# 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.

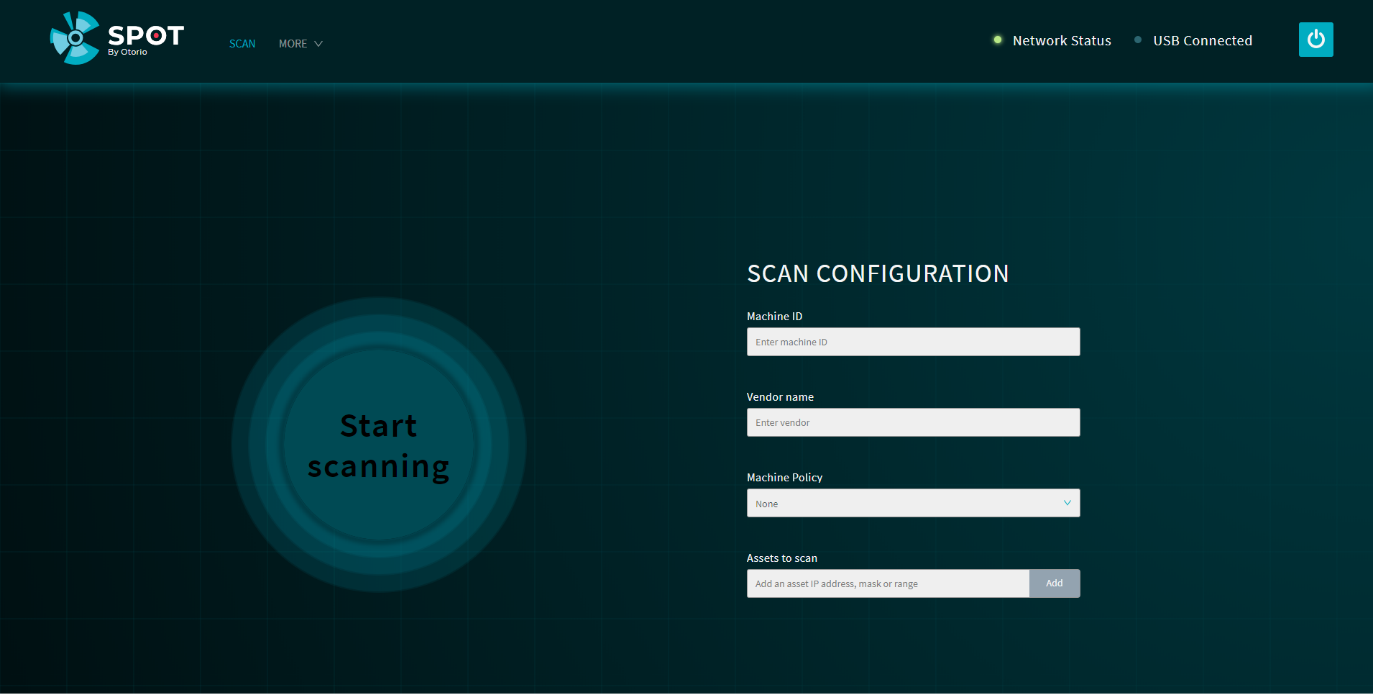
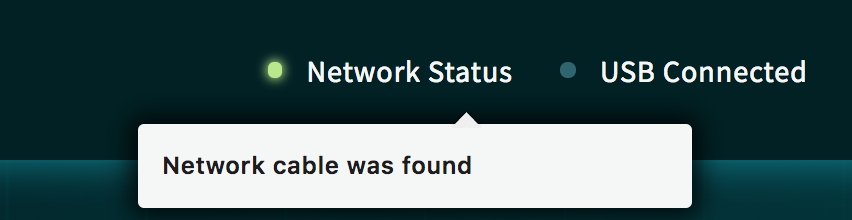


Figure 1 spOT main screen

## 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 the device to be tested

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 define the minimum allowed firmware version for each possible asset in a device
* Assets to scan – enter the IP address, or a range of IP addresses, of the device to be tested (the device can be composed of several assets, each with its own address, on a common subnetwork)

# Scan

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

## Start scan

Press Start scanning 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.

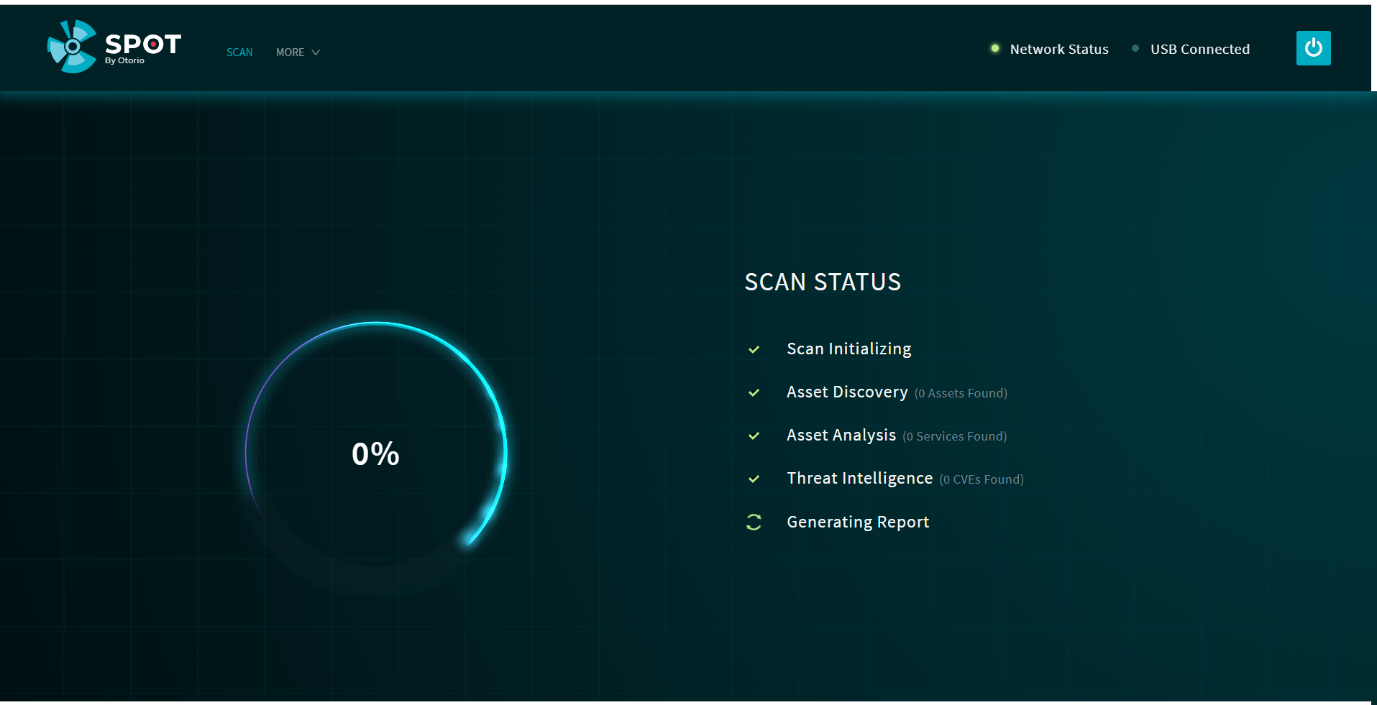


Figure 4 Start scan

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 machine 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.

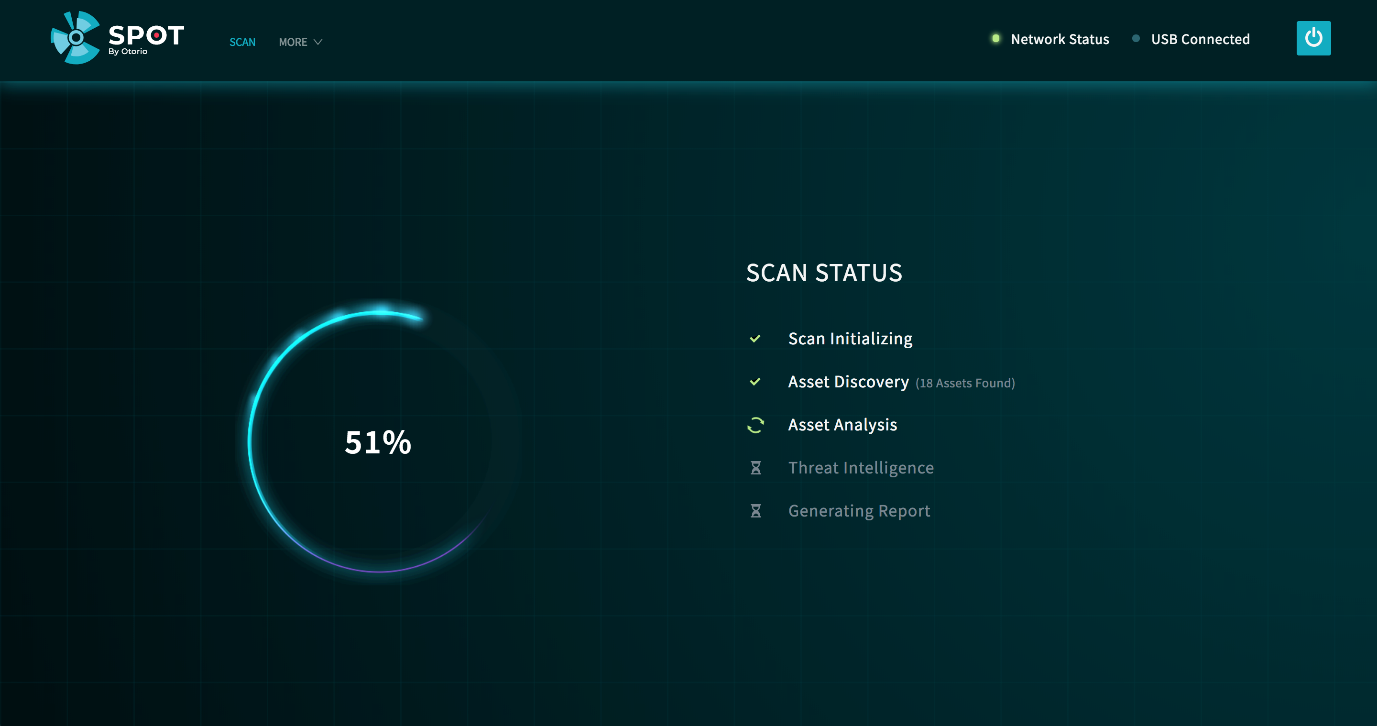


Figure 5 Scan progress

## Scan Results

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

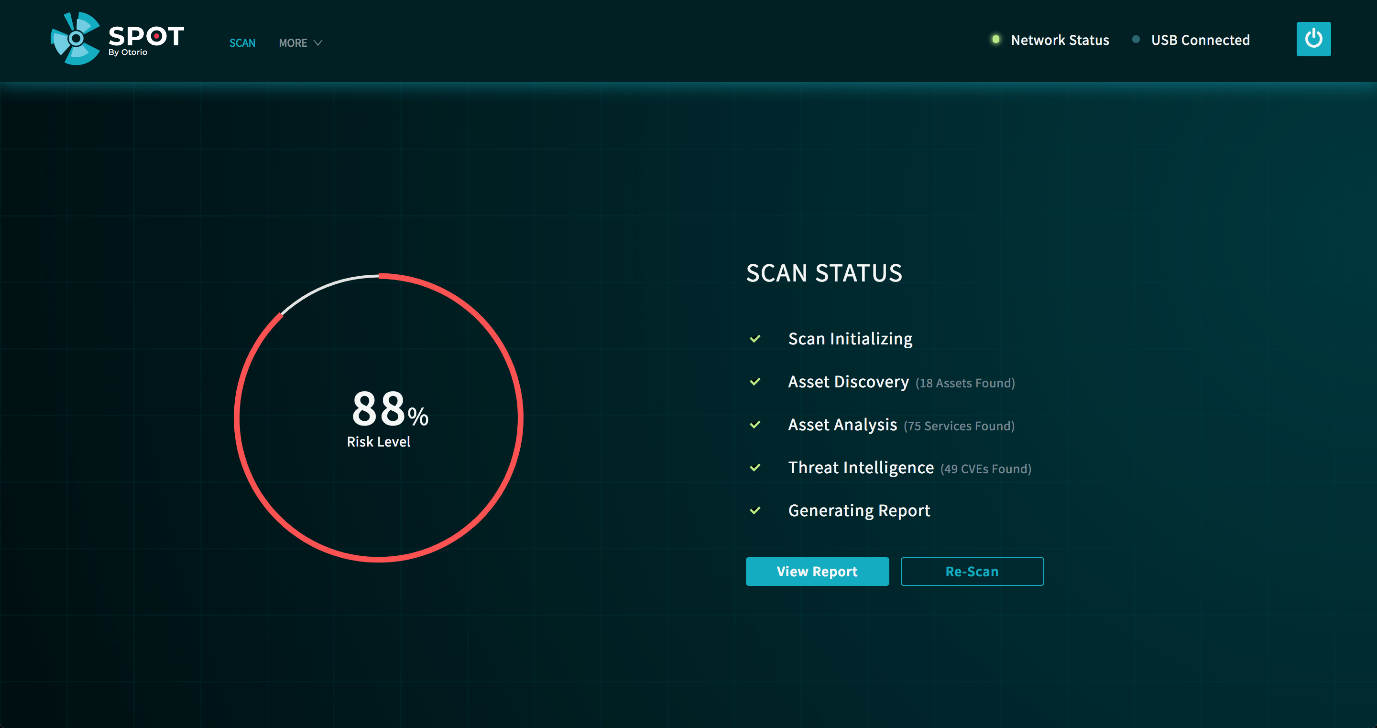
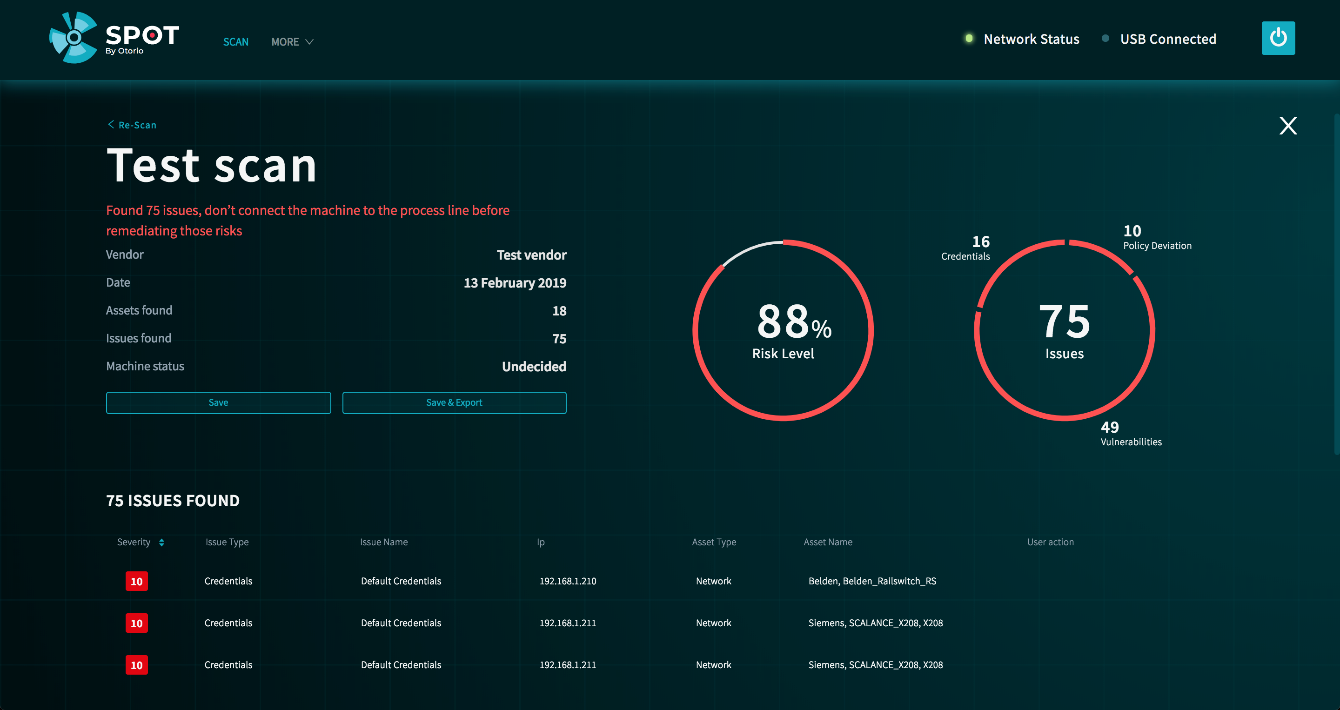


Figure 6 Scan completion

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

The results show the following:

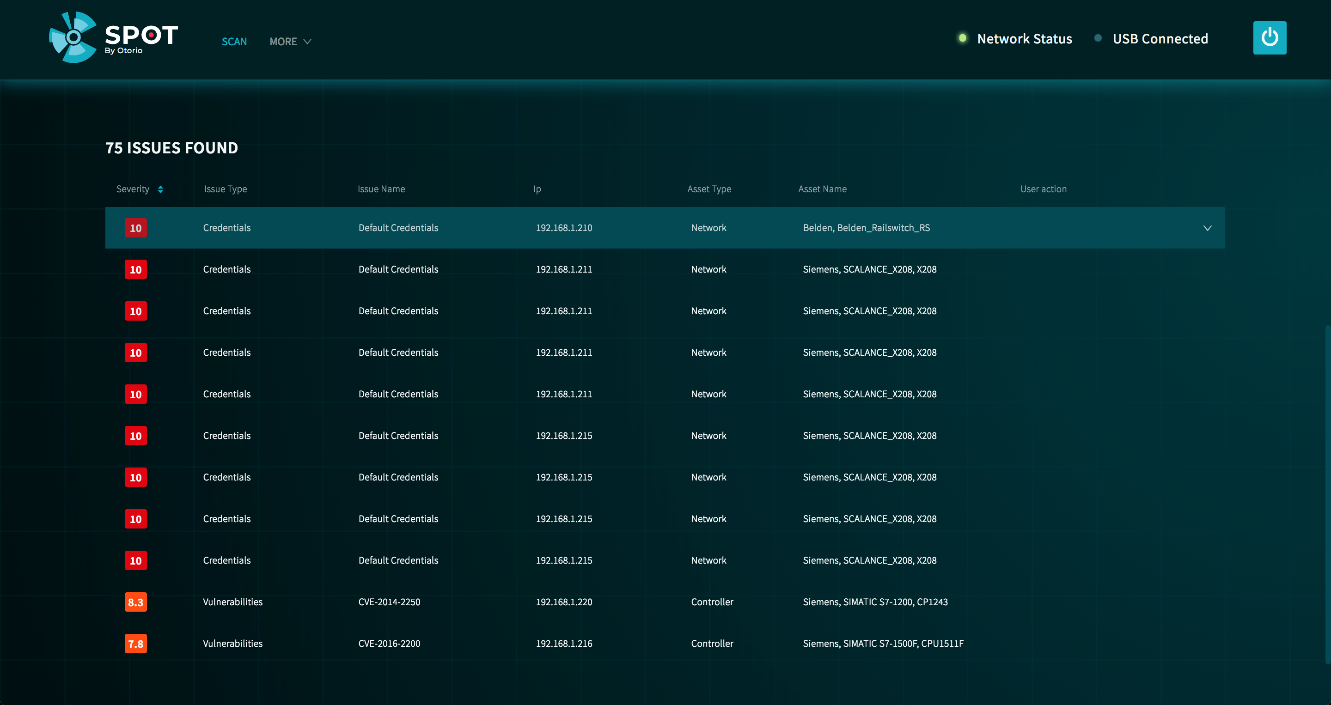
* Details for the device that was tested
* The Risk Level for the device, based on the findings of the scan
* The number of security issues found in the scan, according to type (Credentials, Policy Deviations, Vulnerabilities)
* A list of the issues



### Scan issues

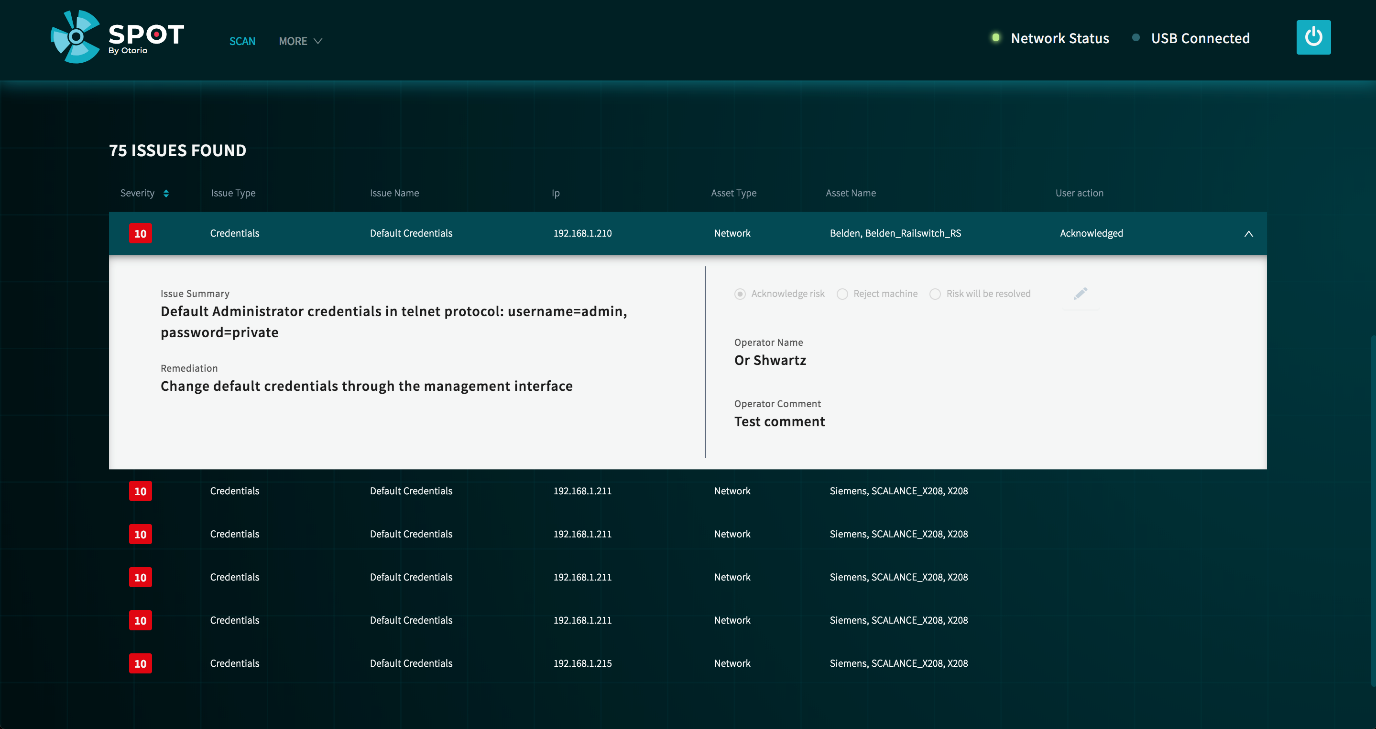
Scroll down in the results screen, to show the list of scan issues. This shows the following details:

* severity of the issue (Critical, High, Medium, Low), including the severity score; the score is between 0 and 10, and is based on publicly available scores for vulnerabilities (for example, from NIST), and Otorio threat intelligence research
* 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



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

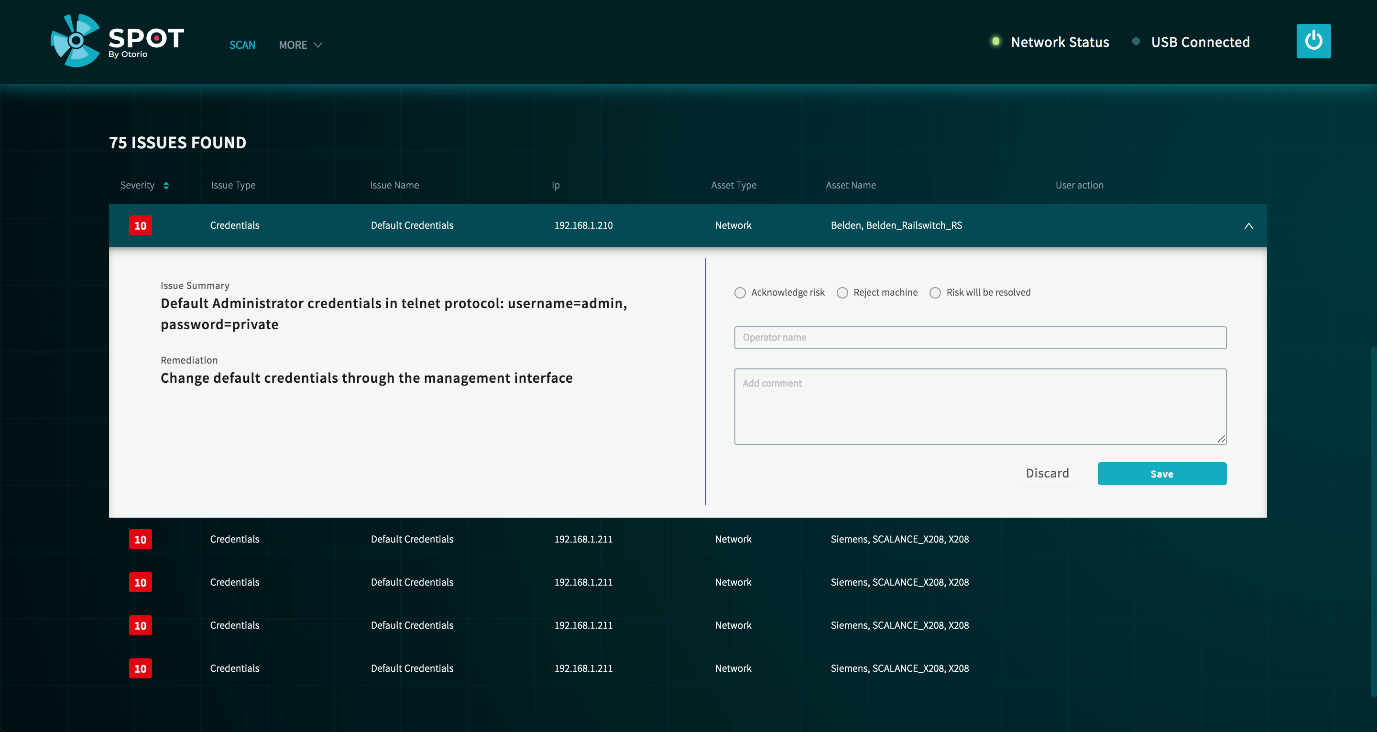
* Summary – a more detailed description of the issue
* Remediation – recommended steps to remedy the issue
* Operator – the operator who entered a comment or acknowledged the issue



### Add comments to an issue

Click  in the Issue detail, to open a comment box for the issue.

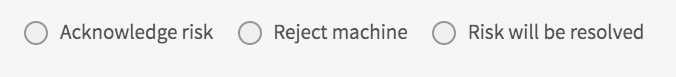
Enter the Operator name (your name), the comment (free text), then click Save. The comment is included in the report.



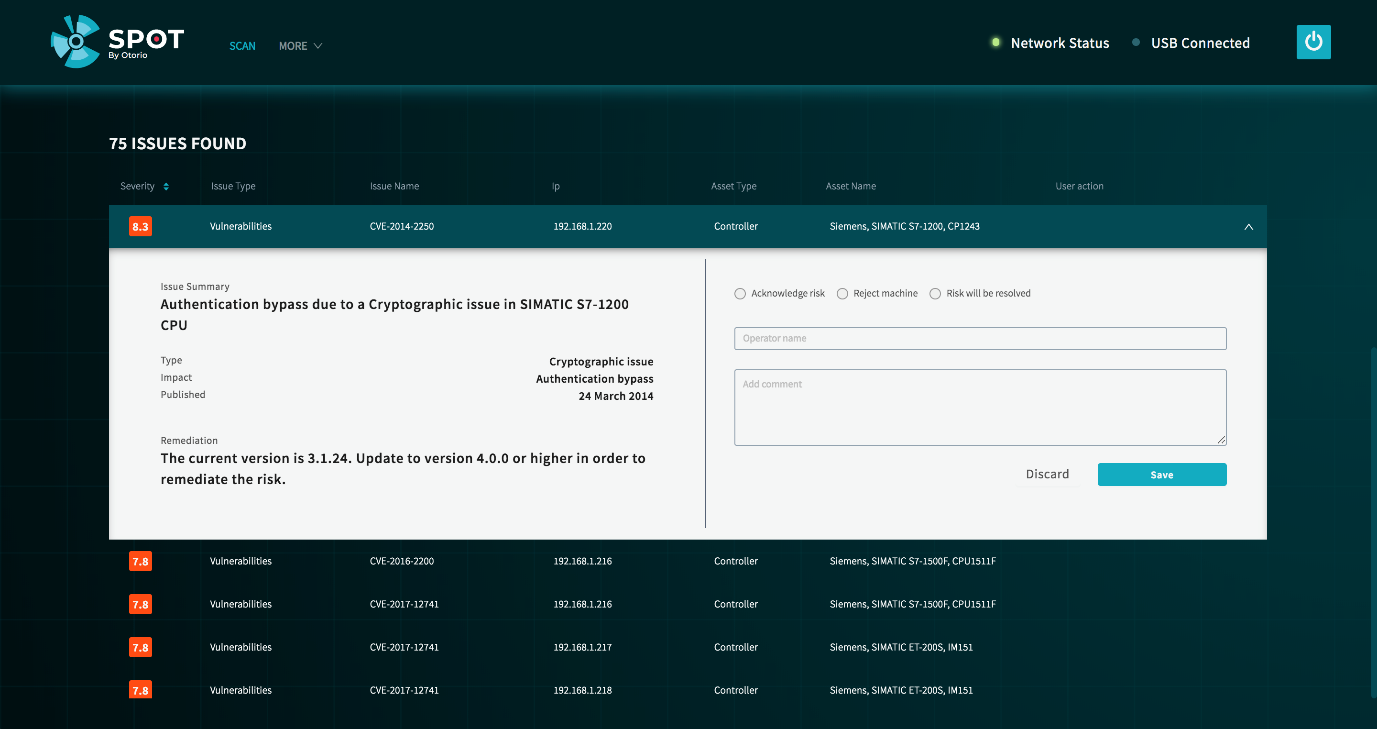
### Acknowledge an issue

You can acknowledge it in spOT. This can indicate the issue is resolved, or will be resolved, or that the device is rejected on account of the issue.

1. Click one of the options:



1. Add the Operator name (your name), and an explanation for the acknowledgement. This information is included in the report.
2. Click Save.



## 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.

# Settings

## Network settings

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 spOT.

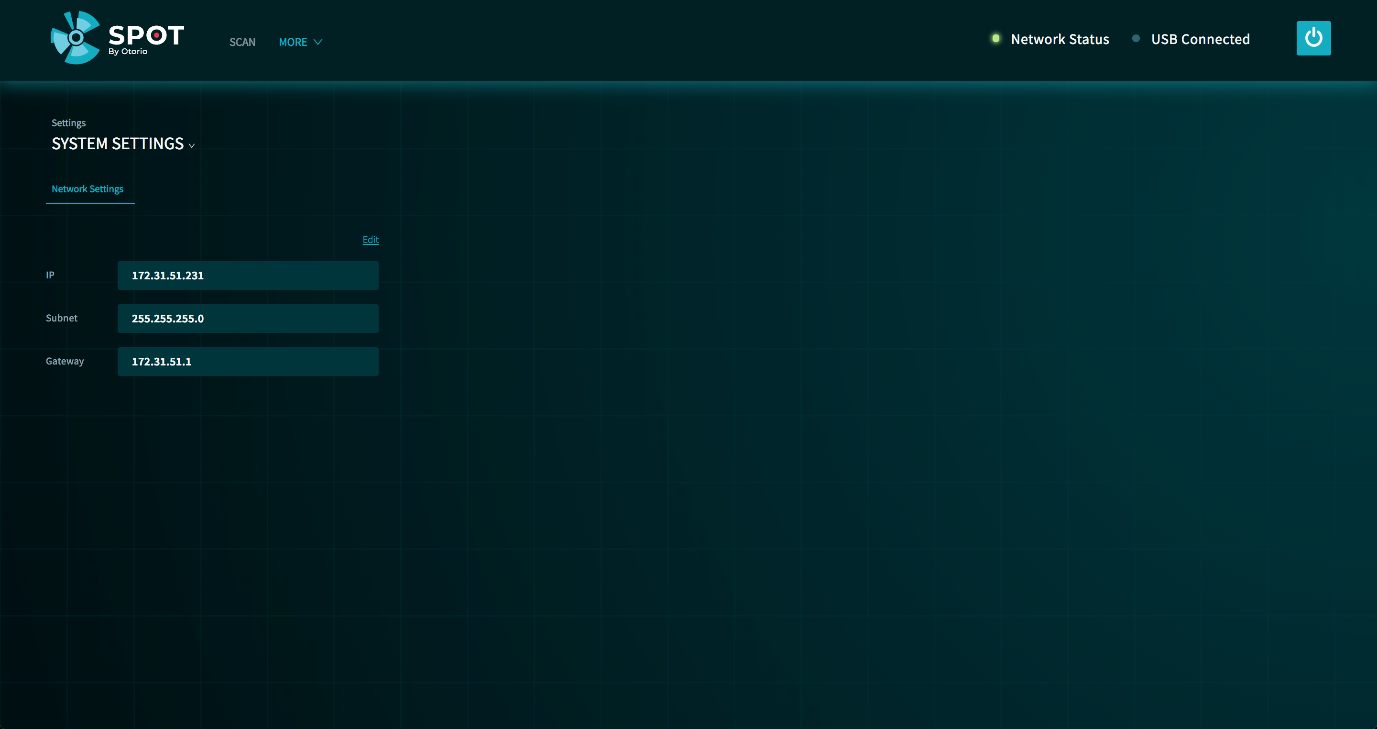


Figure 7 System settings

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

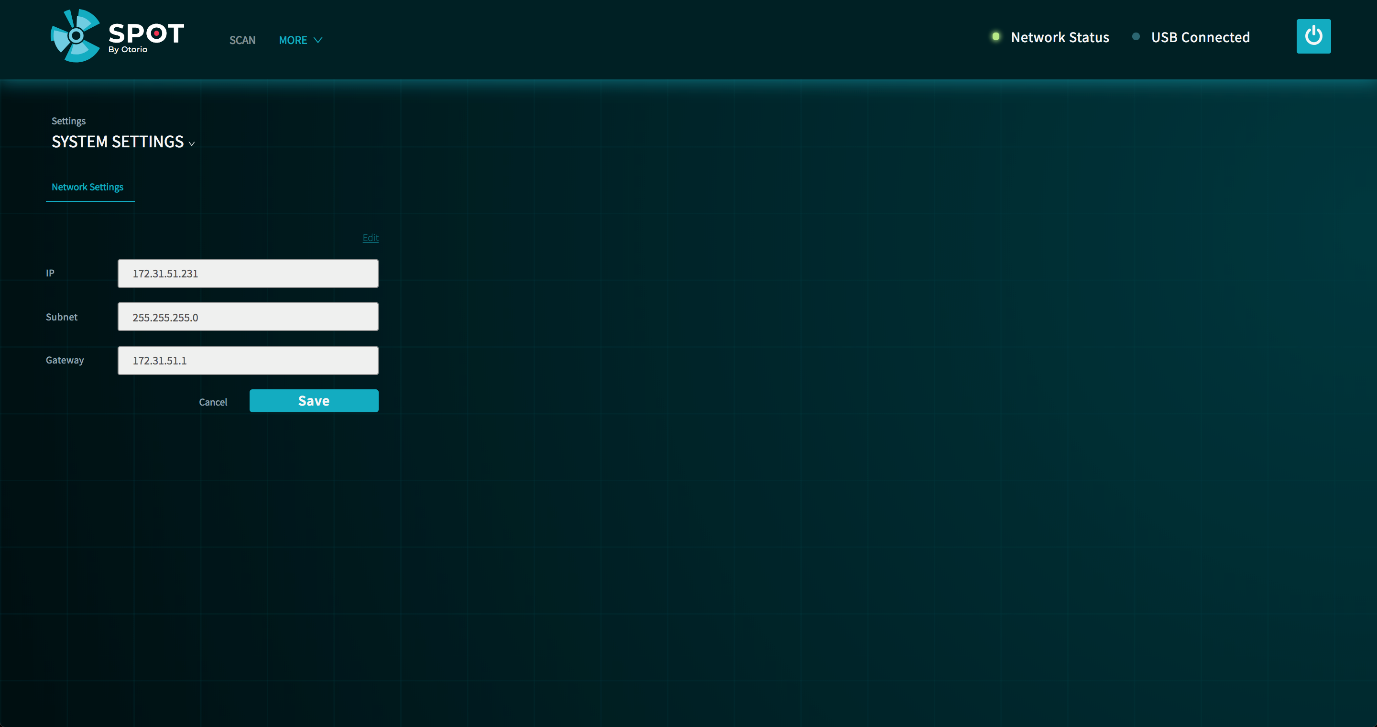


Figure 8 Edit network settings

## Analyzers configuration