IT specialist

ITS INVENTORY

Inventory for QRadar Installation Guide

Introduction

ITS Inventory for QRadar is a full-featured application that provides structured, enriched, relevant information about IT assets configuration. The application extends configuration data in the built-in QRadar Asset DB with information from Network Hierarchy, Log Sources, Reference Data, Active Directory/LDAP, DNS. As a result, you get all available assets configuration parameters in one place: name, IPs, MAC, network group, accounts, linked log sources status, security groups, etc.
The functionality implemented in Inventory gives security analytics and administrators a comprehensive toolbox to address cybersecurity asset management challenges.

Base usage scenarios:

- searching, filtering assets by configuration parameters;
- review asset details card with the most relevant and consolidated information;
- detect assets not covered by security tools and policies;
- use Inventory assets properties in SIEM context (correlation rules, searches, reporting);
- identify SIEM's configuration issues;
- use quick access (in one console) to assets parameters during offense or incident analysis.

ITS Inventory for QRadar is delivered through IBM AppExchange and absolutely free.
This guide provides detailed instructions for installing and initializing the ITS Inventory application in QRadar. To get more information about usage scenario and user operations, please download "Inventory for QRadar. User Guide".

1 Prerequisite

- **QRadar SIEM Version Compatibility:**
  - o 7.3.3 Patch 6+
  - o 7.4.0 is not supported
  - o 7.4.1 Patch 2+
  - o QRadar CE is supported
- **Access to QRadar SIEM with administrative privileges:**
  - o SEC Token generation: yes
  - o Install Application & Content Extensions: yes
- **Free RAM for application: 600 Mb.**

  Consider that only 10% of the QRadar All-in-one (Console) Server's RAM is available for all deployed applications.
- **Free Disk space for application: 1Gb**

2 Installation

2.1 Deploy Application to QRadar

To install QRadar extension “Inventory” follow the next steps:

1. Log in to IBM QRadar and click **Admin** > **Extensions Management**
2. On the Extensions Management page click **Add**
3. On the Add a New Extension page browse to select the content extension compressed file that is needed to upload to the console
4. Select the Install immediately check box and click **Add** > **Install**
5. On the content extension page, that displays the changes to occur after installation, keep the Replace existing items check box selected and then click **Install**
6. Check the installation summary of new or updated reference data elements and click **OK**
7. Close the Extensions Management page
8. **Refresh** browser page

Pre-Setting completed. To use the application go to the Inventory tab to launch **the Inventory Installation Wizard.**

2.2 SEC Token Generation

Before starting the installation it is necessary to generate a QRadar SEC Token.
To do that provide the following steps:

1. Go to **Admin**> **Authorized Services**
2. Click **Add**
3. Choose token settings:
   a. **Authorized Service Label** - The name of the service for which the token is created
4. Configure the permissions
   a. **Security Profile** - choose **Admin**
   b. **User Role** - choose **Admin**
5. Expiry Settings
   a. Token expiration settings. If necessary, the validity period can be made indefinite by disabling The Authorized Service expires
6. Click **Save**

The **Authorized Service Created Successfully** window appears.

IMPORTANT: be sure to copy and save the token, as once the window is closed, it will not be possible to view it!

2.3 Initialize Inventory

The main steps of installing the application:

1. Open the Inventory Installation Wizard and click **Get Started** (Figure 1)

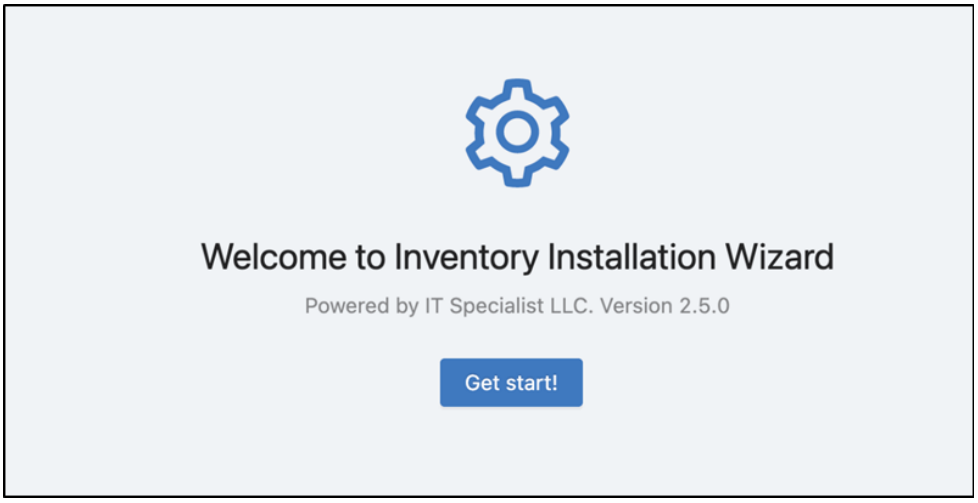

Figure 1

2. After that, the application will start the installation itself. The user only needs to wait for the end of the application installation (Figure 2)

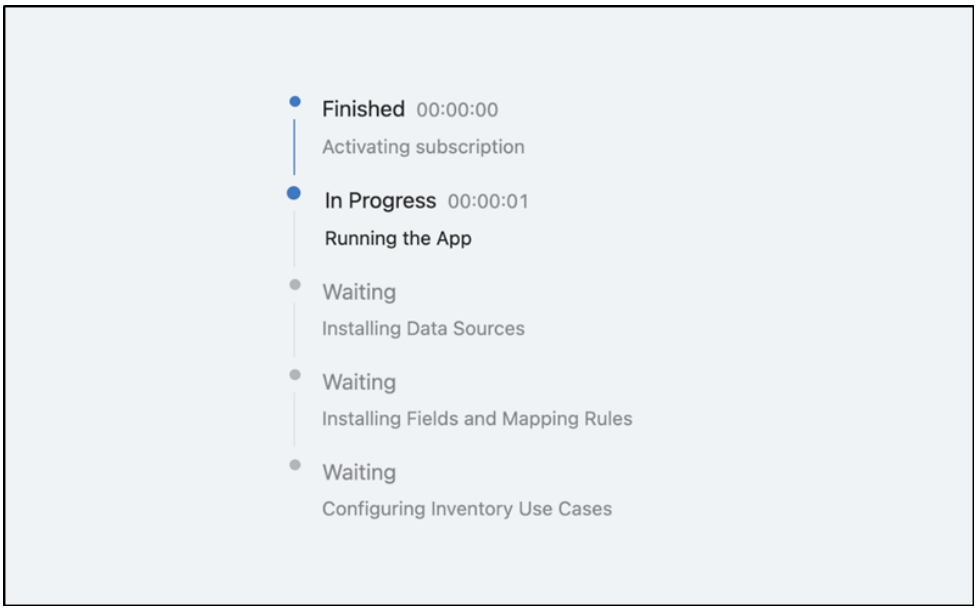

Figure 2

3. Enter the **QRadar SEC Token** (Figure 3)

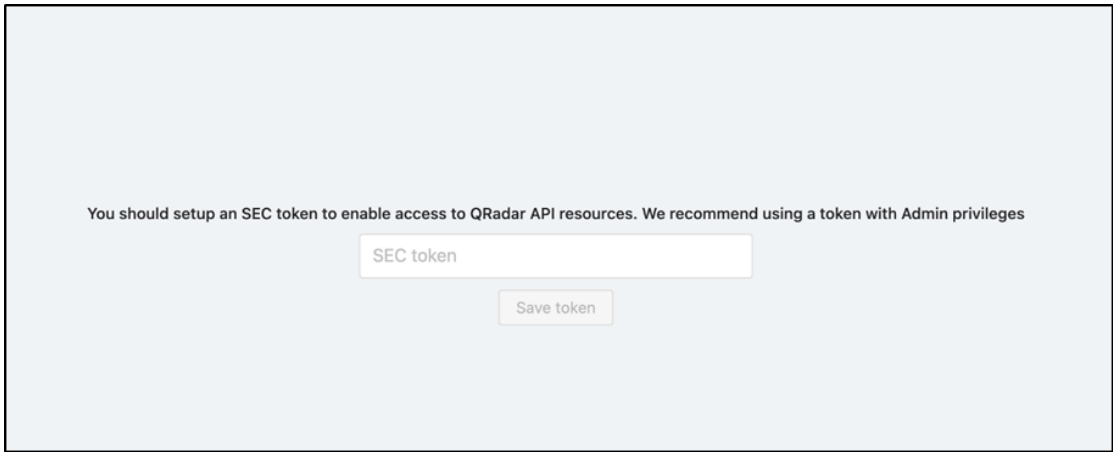

Figure 3

4. After entering the token **Inventory Data Collection Status** window will appear. To start using the application click **View App** (Figure 4).

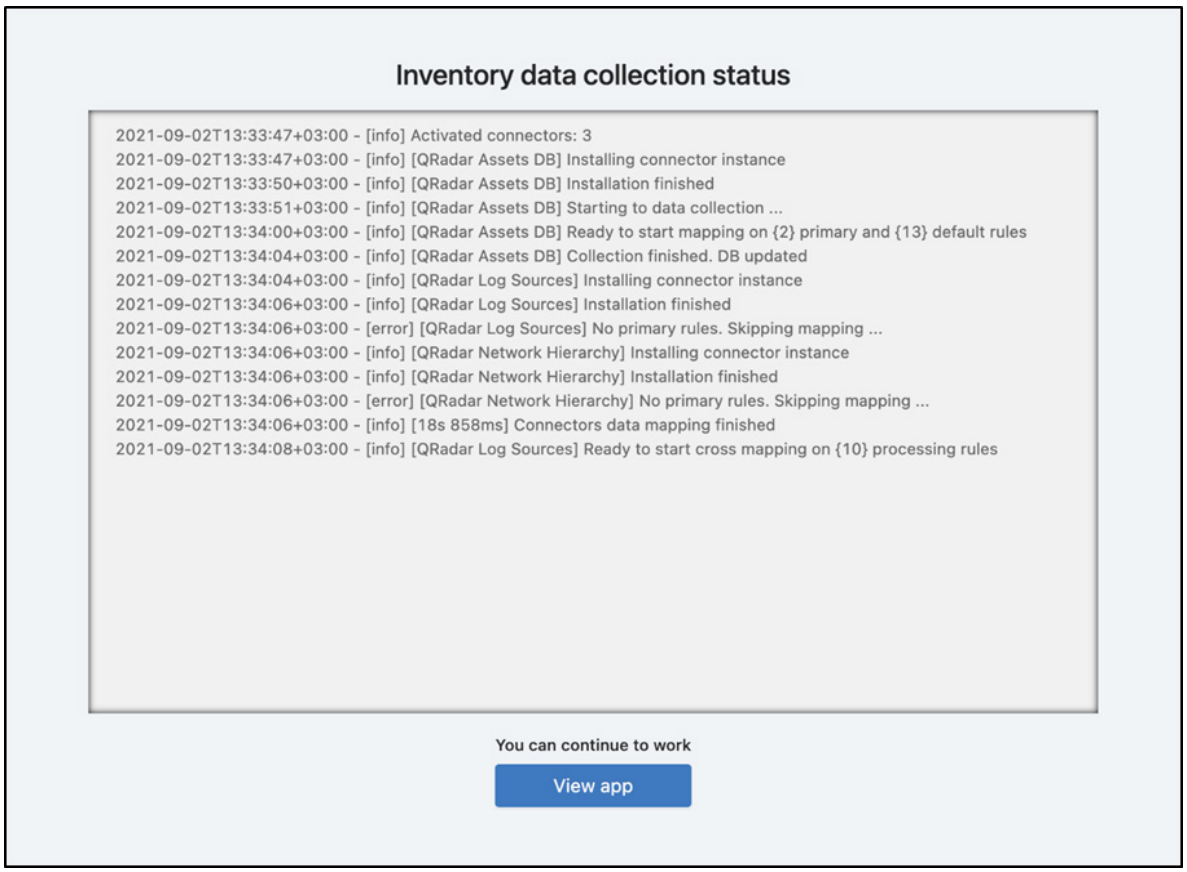

Figure 4

3 Post Installation Check

To check Inventory work provide the following steps:

1. Open the **Assets tab**
2. Double click on any **cell**
3. Investigate the opened **detailed view card** on the right side of the screen (Figure 5)

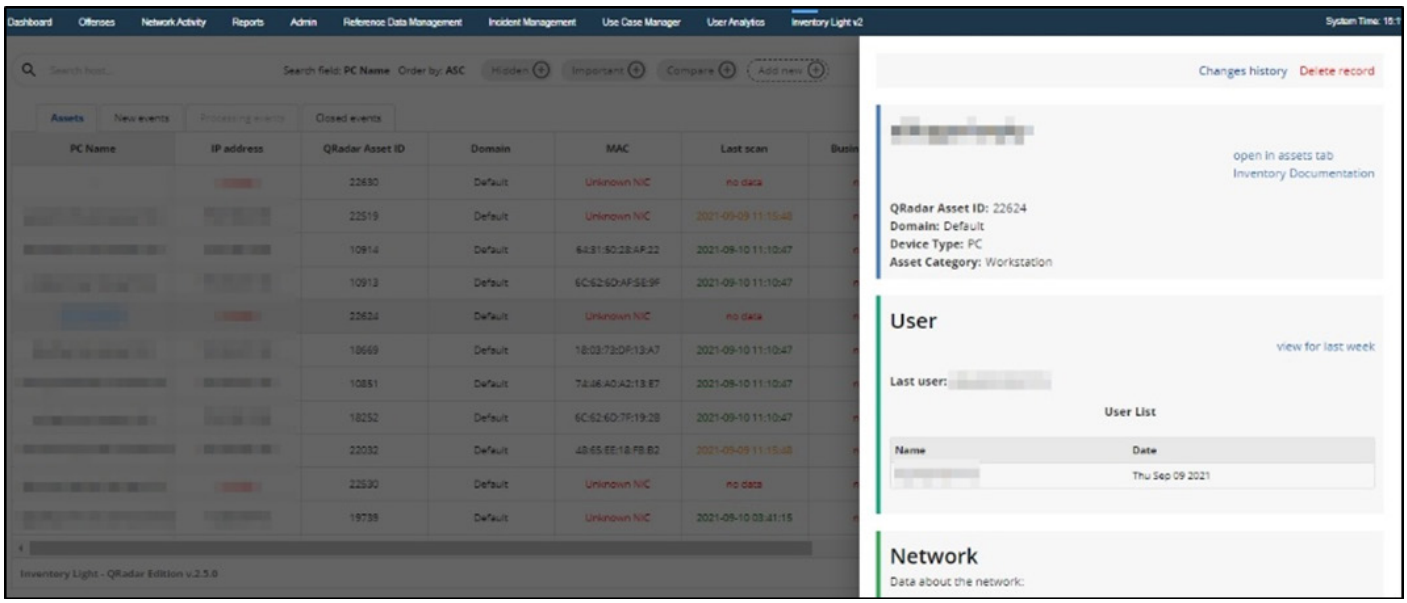

Figure 5