Tenable and IBM QRadar SIEM v3.0 Integration Guide

Last Revised: February 11, 2022
# Table of Contents

Welcome to Tenable for IBM QRadar SIEM ................................................................. 3  
Install Tenable App for QRadar ................................................................................. 4  
Configuration ........................................................................................................... 6  
  Tenable.io Configuration ......................................................................................... 7  
  Tenable.sc Configuration ....................................................................................... 10  
  Tenable.ot Configuration ...................................................................................... 13  
    Sending Tenable.ot Alerts to QRadar ................................................................. 17  
  Tenable.ot Log Extension for QRadar .................................................................. 22  
  Tenable.ad Configuration ...................................................................................... 25  
    Sending Tenable.ad Alerts to QRadar ................................................................. 29  
    Tenable.ad Log Extension for QRadar ............................................................... 34  
Configure Rule-Based Scanning ............................................................................... 37  
Configure Right-Click Scanning ............................................................................... 41  
View Offenses ........................................................................................................ 44  
Uninstall ................................................................................................................ 45  
Troubleshooting ..................................................................................................... 46
Welcome to Tenable for IBM QRadar SIEM

This document provides information and steps for integrating Tenable.io and Tenable.sc applications with IBM QRadar Security Information and Event Management (SIEM).

IBM QRadar SIEM (QRadar) is a network security management platform that provides situational awareness and compliance support. It collects, processes, aggregates, and stores network data in real time. QRadar has a modular architecture that provides real-time visibility of your IT infrastructure that you can use for threat detection and prioritization.

You can use the customized Tenable applications in QRadar. to obtain vulnerability summaries for Tenable.io or Tenable.sc that correspond to the source IP address for each offense.

For additional information about IBM QRadar SIEM, see the IBM QRadar SIEM website.
Install Tenable App for QRadar

Complete the following steps to install the Tenable App For QRadar.

Before you begin:

- Ensure you have a Tenable.io or Tenable.sc account with administrative privileges.
- Ensure you have QRadar 7.4.1+
- Download the Tenable App For QRadar v3.0 from the IBM App Exchange website.

To upgrade the Tenable App For QRadar:

1. Log in to the IBM QRadar SIEM Console.
2. Click the button. The Menu options appear.
5. Click Add. The Add a New Extension window appears.
6. Click Browse and select the Tenable App For QRadar file.
7. Click Add. A Confirm Installation window appears.
8. Click Install. A validation window appears.
9. After the validation completes, the Tenable App For QRadar window appears.
10. Click **Install**.

   A validation window appears.

   A docker container is created.

   After the validation completes, the **Tenable App** appears in the list of **Applications Packages** on the **Tenable App For QRadar** window.

11. Click **OK**.

12. Clear the browser cache and refresh the page.

   The **Tenable App For QRadar** appears on the **Extensions Management** page.
Configuration

You can configure QRadar with Tenable.io or Tenable.sc. Click the corresponding link for configuration steps.

- Tenable.io Configuration
- Tenable.sc Configuration
- Tenable.ot Configuration
- Tenable.ad Configuration
Tenable.io Configuration

**Required Tenable.io Vulnerability Management User Role:** Basic, VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

Complete the following steps to configure the **Tenable App For QRadar**.

To configure the **Tenable App For QRadar**:

1. Log in to the IBM QRadar SIEM Console.
2. Click the ☰ button.
   
   The **Menu** options appear.
3. Click **Admin**.
   
   The **Admin** options appear.
4. Scroll to the **Tenable** section.
5. Click **Tenable App Settings**.
   
   The **Tenable Configuration** appears.
6. Click **Add Tenable.io Account**.
7. Configure the settings for Tenable.io.
a. In the **Address** box, enter the domain name used to access Tenable.io.

b. In the **Access Key** box, enter the API access key for Tenable.io. For information on generating API keys see the [Generate API Key](#) section in the *Tenable.io User Guide*.

c. In the **Secret Key** box, enter the API secret key for Tenable.io. For information on generating API keys see the [Generate API Key](#) section in the *Tenable.io User Guide*.

d. In the **Rule based Scan Name** box, enter a scan name that exists in Tenable.io.

   **Note:** If a scan does not exist, you must create one. The scan needs to be associated to the Tenable user that Qradar logs into the Tenable product with. This scan is used for the rule-based scan function.

e. In the **Right Click Scan Name** box, enter a scan name that exists in Tenable.io.
Note: If a scan does not exist, you must create one. The scan needs to be associated to the Tenable user that QRadar logs into the Tenable product with. This scan is used for the right-click scan function.

Note: This scan can be the same as the Rule Based Scan Name.

f. In the **Authorized Service Token** box, enter your QRadar authorized service token. Authorized tokens are found under **User Management** in the **Authorized Services** section.

   See the [IBM QRadar SIEM](https://ibm.com/qradar) website for steps on creating an authorized service token.

g. (Optional) Click the toggle to enable or disable SSL verification.

h. (Optional) Connect to Tenable.io using a proxy.

   - Click the toggle to **Enable/Disable Proxy**.
   - Type an **IP/Hostname**.
   - Type a **Port**.
   - (Optional) Select the **Require Authentication for Proxy** check box.
   - If you required authentication for proxy, type the proxy **Username**, **Password**, and **Confirm Password**.

8. Click **Save**.

   The **Tenable Configuration** window appears and displays a success message.

9. Create an **Offense Rule** to generate offenses for the offense rule. For steps on creating offense rules, see the [IBM QRadar SIEM documentation](https://ibm.com/qradar).
Tenable.sc Configuration

**Required User Role:** Security Analyst

**Note:** In Tenable App for QRadar v2 and later, you must authenticate using an API Access Key and Secret Key. For more information, see the [Generate API](#) section in the *Tenable.sc User Guide*.

Complete the following steps to configure the **Tenable App For QRadar** v2.0.

To configure **Tenable App For QRadar** v2.0:

1. Log in to the IBM QRadar SIEM console.
2. Click the **Menu** button.
   
   The **Menu** options appear.
3. Click **Admin**.
   
   The **Admin** options appear.
4. Scroll to the **Tenable** section.
5. Click **Tenable App Settings**.
   
   The **Tenable Configuration** appears.
6. Click **Add Tenable.sc Account**.
7. Configure the settings for Tenable.sc.
In the **Address** box, enter the IP address used to access Tenable.sc.

- In the **Access Key** box, enter your generated Tenable.sc access key. For more information, see [Enable API Key Authentication](#) and [Generate API Keys](#).

- In the **Secret Key** box, enter your generated Tenable.sc secret key. For more information, see [Enable API Key Authentication](#) and [Generate API Keys](#).

- In the **Rule based Scan Name** box, enter a scan name that exists in Tenable.sc. **Note:** If a scan does not exist, you must create one. The scan needs to be associated to the Tenable user that Qradar logs into the Tenable product with. This scan is used for the rule-based scan function.

- In the **Right Click Scan Name** box, enter a scan name that exists in Tenable.sc.
f. In the **Authorized Service Token** box, enter your Qradar authorized service token. Authorized tokens are found under **User Management** in the **Authorized Services** section.

   See the [IBM Qradar SIEM](https://ibm.com/qradar) website for steps on creating an authorized service token.

   g. (Optional) Click the toggle to enable or disable SSL verification. It may be required to enter the hostname of the machine hosting Tenable.sc in the **Address** box.

   h. (Optional) Connect to Tenable.sc using a proxy.

   - Click the **Enable/Disable Proxy** toggle.
   - Type an **IP/Hostname**.
   - Type a **Port**.
   - (Optional) Select the **Require Authentication for Proxy** check box.
   - If you required authentication for proxy, type the proxy **Username**, **Password**, and **Confirm Password**.

8. Click **Save**.

   The **Tenable Configuration** window appears and displays a success message.

9. Create an **Offense Rule** to generate offenses for the offense rule. For steps on creating offense rules, see the [IBM Qradar SIEM documentation](https://ibm.com/qradar).
Tenable.ot Configuration

Complete the following steps to configure the Tenable.ot App For QRadar v2.0.

To create a log source, through the Log Source Management application for ingesting data, from the Tenable platform:

1. Go to the QRadar Log Source Management application in the Admin panel.

The Log Source Management page appears.
2. Click **New Log Source** in the upper-right.

   The Log Source Management page appears.

3. Select **Tenable.ot Platform** as the Log Source type.
4. Select **Syslog** as the **protocol type**.

5. In the **Configure Log Source Parameters** section, enter the name of the log source in the **Name** box.
a. Enable the log source by clicking the Enabled/Disabled switch to Enabled.

b. Select TenableotPlatformCustom_ext as the log source extension.

c. Disable Coalescing Events by clicking the Enabled/Disabled switch to Disabled

6. In the Configure Protocol Parameters section, enter the Log Source Identifier. This Identifier is the hostname/IP address from the data to be forwarded.

7. Click Finish.
Sending Tenable.ot Alerts to QRadar

Overview

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 server to Tenable.ot:

1. In the Tenable.ot console, under Local Settings, go to the 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 address 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 value is 514)

6. In the **Transport** field, select from the drop-down 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**

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 check box next each of the desired Policies.

2. Click on the **Bulk Actions** menu and select **Edit** from the drop-down list.
3. The **Bulk Edit** screen is shown with the Policy Actions available for bulk editing.
4. Under **Syslog**, select the check box next to your QRadar system.

5. Click **Save**.

The Policies are saved with the new configuration.
Tenable.ot Log Extension for QRadar

Overview

Tenable.ot enables operational engineers and cybersecurity 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**.
3. The **Add a log source** window opens.

4. In the **Log Source Type** field, select **Tenable.ot**.

5. In the **Log Source Extension** field, select **TenableotCustom_ext**.

6. Fill in the additional fields as needed and click **Save**.

For information on how to send alerts to QRadar, see [Sending Tenable.ot Alerts to QRadar](#).
Tenable.ad Configuration

Complete the following steps to configure the Tenable.ad App For QRadar.

To create a log source, through the Log Source Management application for ingesting data, from the Tenable platform:

1. Go to the QRadar Log Source Management application in the Admin panel.

The Log Source Management page appears.
2. Click **New Log Source** in the upper-right.

   The *Add a Single Log Source* page appears.

3. Select **Tenable.ad** as the **Log Source type**.
4. Select **Syslog** as the protocol type.

5. In the **Configure Log Source Parameters** section, enter the name of the log source in the **Name** box.
a. Enable the log source by clicking the **Enabled/Disabled** switch to **Enabled**.

b. Select **TenableadCustom_ext** as the log source extension.

c. Disable **Coalescing Events** by clicking the **Enabled/Disabled** switch to **Disabled**.

6. In the **Configure Protocol Parameters** section, enter the **Log Source Identifier**. This Identifier is the hostname/IP address from the data to be forwarded.

7. Click **Finish**.
Sending Tenable.ad Alerts to QRadar

Overview

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

Connecting QRadar to Tenable.ad

To connect your QRadar Syslog server to Tenable.ad:

1. In the Tenable.ad console, under Local Settings, go to the Servers > Syslog Servers screen.
2. Click + Add Syslog Server.

   The Syslog Server configuration window appears.
3. In the **Server Name** field, enter a name for your QRadar system.

4. In the **Hostname/IP** field, enter the IP address 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 value is 514)

6. In the **Transport** field, select from the drop-down 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**
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 check box next each of the desired Policies.

2. Click on the **Bulk Actions** menu and select **Edit** from the drop-down list.

3. The **Bulk Edit** screen is shown with the Policy Actions available for bulk editing.
4. Under **Syslog**, select the check box next to your QRadar system.

5. Click **Save**.

   The Policies are saved with the new configuration.
Tenable.ad Log Extension for QRadar

Overview

Tenable.ad features allow users to anticipate threats, detect breaches, and respond to incidents and attacks. Through its policies and alerts mechanism, Tenable.ad generates real-time alerts that are accurate, actionable, and customized for each network and its unique needs.

Tenable.ad 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.ad Extension

In order to integrate Tenable.ad with your QRadar system, you need to download the Tenable.ad 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 appears.

**Configuring a Tenable.ad Log Source**

To configure Tenable.ad 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.ad*.

4. In the **Log Source Extension** field, select *TenableadCustom_ext*.

5. Fill in the additional fields as needed and click **Save**.

For information on how to send alerts to QRadar, see [Sending Tenable.ad Alerts to QRadar](#).
Configure Rule-Based Scanning

In QRadar, you can create a rule based on SIEM data. If the rule conditions are found, a scan launches on the requested IP address. You can also right click an IP address in QRadar to initiate a scan. When scans are launched, rules with the associated IP address scan Tenable.io and Tenable.sc.

A background script runs periodically to launch scans on the IP address. The default time for run is 1200 seconds.

Complete the following steps to create a rule in your Tenable application for IBM QRadar SIEM.

To create a rule:

1. On the IBM QRadar SIEM console, click the button.

   The **Menu** options appear.

2. Click **Offenses**.

   The **Offenses** menu appears.

3. In the **Offenses** menu, click **Rules**.

   The **Rules** page appears.

4. In the **Rules** menu, click **Actions**.

   A drop-down box appears.

5. Select one of the **New Rule** options.

   The **Rule Wizard** window appears.

6. Click **Next**.

7. Select the source where the rules are generated.
8. Click **Next**.

9. Follow the **Rule Wizard** steps to continue the rule configurations.

**Note:** In the **Rule Response** section, you must add the Tenable source IP.
a. In the **Rule Response** section, click the **Add to a Reference** check box.

A drop-down appears.

b. In the drop-down, select **Tenable.io scan IP** or **Tenable.sc scan IP**.

Note: If you want to launch a scan for source IP and destination for both Tenable.io and Tenable.sc, you must create four rules: 1) Scan source IP with Tenable.io, 2) Scan source IP with Tenable.sc, 3) Scan destination IP with Tenable.io, and 4) Scan destination IP with Tenable.sc.

10. After you make your rules selections, click **Finish**.
Configure Right-Click Scanning

QRadar users and administrators can initiate a scan against an IP address by right-clicking on it. In the right-click menu, two buttons, “Tenable.sc scan” and “Tenable.io scan”, initiate a scan against that IP on Tenable.sc or Tenable.io. The user can see the latest scan status of the initiated scan in the dashboard.

To use the right-click scanning for IBM QRadar SIEM:

1. In the QRadar dashboard, click the Log Activity tab in the upper-left.

   The events and log items page appears.

2. Under the Source IP column, right-click on any IP address.

   The pop-up menu options appear.
3. Click **More Options** (if available).

The **Admin** options appear.

4. Click **Tenable.sc scan** or **Tenable.io scan**.

A **Tenable Scan Details** pop-up window opens and the scan initiates.

After successfully initiating, the pop-up window shows information such as:

- Scan Name, Scan ID, Scan Description, Scan Result ID or History ID, Platform, IP Address, and Scan Status.

5. The scan details will be reflected in the dashboard.
Note: You will not be able to launch a scan multiple times on the same, or different, IP addresses until the previous scan is completed for Tenable.io.
View Offenses

After you create an offense rule, the offenses are added to the All Offenses table. Use the Tenable IO: Vulnerability Summary and Tenable SC: Vulnerability Summary buttons to view enriched offense data. Complete the following steps to view the offenses.

For additional information on viewing offenses, see the IBM QRadar SIEM documentation.
Uninstall

To uninstall the Tenable App for IBM QRadar SIEM:

1. On the IBM QRadar SIEM console, click the ☐️ button. The Menu options appear.
2. Click Admin. The Admin options appear.
3. In the System Configuration section, click Extensions Management. The Extensions Management page appears.
4. Click Tenable App for QRadar.
5. Click Uninstall.
Troubleshooting

• **After clicking the action buttons for Tenable.io or Tenable.sc, you get an alert with the message: “Check if the configuration page details are filled.”**

  This occurs if you did not configure an account on the **Configuration** page. See the [Tenable.io Configuration](#) page for steps on how to configure an account.

• **Offense note shows the configuration error message: “Error while reading configurations.”**

  Your configuration file may have been corrupted.

  This can also occur if you upgraded the application to v2.0. from a previous version and you did not reconfigure your files. If you did this, delete the configurations from the configurations page and reconfigure the credentials.

• **How do I view my log files?**

  a. Log in to your QRadar instance.

  b. In the **Admin** section, click **System and License Management**.

  c. Select the host on which the Tenable App is installed.

  d. In the top section, click **Actions** and select **Collect Log Files**.

    The **Log File Collection** window appears.

  e. Click **Advanced Options**.

  f. Click the check box to select **Debug Logs, Application Extension Logs**, and **Setup Logs**.

  g. For data input, select **5 days**.

  h. Click the **Collect Log Files** button.

  i. Click **Click here to download files**.

    The log files download in a zip file on your local machine.
• The configuration page shows the error message: “Failed due to proxy error or invalid credentials. Check logs for more detail.”

Verify that you entered valid credentials for the configuration or proxy.

• New configuration shows the error message: “Failed due to network connection timeout or Failed Proxy Authentication or invalid server address. Check logs for more details.”

This occurs when either the internet for the virtual machine (VM) is down, proxy authentication needs more credentials to proceed, or the provided server address is Invalid. Verify that the internet for your VM is operational, the entered proxy credentials are valid, and the server address is correct.

• New configuration shows the error message: “401 - Authorization service token is not valid.”

You entered an incorrect authorization service token. Enter the correct service token.

• An alert pop-up shows the error message: “Check if the configuration page details are filled.”

Check that you correctly configured your Tenable.io or Tenable.sc account.

• An alert pop-up shows the error message “Failed due to network connection timeout or Failed Proxy Authentication. Check logs for more details.”

This occurs when you have an internet connectivity problem on the VM or proxy authentication failed. Verify the Internet is on and valid proxy credentials are entered.

• An alert pop-up shows the error message “Please enter a valid Address or configure valid proxy settings or verify SSL certificate.”

If you have verified that the Address is set to the IP/FQDN of your Tenable.sc configuration, try disabling the Enable/Disable SSL Verification option and resubmitting. If the error persists, please open a case with Tenable Tech Support.

• An alert pop-up shows the error message “Failed due to invalid credentials or connection error.”
This occurs when Tenable.io or Tenable.sc credentials are updated in the Tenable system, but the updates are not made in the QRadar configuration page. Add the updated credentials to the configuration page.

- **Container proxy settings were overridden, causing the application to stop working as expected.**

The configuration must be updated to allow the local proxy on the application to make tunneled connections. For steps on updating the proxy connections, see the [IBM QRadar Support Documentation](#).

- **An alert pop up shows the error message: "Failed to connect flask server."**

When there are multiple IP addresses or multiple vulnerabilities for all of the IP addresses present in the offense, it may take more than one minute to fetch vulnerability data from Tenable and populate notes. The dashboard will display "Failed to connect flask server." If the total time of initiating a scan exceeds one minute for Tenable.io and Tenable.sc both, the "Failed to connect flask server" message shows in the backend.

The scan will initiate and ingest the event with the scan status "In progress" in QRadar. You can see this scan event in the dashboard.

Reload the webpage.

- **After upgrading from Tenable.ot v1.0.0, or AlsidForActiveDirectory, to Tenable v4.0.0, Tenable.io or Tenable.sc events are parsed as "Unknown" or "Tenable Message."**

Installing Tenable v4.0.0 on Tenable.ot v1.0.0 DSM, or AlsidForActiveDirectory, Tenable.io or Tenable.sc events are parsed as "Unknown" or "Tenable Message." In the **Log Source Extensions** tab, extensions may be appear disarranged.

1. Go to the **Log Source Extensions** tab under the **Admin** section.
2. Confirm that the **Log Source Extensions** appear jumbled up.
3. Click **TenableCustom_ext**. An XML file downloads to your local machine.
4. Open the instance SSH and run the following command: `/opt/t/qradar/bin/contentManagement.pl -a search -c 24 -r .*Tenable`
5. Copy the ID corresponding to Tenable. For example, if the ID copied is 4002, then in the XML file, change `device-type-id-override="4001"` to `device-type-id-override="4002"`.

6. Click Upload and select the modified XML file. Select **Default Log Source Type** as Tenable.

7. Click Save.

8. Confirm that the value of `device-type-id-override` is correct for all of the extensions.

**Note:** If events of Tenable.io or Tenable.ot are parsed as "Unknown" or "Custom Message", then follow the same steps for those respective log source extensions.

- **After upgrading from v2.0.0 (QRadar app framework v1 app) to v3.0.0 (QRadar app framework v2), unable to launch scan, unable to populate offense notes in the backend.**

There are multiple errors which contain the "EncryptionError" exception in the log files. To check the logs:

1. Go to the **Admin** tab of the QRadar console. Open the configuration page and click the **Edit** icon.
2. Save the configurations again.
3. If that does not work, delete the configurations and save again.

- **Configuration page, dashboard, or offense note shows error or unintended behavior.**

Clear the browser cache and reload the webpage.

- **"Error while initiating socket connection with IBM QRadar" observed in log files.**

This issue might be observed in QRadar v2 app framework (< v7.4.2 P2).

For more information, see the [IBM QRadar documentation](#).

- **Unable to save configuration using self-signed certificates for Tenable.sc.**

If the user is using self-signed certificates and keeping the SSL toggle button on and is receiving “Please enter valid Address or configure valid proxy settings or verify SSL certificate.” error messages in the UI, the probable cause is that the SSL certificate is not present on QRadar.
If you want to use self-signed SSL certificates for Tenable.sc, before installing the app (or upgrade from v2.0.0 app), perform the following steps:

1. Copy the CA's root certificate to `/etc/pki/ca-trust/source/anchors/` on the QRadar console.

2. Run the following commands at the SSH command line on the console.
   - `/opt/qradar/support/all_servers.sh -p /etc/pki/ca-trust/-source/anchors/<root_certificate> -r /etc/pki/ca-trust/-source/anchors`
   - `/opt/qradar/support/all_servers.sh -C update-ca-trust`

Continue with the standard installation steps. For more information, see the IBM documentation.

If the app is already installed, restart the Docker container of the app:

1. Login into your QRadar instance.

2. Go to the Admin panel.

3. Open configuration page of Tenable App for QRadar.

4. From the configuration window, copy the app ID found within the URL. The app ID is the number after `/console/plugins/` within the URL. For example, if the URL is: `https://198.51.100.0/console/plugins/1062/app_proxy/index`, copy the number "1062."

To get into the Docker container, run the following commands on your QRadar instance via SSH:

1. Run the command `docker ps` on your QRadar instance via SSH.

2. Find the container ID of Tenable App. This will be under the Image column containing the previous copied number. For example, "qapp-1062."

3. To open the docker, run the command `docker exec -it <container-id> /bin/bash`.
Dashboard is showing the error message: "No data available."

1. Make sure the user has initiated scans.

2. Run the below query in Log Activity to see if there are any scans initiated:

   Select "Product" as 'Product', "Scan ID" as 'Scan ID', "Scan Result ID" as 'Scan Result ID', "Scan History ID" as 'History ID', "Scan Name" as 'Scan Name', "Scan Type" as 'Scan Type', "Scan description" as 'Scan description', "Scan Status" as 'Scan Status', "Scan Targets" as 'Scan Targets', "Note" as 'Note', "Redirect URL" as 'Redirect URL' from events where LOGSOURCEYPENAME(devicetype) = 'Tenable' AND QIDNAME(qid) NOT IN ('Tenable Message', 'Unknown') AND "Scan ID" is not null ORDER BY devicetime DESC LIMIT 1000 LAST 7 DAYS.

3. If this query result returns the events, open any event and check if all of the CEP are getting extracted. If the query returns nothing, or CEPs are not getting parsed, check the After upgrading from v2.0.0 (QRadar app framework v1 app) to v3.0.0 (QRadar app framework v2), unable to launch scan, unable to populate offense notes in the backend troubleshooting topic in this document.

You have scanned an IP address once and are trying to scan the same IP again, but Scan Result ID is not updated for the second scan.

1. Launch the scan on the IP address.

2. Open the developer tool of the browser.

3. Hard reload the browser or clear the cache.

4. Launch the scan on the same IP address.

Now the scan can be initiated on the same IP address.