Connector Guides

1. Ingestion Guides

1.1. CrowdStrike Falcon — Alert Ingestion Guide

This guide covers two approaches for ingesting CrowdStrike Falcon alerts into Swimlane Turbine, normalized to Turbine Schema format:

- **Connector** — Use the CrowdStrike Falcon V2 connector actions directly in a playbook for full control over your workflow.
- **Component** — Use the CrowdStrike Falcon Alert Ingestion component for a turnkey webhook-based pipeline with automatic checkpointing and retry.

Both approaches deliver alerts in Swimlane's Turbine Schema format. One downstream playbook handles alerts from any source.

Key Capabilities

- **Unified alert format** — Every CrowdStrike alert is normalized to Turbine Schema, enabling cross-vendor playbooks and dashboards.
- **Rich alert context** — Full host details (hostname, IP, OS, agent version), MITRE ATT&CK tactic and technique mappings, file hashes and observables, and pre-built Falcon Query Language (FQL) strings for threat hunting.
- **Ready-to-use response actions** — Alerts include available response actions (Contain host, Release from containment, Run RTR script) that can be wired directly into automated response playbooks.
- **Incremental polling** — Checkpoint-based polling ensures no duplicate alerts.

2.6. Akamai

Introduction

This guide explains how to authenticate the Akamai connector in Swimlane using **Akamai EdgeGrid Authentication.**
You will generate API credentials in Akamai Control Center, collect the required identifiers, and configure the connector inside Swimlane.

Prerequisites

Akamai Access Requirements

You must have permissions in Akamai Control Center to:

- Create and manage API credentials
- Assign API access scopes
- Access Akamai EdgeGrid credentials

Required Credentials

During setup, you will collect:

- Client Token
- Access Token
- Client Secret
- API Host (xxxx.luna.akamaiapis.net)

Authentication Method Overview

The Akamai connector uses EdgeGrid Authentication. EdgeGrid secures API requests by cryptographically signing each request using a Client Token, Access Token, and Client Secret.

Akamai Setup

Take the following steps to create EdgeGrid API credentials:

2.16. AbuseIPDB

Introduction

This guide explains how to authenticate the AbuseIPDB connector in Swimlane using API Key authentication. You will create an AbuseIPDB account, generate an API key, and configure the connector asset in Swimlane Turbine.

Prerequisites

AbuseIPDB Access Requirements

You must have access to an AbuseIPDB account with permissions to generate API keys.

Required Credentials

During setup you will collect:

- AbuseIPDB API URL
- AbuseIPDB API Key

Generate AbuseIPDB API Key

1. Navigate to https://www.abuseipdb.com/
2. Click Sign Up to create a new account or Login if you already have an account.
3. After logging in, open your user profile menu.
4. Navigate to Account settings.
5. Open the API tab.
6. Click Create Key.
7. Provide a name for the API key.
8. Click Create to generate the key.
9. Copy the generated API key and store it securely.

Connector Configuration in Swimlane

2.26. ConnectWise Manage

Introduction

This guide explains how to authenticate the **ConnectWise Manage** connector in Swimlane using custom API authentication.

The ConnectWise Manage connector enables Swimlane Turbine to integrate with ConnectWise Manage for automating company management, contacts, tickets, SLAs, service boards, and invoice operations.

Prerequisites

Before configuring the connector, ensure you have:

- Access to ConnectWise Manage
- Administrator permissions in ConnectWise Manage
- Permission to create API integrations
- Permission to create API Members and Security Roles

This connector requires ConnectWise API version **2020.2 or newer**.

Required Credentials

You will need the following authentication details:

Credential	Description
API Version	ConnectWise API version
Client ID	Integration Client ID
Company Identifier	Company identifier used for authentication
Host URL	ConnectWise server URL
Public Key	API public key
Private Key	API private key

2.36. Google Workplace

Introduction

This guide tells you how to authenticate the Google Workspace connector in Swimlane.

You will create a Google Cloud project, enable required APIs, configure a service account, optionally enable domain-wide delegation, and configure the connector in Swimlane.

This connector supports Google authentication using one of the following:

- Service Account JSON credentials (Base64-encoded)
- OAuth 2.0 Client ID, Client Secret, and Refresh Token

Prerequisites

Google Access Requirements

You must have permissions to:

- Create and manage projects in Google Cloud Platform
- Enable APIs in Google Cloud Console
- Create service accounts and download JSON key files
- Manage domain-wide delegation in Google Admin console (recommended)
- Create OAuth 2.0 client credentials (optional)

Required Credentials

During setup, you will collect:

- Service Account JSON key file (Base64-encoded) or OAuth 2.0 Client ID and Client Secret
- Delegate account email address (recommended)
- Customer ID or my_customer alias (optional)
- OAuth scopes for domain-wide delegation (recommended)
- Refresh token (if using OAuth 2.0 client credentials)

2.46. Microsoft 365

Introduction

This guide explains how to authenticate the Microsoft Graph API connector in Swimlane using one of the following authentication methods:

- OAuth 2.0 Client Credentials (Application permissions)
- OAuth 2.0 Refresh Token Grant (Delegated permissions with MFA)

You will create an Azure app, assign permissions, collect the required identifiers, and configure the connector inside Swimlane.

Prerequisites

Azure Access Requirements

You must have Azure permissions to:

- Register applications in Azure Active Directory
- Assign API permissions
- Grant admin consent
- Create and manage client secrets
- Assign directory roles (Global Reader, Security Reader)
- View tenant, subscription, and organizational properties

Required Credentials

During setup, you will collect:

- Client ID
- Client Secret
- Tenant ID
- Token URL (for Client Credentials flow)
- Refresh Token (for Refresh Token flow)

2.56. Palo Alto Networks Cortex XDR

Introduction

This guide explains how to authenticate the Palo Alto Networks Cortex XDR connector in Swimlane using Cortex API Token authentication.
You will generate Cortex XDR API credentials, collect the required identifiers, and configure the connector inside Swimlane Turbine.

Prerequisites

Cortex XDR Access Requirements

You must have administrative access to the Palo Alto Networks Cortex XDR tenant to:

- Generate API keys
- View tenant base URL
- Access Cortex XDR API settings

Required Credentials

During setup, you will collect:

- Cortex XDR Base URL
- API Token
- Cortex XDR API Key ID

Authentication Overview

Cortex XDR uses token-based authentication with a custom HTTP header.
Authentication requires:

- API Token
- API Key ID (x-xdr-auth-id header)

Cortex XDR Setup

2.66. Splunk Trustar

Introduction

This guide tells you how to authenticate the Splunk TruSTAR connector in Swimlane using **OAuth 2.0 Client Credentials**.

You will collect your TruSTAR API credentials, confirm required endpoints, and configure the connector in Swimlane.

Prerequisites

TruSTAR Access Requirements

You must have TruSTAR permissions to:

• Access TruSTAR Station (account settings) to generate or retrieve API credentials

• Confirm your tenant/environment details for API access

Required Credentials

During setup, you will collect:

• API Base URL

• Token URL

• API Key (used as client_id)

• API Secret (used as client_secret)

URLs

API Base URL

The TruSTAR REST API is accessible at the following base URL:

https://api.trustar.co/api/2.0

2.76. VirusTotal Analysis

Introduction

This guide tells you how to authenticate the VirusTotal Analysis connector in Swimlane using API Key Authentication.

You will obtain a VirusTotal API key (public or premium) and configure the connector asset in Swimlane.

Prerequisites

VirusTotal Access Requirements

You must have VirusTotal permissions to:

- Register a VirusTotal account
- Access your API key from the VirusTotal portal
- Request a premium API key (optional)

Required Credentials

During setup, you will collect:

- URL
- API Key (x-apikey)

VirusTotal Setup

Public API Key

Take the following steps to obtain a public API key:

1. Register with the VirusTotal Community by going to the VirusTotal website and clicking **New? Join the community**.
2. Provide a name, email, username, and password. Once complete, click **Join us**.
3. An activation link will be sent to the email you provided. Click on the activation link to