

SpOT User Manual

Version 1.0

# Introduction

spOT is a standalone, ruggedized mobile industrial compliance and security risks platform that you can use to scan devices for security vulnerabilities and misconfigurations, before they are introduced into an operational environment.

spOT scans devices, analyzes their security posture using built-in threat intelligence information about vulnerabilities, and produces a full report of issues, along with recommendations for remediation.

## spOT Overview

spOT has the following features:

* Built-in policies based on threat intelligence, to evaluate compliance of a device
* Automated scan of devices to determine their security posture, while they are offline from a production environment
* Full results, with details of security and vulnerability issues discovered during the scan
* Trend analysis of scan results over time
* Ruggedized portable device that can be carried to the production floor and connect directly to the device

# Setup

spOT can scan a single industrial device, using a direct network connection to the device (the device may include several assets in an internal network segment, all of which will be scanned).

Follow these steps to connect and configure the device to be scanned.

## Start spOT

Turn on the spOT device. The main screen will be displayed.

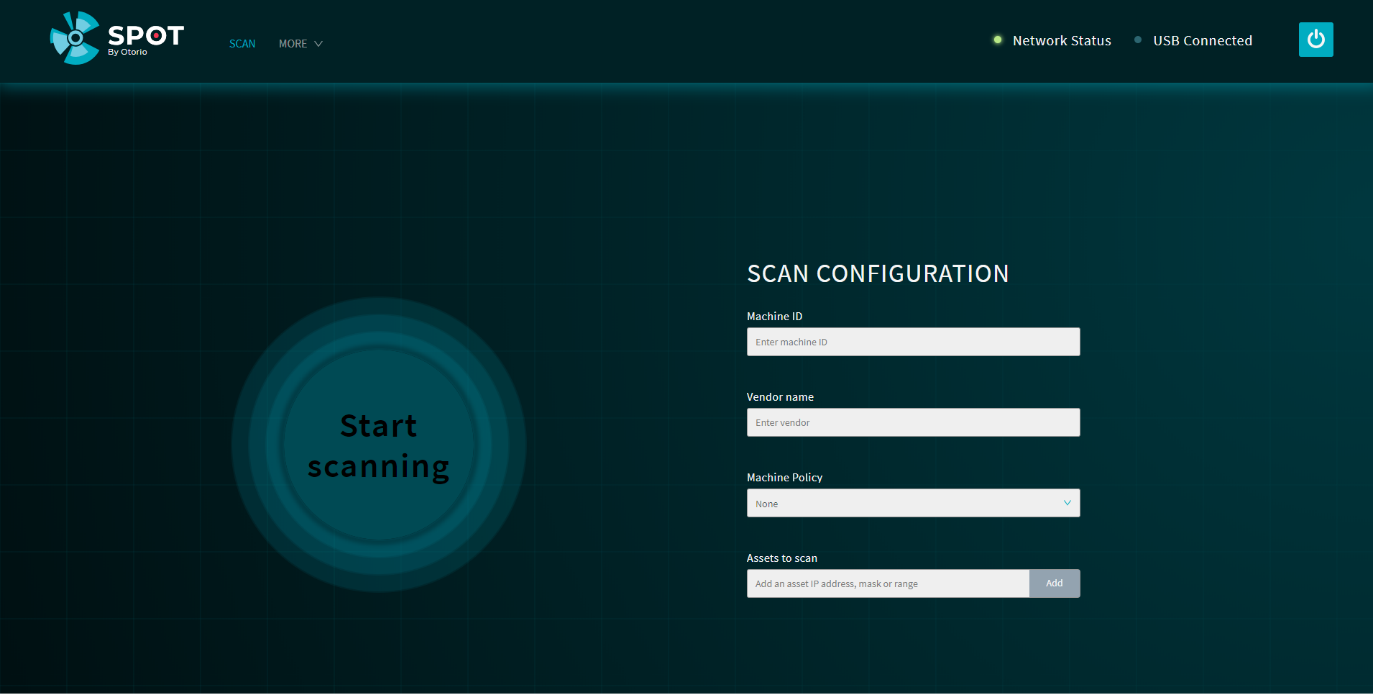
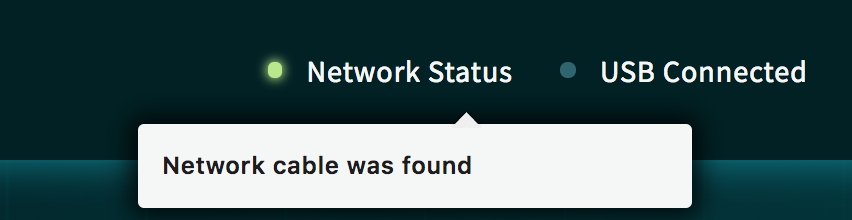


Figure 1 spOT main screen

## Connect to device

Connect spOT to the device to be scanned with a standard network cable, connected to the RJ-45 network port on spOT, to the network port of the device.

When connected, the Network Status indicator on spOT will be green.



## Configure a new scan

Before you scan the device, enter details for it in the main screen. These details are:

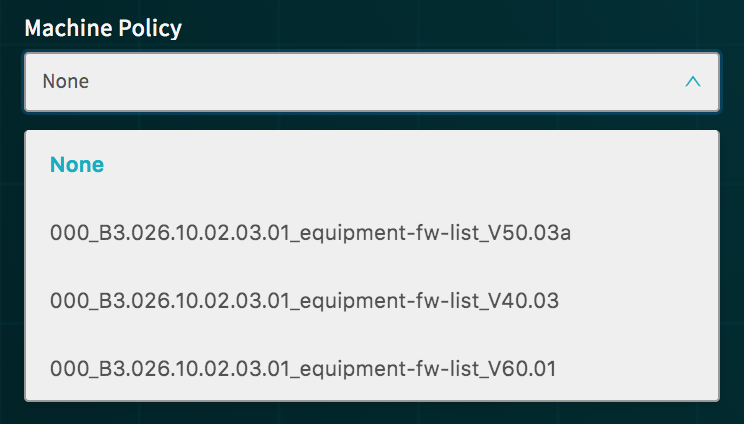
* Device Name – the name of the device
* Vendor – the device vendor
* Machine Policy - select a policy from the list; policies are lists of allowed firmware versions. Select ‘None’ to disable this check in the scan.  
  

Figure 2 - Machine policy

* Assets to scan – enter the IP address, or a range of IP addresses, of the device to be tested (devices can be composed of several assets, each with its own address, on a common subnetwork); *examples*: 192.168.1.1 (single IP), 192.168.1.211-192.168.1.218 (range), 192.168.1.0/24 (CIDR)

# Scan

Follow these steps to scan the device and view the results.

## Start scan

Once all details for the scan have been entered, the Start scanning button is enabled. Press this to start the scan. The scan typically takes a few minutes.

The scan progresses in a series of steps. The status of the scan as it progresses is shown on the screen.

The scan goes through these phases:

* Initiation - the scan is starting
* Asset Discovery – the different assets in the device are discovered
* Asset Analysis – information about the assets is obtained from the device, and credentials, configurations, and policies are checked for security issues
* Threat Intel – threat intelligence information is applied to the information obtained from the assets, to determine if there are vulnerability issues, and to calculate the Risk Level and compliance score
* Report – the detailed report is prepared of all findings for the device

The phases are shown on the display, as the scan progresses.

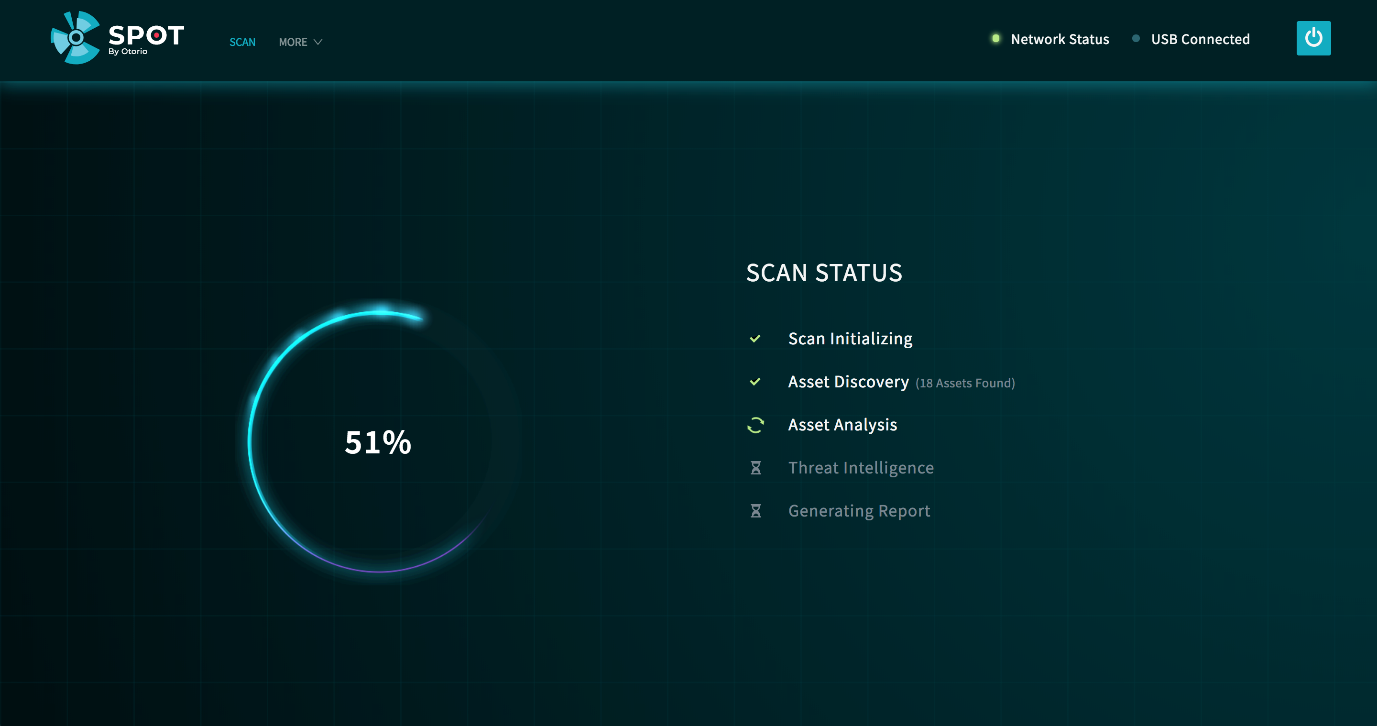


Figure 3 Scan progress

## Scan Results

When the scan is complete, the Risk Level, calculated for the device, is shown.

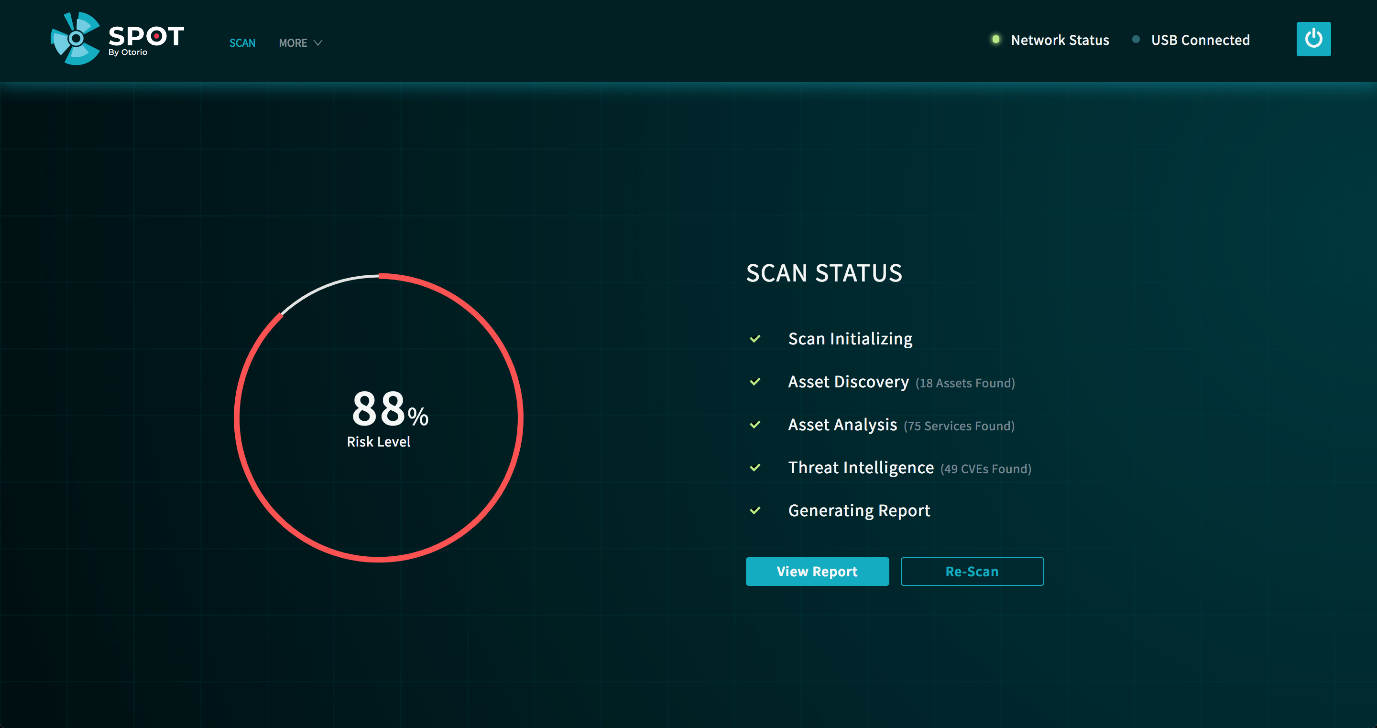


Figure 4 Scan completion

Press  to view the results. Alternatively, press to perform the scan again, with the same configuration.

## Scan Report

The scan results show the following:

* Details for the device that was tested
* The Risk Level for the device, based on the findings of the scan
* The number of security issues found in the scan, according to type (Credentials, Policy Deviations, Vulnerabilities)
* A list of the issues

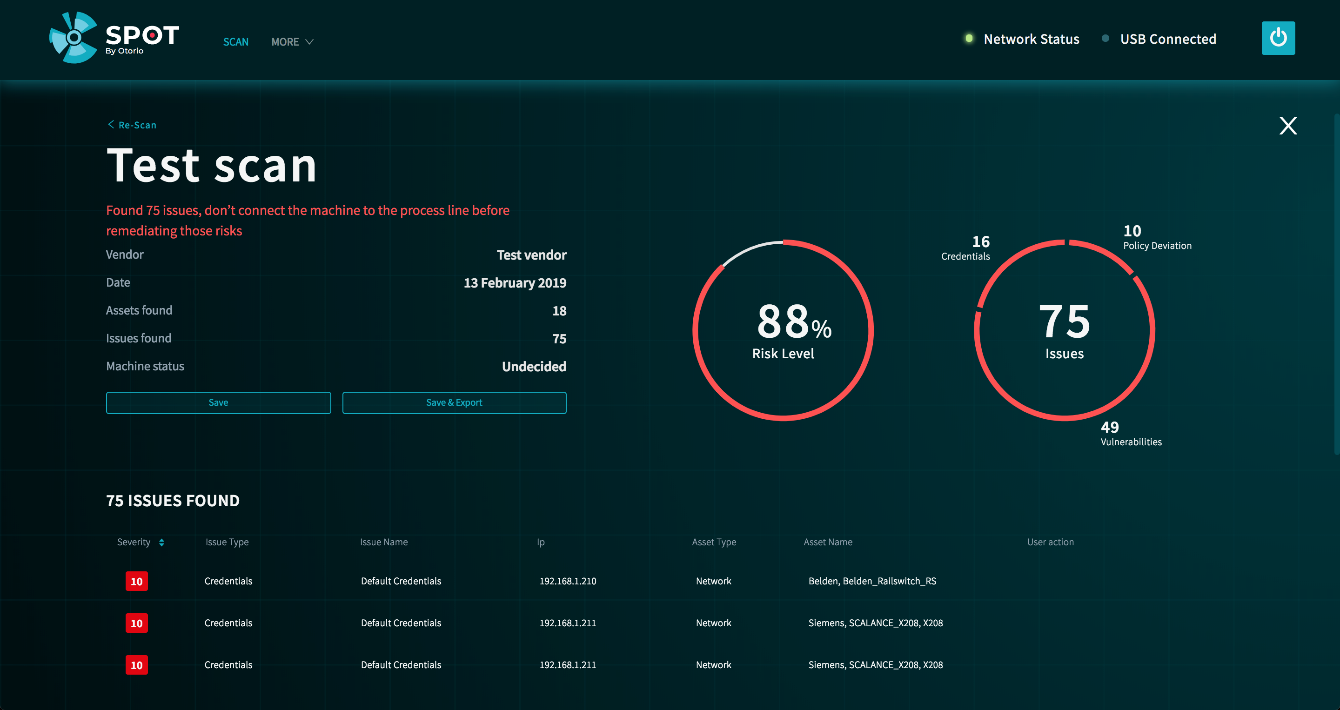


Figure 5 Scan results

### Scan issues

Scroll down in the results screen, to show the list of scan issues. For each issue, these details are shown:

* severity of the issue (Critical, High, Medium, Low), including a severity score, ranging from 0 (lower)– 10 (highest), based in part on the NIST CVSS system, that indicates the risk level of the issue
* Issue type
* Issue Name (description)
* IP address of asset in which the issue was found
* Asset type
* Asset name
* User action – indicates whether the user acknowledged or commented on the issue

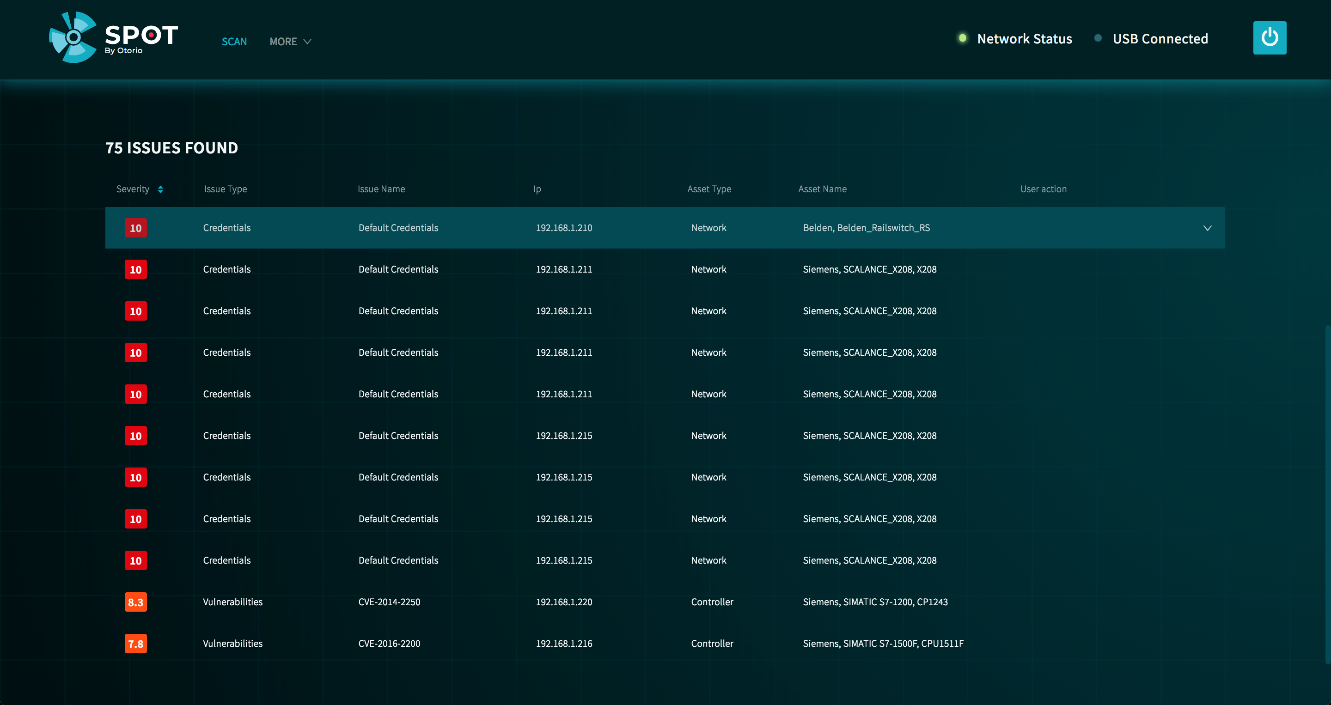


Figure 6 Scan issues

Click on an issue to show more detail. This includes the following:

* Summary – a more detailed description of the issue
* Remediation – recommended steps to remedy the issue
* Operator – the operator who entered a comment or acknowledged the issue

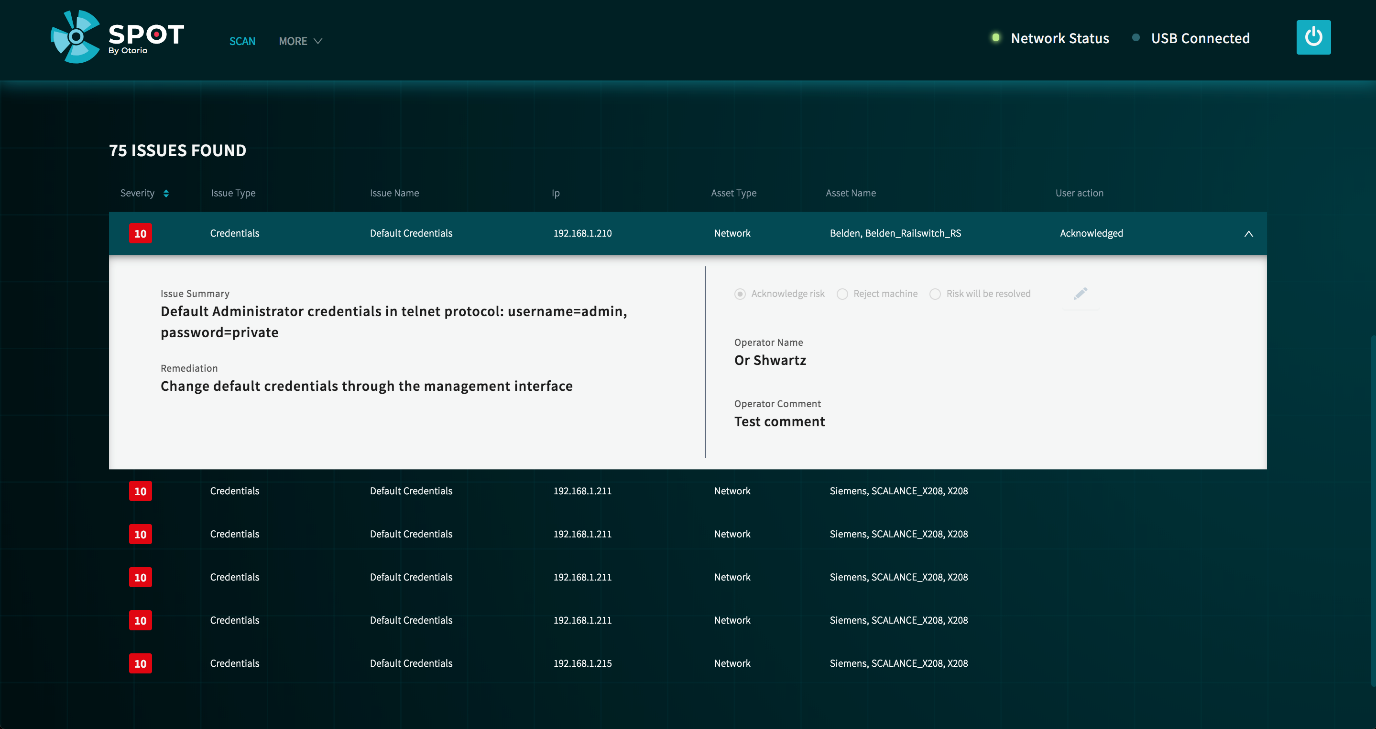


Figure 7 Issue details

### Update issue status & add comments

You can select a status for an issue, and add comments.

1. Click  in the Issue detail
2. Select a status for the issue.The status indicates the resolution of the issue:

* Acknowledge – the issue is known and accepted (could also include the possibility that it cannot be fixed)
* Risk will be resolved – the issue as a known issue that will be remedied after the scan
* Reject machine – the issue is unknown and unacceptable; as a result, the machine will not be connected to the network

1. Add a comment to the Issue, explaining the status selection, The comment is included in the report.Enter the Operator name (your name), and a comment (free text).
2. Click Save.

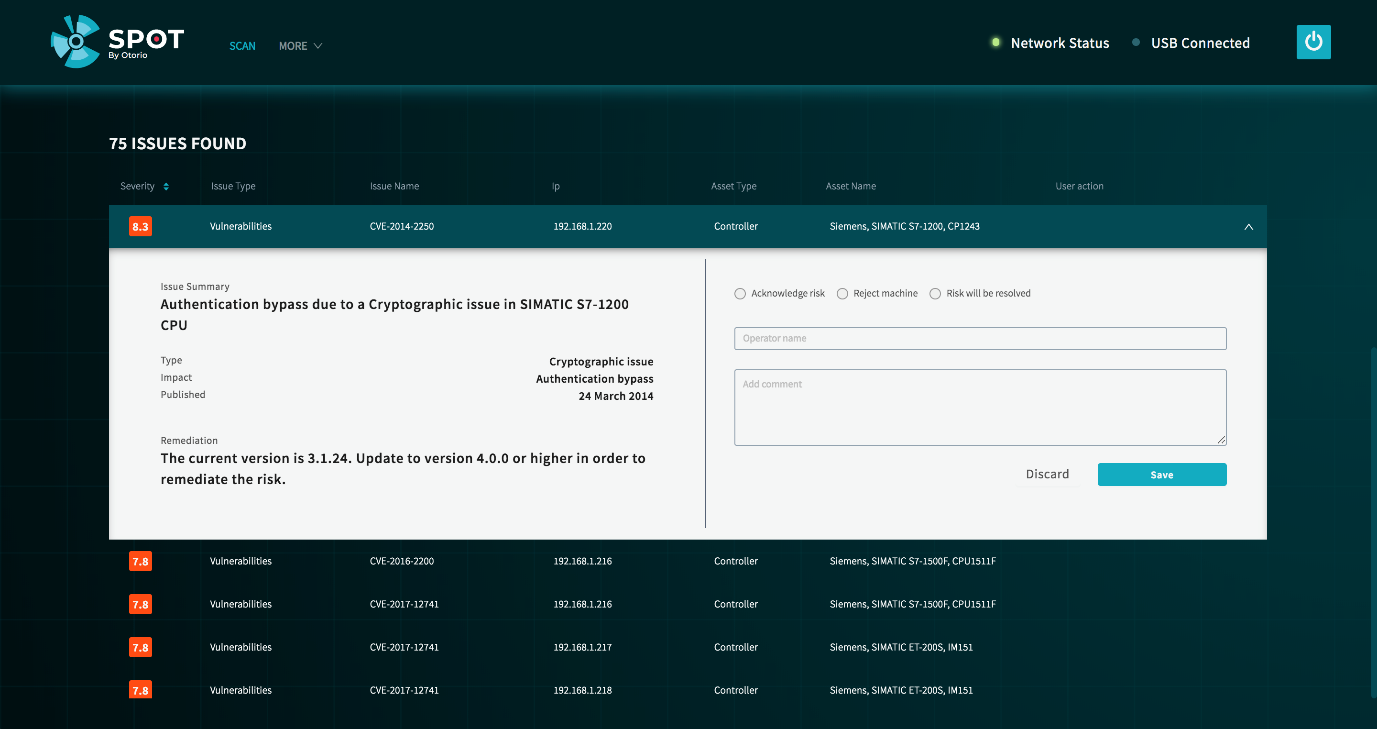


Figure 8 - Update issue

### Save the report

From the displayed test results, click Save to save the report. The report is saved internally in spOT.

### Export the report to PDF

You can export scan results to a PDF file on a USB drive. In the scan results page, click Save & Export to save the report as a PDF file on the USB drive. If there is no USB drive inserted, the report will not be saved.

The report includes the overall risk score for the device, and all the issues and comments.

# Settings

## Network settings

In this section, you set the network address and gateway for the spOT appliance. Ensure the address is unique and does not conflict with other addresses.

1. Select Settings from the More menu at the top of the main page. The System Settings page is shown, which shows the Network Settings for the spOT appliance.

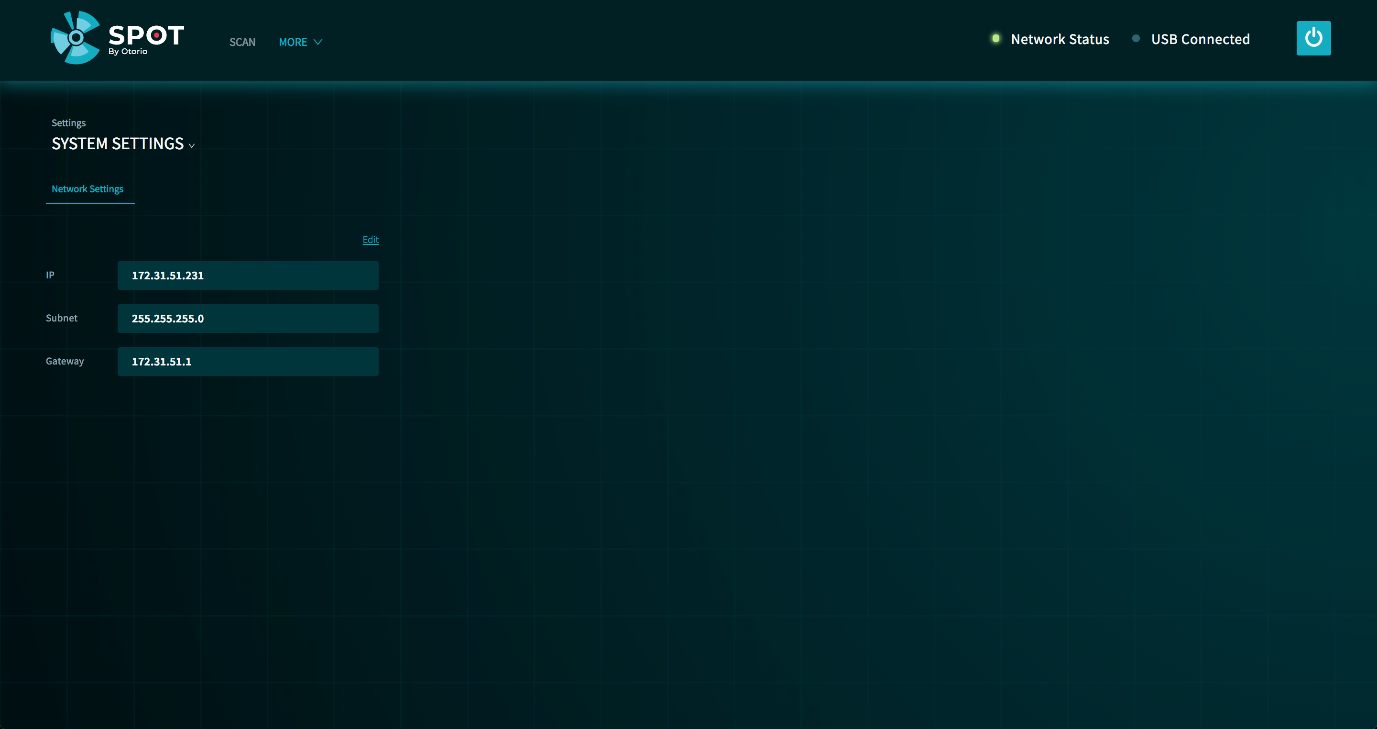


Figure 9 System settings

1. Click Edit to change settings. Make changes to the settings, then click Save.

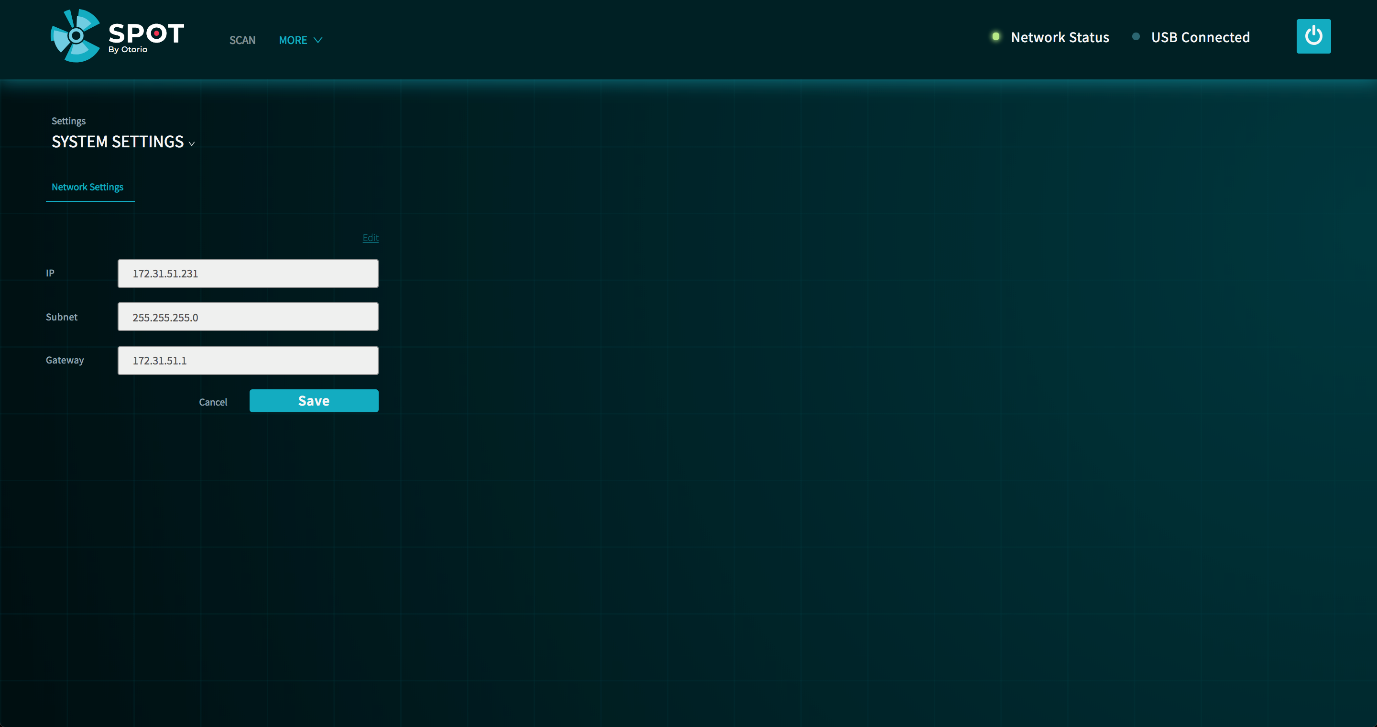


Figure 10 Edit network settings

## Analyzers configuration

spOT has modules, called Analyzers, that attempt to identify assets in a device, and then connect to them to determine their properties. These Analyzers use different protocols, such as SNMP or HTTP, depending on the type of asset. spOT has default authentication credentials for each protocol type, which are tried on assets that are discovered, until one succeeds.

In this section, you can configure additional authentication credentials for specific protocols, that are used in addition to the default ones. *In the current version, only SNMP can be configured.*



Figure 11 Analyzer configuration