How-to Guide: Tenable App for IBM QRadar SIEM

Last Revised: January 16, 2020

Table of Contents

How-to Guide: Tenable App for IBM QRadar SIEM 1

Welcome to Tenable App for IBM QRadar SIEM 3

Installation 4

Configuration 6

View Offenses 10

Uninstall 11

Troubleshooting 12

Glossary 13

Welcome to Tenable App 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).

You can use the customized Tenable applications in IBM QRadar SIEM (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.

Installation

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

Requirements:

- Tenable.io or Tenable.sc account
- QRadar 7.3.1 +
- Tenable App Bundle v1.1.0
- Tenable App For QRadar file downloaded from the IBM App Exchange website

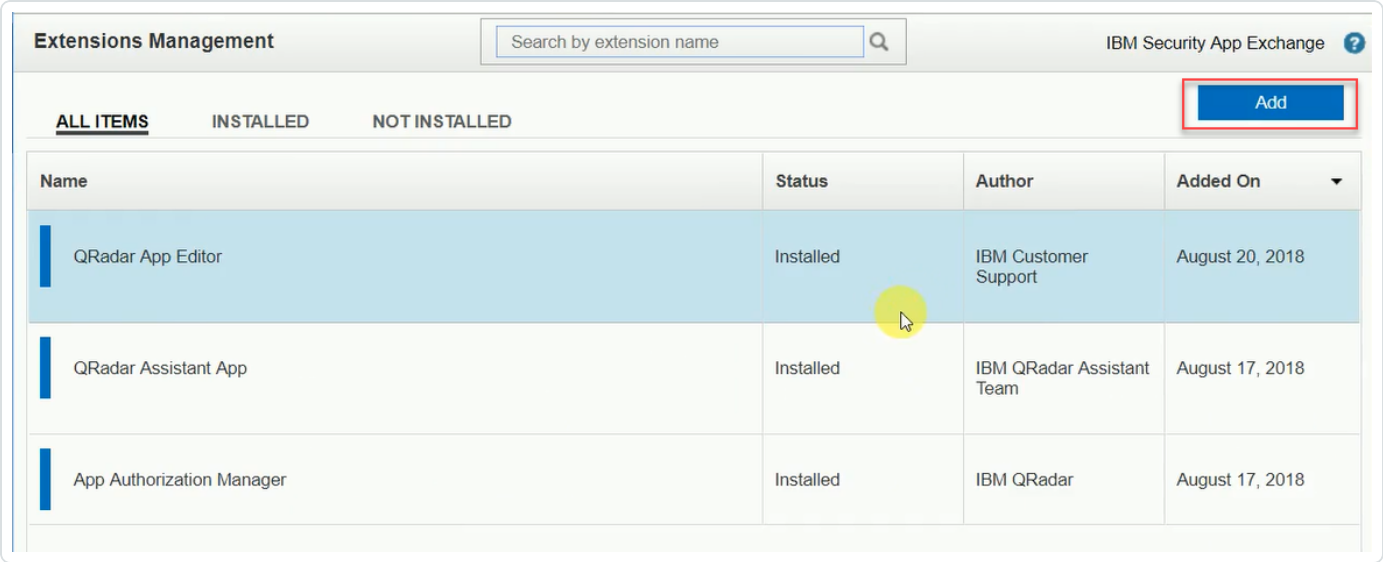
To install the Tenable App For Qradar:

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 the **Add** button.



The **Add a New Extension** window appears.

6. Click **Browse** and select the **Tenable App For QRadar** file.
7. Click the **Add** button.

   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.
11. After the validation completes, the **Tenable** app appears in the list of **Applications Packages** on the **Tenable App For QRadar** window.
12. Click **OK**.

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

Configuration

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.

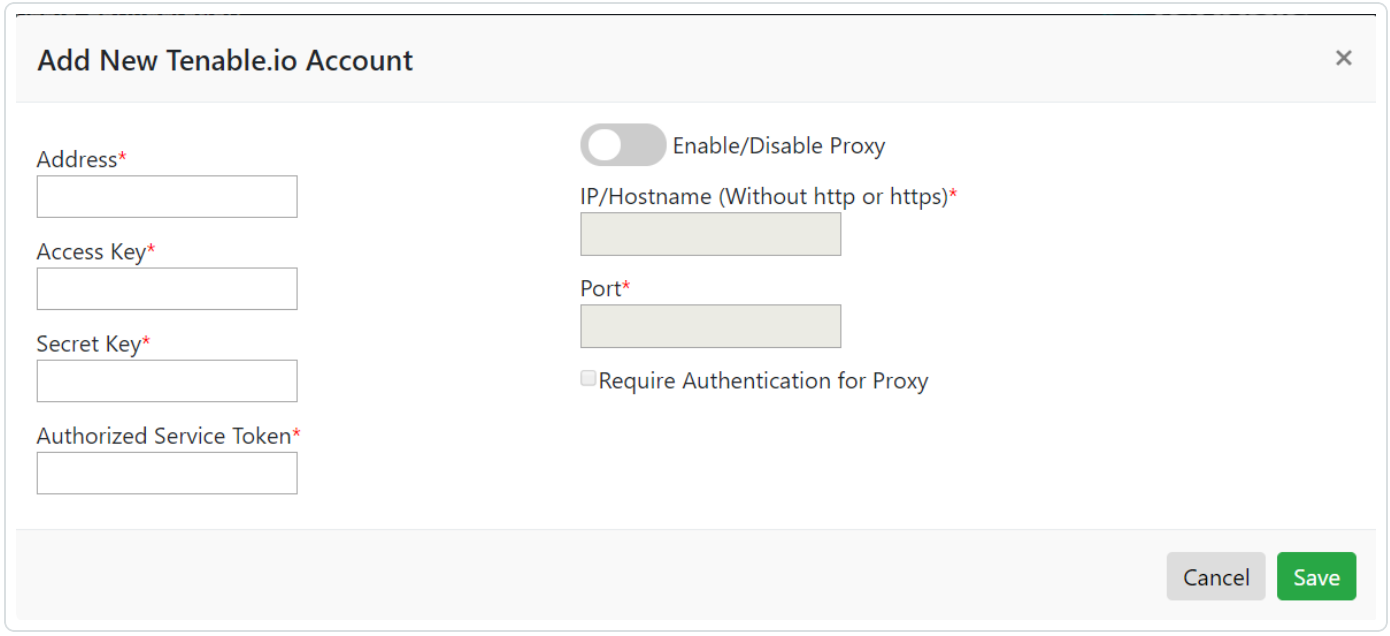
   The **Menu** options appear.
3. Click **Admin**.

   The **Admin** options appear.
4. Scroll to the **Tenable** section.
5. Click **Tenable App Settings**.

   The **Tenable Configuration** appears.
6. Depending on the Tenable product you want to configure, do one of the following:
   - Click **Add Tenable.io Account**.
   - Click **Add Tenable.sc Account**.
7. Configure the settings for your product.

   To configure Tenable.io:

   > **Required User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator



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

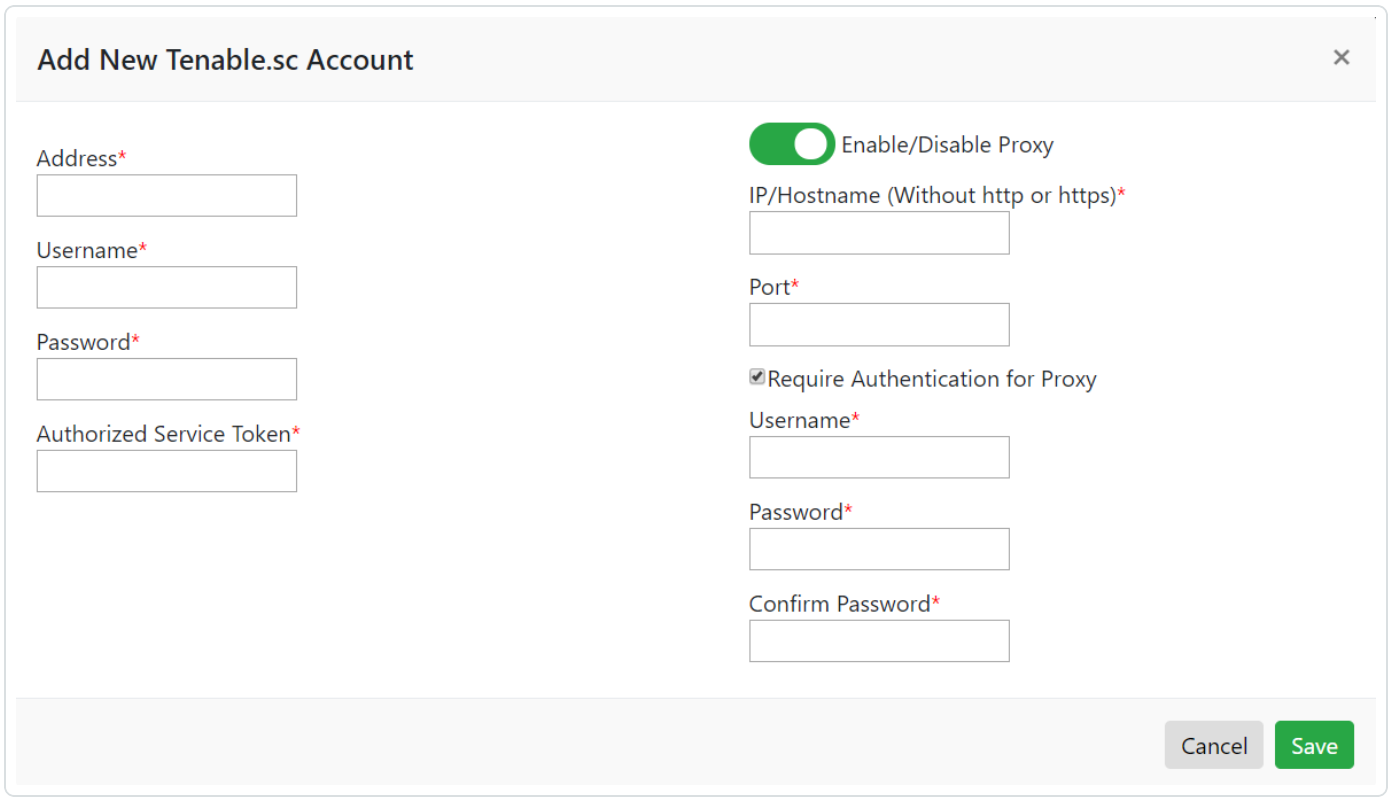
   See the IBM QRadar SIEM website for steps on creating an authorized service token.

e. (Optional) Connect to Tenable.io 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**.

To configure Tenable.sc:

Required User Role: Security Analyst



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

b. In the **Username** box, enter your Tenable.sc username.

c. In the **Password** box, enter your Tenable.sc password.

d. 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.

e. (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.

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.

To view offenses:

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

   The **Menu** options appear.

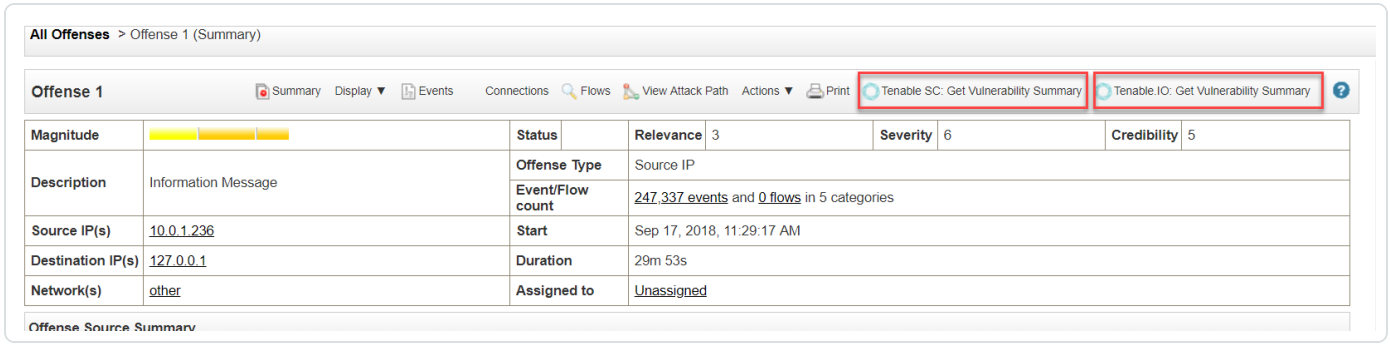
2. Click **Offenses**.

   The **Offenses** menu appears.

3. Click **All Offenses**.

   The **All Offenses** page appears with a table of offenses.

4. Click an offense.



   When you click **Tenable SC: Vulnerability Summary** or **Tenable IO: Vulnerability Summary**, the source IP address brings data from Tenable.io or Tenable.sc and adds it to the notes section.

   > **Note:** Both Tenable.io and Tenable.sc options display in the interface. However, if you do not have a Tenable.io account and click the **Tenable IO: Vulnerability Summary**, you will not get results. In turn, if you do not have a Tenable.sc account and click the **Tenable SC: Vulnerability Summary**, you will not get results.

   A page with offense details appear.

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

The configuration page shows 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 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 error message “Authorization service token is not valid.”

You entered a wrong authorization service token. Enter the correct service token.

An alert pop up shows 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 with 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 with message “Failed due to Invalid credentials.”

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.

Glossary

M

My Term

My definition