SWIMLANE

Connector Guides

CONTENTS

1. Ingestion Guides

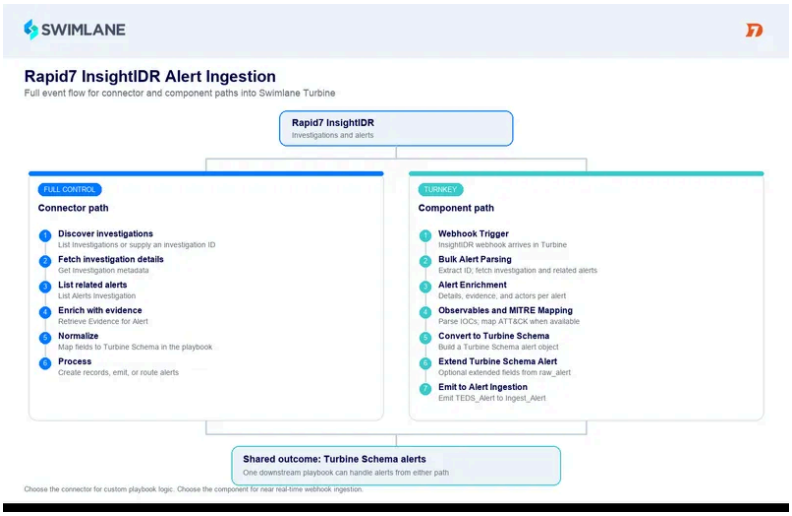
1.1. Rapid7 InsightIDR — Alert Ingestion Guide

This guide covers two approaches for ingesting Rapid7 InsightIDR investigations and alerts into Swimlane Turbine, normalized to Turbine Schema format:

- **Connector** — Use the Rapid7 InsightIDR V2 connector actions directly in a playbook for full control over your workflow.
- **Component** — Use the Rapid7 InsightIDR Alert Ingestion component for a turnkey webhook-based pipeline with investigation enrichment, observable extraction, and Turbine Schema emission.

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

Ingestion Flow



Key Capabilities

- **Unified alert format** — Every InsightIDR investigation/alert is normalized to Turbine Schema, enabling cross-vendor playbooks and dashboards.
- **Investigation enrichment** — Fetches investigation details, related alerts, evidence, and actors via the InsightIDR API before ingestion.
- **Observables and MITRE ATT&CK** — Parses IOCs from enriched alert content and maps MITRE ATT&CK tactics and techniques when available.
- **Near real-time webhook ingestion** — Investigation webhooks trigger enrichment and emission as investigations are created or updated in InsightIDR (no polling loop required for the primary component flow).

2.5. Atlassian Jira On-Premise

Introduction

This guide explains how to authenticate the Atlassian Jira On-Premise connector in Swimlane using the supported authentication methods.

You will generate Jira credentials, collect the required instance details, and configure the connector inside Swimlane Turbine.

Authentication Methods Overview

The Atlassian Jira On-Premise connector supports the following authentication methods:

- HTTP Basic Authentication (Username + Password or Personal Access Token)
- HTTP Bearer Authentication (Personal Access Token)

Prerequisites

Jira Access Requirements

You must have Jira permissions to:

- Access your Jira On-Premise instance
- Generate or use a Personal Access Token (if enabled)
- Access Jira REST APIs

Required Credentials

During setup, you will collect:

- Jira Base URL
- Username
- Password or Personal Access Token

Jira Setup

Method 1 – HTTP Basic Authentication

This method authenticates using a Jira username and either a password or a Personal Access Token. Using a Personal Access Token is recommended.

Take the following steps to generate a Personal Access Token:

1. Log in to the Jira On-Premise web interface.
2. Navigate to your user profile.
3. Open the Personal Access Tokens section.
4. Click Create token.

2.15. AlienVault Open Threat Exchange

Introduction

This guide tells you how to authenticate the AlienVault Open Threat Exchange connector in Swimlane using API Key Authentication.

You will create an AlienVault Open Threat Exchange account, obtain an API key, and configure the connector in Swimlane.

Prerequisites

AlienVault Open Threat Exchange Access Requirements

You must have access to an active AlienVault Open Threat Exchange account with permission to view and use API keys.

Required Credentials

During setup, you will collect:

- OTX API Key
- API Endpoint URL

AlienVault Open Threat Exchange Setup

Take the following steps to register for AlienVault Open Threat Exchange and obtain an API key:

1. Navigate to the AlienVault Open Threat Exchange website at **https://otx.alienvault.com/**.
2. Create a new account or sign in with an existing account.
3. After signing in, navigate to your account settings.
4. Locate the **OTX API Key** section.
5. Copy and save the API key. This value will be used when configuring the Swimlane asset.

Connector Configuration in Swimlane

Take the following steps to configure the AlienVault Open Threat Exchange connector asset in Swimlane:

1. Log in to Turbine.
2. From the left-hand navigation pane, click **ORCHESTRATION** and click **Assets**.
3. Click the **plus** icon to create a new asset.
4. Select **AlienVault Open Threat Exchange** from the **Asset Type** list.
5. Fill in the **Asset Settings** and **Asset Input** fields as per the following:

Configuration Parameters

2.25. Cyberint

Introduction

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

You will generate an API key in Cyberint, collect the required identifiers, and configure the connector in Swimlane.

Prerequisites

Cyberint Access Requirements

You must have Cyberint permissions to:

- Access the Cyberint platform
- Generate or retrieve API keys
- Access threat intelligence APIs

Required Credentials

During setup, you will collect:

- API Base URL
- API Key (Access Token)

Authentication Methods Overview

The Cyberint connector supports:

- **API Key Authentication**

Cyberint Setup

Take the following steps to generate an API Key:

1. Log in to the **Cyberint platform**.
2. Navigate to **Settings / API Access** (location may vary by tenant).
3. Locate the **API Keys / Access Tokens** section.
4. Click **Generate API Key** or **Create Token**.
5. Enter a name or description for the key.
6. Assign required permissions (if applicable).
7. Click **Create / Generate**.
8. Copy and securely store the API key.

Ensure the key is stored securely, as it may not be visible again.

2.35. Exabeam AA V2

Introduction

This guide explains how to authenticate the **Exabeam AA V2** connector in Swimlane using OAuth 2.0 Client Credentials.

Prerequisites

Exabeam Access Requirements

You must have permissions to:

- Access the Exabeam Advanced Analytics console
- Generate and manage API credentials
- Access Exabeam API services
- View and manage correlation rules
- Perform event searches through the API

Required Credentials

During setup, you will collect:

Credential	Description
URL	Exabeam API endpoint URL
Client ID	Exabeam API Key
Client Secret	Exabeam API Key Secret
Verify SSL	Optional SSL verification setting
HTTP Proxy	Optional proxy configuration

Exabeam Setup

Take the following steps to generate API credentials:

1. Log in to the Exabeam console.
2. Navigate to:
   Settings → API Access
   or
   Administration → API Keys
3. Click **Create API Key**.
4. Enter:
   - API Key Name
   - Description (optional)
   - Required permissions/scopes

2.45. IPINFO

Introduction

This guide tells you how to authenticate the **IPInfo** connector in Swimlane using an API token.

You will copy your IPInfo API token, confirm your subscription access, and configure the connector in Swimlane.

Prerequisites

IPInfo Access Requirements

You must have:

- An active **IPInfo** account.
- A valid **IPInfo API token**.
- An active subscription to use IPInfo API services.
- **Business** or **Enterprise** plan access if you need all available outputs or the **Hosted Domains** action.

Required Credentials

During setup, you will collect:

- API Token

IPInfo Setup

Take the following steps to get an API Token:

1. Log in to **IPInfo** or create an account at https://ipinfo.io.
2. From your account dashboard, click **Token**.
3. Click **Copy to Clipboard**.
4. Securely save the copied token.

Connector configuration in Swimlane

1. Log in to Turbine.
2. From the left-hand navigation pane, click **ORCHESTRATION** and click **Assets**.
3. Asset homepage opens.
4. Click the plus icon to open the **Configure your Connector Asset** window.
5. Select **IPInfo** from the Asset type list.
6. Fill in the Asset Settings and Asset Input as shown:

Field	Description	Required/Optional
token	IPInfo API token	Required

2.55. Microsoft Graph API SharePoint

Introduction

This guide explains how to authenticate the **Microsoft Graph API SharePoint** connector in Swimlane using **OAuth 2.0 Client Credentials**.

The connector uses an Azure AD (Microsoft Entra ID) application to securely authenticate with Microsoft Graph and perform SharePoint operations such as managing sites, lists, folders, files, and document libraries.

Prerequisites

Before configuring the connector, ensure that you have:

- A Microsoft 365 tenant
- Administrator access to Microsoft Entra ID (Azure AD)
- Permission to register applications
- A SharePoint Online site
- Permission to grant Microsoft Graph API application permissions

Required Credentials

Collect the following information during setup:

Credential	Description
URL	Microsoft Graph API endpoint
Token URL	OAuth token endpoint
Client ID	Azure application (client) ID
Client Secret	Azure application client secret
Scope	Microsoft Graph permission scope

Register an Application in Microsoft Entra ID

Take the following steps to create an Azure application.

1. Sign in to the **Microsoft Azure Portal**.
2. Navigate to **Microsoft Entra ID** > **App registrations**.
3. Click **New registration**.
4. Enter a name for the application.
5. Select **Accounts in this organizational directory only**.
6. Click **Register**.

Configure Microsoft Graph Permissions

2.65. 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

Take the following steps to generate the Cortex XDR API credentials:

1. Log in to the Palo Alto Networks Cortex XDR Console.
2. Navigate to Settings > Configurations > Integrations > API Keys.
3. Click Generate API Key.
4. Enter a name for the API key.
5. Copy and securely store the API Key ID and API Token.

> The API Token is shown only once. Copy and save it for further usage.

2.75. Recorded Future Sandbox

Introduction

This guide tells you how to authenticate the **Recorded Future Sandbox connector** in Swimlane using:

- **HTTP Bearer Token Authentication**
- **OAuth 2.0 Client Credentials**

You will generate an API token or OAuth client credentials in Recorded Future, collect the required identifiers, and configure the connector in Swimlane.

Prerequisites

Recorded Future Access Requirements

You must have Recorded Future permissions to:

- Access the Recorded Future platform
- Generate API tokens
- Create OAuth clients (if applicable)
- Access API services

Required Credentials

During setup, you will collect:

- API Base URL
- API Token (Bearer Token)
- Client ID (OAuth)
- Client Secret (OAuth)
- Token URL (OAuth)

Authentication Methods Overview

The Recorded Future Sandbox connector supports:

1. **HTTP Bearer Token Authentication**
2. **OAuth 2.0 Client Credentials**

Recorded Future Setup

Take the following steps to generate an API Token (Bearer Authentication):

1. Log in to the **Recorded Future Platform**.
2. Click your **profile icon** (top-right corner).
3. Select **Settings**

2.85. ThreatQuotient ThreatQ

Introduction

This guide tells you how to authenticate the ThreatQuotient ThreatQ connector in Swimlane using **OAuth 2.0 Password Grant** authentication.

You will enable API access in ThreatQ, collect the required credentials, and configure the connector in Swimlane.

Prerequisites

ThreatQ Access Requirements

You must have access to a ThreatQuotient ThreatQ account with permissions to:

- Access the ThreatQ API
- Authenticate using OAuth (username/password-based grant)
- Create, read, update, and delete indicators, events, and import sessions
- View API version information (standard or beta)

> Permissions are managed through ThreatQ roles. Ensure the API user has sufficient privileges for the actions you intend to automate.

Required Credentials

During setup, you will collect the following:

- API Base URL
- API User Email
- Client Password
- OAuth Client ID
- API Type (standard or beta)

API Types

ThreatQ supports different API types depending on your deployment.

API Type	Description
standard	Default ThreatQ production API
beta	Beta or preview API features (if enabled in your environment)

Ensure the API type selected in Swimlane matches your ThreatQ instance.

ThreatQ Setup

2.95. xMATTERS

Introduction

This guide tells you how to authenticate the xMatters connector in Swimlane using:

- HTTP Basic Authentication
- OAuth 2.0 Password Credentials

You will obtain xMatters credentials, configure OAuth (if applicable), collect required identifiers, and configure the connector in Swimlane.

Prerequisites

Requirement	Description
Platform Access	Access the xMatters platform
User Management	View and manage users and devices
Workflow Management	Create and manage workflows
OAuth Configuration	Configure OAuth clients (for OAuth authentication)
API Access	Access API endpoints

Required Credentials

During setup, you will collect:

For HTTP Basic Authentication:

- URL
- Username
- Password

For OAuth 2.0 Password Credentials:

- URL
- Username
- Password
- Client ID

xMatters Setup

Take the following steps to retrieve API endpoint URL:

1. Log in to your xMatters instance.
2. Identify your base API URL in the following format: https://<company>.xmatters.com/api/xm/1
3. Verify access to the API endpoint.