



Qualys Context Extended Detection and Response (XDR) Day 1 Enablement Guide

February 15, 2022

Copyright 2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

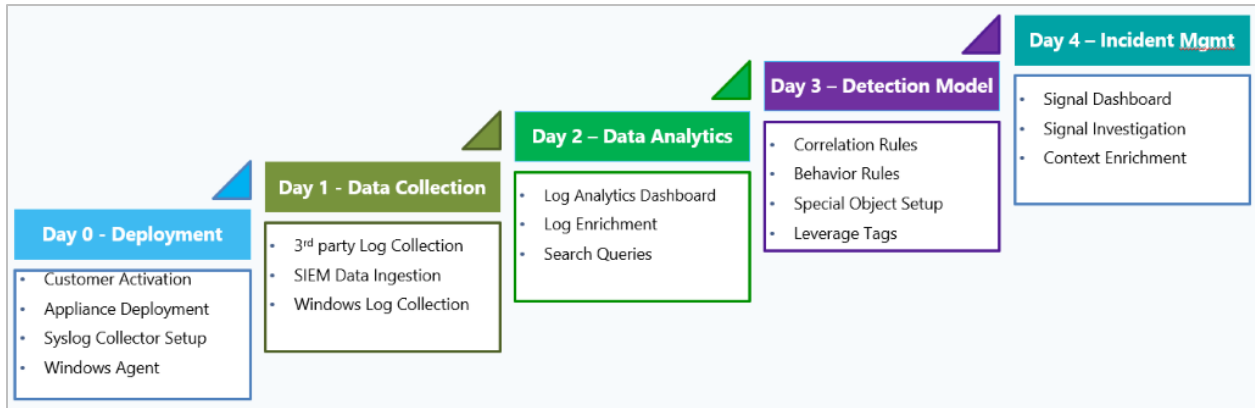
Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Summary	4
Day 1 – Data Collection	4
Collect Windows Logs using Qualys Cloud Agents	5
Collect Logs from Third-Party Sources	9

Summary

The purpose of this guide is to provide a detailed overview of how to enable Qualys Context Extended Detection and Response (XDR). Qualys splits the enabling process over several phases. This guide covers the activities of Day 1, during which Qualys Context XDR is configured for a variety of data collection.



Day 1 - Data Collection

On Day 1, we will walk you through the steps to:

1. Collect Windows Logs using Qualys Cloud Agents
2. Collect Logs from Third-Party Sources

NOTE: Before you proceed, ensure you have deployed an appliance and configured a collector as laid out in the Day 0 Enablement guide. Also, if you intend to use Qualys Cloud Agents to collect Windows logs, ensure that you have enabled the agents for XDR.

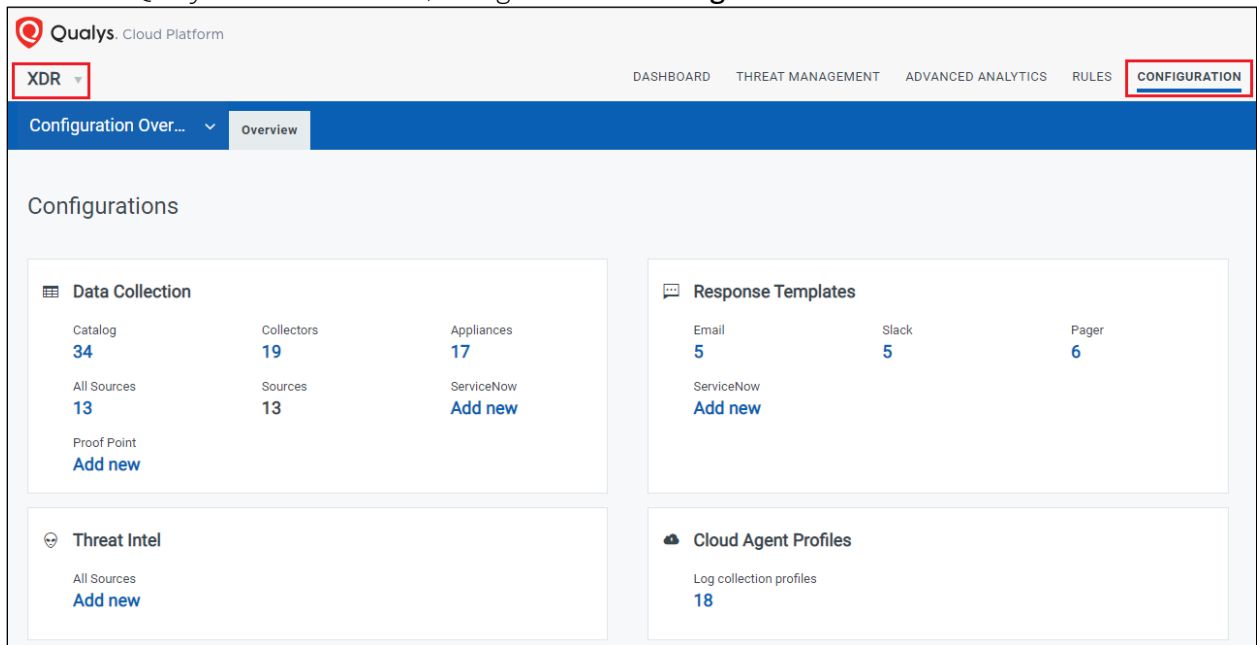
Collect Windows Logs using Qualys Cloud Agents

Qualys Context XDR allows you to leverage existing Qualys Cloud Agents (Windows only) to collect event logs from assets on which agents are deployed. You can also deploy fresh agents and configure them to collect logs for XDR.

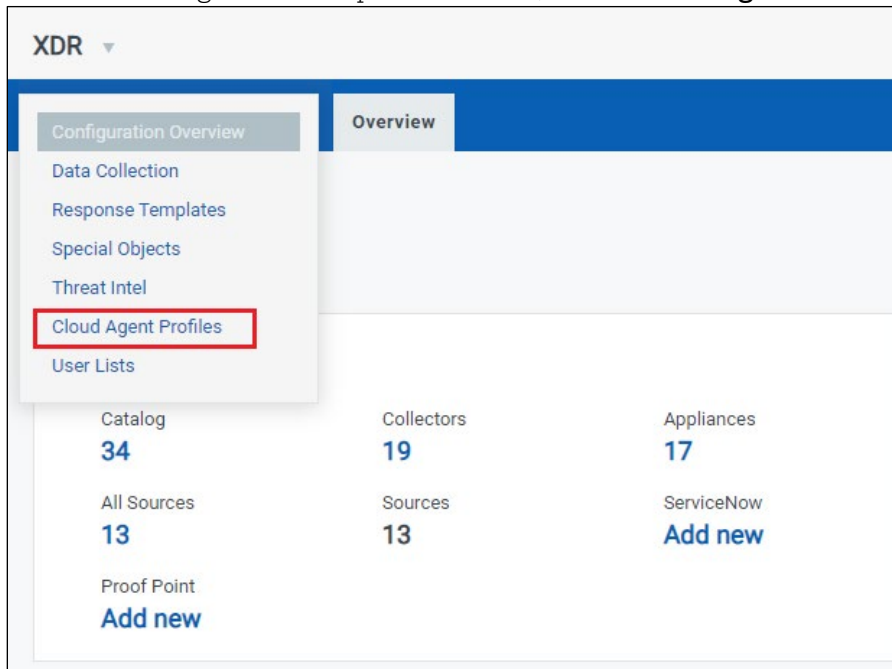
After you have enabled XDR via a configuration profile and activated agents for XDR as part of Day 0, you now need to create a Cloud Agent Profile to define what logs you want to collect from hosts, where you want to collect them, and the assets you want to collect from.

Follow these steps to configure a Cloud Agent Profile:

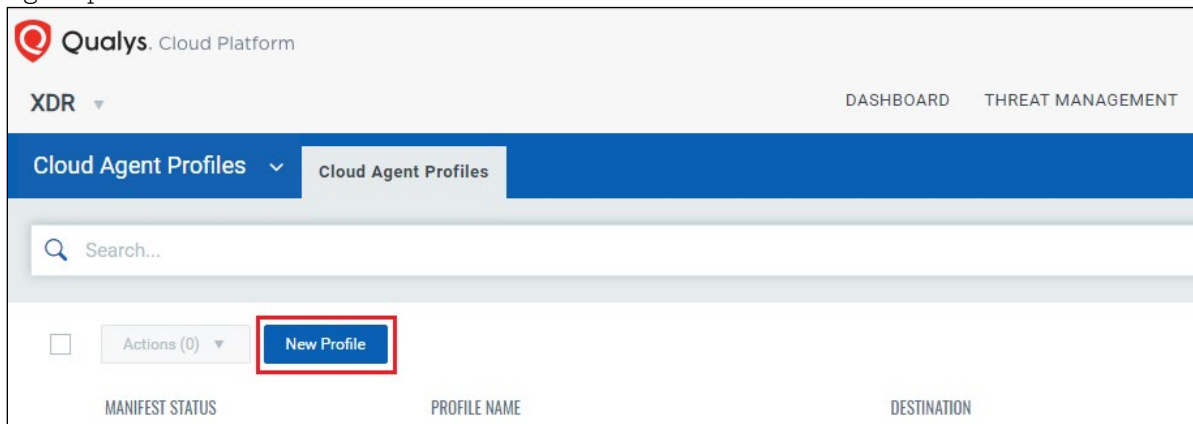
1. From the Qualys Context XDR UI, navigate to the **Configuration** tab.



- From the Configuration drop-down menu, select **Cloud Agent Profiles**.



- On the Cloud Agent Profiles tab, click the **New Profile** button to begin creating a new Cloud Agent profile.



4. Creating a new Cloud Agent Profile is a 4-step process. On the Basic Details step, enter a name and description for your profile. Also, select **Windows** as the **Operating System**. Click **Next** when done.

The screenshot shows the 'New Profile' wizard at Step 1/4, 'Profile Basic Details'. The left sidebar shows the progress: 1 Basic Detail (active), 2 Log Collection Details, 3 Destination Details, and 4 Assign Assets. The main content area has the following fields:

- Name ***: Text input field containing 'Test_profile'.
- Description**: Text area containing 'Test'.
- Operating System**: Dropdown menu with 'Windows' selected.

At the bottom, there are 'Cancel' and 'Next' buttons.

5. On the Log Collection Details step, select the type of logs you want to collect from hosts. Click **Next** when done.

The screenshot shows the 'New Profile' wizard at Step 2/4, 'Log Collection Details'. The left sidebar shows the progress: 1 Basic Detail, 2 Log Collection Details (active), 3 Destination Details, and 4 Assign Assets. The main content area has the following elements:

- Log Collection Details**: Section header.
- Please select atleast one type of log to collect from below list:**: Instructional text.
- Application
- Security
- System
- Windows Powershell
- DNS (Applicable to Windows Server Only)

At the bottom, there are 'Cancel' and 'Next' buttons.

- On the Destination Details step, choose where you want to forward the logs. You can choose to send the logs to Qualys Context XDR or to a third-party destination. If you decide to send it to a third-party destination, configure the destination details. Click **Next** when done.

The screenshot shows the 'New Profile' configuration page at Step 3/4, 'Destination Details'. The left sidebar shows the progress: 1 Basic Detail, 2 Log Collection Details, 3 Destination Details (current), and 4 Assign Assets. The main content area is titled 'Destination Details' and asks the user to 'Please select the destination where logs to be forwarded to:'. There are two radio button options: 'Extended Detection and Response' (selected) and 'Third Party Destination Details'. Below these are three input fields: 'Host IP/Host name *' with the value '192.168.2.1', 'Port *' with the value '534', and 'Protocol *' with a dropdown menu set to 'Select one'. At the bottom are 'Cancel' and 'Next' buttons.

- Next, select the assets you want to collect logs from. You can select assets directly or by selecting tags associated with these assets.

The screenshot shows the 'New Profile' configuration page at Step 4/4, 'Assign Assets'. The left sidebar shows the progress: 1 Basic Detail, 2 Log Collection Details, 3 Destination Details, and 4 Assign Assets (current). The main content area is titled 'Assign Assets' and asks the user to 'Select Assets for this profile'. There is a search bar containing 'WIN7-213 x' and 'WIN8-207 x', with a 'Select Assets' button below it. Below that, it asks to 'Select Asset Tags for this profile'. There is a search bar containing 'CM Tag x' and 'EUZ_San x', with a 'Select Asset Tags' button below it. At the bottom are 'Cancel' and 'Save Profile' buttons.

- Finally, click **Save Profile** to save this new Cloud Agent Profile.

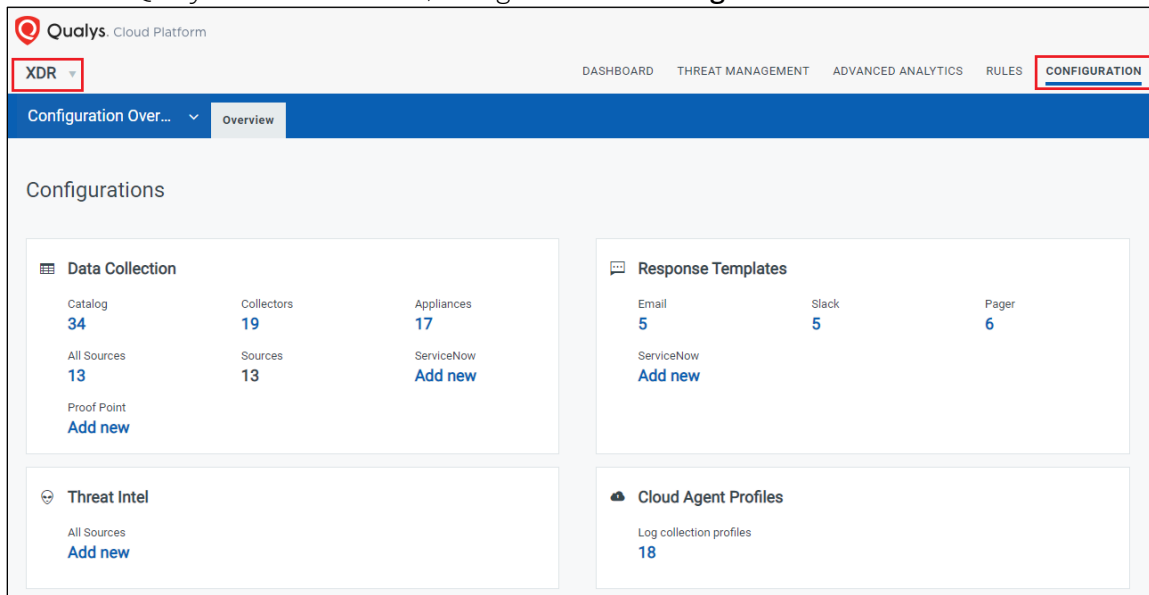
When the profile is created, Qualys Cloud Agents collect the logs you chose from the assets you selected and forwards them to the destination you configured.

Collect Logs from Third-Party Sources

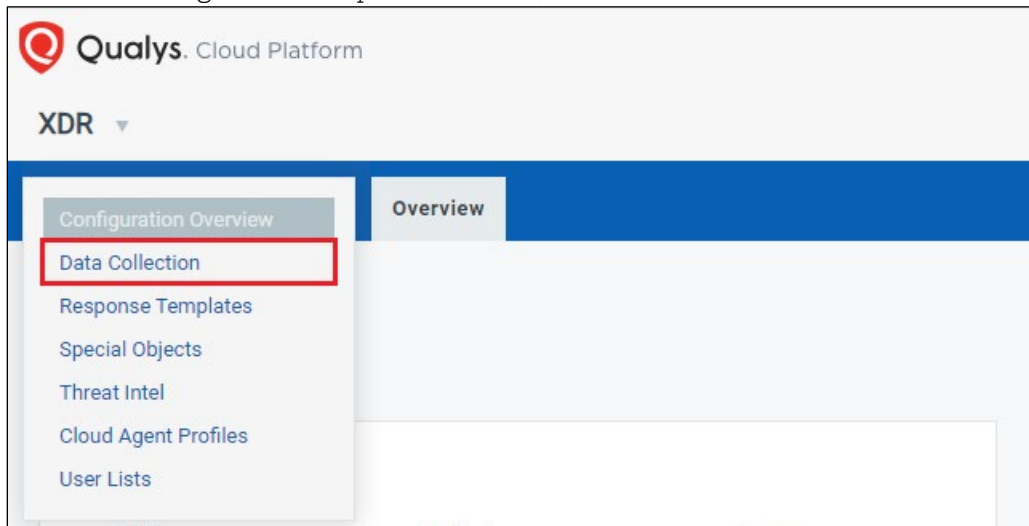
With Qualys Context XDR, you can ingest logs from several different third-party sources. Before you ingest data from other systems, ensure you have deployed an appliance and configured a collector on it. See the Online Help or the Day 0 Enablement guide for more information.

Follow these steps to configure XDR to receive logs from third-party sources:

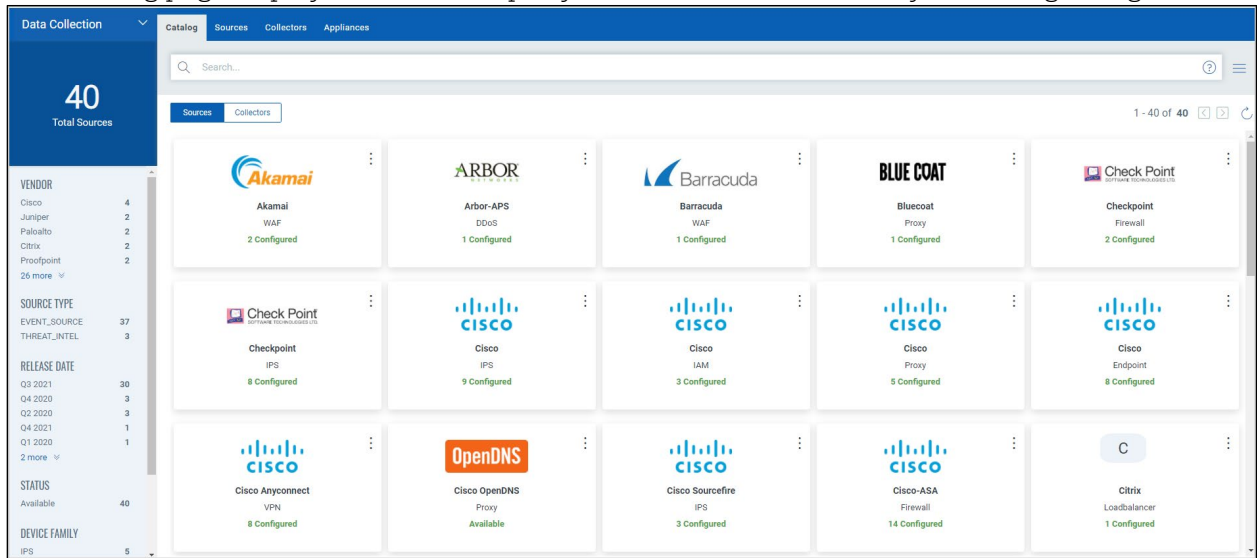
1. From the Qualys Context XDR UI, navigate to the **Configuration** tab.




2. From the Configuration drop-down menu, select **Data Collection** to view the Catalog page.

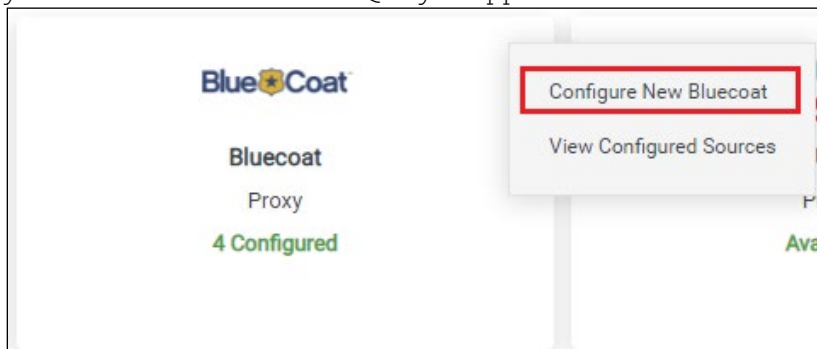


- The Catalog page displays all the third-party data sources from where you can ingest logs.

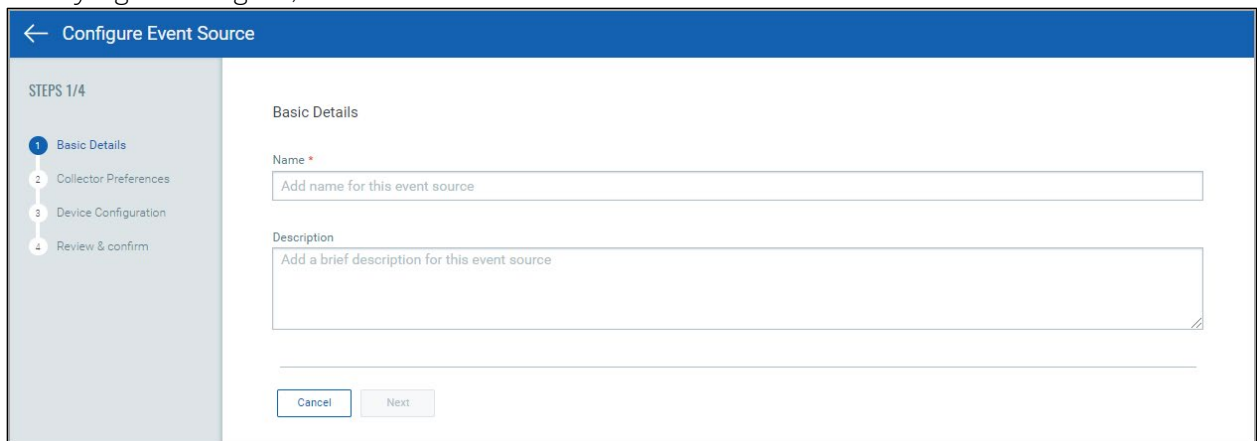


- In this guide, we will use Bluecoat Proxy as an example. Click the  icon on the Bluecoat Proxy card and then click the **Configure New Bluecoat** option.

NOTE: Each source might require different parameters, so if you run into any issues, contact your Solutions Architect or Qualys Support.



- On the Configure Event Source screen, enter a name and description for this data source you are trying to configure, and then click **Next**.



6. On the Collector Preferences step, select a collector that you want to use to collect data from this source. The **Collector** drop-down displays all the collectors you configured so far. If you do not have a collector configured so far, see the Online Help or the Day 0 Enablement guide.

← Configure Event Source

STEPS 2/4

- 1 Basic Details
- 2 Collector Preferences
- 3 Device Configuration
- 4 Review & confirm

Collection setup
Select from existing collectors to use a collector that has already been installed or click New Collector to create a new one.

Collector *
New_test-sys_10.114.252.16

Selected collector details

Name	New_test-sys_10.114.252.16
Description	New_test-sys_10.114.252.16
Status	Active
Created on	Jul 5, 2021 11:22 pm

Device Type *
Proxy

Model *
Bluecoat

Cancel Previous Next

7. Confirm the collector details, the device type, and the device model and click **Next**.
8. On the Device Configuration step, define the following:
 - i. **Log Format**
 - ii. **Version**
 - iii. **Host/IP Address of the Device Type** – Host/IP address of the device from where you want to send logs
 - iv. **Timezone**
 - v. **Filter** – Define a filter to include only events that match the specific attributes

← Configure Event Source

STEPS 3/4

- 1 Basic Details
- 2 Collector Preferences
- 3 Device Configuration
- 4 Review & confirm

Device Configuration

Log Format *
SYSLOG

Version *
v1.0

Host/IP Address of Device Type *
192.128.11.123

Timezone *
(GMT 00:00) Coordinated Universal Time (UTC UTC)

Filter ⓘ
Filters are used to identify eventsources and filter the events. For Ex. paloalto and (THREAT or CONFIG). For more info click on help

Cancel Previous Next

9. Finally, review all the configuration details before saving. If the details are correct, click **Add Event Source**.

The screenshot shows the 'Configure Event Source' interface. On the left, a sidebar indicates the current step is 4/4, 'Review & confirm'. The main area is divided into sections: 'Basic Details', 'Selected collector details', and 'Device Configuration'. At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Add Event Source'.

Basic Details	
Name	sf
Description	

Selected collector details	
Name	New_test-sys_10.114.252.16
Description	New_test-sys_10.114.252.16
Status	Active
Created on	Jul 5, 2021 11:22 pm

Device Configuration	
Device Type	Proxy
Device Model	Bluecoat
Log Format	SYSLOG
Version	v1.0
Host/IP Address	192.128.11.123
Directory Configuration	NA
TimeZone	UTC
Filter	

When the event source is configured, the event source is listed under **Configuration > Data Collection > Sources** tab. Based on your configurations, the event source will start receiving data from this source on the configured appliance's IP address and collector's port address.

NOTE: For information on collecting logs from ServiceNow or Proof Point, refer the Online Help.