Contents

Contents **1**

Get started with ZYX Product **2**

To get started with ZYX Product: 2

Choose deployment type **3**

Available deployment types 3

Public cloud 3

The ZYX Company agent 3

Virtual appliance 3

Remote collector 3

Physical appliance 3

Set up log collection **4**

Verify log collection **6**

Maintain ZYX Product **7**

After ZYX Product is installed and configured 7

Maintain properly running networks and systems 7

Update contact processes 7

Get started with ZYX Product

ZYX Product is a cloud based log management solution, delivered using a software-as-a-service (SaaS) model. Effective log management is not only imperative in maintaining compliance, but is also a powerful security tool that can prevent intrusion and security breaches. ZYX Product provides you with on-demand and automated log collection, storage, reporting, correlation, and alerting across your entire environment.

To get started with ZYX Product:

1. Choose a deployment type.
2. Set up log collection.
3. Verify log collection.
4. Maintain ZYX Product.

Choose a deployment type

The primary methods of deploying ZYX Product within your environment include:

- The ZYX Company agent deployment
- Remote collector deployment
- Virtual Appliance deployment
- Physical Appliance deployment
- Combination of deployment methods

Selection for the method or method combination you chose depends on the IT environment that contains the host devices, the types of devices, and the preferred collection method. The ZYX Company recommends utilizing the agent whenever possible.

Review the chart and workflow below to determine which collection method(s) best meet your needs.

Available deployment types

Public cloud

To install and configure ZYX Product in the public cloud, see Configure ZYX Product in the public cloud.

The ZYX Company agent

To install and configure the agent, see Configure the ZYX Company agent.

Virtual appliance

To install and configure a virtual appliance, see Configure a ZYX Product virtual appliance.

Remote collector

To install and configure a remote collector, see Configure a ZYX Product remote collector.

Physical appliance

To install and configure a physical appliance, see Configure a Product physical appliance.

 **Next** Set up log collection.

Set up log collection

To set up log collection, you must determine your IT infrastructure needs and choose a deployment option. For more information, see: Choose a deployment type.

The ZYX Company agent log collection set up

To begin log collection:

1. Configure the ZYX Company agent.
   When you install the agent on a host, the agent automatically assigns a default Windows event log or Syslog collection source on the host. ZYX Product receives the specific requirements for log collection from each default collection source, and then collection begins. For more information, see About collection.

2. Verify log collection.
3. Create and apply a collection alert rule.
4. (Optional) Create a correlation policy.
5. (Optional) Create a correlation alert rule.

The ZYX Product virtual appliance log collection set up

To begin log collection:

1. Configure a ZYX Product virtual appliance.
2. Create a Collection Policy.
3. Create collection sources.
4. Verify log collection.
5. Create and apply a collection alert rule.
6. (Optional) Create a correlation policy.
7. (Optional) Create a correlation alert rule.

The ZYX Product remote collector log collection set up

To begin log collection:

1. Configure a ZYX Product remote collector.
2. Create a Collection Policy.
3. Create collection sources.
4. Verify log collection.
5. Create and apply a collection alert rule.
6. Create and apply a collection alert rule.

7. (Optional) Create a correlation policy.
8. (Optional) Create a correlation alert rule.

The ZYX Product physical appliance log collection set up

To begin log collection:

1. Configure a ZYX Product physical appliance.
2. Create a Collection Policy.
3. Verify log collection.
4. Create collection sources.
5. Create and apply a collection alert rule.
6. Create and apply a collection alert rule.
7. (Optional) Create a correlation policy.
8. (Optional) Create a correlation alert rule.

Verify log collection

After initial log source setup, it may take a few minutes before the new source appears and has registered on the sources page.

Once you have set up your log collection, you should verify your collection sources have registered in the ZYX Company user interface (UI) and are sending log data.

To verify log collection:

1. At the top of the ZYX Company UI, from the drop-down menu, select **ZYX Product**.
2. In the left navigation, under **Collection**, click **Sources**.
3. For each **log source** row, in the **Collection Enabled** column, verify the box contains a **yes**.
4. For each **log source** row, in the **Current Status** column, verify the box contains a new or ok label.
5. For each **log source** row, in the **Recent Message Hour Count** column, verify the box contains a number greater than or equal to one.
6. For each **log source** row, in the **Recent Message Hour Size** column, verify the box contains a number greater than or equal to one.

Maintain ZYX Product

ZYX Product provides 24x7x365 log collection. ZYX Product requires your participation to ensure that ZYX Company can continue to receive log data. The sections below detail your ongoing maintenance responsibilities and interactions with ZYX Product.

After ZYX Product is installed and configured

You must identify target systems, network devices, and applications within your environment and ensure that ZYX Product service assets are installed appropriately to enable log collection.

Maintain properly running networks and systems

ZYX Product depends upon a reliable connection from the ZYX Company service assets within the customer's network to ZYX Company's cloud environment. If the source network is unavailable for any reason then ZYX Company will not be responsible for the service level agreement for that period.

Update contact processes

To ensure timely communications in the event of a support issue, ZYX Company requires identification of a primary, secondary, and tertiary customer contact. To better integrate with existing customer and/or partner processes, ZYX Company can accommodate specific client-defined escalation preferences as well.