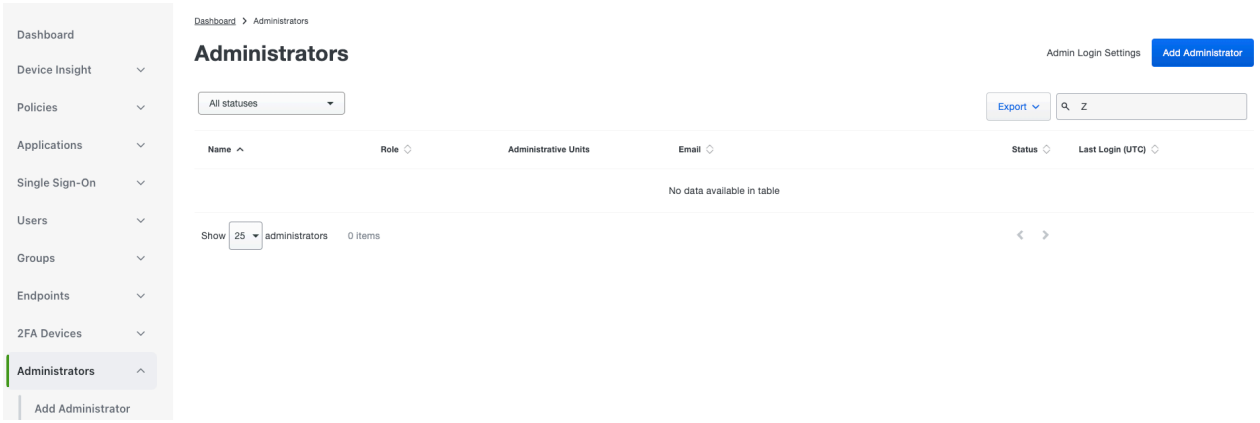
Intro

Use this guide to add Duo Security as a secured SaaS application in FortiCASB-SSPM SaaS Security platform.

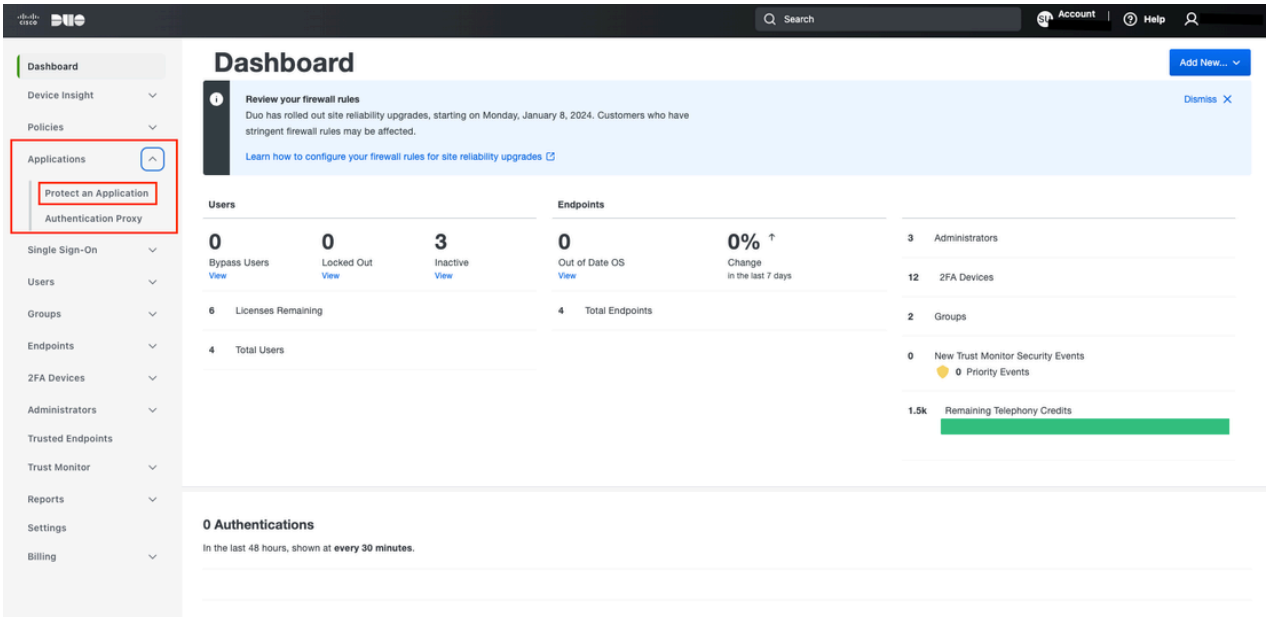
Part A: Preparing the Duo Security Admin user and Admin API

1. Log-in to Due Security admin console with your Owner account (**Owner is only used for initial setup**).
2. Create a dedicated Administrator user account for the integration:

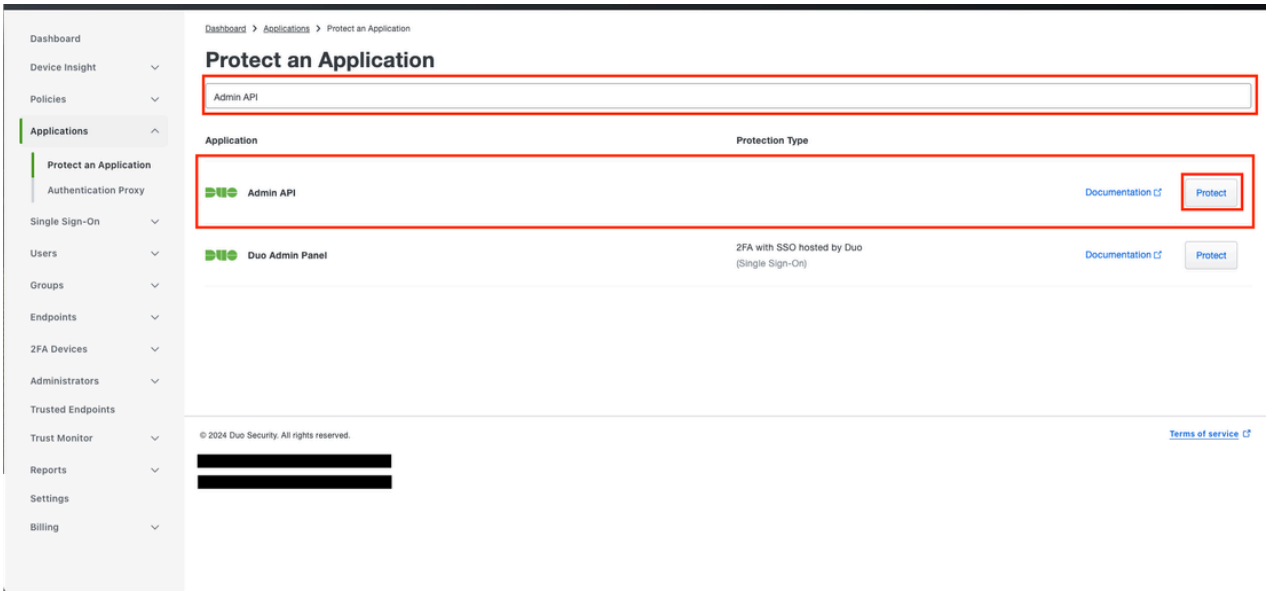
Navigate to Administrators, then click on Add Administrator



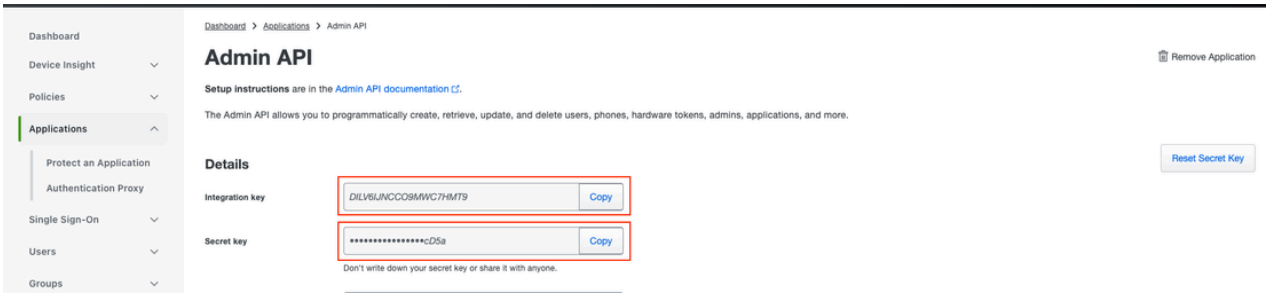
3. Next, need to create an "**Admin API**"
4. Go to "Applications" in the menu - Click on "Protect an Application"
5. If "Admin API" exists and you want to reuse it then select it OR you can create a new dedicated Admin API with a new name



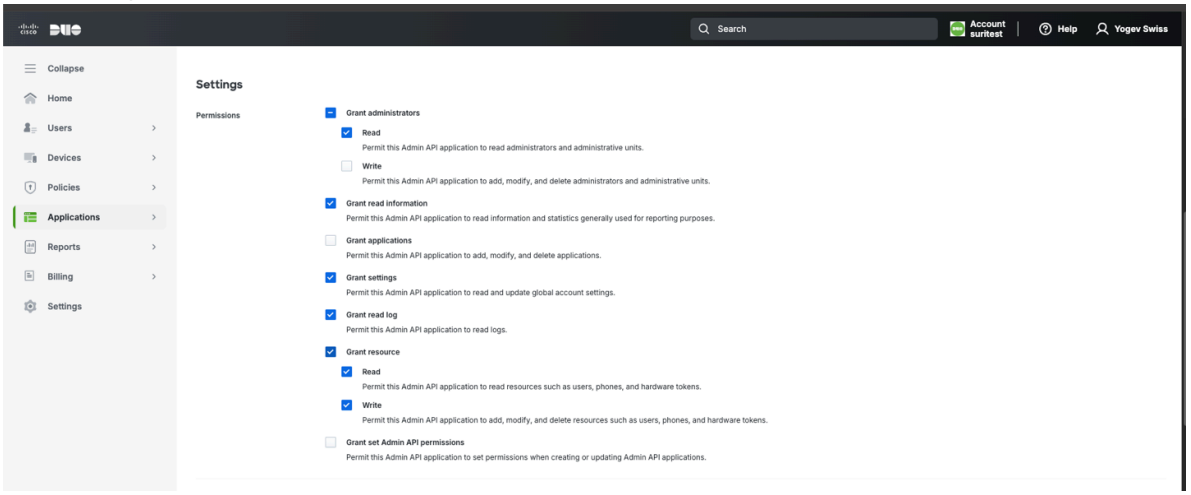
6. Search for "Admin API" and click on "Protect"



7. Copy the Integration Key and Secret Key, they will be required for theintegration



8. Under the "Settings" section, ensure the following permissions are selected:
    - Grant Administrator
    - Grant read information
    - Grant read resource
    - Grant Setting
    - Grant write resource - Required for the initial Hardware Token creation, will be removed after initial setup

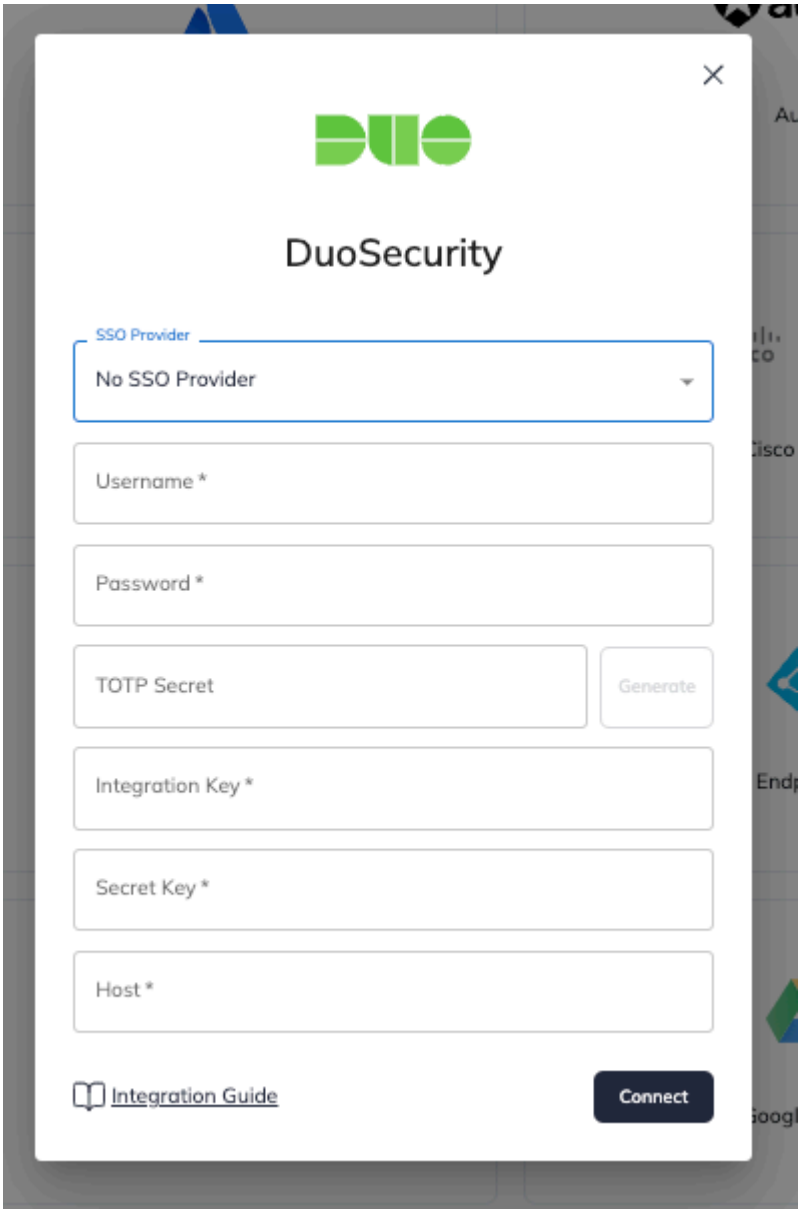


9. Save Changes

> **Note**
>
> Please note, do not log out of your Duo Owner Account just yet, you will need to return here to complete 2 final steps AFTER completing the configuration of the Duo Security application integration in FortiCASB-SSPM (Part C in the guide).

Part B: Connecting Duo Security

1. Navigate to the App Store > Click on Duo Security

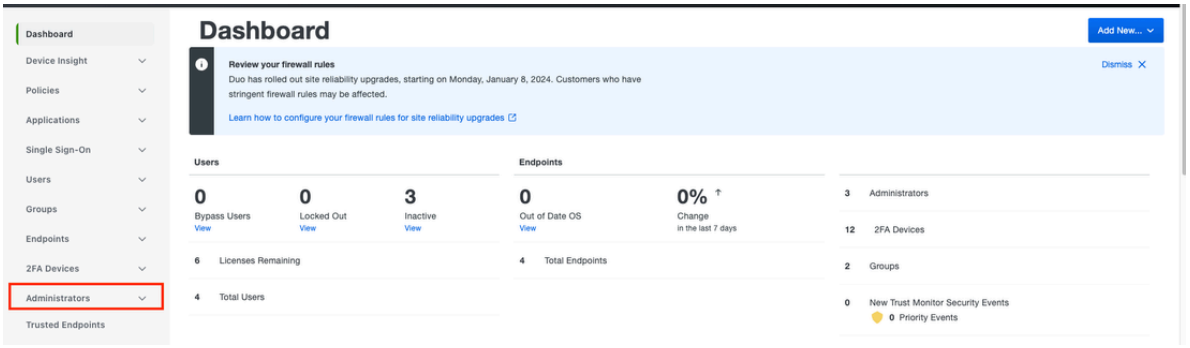


2. Provide all the following information:
    - **Username / Password / TOTP Secret -** Enter the credentials of the dedicated *Admin service account* created in Part A (If you're using SSO provide the credentials of the SSO account).
    - **Integration Key and Secret Key -** Enter the information from the Admin API creation (Step 7 under Part A).
    - **Host -** Copy from the Admin portal URL. Enter only the text that comes between the "admin-{HOST}.duosecurity.com".
      For example : "admin-host1234.duosecurity.com" > **host1234**
3. Click "Connect"

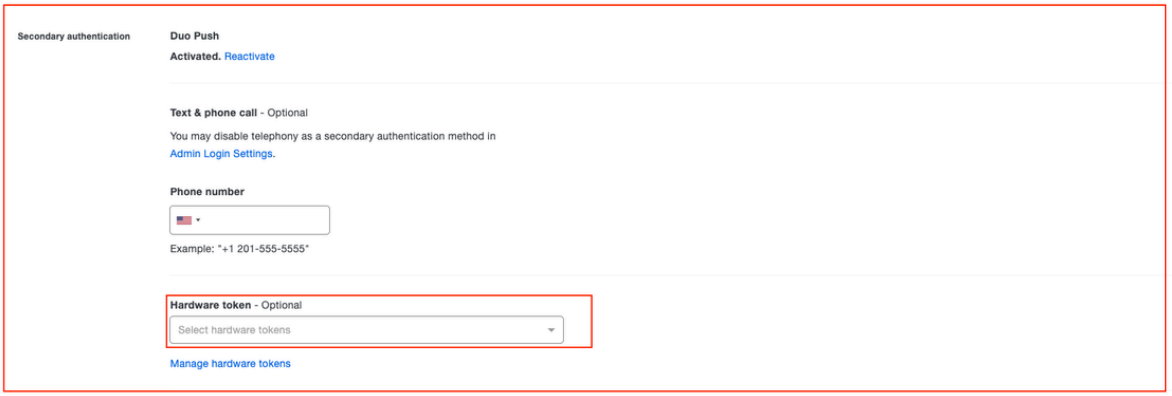
Part C: Return to the Duo admin Console (logged in with your OWNER account)

1. Remove the "Write" permission from the Admin API :
   Admin API > Grant Resource > Uncheck "Write".
   All other permissions remain.
2. Connect the "Hardware Token" to the Admin service account:

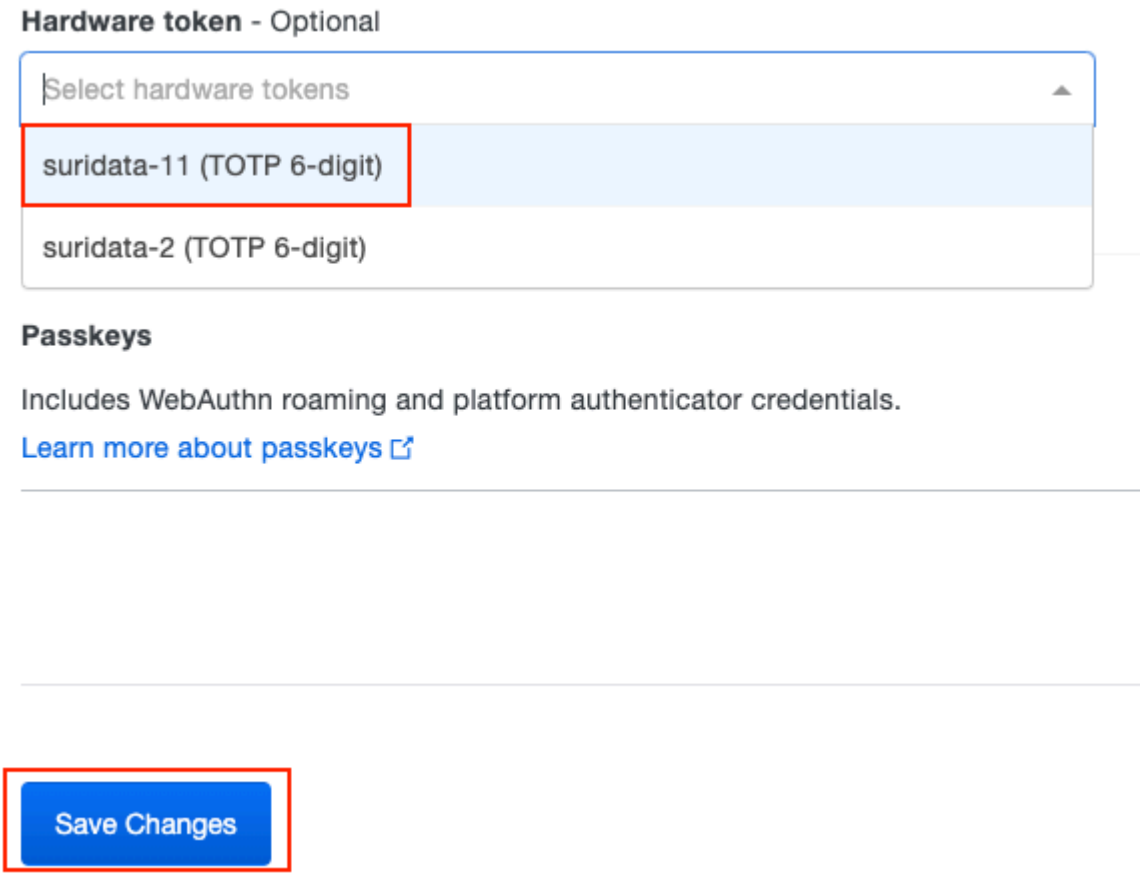
- Go to "Administrators" in the menu.



- Search for the dedicated Admin service account and select it.
- Once in the admin settings page, scroll down to "**Secondary authentication**" section and search for the "**Hardware Token**" dropdown



- Select the **latest** "FortiCASB-SSPM" token and click "Save Changes"



3. Return to FortiCASB-SSPM to start the newly created DuoSecurity instance (via the 3-dot menu) to initiate the scanning.

That's it! You're all set.

Your SaaS security is our priority!

The Fortinet Team