Integrating Duo

https://campus.barracuda.com/doc/96767841/

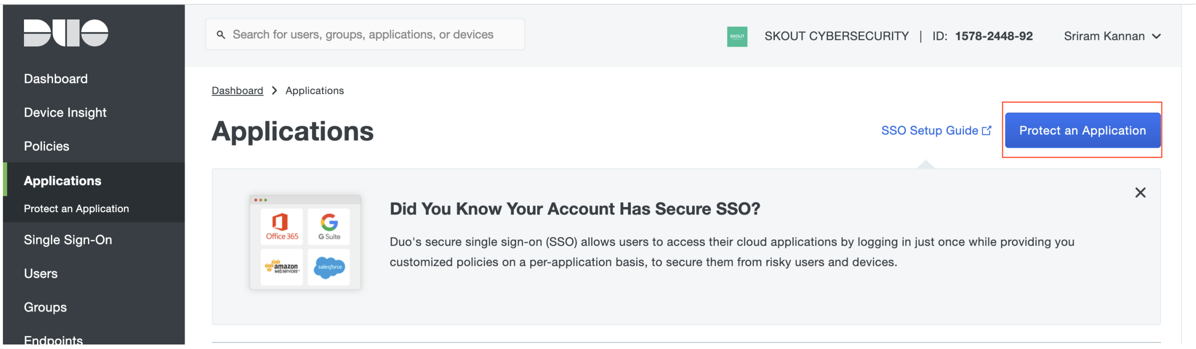
To integrate with Duo, perform the following procedures, below:

- To set up Duo
- To set up Barracuda XDR Dashboard

To set up Duo

In this procedure, you will create New App and API Keys.

1. Log in to the Duo Admin Panel as an administrator with the **Owner** role.
2. Navigate to **Applications**.

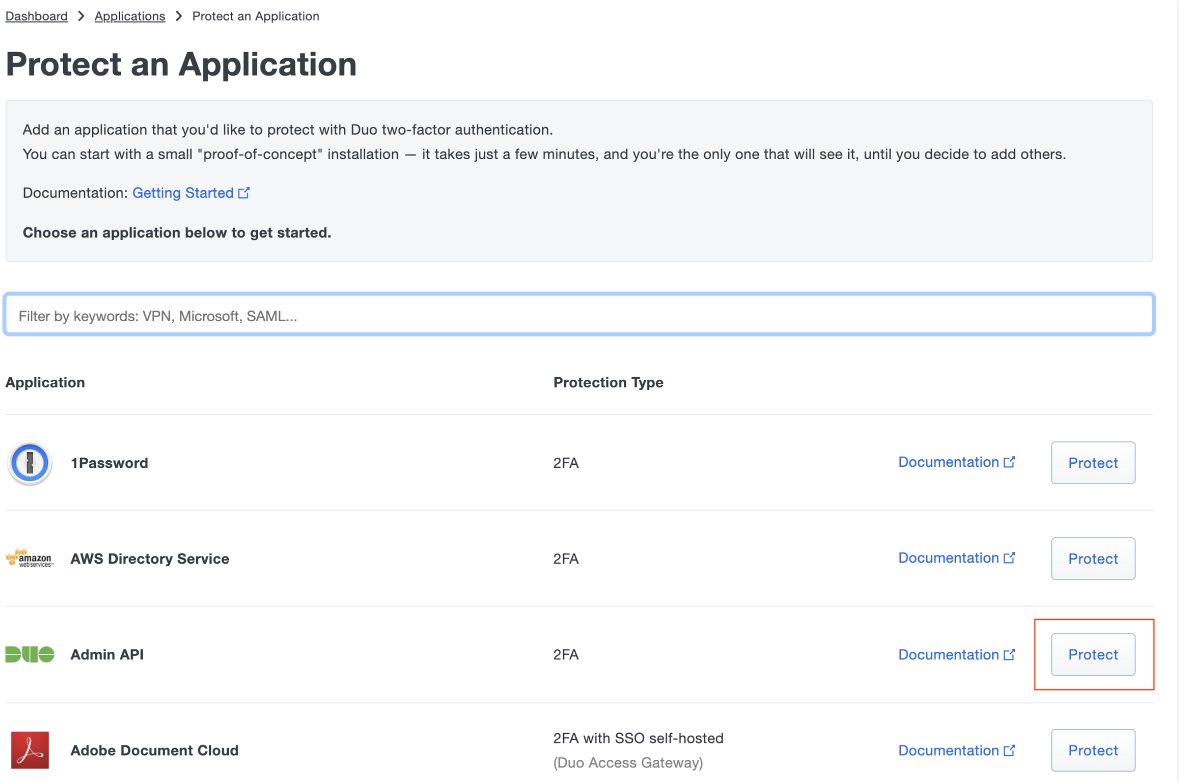


Did You Know Your Account Has Secure SSO?

Duo's secure single sign-on (SSO) allows users to access their cloud applications by logging in just once while providing you customized policies on a per-application basis, to secure them from risky users and devices.

3. Click **Protect an Application**. In the applications list, find **DUO Admin API**. Click **Protect**.

   If Admin API isn't in the list (and doesn't appear when you filter by keyword), Contact Duo Support to request Admin API access.



Dashboard > Applications > Protect an Application

Protect an Application

Add an application that you'd like to protect with Duo two-factor authentication.
You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

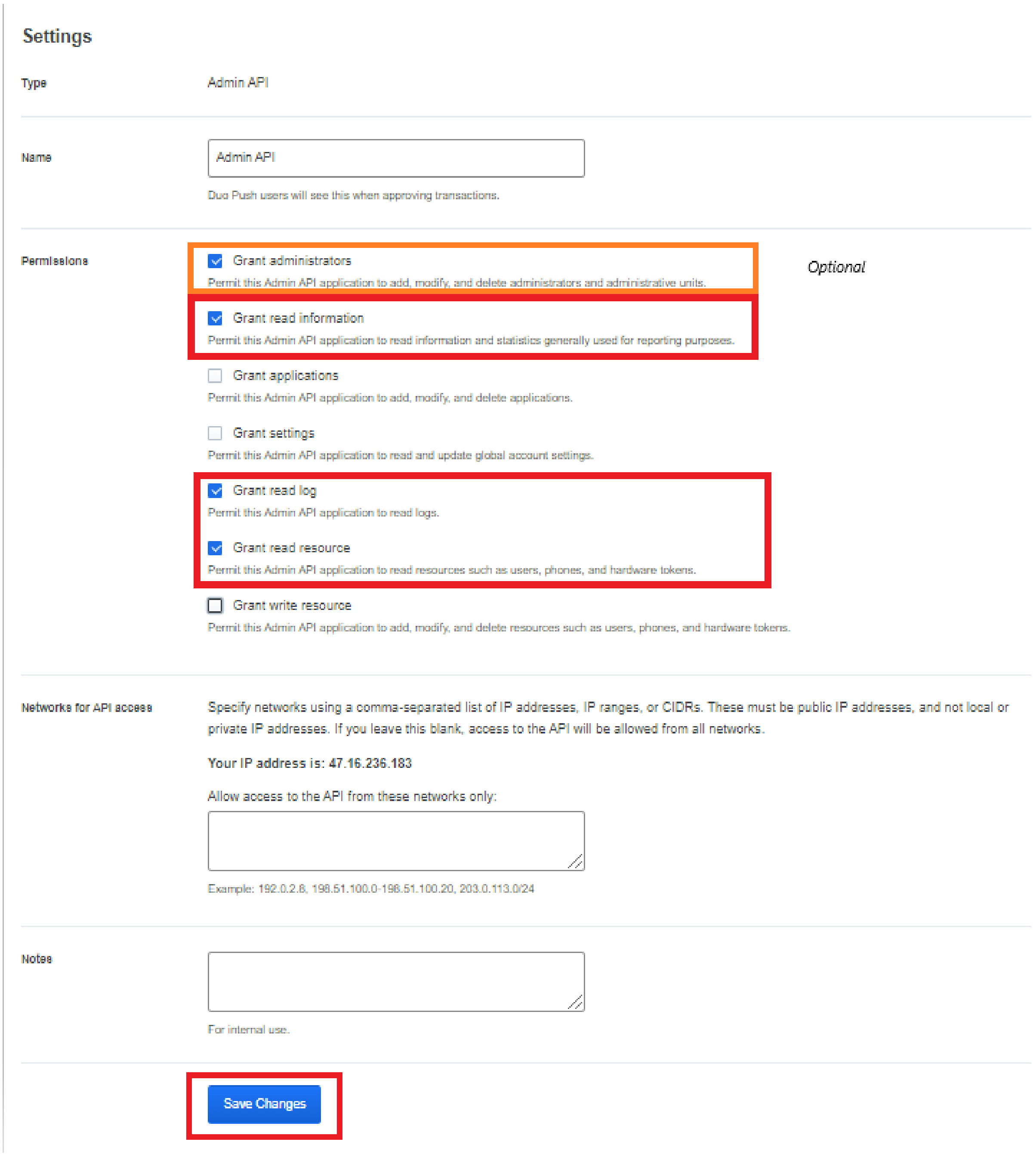
Documentation: Getting Started

Choose an application below to get started.

Filter by keywords: VPN, Microsoft, SAML...

Application	Protection Type		
1Password	2FA	Documentation	Protect
AWS Directory Service	2FA	Documentation	Protect
Admin API	2FA	Documentation	Protect
Adobe Document Cloud	2FA with SSO self-hosted (Duo Access Gateway)	Documentation	Protect

4. In **Settings,** under **Permissions**, check the boxes for **Grant read information**, **Grant read log**, and **Grant read resource**.
   These are the only permissions needed for the Barracuda XDR integration to function, however, to support remediation actions (suspend user) you can also check the box for **Grant Administrators**.
5. Click **Save Changes**.



Settings

Type Admin API

Name Admin API

Duo Push users will see this when approving transactions.

Permissions

☑ Grant administrators
Permit this Admin API application to add, modify, and delete administrators and administrative units.

Optional

☑ Grant read information
Permit this Admin API application to read information and statistics generally used for reporting purposes.

□ Grant applications
Permit this Admin API application to add, modify, and delete applications.

□ Grant settings
Permit this Admin API application to read and update global account settings.

☑ Grant read log
Permit this Admin API application to read logs.

☑ Grant read resource
Permit this Admin API application to read resources such as users, phones, and hardware tokens.

□ Grant write resource
Permit this Admin API application to add, modify, and delete resources such as users, phones, and hardware tokens.

Networks for API access

Specify networks using a comma-separated list of IP addresses, IP ranges, or CIDRs. These must be public IP addresses, and not local or private IP addresses. If you leave this blank, access to the API will be allowed from all networks.

Your IP address is: 47.16.236.183

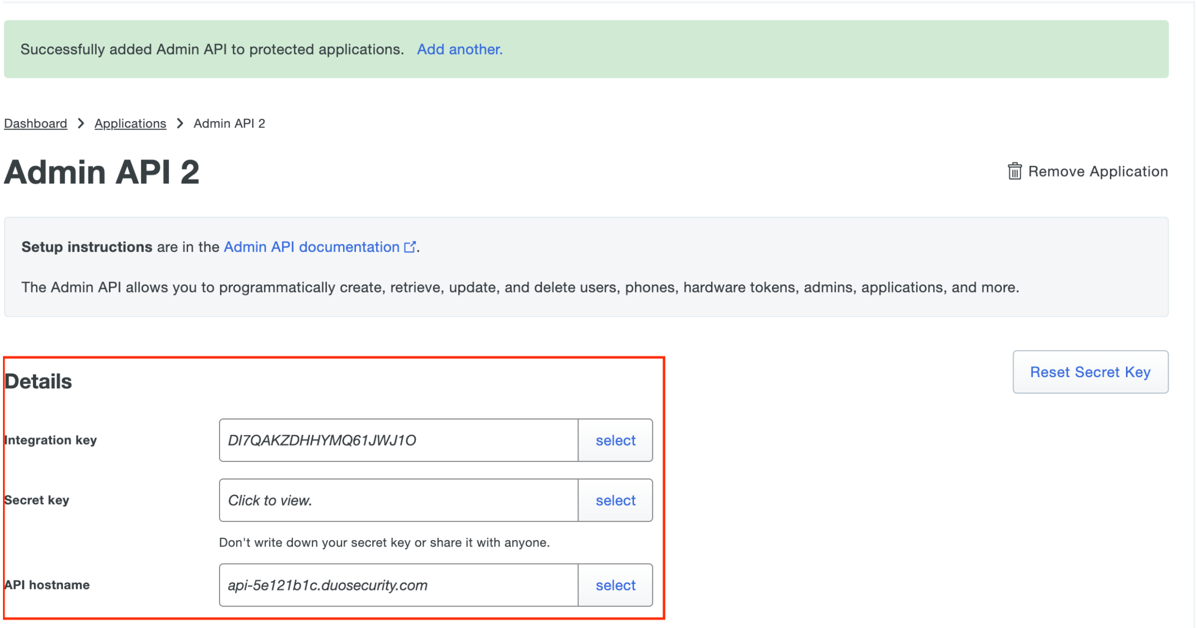
Allow access to the API from these networks only:

Example: 192.0.2.8, 198.51.100.0-198.51.100.20, 203.0.113.0/24

Notes

For internal use.

You can find your API hostname, integration key, and secret key at the top of the new Admin API application's page. You will need those values for the next step.



Successfully added Admin API to protected applications. Add another.

Dashboard > Applications > Admin API 2

Admin API 2

Remove Application

Setup instructions are in the Admin API documentation.

The Admin API allows you to programmatically create, retrieve, update, and delete users, phones, hardware tokens, admins, applications, and more.

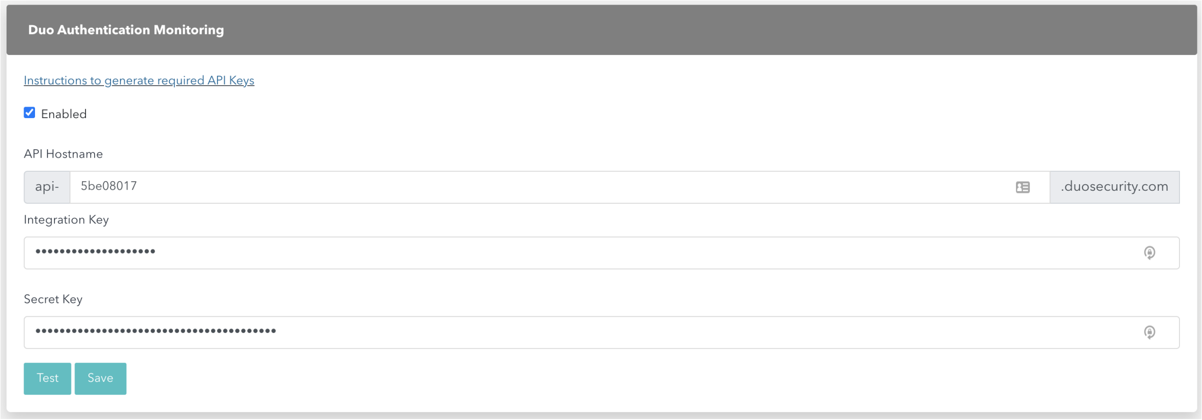
Details

Reset Secret Key

Integration key	*DI7QAKZDHHYMQ61JWJ1O*	select
Secret key	*Click to view.*	select
	Don't write down your secret key or share it with anyone.	
API hostname	*api-5e121b1c.duosecurity.com*	select

To set up Barracuda XDR Dashboard

1. In **Barracuda XDR Dashboard**, click **Administration** > **Integrations**
2. On the **Duo** card, click **Setup**.
3. Enter the **API hostname**, **integration key**, and **secret key** for the DUO app you just created.
4. Click the **Test** button to validate your settings and permissions.
5. Click **Save**.



Duo Authentication Monitoring

Instructions to generate required API Keys

☑ Enabled

API Hostname

api- 5be08017 .duosecurity.com

Integration Key

••••••••••••••••••••

Secret Key

••

Test Save

Figures