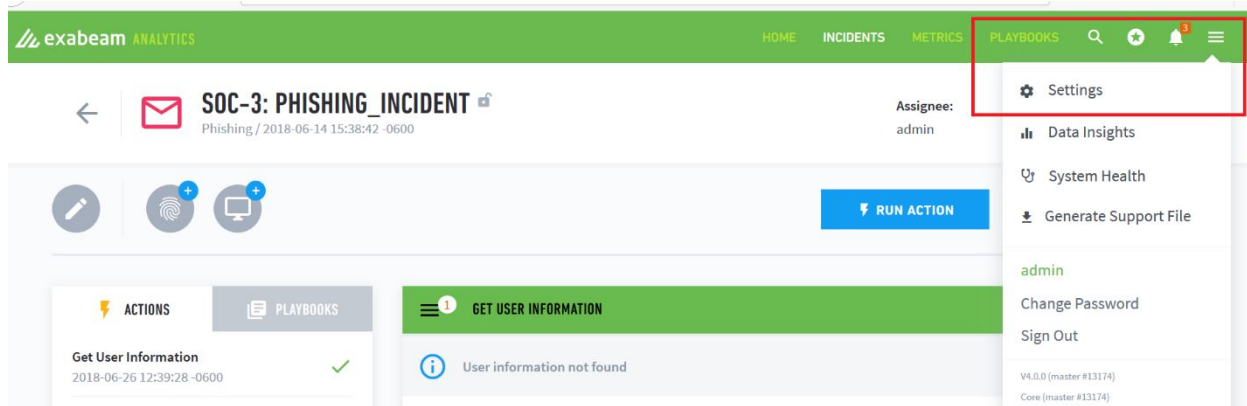


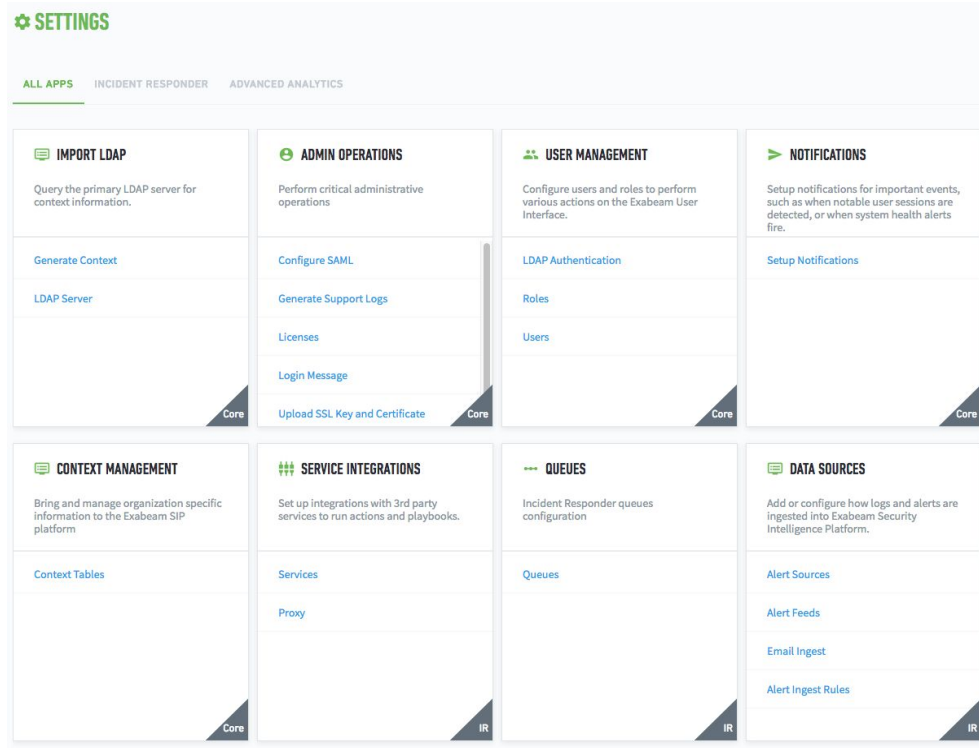
Exabeam – Duo Configuration Guide

There are (2) Services that needs to be configured in Exabeam Incident Responder: Duo Admin Service and Duo Auth Service.

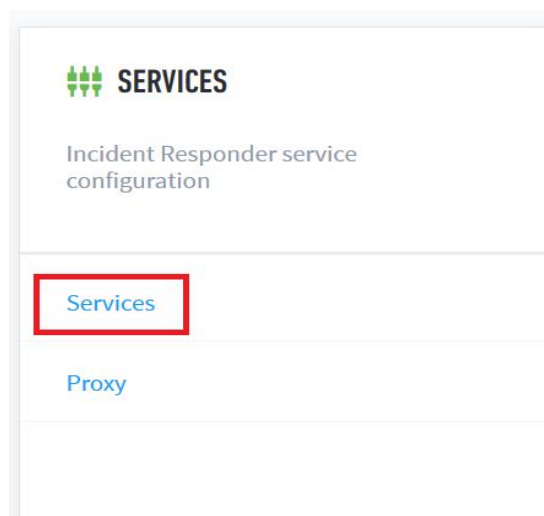
Login to Exabeam Incident Responder and click on the sandwich icon in the upper right-hand corner and then click Settings...



The Settings Page will load...



Scroll down to the Service Integrations panel and click on Services...



All supported Vendors and Integration Services will appear...

SETTINGS

SERVICE INTEGRATIONS

SERVICES PROXY

ALL SERVICES (56) CONFIGURED (13)

Search by vendor name Filter by Action

 Web Services Amazon	 Anomali ThreatStream API Anomali ThreatStream	 Jira Atlassian	 CarbonBlack CarbonBlack
 Checkpoint Firewall CheckPoint	 CiscoAMP Cisco	 ThreatGrid Cisco	 Umbrella Enforcement Cisco

Configure the Duo Admin Service:

Click on the Add a new services button to the right...

SETTINGS

SERVICES

SERVICES PROXY

SERVICES (40) CONFIGURED (7)

Search by vendor name Filter by Action

Add a new service

Click the Service:* dropdown and select Duo Admin and then Create Service...

Service:*

Service Name:*

Description:

Owner:

- Umbrella Investigate product
- CiscoAMP - CiscoAMP Endpoint
- CrowdStrikeFalcon - Falcon Host API
- Cuckoo - Cuckoo
- Duo Admin - Allows access to the Duo Admin service**
- Duo Auth - Allows access to the Duo Auth service
- Exabeam Advanced Analytics - Allows access to the Exabeam AA service
- FireEye AX - Allows access to FireEye AX sandbox to detonate file
- FireEye HX - Allows access to endpoints via the FireEye HX agent

The Service Name:* will auto-populate. Add your Host*:, Integration key*, and Secret key*:

Service:* Duo Admin

Service Name:* Duo Admin

Description:

Owner: Email address of the person/group owner.

Host*:

Integration key*:

Secret key*:

Service name needs to be unique.

To find the Duo Host*, Integration Key*, and Secret Key* log into the Duo Admin Portal (<https://admin.duosecurity.com>), navigate to Applications and click on Admin API. The following screen will appear...

Integration key YOUR_INTEGRATION_KEY select

Secret key Click to view. select

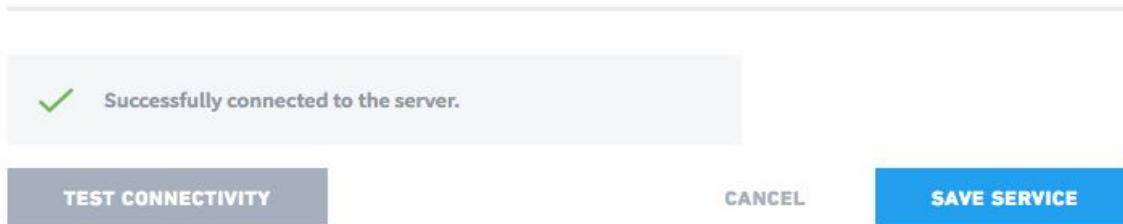
Don't write down your secret key or share it with anyone.

API hostname YOUR_API_HOST_NAME select

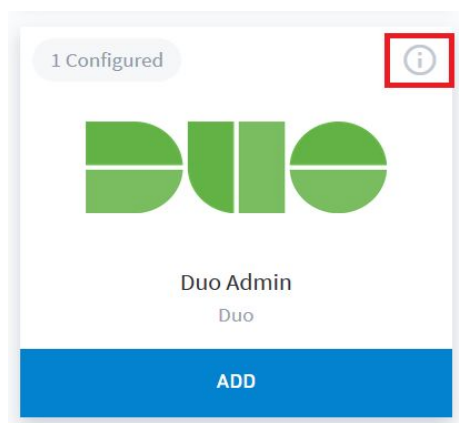
After adding the Duo Host*, Integration Key*, and Secret Key* click the Test Connectivity button...

TEST CONNECTIVITY CANCEL SAVE SERVICE

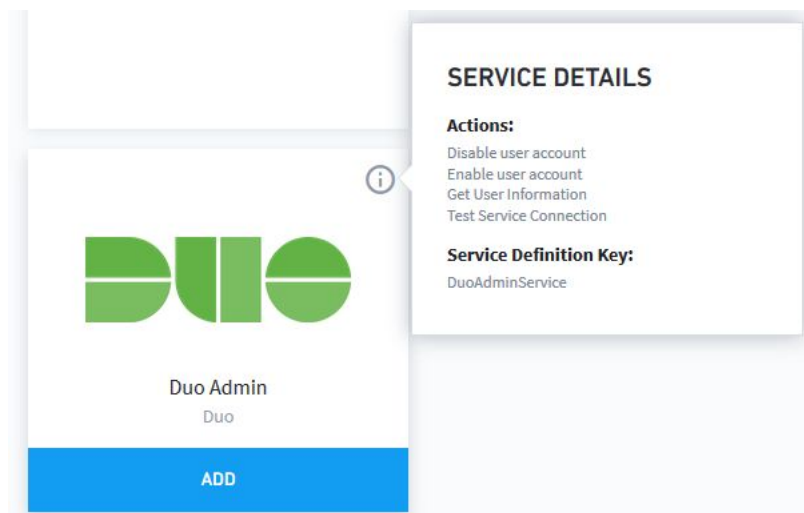
A successfully connected message should appear...



Click Save Service and then the All Services panel will appear. Scroll down to the Duo Admin panel and hover on it. You should see that one integration is configured and the circle-i icon will appear...

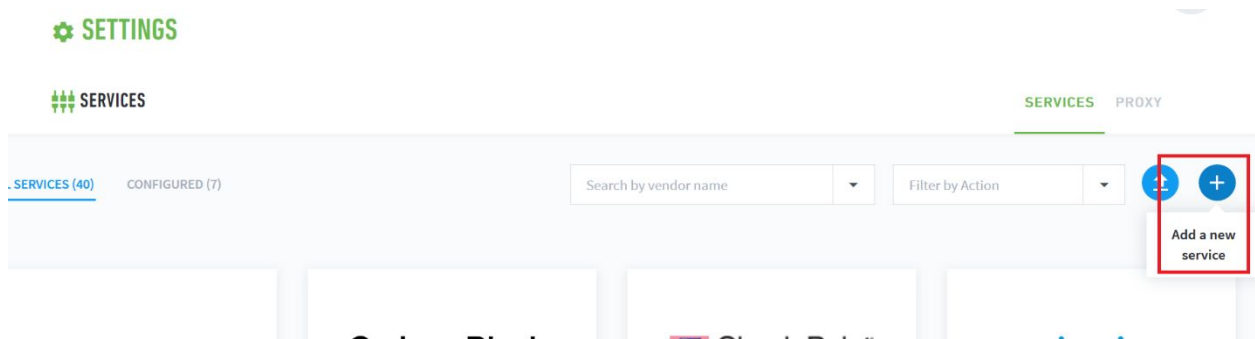


Hover over the circle-i icon to see the Exabeam Incident Responder Actions that are available...

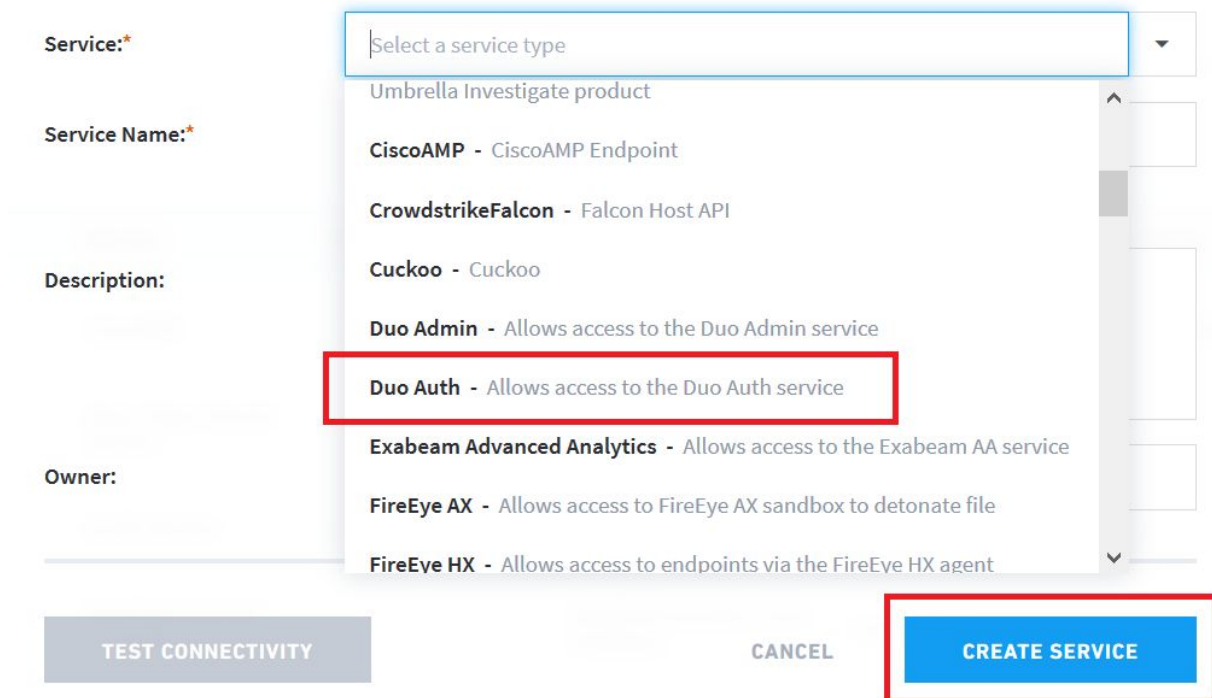


Configure the Duo Auth Service:

Click on the Add a new services button to the right...



Click the Service:* dropdown and select Duo Auth and then Create Service...

A screenshot of a service configuration form. The form has several fields: 'Service:*' (a dropdown menu), 'Service Name:*' (a text input field), 'Description:' (a text input field), and 'Owner:' (a text input field). The dropdown menu is open, showing a list of service types. The 'Duo Auth - Allows access to the Duo Auth service' option is highlighted with a red box. Below the form, there are three buttons: 'TEST CONNECTIVITY' (disabled), 'CANCEL', and 'CREATE SERVICE' (highlighted with a red box).

The Service Name:* will auto-populate. Add your Host*:, Integration key*, and Secret key*:

Service:*

Service Name:*
Service name needs to be unique.

Description:

Owner:

Host*:
Integration key*:
Secret key*:

To find the Duo Host*, Integration Key*, and Secret Key* log into the Duo Admin Portal (<https://admin.duosecurity.com>), navigate to Applications and click on Auth API. The following screen will appear...

Integration key

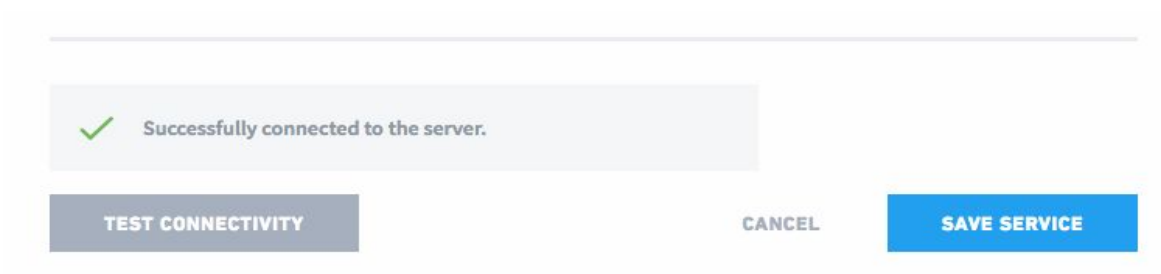
Secret key

Don't write down your secret key or share it with anyone.

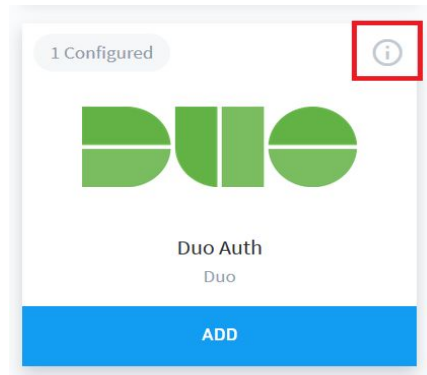
API hostname

After adding the Duo Host*, Integration Key*, and Secret Key* click the Test Connectivity button...


A successfully connected message should appear...



Click Save Service and then the All Services panel will appear. Scroll down to the Duo Auth panel and hover on it. You should see that one integration is configured and the circle-i icon will appear...



Hover over the circle-i icon to see the Exabeam Incident Responder Actions that are available...



Duo Auth
Duo

ADD

SERVICE DETAILS

Actions:

- Send 2FA Push
- Test Service Connection

Service Definition Key:

DuoAuthService