Exabeam – Okta Configuration Guide

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

	HOME INCIDENTS METRICS	
← SOC-3: PHISHING_INCIDENT ☞ Phishing/2018-06-14 15:38:42-0600	Assignee: admin	Settings In Data Insights
	F RUN ACTION	안 System Health 뢒 Generate Support File
		admin Change Password
Get User Information		Sign Out
2018-06-26 12:39:28 -0600		V4.0.0 (master #13174) Core (master #13174)

The Settings Page will load...

L APPS INCIDENT RESPONDER ADV	ANCED ANALYTICS		
IMPORT LDAP	ADMIN OPERATIONS	USER MANAGEMENT	> NOTIFICATIONS
Query the primary LDAP server for context information.	Perform critical administrative operations	Configure users and roles to perform various actions on the Exabeam User Interface.	Setup notifications for important events such as when notable user sessions are detected, or when system health alerts fire.
Generate Context	Configure SAML	LDAP Authentication	Setup Notifications
DAP Server	Generate Support Logs	Roles	
	Licenses	Users	
	Login Message		
Core	Upload SSL Key and Certificate Core	Соге	
CONTEXT MANAGEMENT	+++ SERVICE INTEGRATIONS	QUEUES	💷 DATA SOURCES
Bring and manage organization specific nformation to the Exabeam SIP slatform	Set up integrations with 3rd party services to run actions and playbooks.	Incident Responder queues configuration	Add or configure how logs and alerts are ingested into Exabeam Security Intelligence Platform.
Context Tables	Services	Queues	Alert Sources
	Proxy		Alert Feeds
			Email Ingest
			Alert Ingest Rules

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

‡ ‡‡ SERV	CES
Incident Re configurati	esponder service on
Services	

All supported Vendors and Integration Services will appear...

\$ SETTINGS



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

SERVICES (40) CONFIGURED (7) Search by vendor name Filter by Action Add a new Search by vendor name

Click the Service:* dropdown and select Okta...

Configure service

Service:*	Select a service type	•
Service Name:*	Microsoft Exchange - Allows access to Exchange EWS API	^
Description: Owner:	Microsoft Exchange Email - Microsoft Exchange Service	
	MxToolBox - This app interfaces with MxToolBox	
	Office365 - Office 365 Service	
	Okta - Allows access to the Okta service	١.
	Paio Aito Networks Autofocus - Enables API access to PAN AutoFocus devices and services	
	Palo Alto Networks Firewall - Enables API access to PAN Firewall devices	

The Service Name:* will auto-populate. Add your Okta API URL*: and API Token*:

Service:*	Okta 🗸
Service Name:*	Okta
	Service name needs to be unique.
Description:	
Owner:	Email address of the person/group owner.
API URL*:	
API Token*:	

Then click the Test Connectivity button...

TEST CONNECTIVITY	CANCEL	SAVE SERVICE
A successfully connected message should appear		
Successfully connected to the server.		
TEST CONNECTIVITY	CANCEL	SAVE SERVICE

Click Save Service and then the All Services panel will appear. Scroll down to the Okta 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...

	SERVICE DETAILS
	Actions:
	Add User to Group
	Get User Information
1 Configured	Reset Password
1 Comguleu	Send 2FA Push
	Suspend User Test Service Connection
	Unsuspend User
OKC	Service Definition Key:
	OktaService
Okta	AutoFocus
Okta	Palo Alto Networks