Tenable.ot Log Extension for QRadar

Version 3.7

Revision History

Product version: Tenable.ot 3.7

Document revision history:

Document Revision	Date	Description
1.0	September 6, 2020	Document created for Tenable.ot version 3.7

Table of Contents

Overview

Tenable.ot enables operational engineers and cyber security personnel to gain visibility into and control over Industrial Control System (ICS) networks. Through its policies and alerts mechanism, Tenable.ot generates real-time alerts that are accurate, actionable, and customized for each network and its unique needs.

Tenable.ot detects unauthorized changes made to industrial processes in ICS networks. It can produce various alerts on changes in the configuration of controllers (PLC, DCS, IED), details, communications, and alert on a range of network attack vectors that may threaten industrial processes. Tenable.ot also actively verifies the controllers' configuration and alerts on changes made to them.

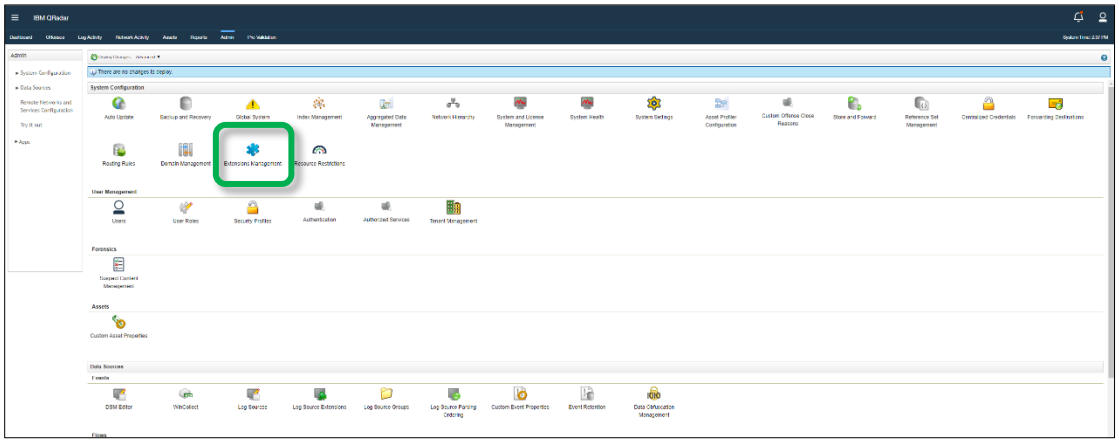
Tenable.ot reports these alerts to QRadar via Syslog. For each individual policy, users can decide whether an alert should be sent to QRadar via Syslog; this offers them maximum control over which information is being sent.

Installing the Tenable.ot Extension

In order to integrate Tenable.ot with your QRadar system, you need to download the *Tenable.ot extension* from the IBM X-Force Exchange and install it.

➡ **To download and install the extension:**

1. In the IBM QRadar console, open the **Admin** tab.
2. In the **System Configuration** section, click on **Extension Management.**

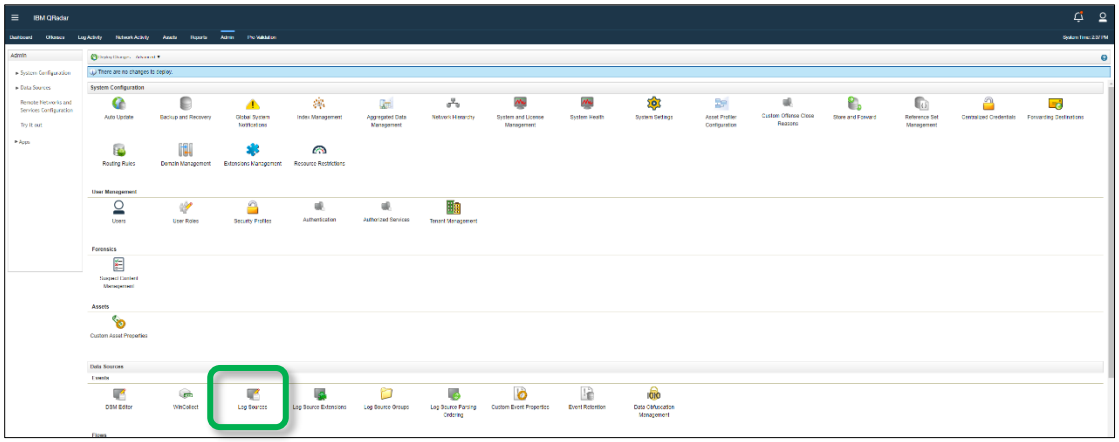


3. In the **Extension Management** window, click **Add** and select the *TenableotCustom_ext* archive file.
4. Select the **Install Immediately** checkbox to install the extension immediately.
   Before the extension is installed, a preview list of the content items is displayed.

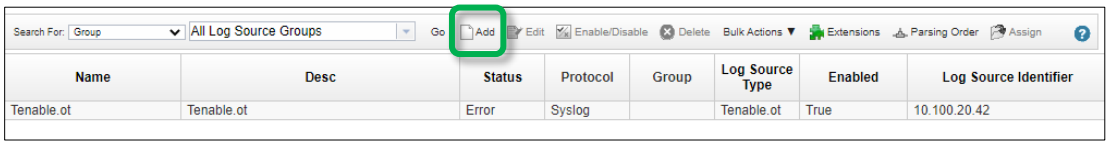
Configuring a Tenable.ot Log Source

➡ **To configure Tenable.ot as a log source:**

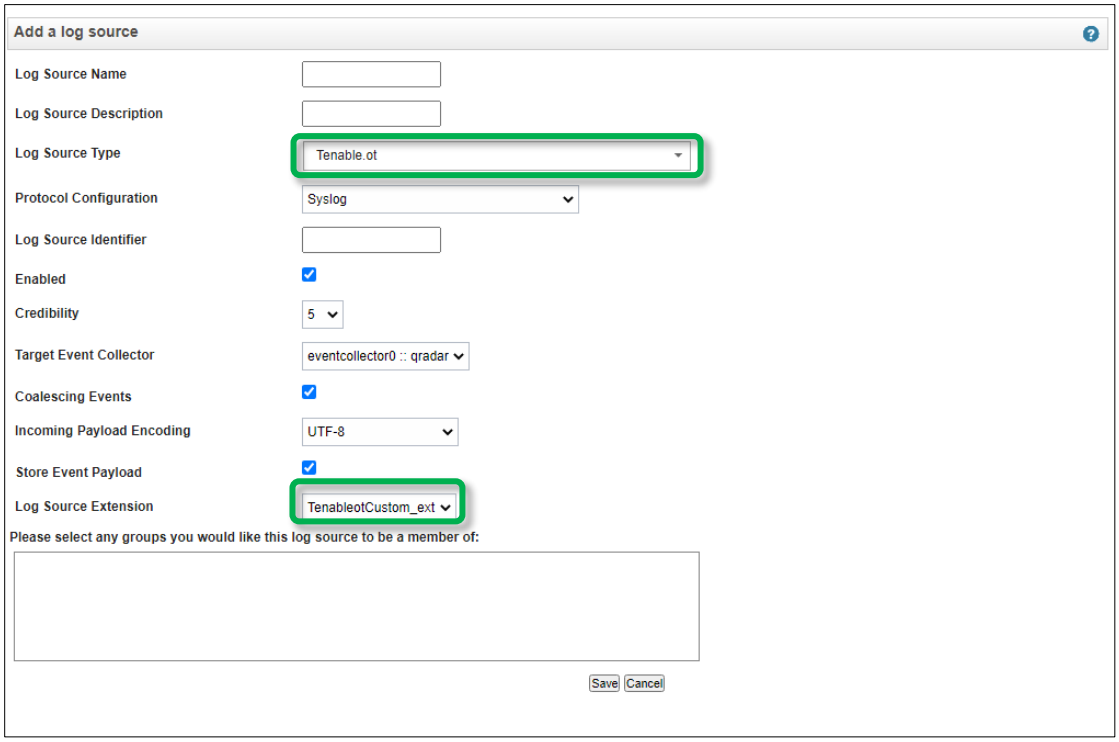
1. In the **Data Sources** section of the **Admin** tab, click on **Log Sources**.



2. In the Log Source window click on **Add**.



The Add a log source window opens.



3. In the **Log Source Type** field, select ***Tenable.ot.***
4. In the **Log Source Extension** field, select ***TenableotCustom_ext***.
5. Fill in the additional fields as needed and click **Save**.

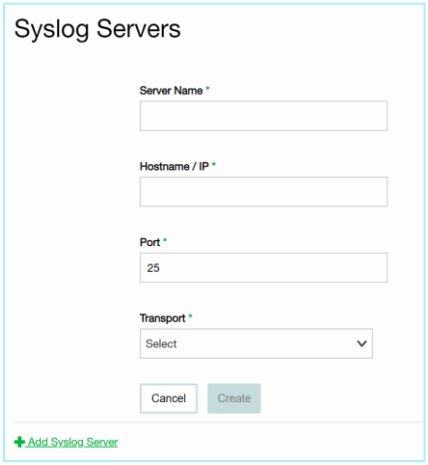
Sending Tenable.ot Alerts to QRadar

In order to send Tenable.ot alerts to QRadar, you first need to configure Tenable.ot for your QRadar system. Then, for each relevant Policy, you can specify QRadar as a target for receiving alerts.

Connecting QRadar to Tenable.ot

➡ **To connect your QRadar Syslog serever to Tenable.ot:**

1. In the Tenable.ot console, under **Local Settings**, go to **Servers** > **Syslog Servers** screen.
2. Click **+ Add Syslog Server**.
   The **Syslog Server** configuration window is displayed.



3. In the **Server Name** field, enter a name for your QRadar system.
4. In the **Hostname\IP** field, enter the IP of your QRadar system.
5. In the **Port** field, enter the port number on the QRadar system to which the events will be sent. (Default: 514)
6. In the **Transport** field, select from the dropdown list the transport protocol to be used. Options are *TCP* or *UDP*.
7. Click **Send Test Message** to send a test message to verify that the configuration was successful, and check if the message has arrived. If the message did not arrive, then troubleshoot to discover the cause of the problem and correct it.
8. Click **Save**.

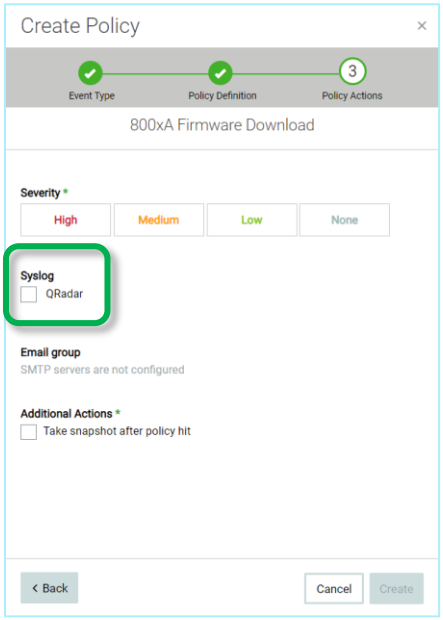
Specifying QRadar as a Target for Policy Alerts

For each Policy shown on the Polices screen of the Tenable.ot console, you can configure the Policy to send alert notifications via Syslog to your QRadar system. This can be done when creating a new policy or when editing an existing one. You can use a bulk action to add QRadar to several Policies at once. All new alerts generated from Tenable.ot for the specified Policies will flow regularly to QRadar and be mapped to QRadar events through the log source extension.

	Only Policies that were specifically configured to do so will send alerts to your QRadar system.

To configure a Policy to send alerts to QRadar:

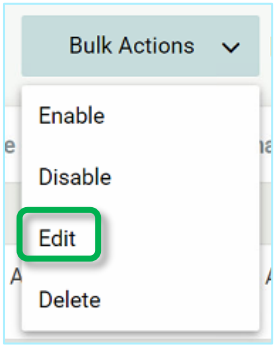
1. Create a new Policy or edit an existing Policy.
2. Fill in all fields as needed.
3. On the **Policy Actions** page, under **Syslog**, select your QRadar system.



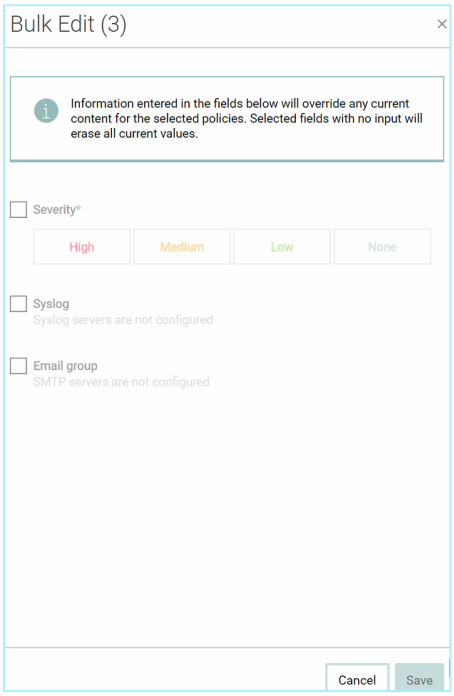
4. Click **Create** (or **Save** if you are editing a Policy).

To configure multiple Policies (bulk process) to send alerts to QRadar:

1. On the **Policies** screen, select the checkbox next each of the desired Policies.
2. Click on the **Bulk Actions** menu and select **Edit** from the dropdown list.



The **Bulk Edit** screen is shown with the Policy Actions available for bulk editing.



3. Under **Syslog**, select the checkbox next to your QRadar system.
4. Click **Save**.
   The Policies are saved with the new configuration.