Table of Contents

Welcome to Tenable for IBM QRadar SIEM v3.0 ................................................................. 3
Install Tenable App for QRadar v3.0 ................................................................................. 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
Create a Rule ...................................................................................................................... 25
View Offenses ..................................................................................................................... 29
Uninstall ................................................................................................................................ 30
Troubleshooting .................................................................................................................. 31
Welcome to Tenable for IBM QRadar SIEM v3.0

This document provides information and steps for integrating Tenable.io and Tenable.sc applications with IBM QRadar Security Information and Event Management (SIEM) v3.0.

IBM QRadar SIEM v3.0 (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 v3.0 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 v3.0. 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 v3.0

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.
3. Click Admin.
   The Admin options appear.
4. In the Systems Configuration section, click Extensions Management.
   The Extensions Management window appears.
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.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 v2.0**.

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

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.

   If a scan does not exist, you must create one with the associated QRadar credentials in Tenable.io. 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.

   If a scan does not exist, you must create one with the associated QRadar credentials in Tenable.io. 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 website for steps on creating an authorized service token.

   (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.
**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 **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.
a. In the **Address** box, enter the IP address used to access Tenable.sc.

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

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

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

   If a scan does not exist, you must create one with the associated QRadar credentials in Tenable.sc. 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.sc.

   If a scan does not exist, you must create one with the associated QRadar credentials in Tenable.sc. 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://www.ibm.com/docs/en/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://www.ibm.com).
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**.

   ![Select a Log Source Type](image)
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](#).
Create a Rule

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 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**.
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 v2.0:

1. On the IBM QRadar SIEM console, click the button.
   The 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 displays the configurations error message “Error while reading configurations.”

  Your configuration file may have been corrupted.

  This can also occur if you upgraded the App to v2.0. from a previous version and you did not reconfigure your files. If you did this, delete the configurations from 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 a wrong 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 on Tenable App For 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.