

KnowBe4

1. Overview

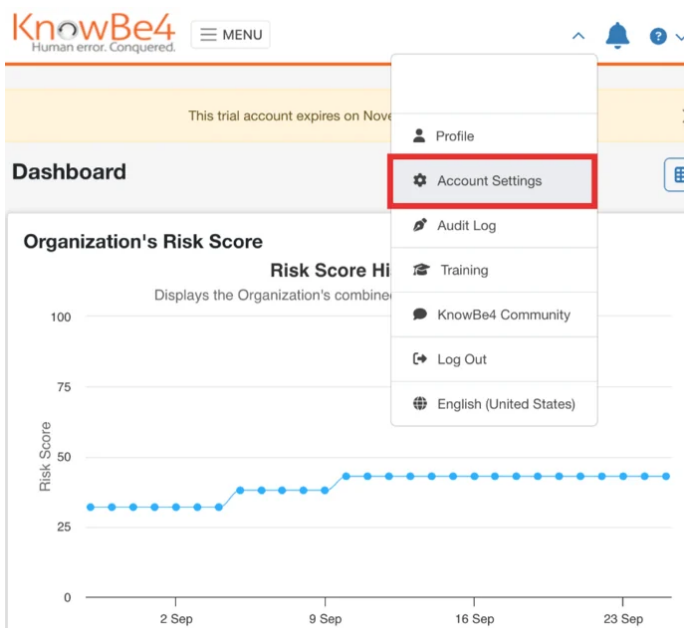
This document explains how to integrate **KnowBe4** with a **SIEM** solution using the KnowBe4 REST API. This allows ingestion of phishing simulation logs for monitoring, alerting, and reporting.

2. Requirements

- Admin access to KnowBe4
- API access enabled on KnowBe4
- API-capable SIEM (e.g., Elastic, Splunk, QRadar, etc.)
- Internet access from the SIEM/log collector

3. Generate API Token in KnowBe4

- Go to KnowBe4 and navigate to '**Account Settings**'.



- Under '**Account Integrations**', select '**API**'.

Account Information



Purchased Products and Add-ons

Organization Information

Branding

Placeholders

User Management



Phishing



Training



Account Integrations



SAML

Phish Alert

API

Expand All

Account Information

Purchased Products and Add-ons

- Select '**Reporting API**'.

API

Reporting API

☒ Enable Reporting API Access

 Reporting API 

 Reference Documentation

User Event API

 User Event API 

 Reference Documentation

Save Changes

- Select '**Create New API Token**'.

KnowBe4
Human error. Conquered.

MENU

KnowBe4 APIs

← Back to Account Settings

Reporting API

User Event API

Reference Documentation

+ Create New API Token

Key ?	Name	Generated By	Generated On	Status	Actio
			08/30/2024	✓	▼
			09/22/2024	✓	▼
			09/24/2024	✓	▼
			09/22/2024	✓	▼

- Enter a name for the API token, such as "ScytaleAPI." Then, select '**Create Token**'.

KnowBe4
Human error. Conquered.

MENU

Create New API Token

← Back to Reporting API Tokens

Name

Name

Generated By

Status

✓ Enabled

Disable

Create Token

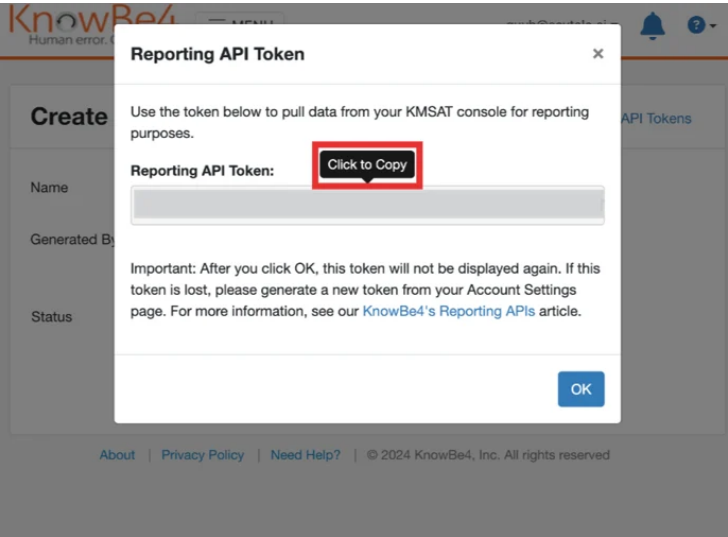
About

Privacy Policy

Need Help?

© 2024 KnowBe4, Inc. All rights reserved

- Copy the token for use in your integration.



Configure SIEM to Pull Logs

Option A: SIEM with HTTP Polling Support

1. Use built-in HTTP pull or script-based log ingestion
2. Schedule API calls to poll the KnowBe4 endpoint
3. Parse and map JSON fields

Option B: Use a Log Collector (e.g., Logstash)

1. Set up an HTTP poller input with API headers
2. Output parsed data to your SIEM (via syslog, Elastic, etc.)

Field Mapping (Common Fields)

Field	Description
user_email	Targeted user
clicked	User clicked link (true/false)
reported	User reported the email
test_status	Status of phishing test
event_time	Timestamp of action

Validation Steps

- Run a test phishing campaign in KnowBe4

- Check SIEM logs for new entries
- Validate parsing of key fields
- Create filters/dashboards to view data

Reference Link: <https://docs.scytale.ai/knowbe4-user-guide>

Revision #1

Created 20 June 2025 01:28:43 by Albert Alombro

Updated 20 June 2025 01:51:32 by Albert Alombro