# Introduction

SPOT compliance and security risks platform, is a mobile platform that allows complete and tighter control of any 3rd party introduced to production network. SPOT supplies full visibility into the supply chain, spotting hidden OT cyber vulnerabilities. SPOT yields automatic reports and

recommendations with threat intelligence incorporation. SPOT smoothly assimilate into plant’s operational routine, with patch, asset management and configuration integration

## spOT Overview

Standalone, ruggedized

Scan an asset for vulnerabilities before deployment to factory-floor

Built-in Policies – threat intel list of vulnerabilities

Check for vulnerabilities, misconfigurations, sensitive data, credentials, policy violations

Threat Intel – Otorio research team – DB of vulnerabilities -

Generate report, calculate Risk & Compliance Score

Maintain history of scans to build trend analysis

# Setup

Simple setup. Configure details for device to be tested. Connect to device over network port..

## Configure the device to be tested

Name, vendor, IP Address

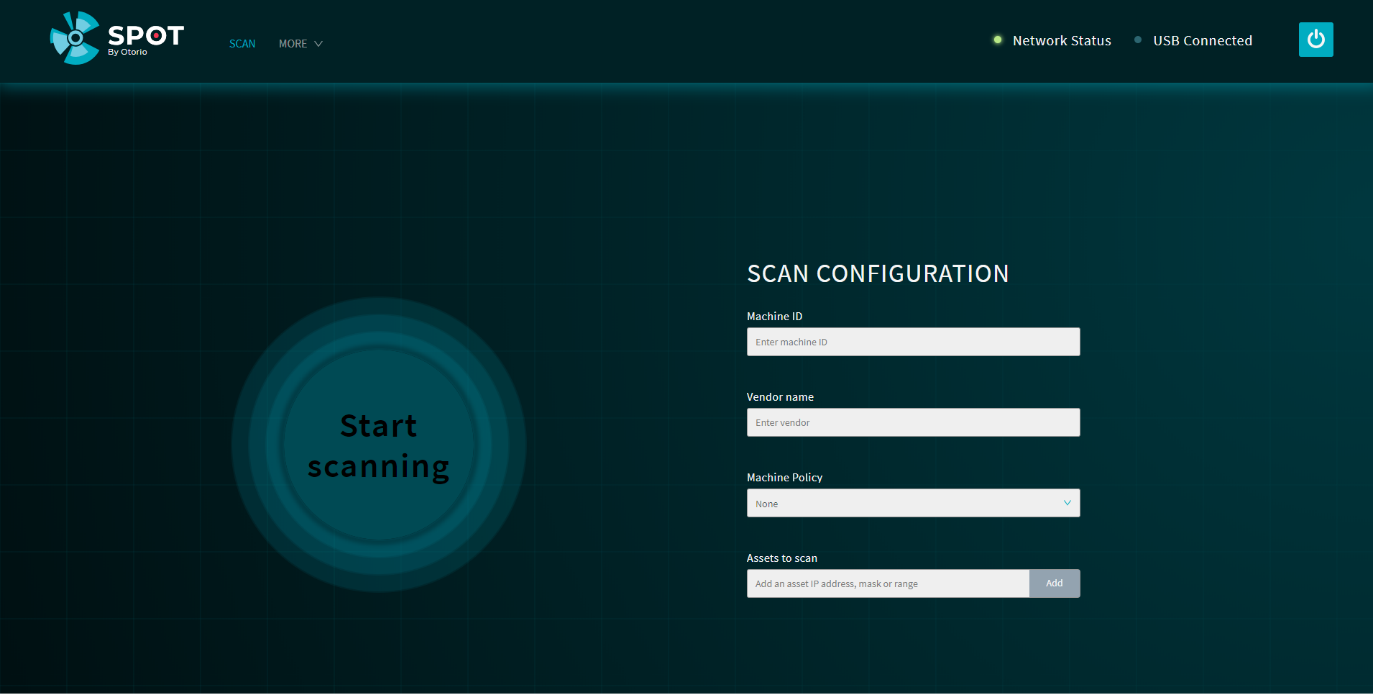
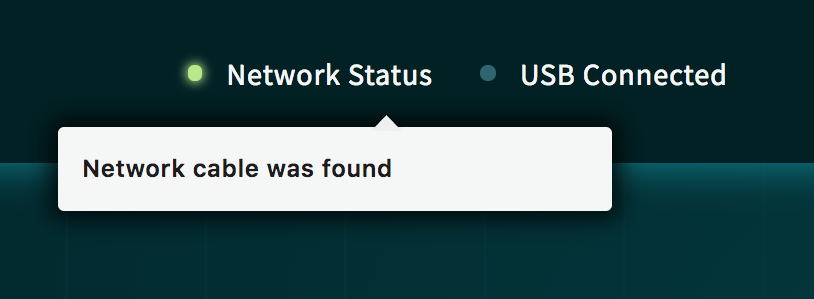


Figure Configure scan

In the upper right, the Network Status indicator indicates whether a network cable is connected to spOT. The USB Connected indicated indicate whether a USB drive is inserted in the USB slot.



# Scan

Single, simple operation.

## 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.

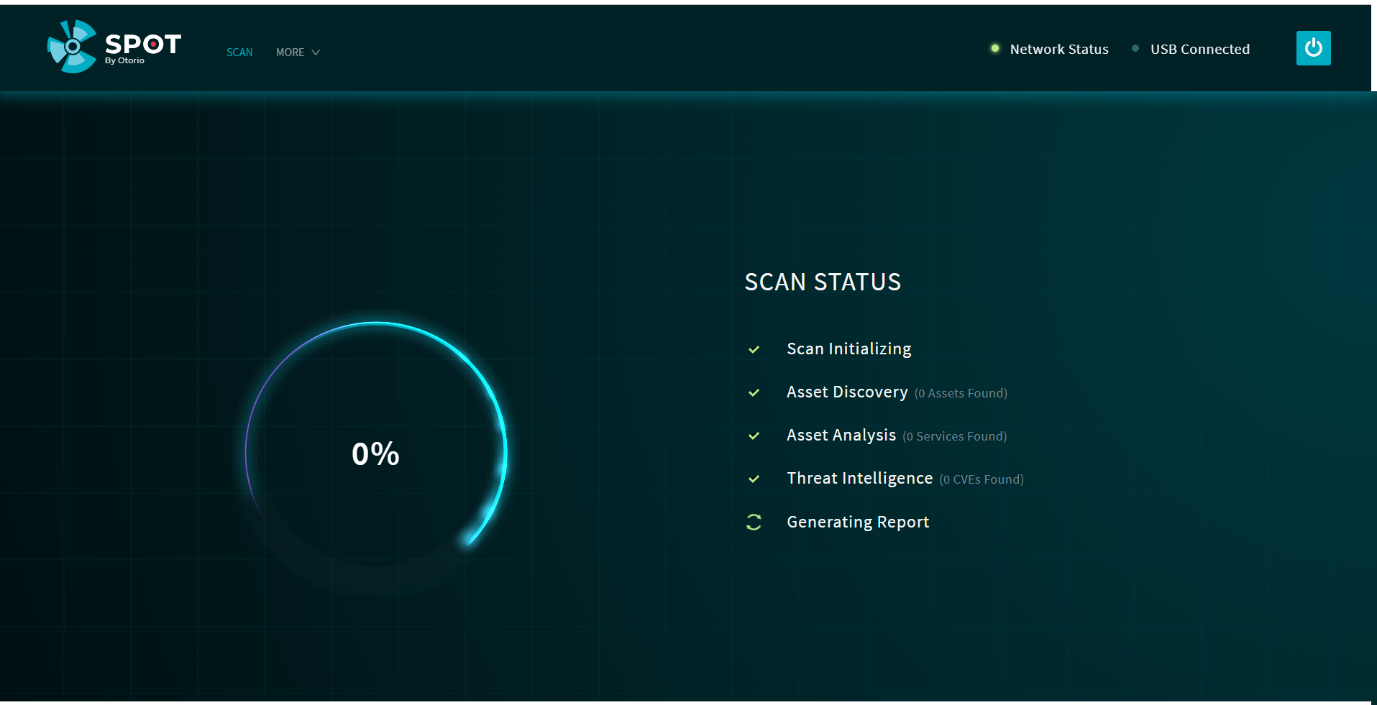


Figure Start scan

The scan goes through a number of 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.

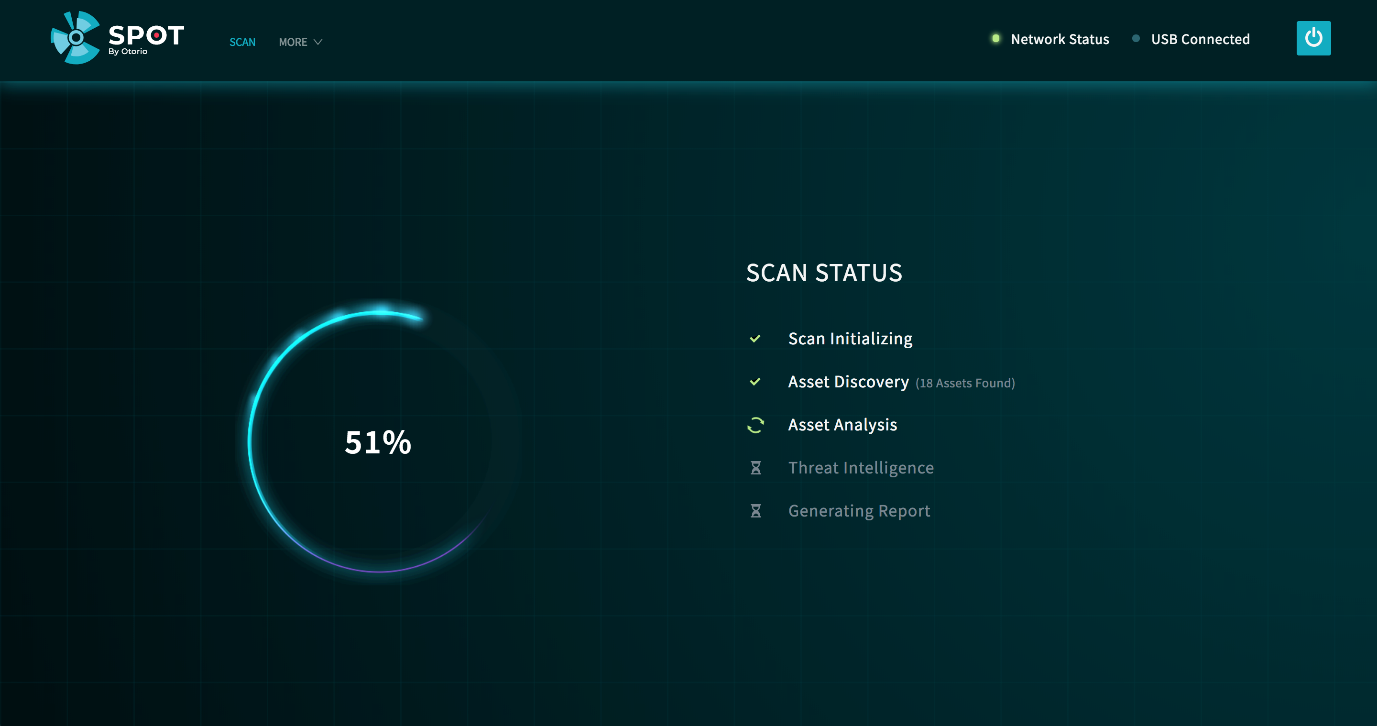


Figure Scan progress

## Scan Results

When the scan is complete, the Risk Level is shown.

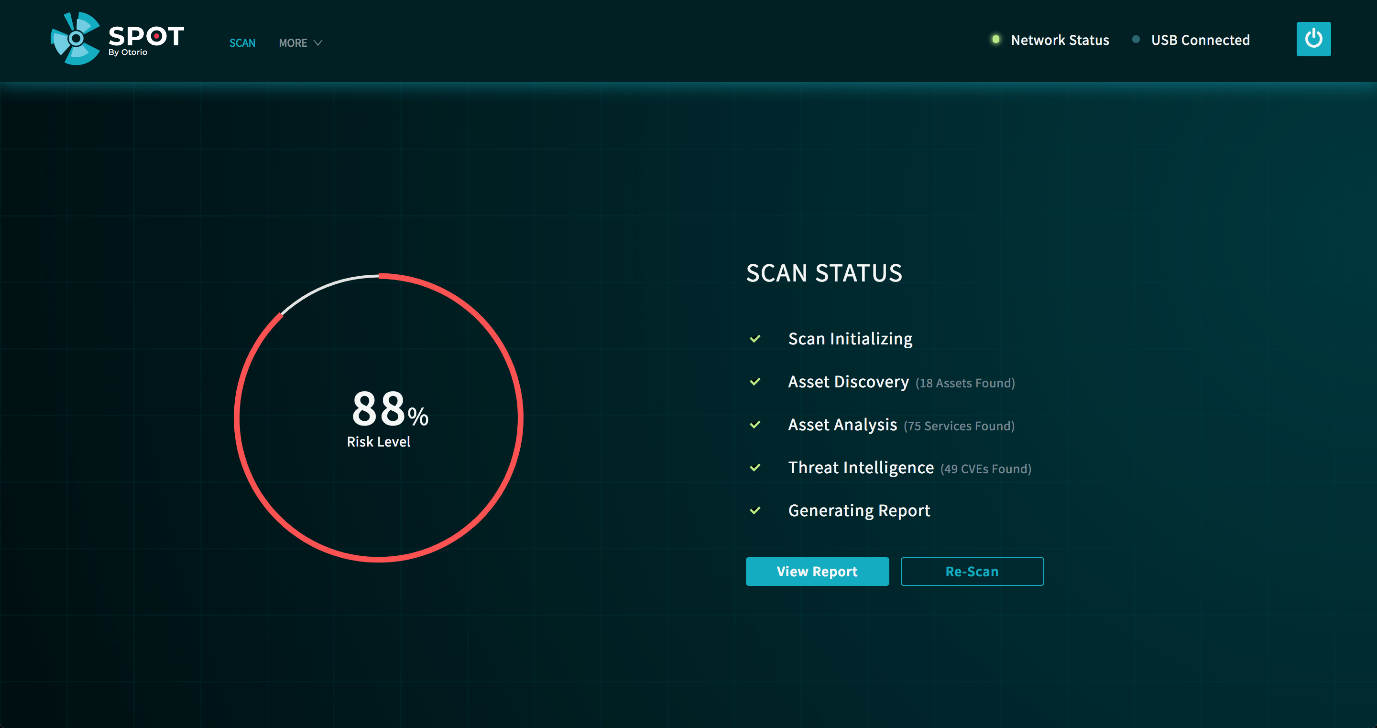
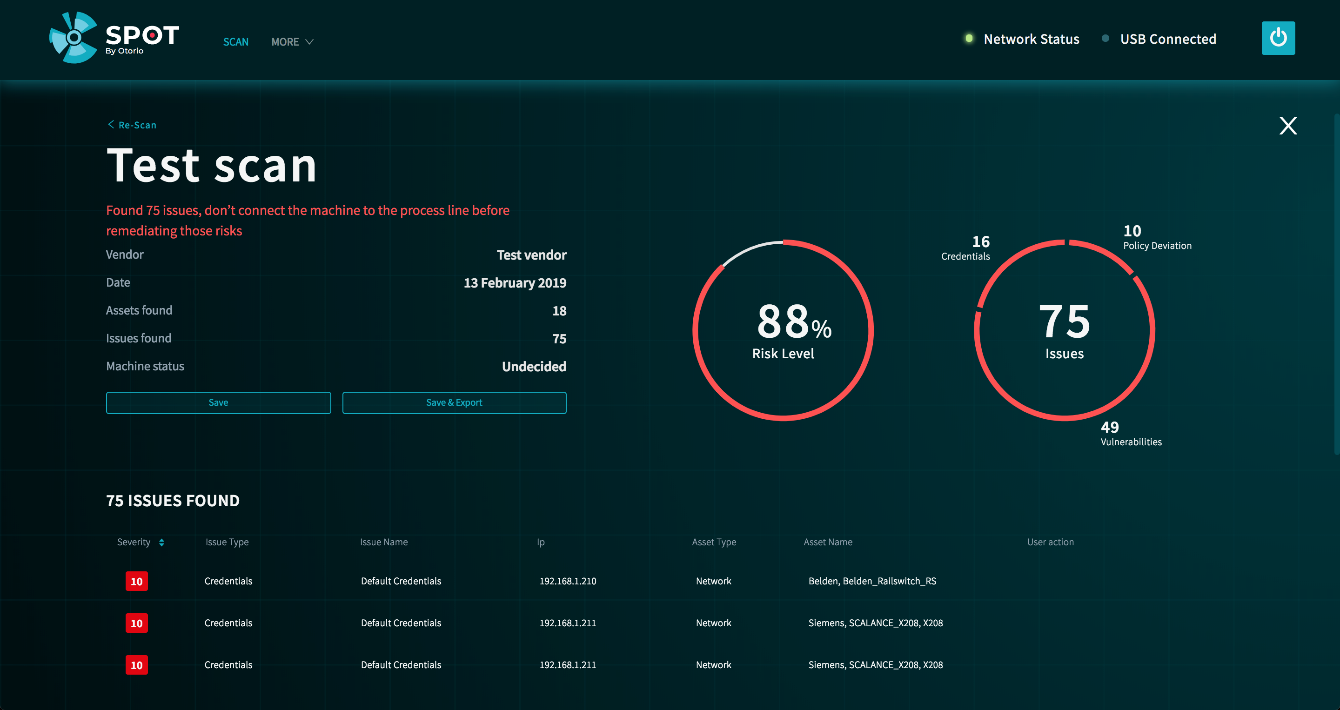


Figure Scan completion

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

The results show the following:

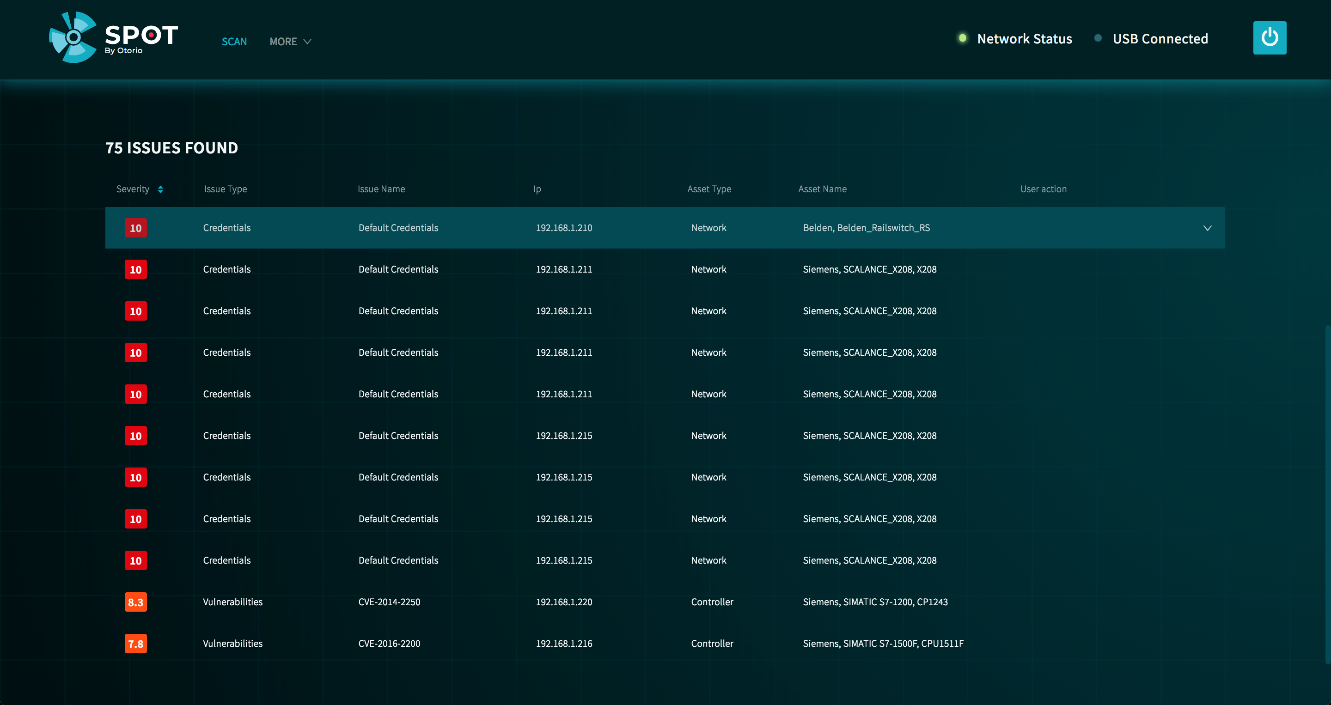
* Details for the device that was tested
* The Risk Level for the device, based on the findings of the scan
* The number of security issues found in the scan, according to type (Credentials, Policy Deviations, Vulnerabilities)
* A list of the issues



### Scan issues

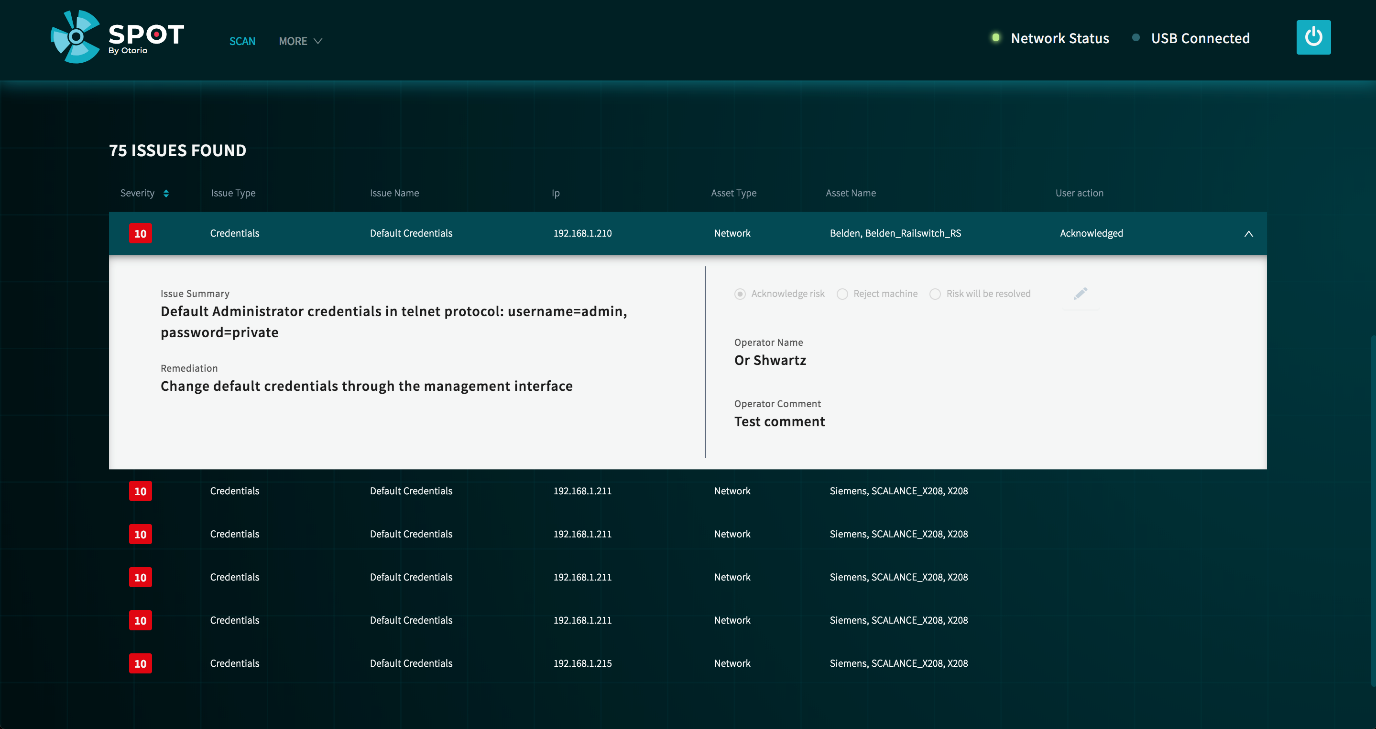
The list of scan issues shows the following details:

* severity of the issue (Critical, High, Medium, Low), including the [tbd – score?]
* 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:

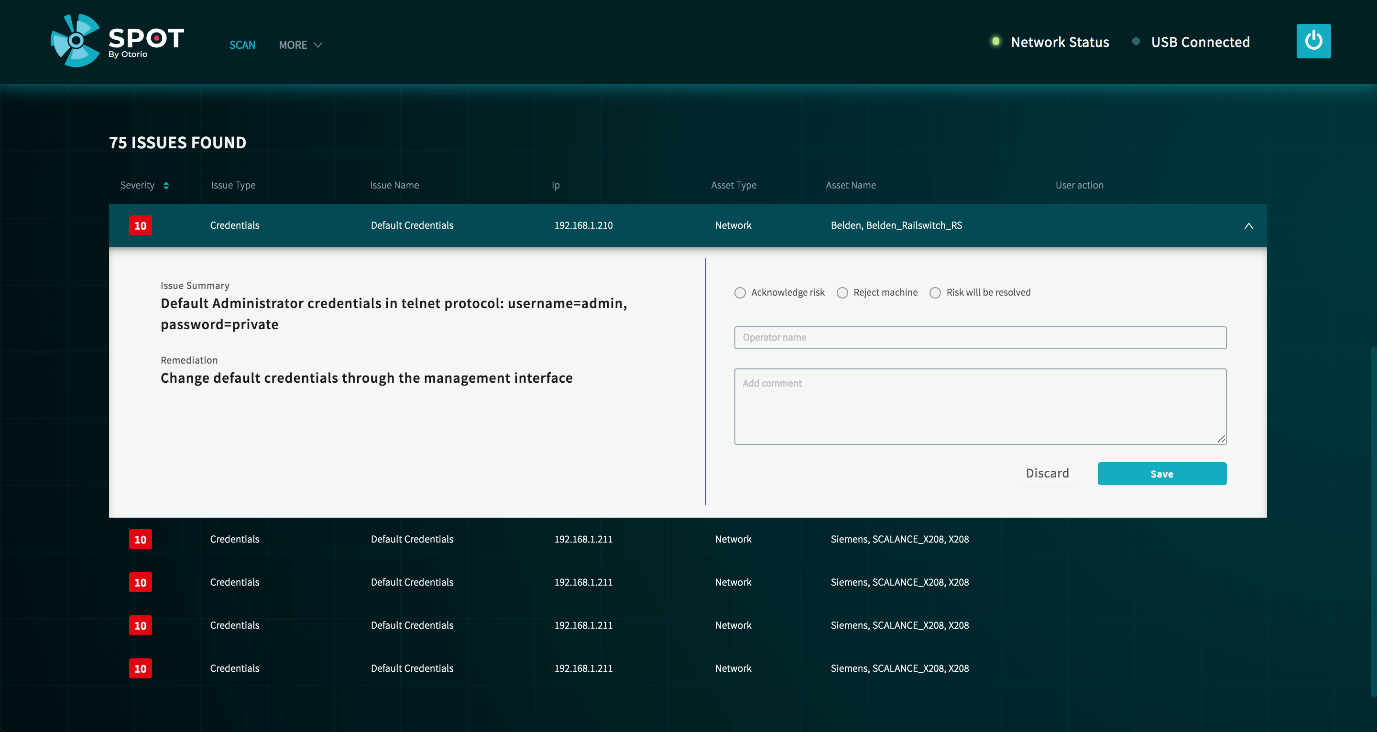
* Summary – a more detailed description of the issue
* Remediation – recommended steps to remedy the issue
* Operator – the operator who entered a comment or acknowledged the issue



### Add comments

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

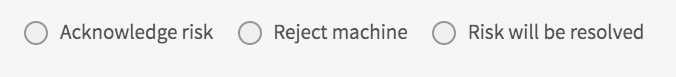
Enter the Operator name (your name), the comment (free text), then click Save. The comment is included in the report.



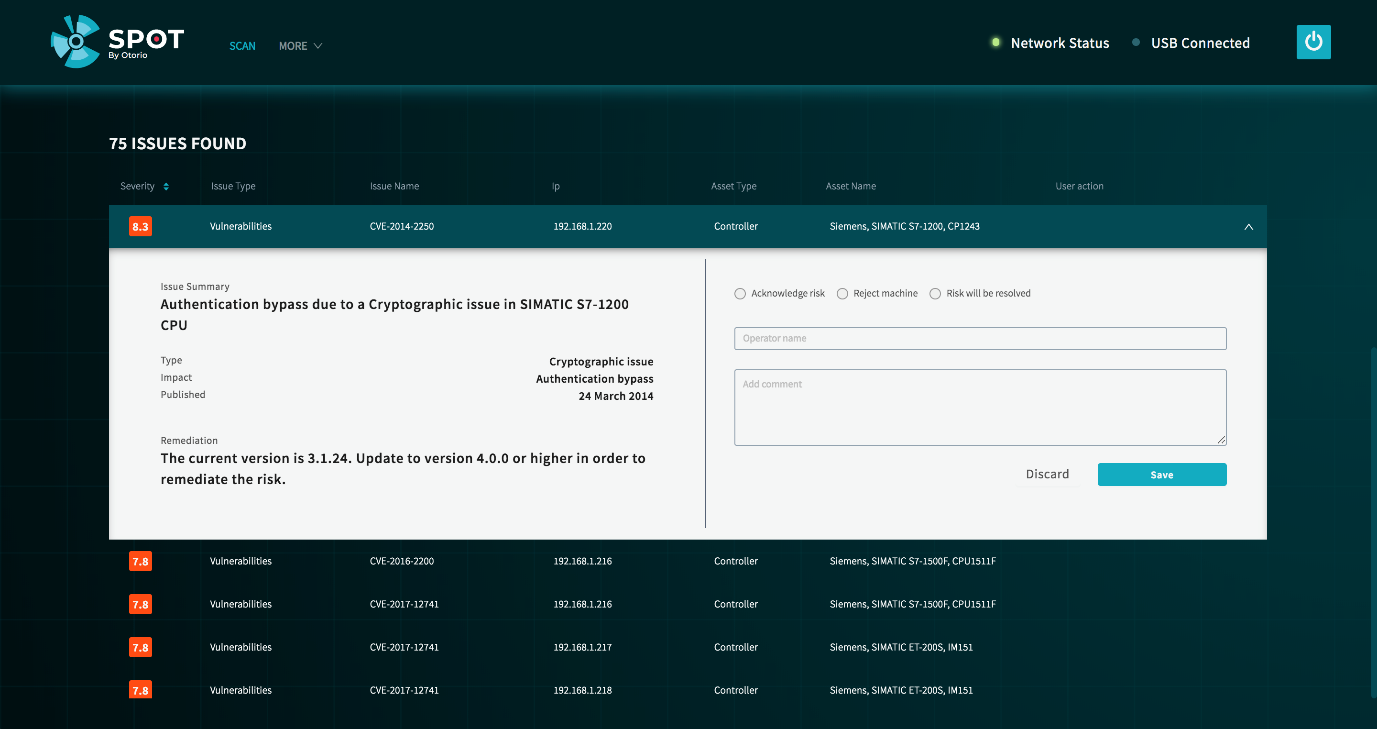
### Acknowledge an issue

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 report

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

## Export 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.

# Scan History

## Trends

# 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.

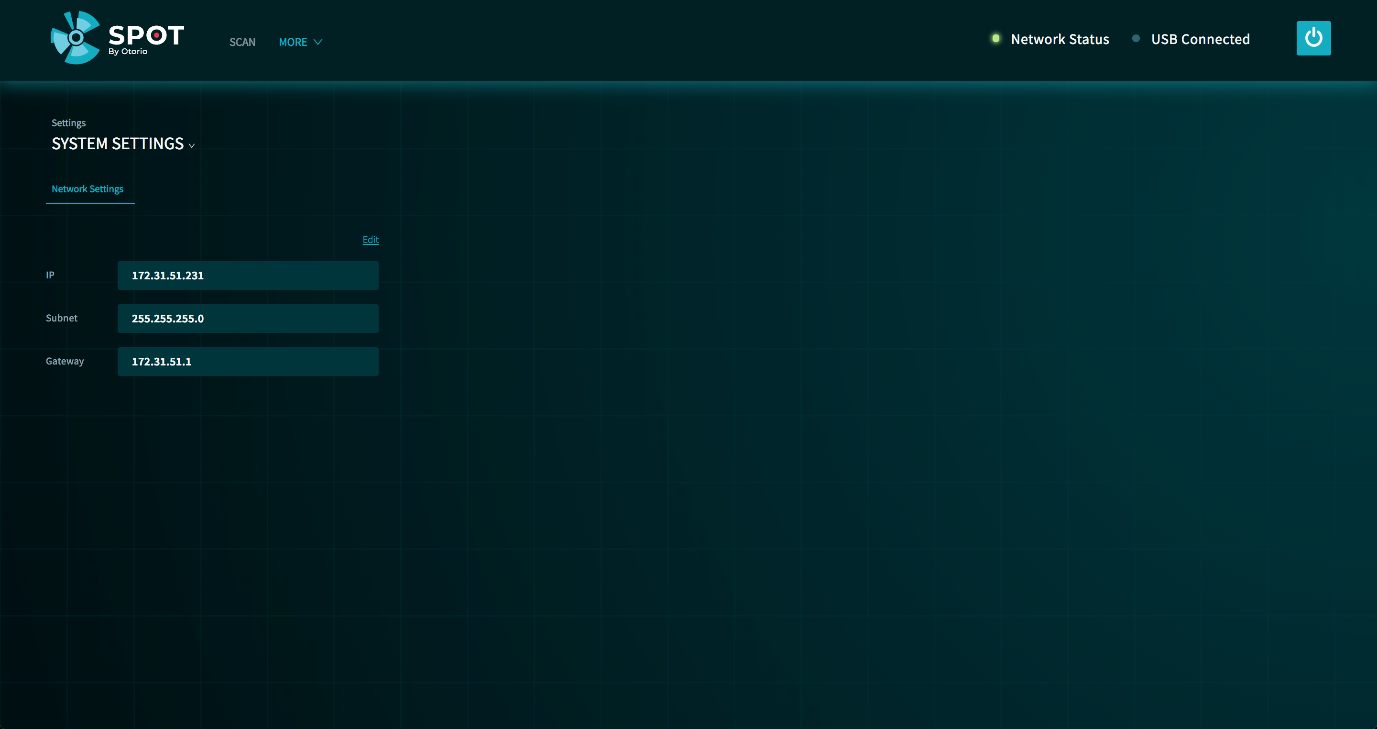


Figure System settings

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

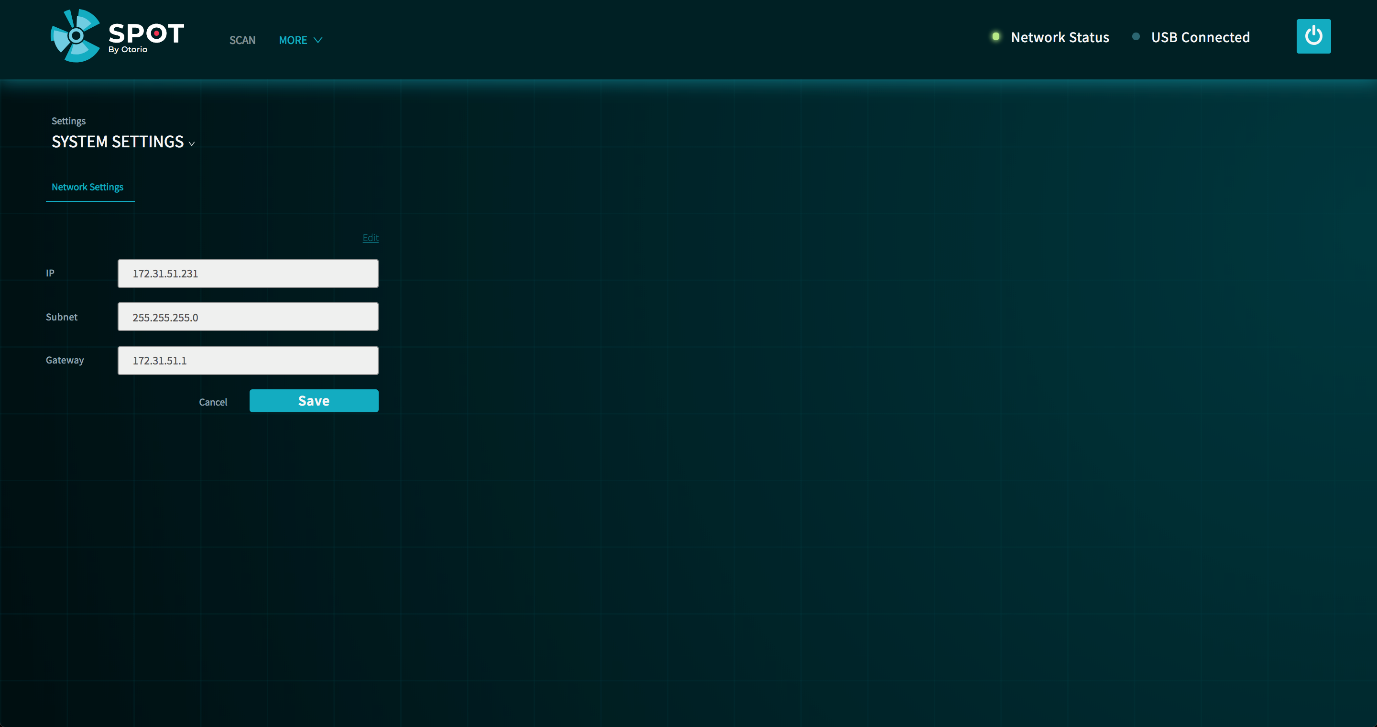


Figure Edit network settings

## Analyzers configuration