

# **Azure Defender for IoT Data Connector Configuration**

**Table of Contents**

1. Getting Started
   * Prerequisites
   * Installation
2. Usage
3. Contact

**Getting Started**

Use the following steps to correctly configure Defender for IoT data connector in your Azure Sentinel instance

This Data connector contains the following components:

1. Configuration of Syslog Server
2. Installing of Azure Sentinel Parser
3. Configuration of Azure Sentinel Watchlist

**Prerequisites**

* Instance of Azure Sentinel [Deployed](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard).

**Installation**

## Syslog Server Configuration

**1. Linux Syslog agent configuration**

Install and configure the Linux agent to collect your Common Event Format (CEF) Syslog messages and forward them to Azure Sentinel.

Notice that the data from all regions will be stored in the selected workspace

**1.1 Select or create a Linux machine**

Select or create a Linux machine that Azure Sentinel will use as the proxy between your security solution and Azure Sentinel this machine can be on your on-prem environment, Azure or other clouds.

**1.2 Install the CEF collector on the Linux machine**

Install the Microsoft Monitoring Agent on your Linux machine and configure the machine to listen on the necessary port and forward messages to your Azure Sentinel workspace. The CEF collector collects CEF messages on port 514 TCP.

1. Make sure that you have Python on your machine using the following command: python –version.
2. You must have elevated permissions (sudo) on your machine.
3. The install script can be located under **CEF data connector** in Azure Sentinel

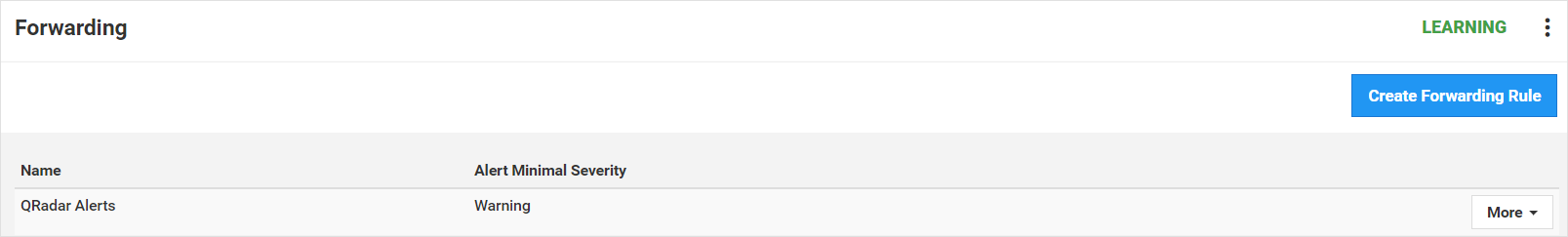
Graphical user interface, text, application

Description automatically generated

**2. Forward Common Event Format (CEF) logs to Syslog agent**

To create a new forwarding rule on a IoT sensor:

1. Sign into the sensor.
2. Select **Forwarding** on the side menu.
3. Select **Create** Forwarding Rule.



1. Enter a name for the forwarding rule.
2. Select **Warning and Above** option from severity level drop down.
3. Set protocols drop down to **ALL**.

1. Set the Engines drop down to **ALL**.
2. Select Send To SYSLOG Server (CEF Format) for actions drop down
3. Enter syslog host IP address and set port to 514

Graphical user interface, application, email

Description automatically generated

1. Click Submit to create the forwarding rule

## Installing Azure Sentinel Parser

**1. Install Log Analytics Parser**

1. Navigate to \*\*\*Enter URL for Parser Here
2. Copy parser query available
3. Navigate to **Azure Sentinel->Logs** and paste the parser query
4. Select **Save As Function**
5. Provide function name as **DefenderForIoT\_CL** and save

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

## Configuration of Azure Sentinel Watchlist

Watchlist is only required if you want the IoT-Hub Device name to be included in the **DefenderForIoT\_CL** table. If not need than edit the Function query in the previous step to remove WatchList dependency. Having IoT-Device name will help identify the correct IoT-Hub for incident response.

Graphical user interface, text, application, email

Description automatically generated

**1. Create CSV Upload File**

1. Create a two column CSV file. Column names should set as below

***Note:*** Column name should be exactly as shown below. Use the template provided here.

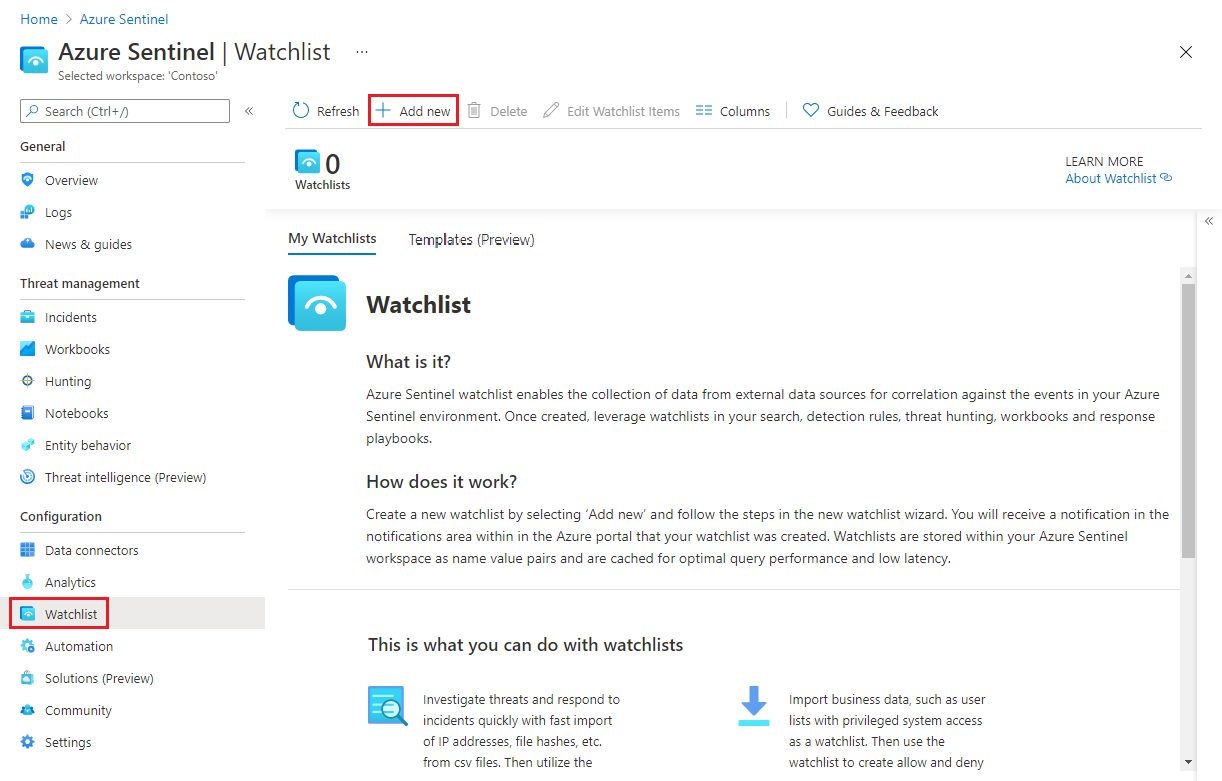
Graphical user interface, application, table, Excel

Description automatically generated

1. SrcIP Column should have IP address assigned to individual IoT Devices and IoTHubDevice\_Name column should have the corresponding IoT Service Device name (e.g. Azure IoT Hub Device name)

## **2. Create a new watchlist**

1. From the Azure portal, navigate to **Azure Sentinel** > **Configuration** > **Watchlist** and then select **+ Add new**.

[](https://docs.microsoft.com/en-us/azure/sentinel/media/watchlists/sentinel-watchlist-new.png#lightbox)

1. On the **General** page, provide the following details

Name: **D4IoT\_Watchlist**

Description: **Used by DefenderForIoT parser Function**

Alias: **D4IoT\_Watchlist**

Graphical user interface, text, application, email

Description automatically generated

1. Select **Next: Source**.
2. On the **Source** page, select the dataset type (currently only CSV is available)
   1. Click the **Browse for files** link in the **Upload file** box and select the CSV file create in the previous step and upload.
   2. You will see a preview of the first 50 rows of results in the wizard screen.
3. In the **SearchKey** field, Select **SrcIP**
4. Select **Next: Review and Create**.

Graphical user interface, text, application, email

Description automatically generated

**Usage**

After the parser is install correctly, you can query **DefenderForIoT\_CL** table in Azure Sentinel logs.

Graphical user interface, application

Description automatically generated

**Contact**

Email: [MicrosoftTeam@criticalstart.com](mailto:MicrosoftTeam@criticalstart.com)

**About**

Add Something Here