# Introduction

## Overview

The Otorio Risk Assessment Monitoring & Management platform, RAM2, is an industrial-tailored Security Orchestration, Automation and Response (SOAR) platform. The RAM2 offers a comprehensive, centralized, simplified, and automated industrial cyber risk management solution.

RAM2 easily integrates a variety of production floor data sources (e.g. OT, IT, security logs and network data) and provides actionable views of factory assets and alerts, based on powerful machine analytics. Business Information Security Officers (BISO) and operations engineers can use the customized dashboard to more effectively carry day-to-day tasks.

## Main Features

### Factory Management

The RAM2 platform manages security for assets (such as shop-floor machines) in a single factory.

The factory is divided hierarchically into the following entities:

**Factory** – the factory can be distributed over several geographical locations, but is one business or industrial unit.

**Shops** – an element of a factory, in which specific activities are performed.

**Cells** – a unit in a shop

**Assets** – a single machine or device in a cell. An asset can belong to only one cell.

RAM2 scans assets in cells to assess their security and risk level, and then assesses an overall risk level for the cell, based on the vulnerabilities found. It then determines the risk level for cells and shops, based on the security levels of the component assets.

### Asset Management

RAM2 discovers assets in the plant automatically (if they are connected to the plant network and discoverable).

You can define shops and cells for the plant, and then assign cells to shops, and assets to cells. Discovered assets are initially unassigned to any cell or shop.

RAM2 scans assets, once they are discovered, whether or not they are assigned to a cell.

RAM2 also has views to show the security and risk status of the plant, shops, cells, and assets, as well as alerts that are generated when security issues are found in the course of a scan.

You can perform the following actions:

**Add shops to plant** – define new shops, which are automatically included in the plant

**Associate cells to shops** – define new cells, and associate them with a shop, or move existing cells from one shop to another

**Associate assets to cells** – associate assets to a cell, or move assets from one cell to another

### Alerts

RAM2 generates alerts for security issues discovered in assets in the course of a scan. The alert indicates the severity of the issue, and details for it (such as the specific vulnerability for the issue). There are filterable views to see alerts for shops, cells and assets, or for specific risk levels or vulnerabilities.

You can acknowledge an alert for a specific asset.

### Vulnerabilities

RAM2 assesses the risk level for an asset using a list of vulnerabilities compiled by the Otorio threat intelligence research team, and based on published open source vulnerabilities, industrial best practices, etc.

You can view the list of vulnerabilities, and filter views and alerts according to specific vulnerabilities. You can also disable specific vulnerabilities, in which case, asset scans will not report or show on issues relating to them.

## What RAM2 does

* Discover & map assets in plant network
* Regularly collect information about assets (MSB)
  + Device, FW, IP,
* Correlate asset info with vulnerability information to generate an asset risk assessment & score
  + CVEs
  + Otorio Threat Intel Research Team
* Generate Shop-level risk level, based on cell & asset risk assessments
  + Otorio proprietary algorithm
* Generate alerts about assets

# Views

RAM2 has several views, to show entities in the plant, and alerts.

The home page is the Dashboard view.

## Dashboard View

The Dashboard view is the first view you see when the RAM2 application starts. It shows summary information for each shop in your plant. You can select from the list of shops on the left. For each shop it shows:

* The overall Risk Level for the shop
* The number of production cells in the shop
* The number of assets in the shop (assigned to cells)
* The number of alerts that have been logged for the shop

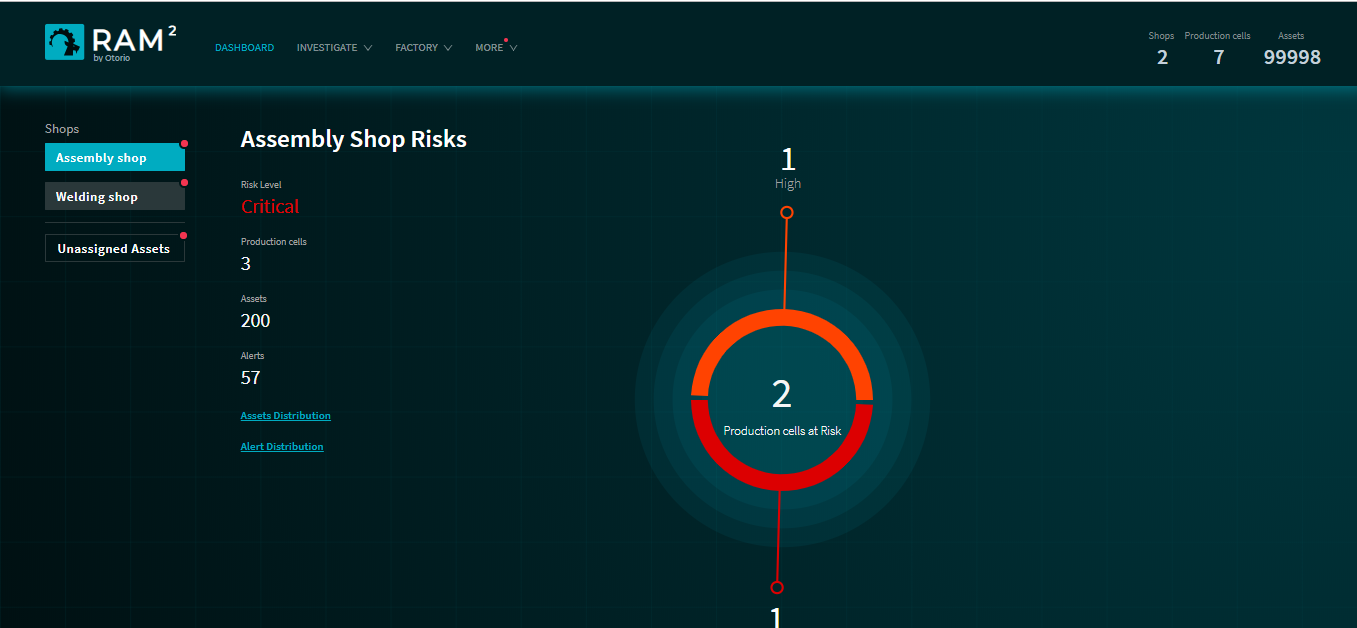


Figure 1 Dashboard view

Click on  or the Dashboard link to return to the Dashboard from any other RAM2 view.

At the top of the Dashboard is the top-level menu-bar.



Use these menus to navigate to different views, described in this section, and to perform other actions (discussed in later sections).

The center of the Dashboard shows graphically the Risk Level distribution of the production cells in the shop. This is color-coded by Risk Level.



Figure 2 Cell Risk Level distribution

In the example above, there is one cell at Risk Level ‘High’, and one at ‘Critical’ (and the third not at risk).

Click on one of the Risk Levels, to show more detail. In the example below the cell at High Risk has 7 assets affected by risk, with 10 alerts generated.

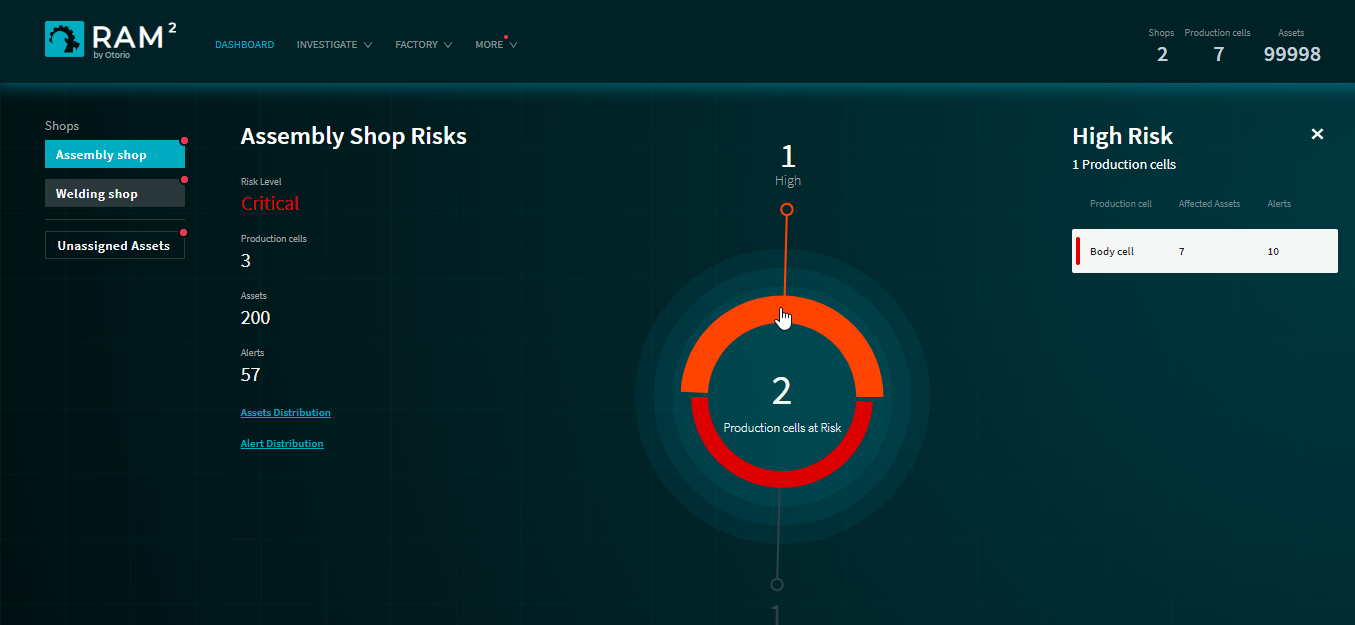


Figure 3 At-risk production cell details

Click on the detail (at the right) to open a list of the alerts for the cell.

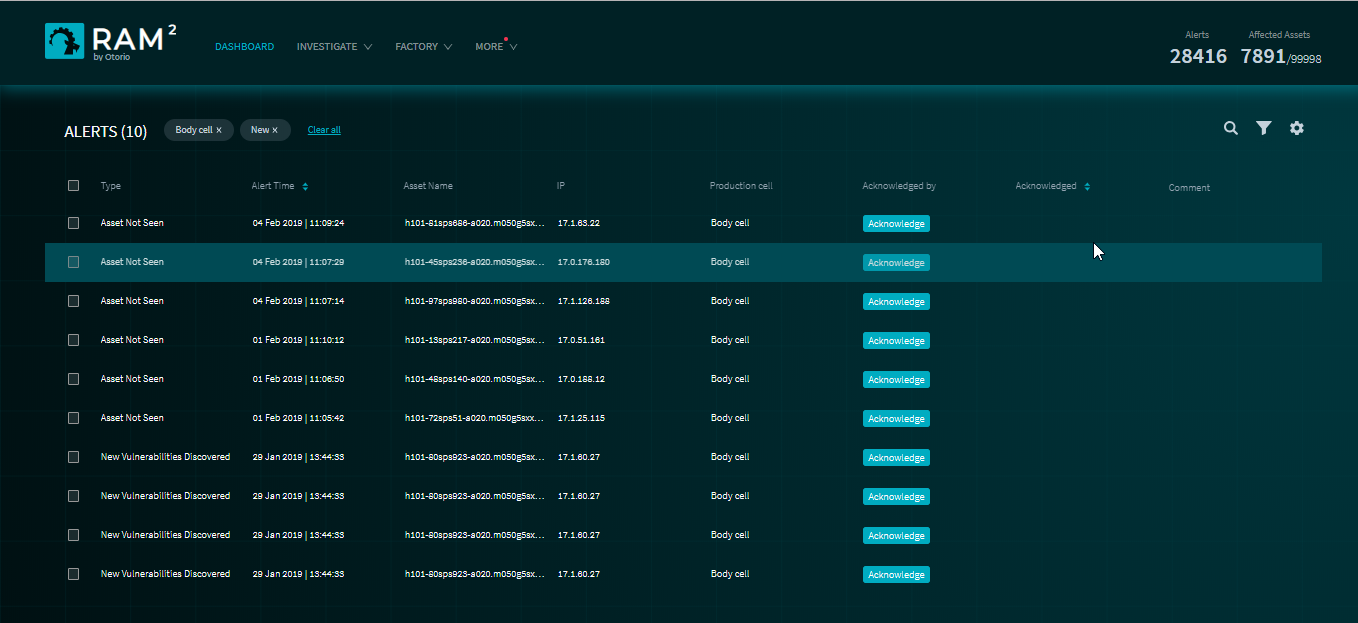


Figure 4 Alerts for Production Cell

### Shop information

From the Dashboard, select Shop from the Factory menu.

### Asset Distribution

From the Dashboard, you can see a distribution of assets according to asset type or production cell.

Click on the Assets Distributio*n* link on the Dashboard, and select the distribution type.

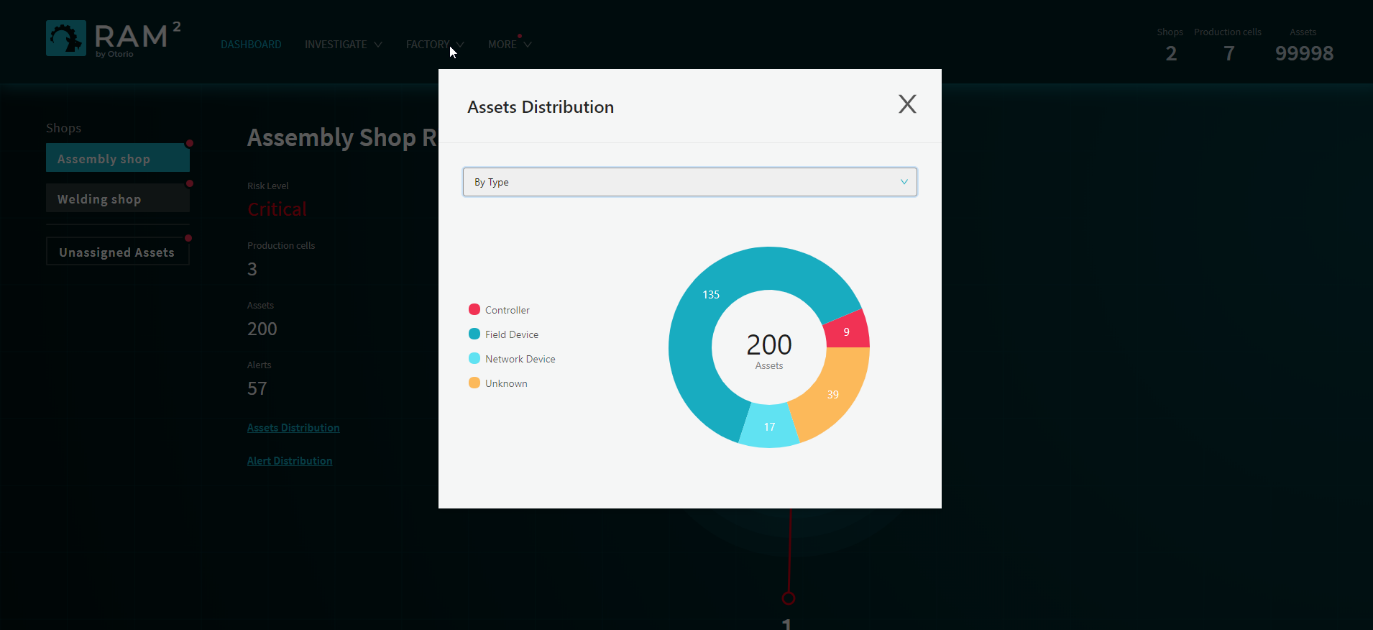


Figure 5 Asset Distribution by Asset Type

### Alert Distribution

From the Dashboard, you can also see a distribution of alerts according to alert type or production cell.

Click on the Alert Distribution link on the Dashboard, and select the distribution type.

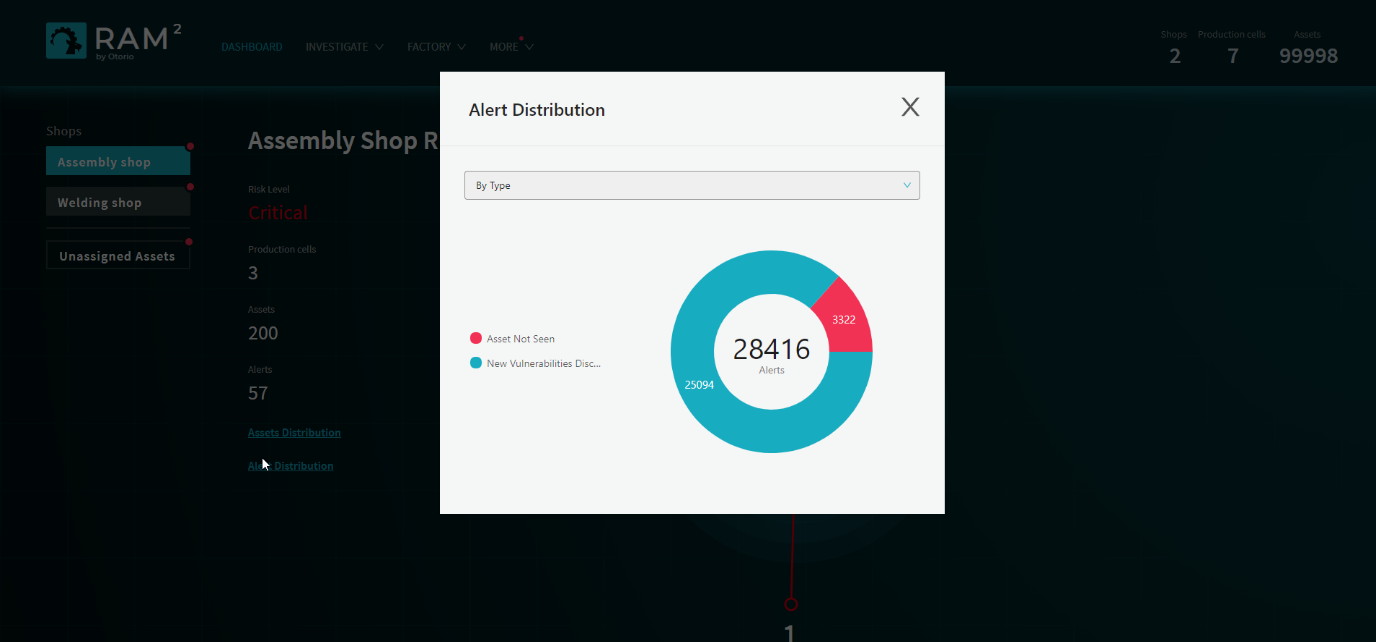


Figure 6 Alert Distribution by Alert Type

### Unassigned Assets

You can see a list of unassigned assets (assets that are not assigned to any production cell) from the Dashboard. Click on Unassigned Assets in the list of shops, on the left. This view is similar to the Shops view, and shows an overall Risk Level (based on all the unassigned cells taken together).

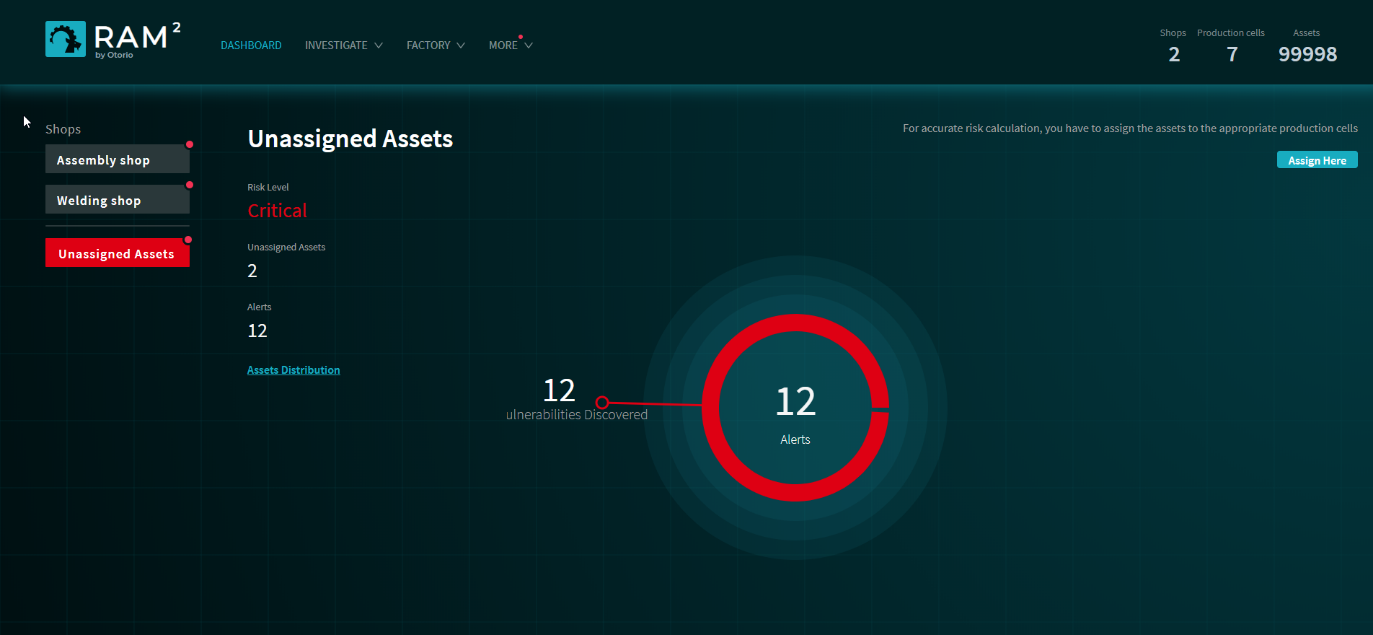


Figure 7 Unassigned Assets

## Assets

You can view assets in your plant in various asset views. Select these from the top-level Factory menu.

### Shops view

Select Shops from the Factory menu to see the shops you have defined for the plant.

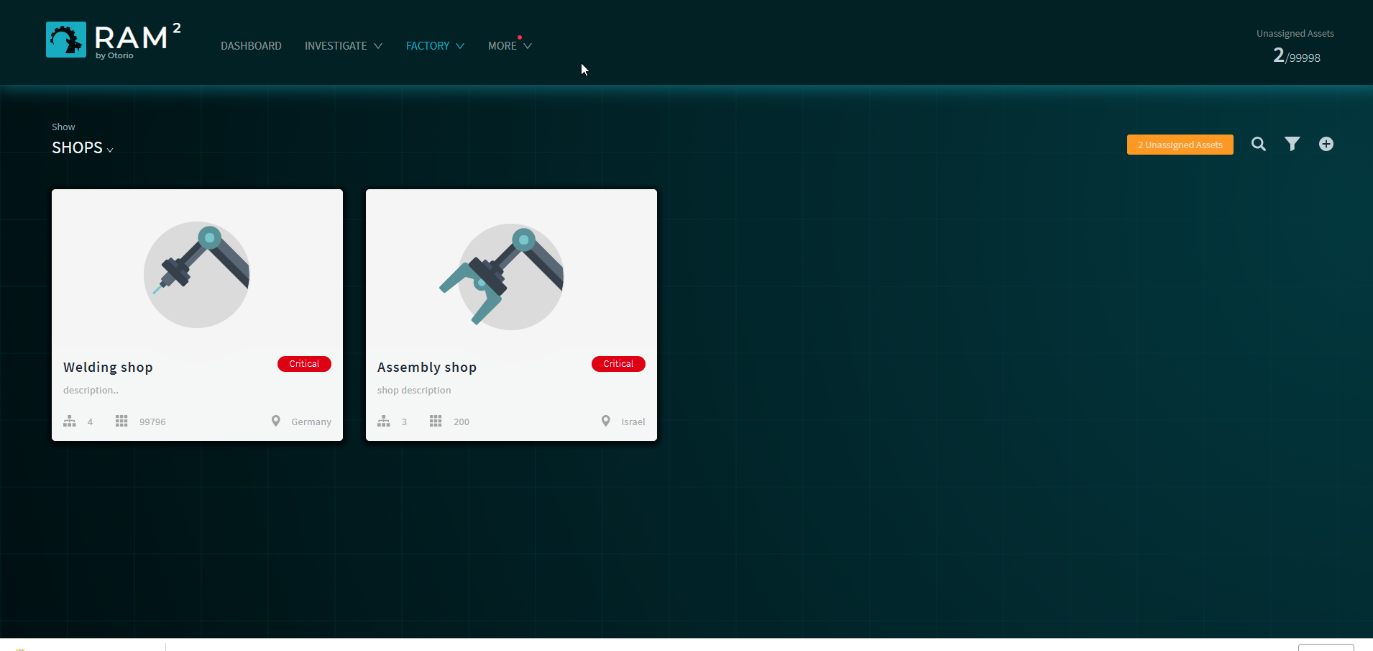


Figure 8 Shops

Each image in this view represents a shop, and shows the following information for it:

* the overall shop Risk Level
* the number of cells
* the number of assets
* the geographic location of the shop

### Production cells view

Click on a shop to show the production cells in it. Alternatively, select Cells from the top-level Factory menu, to show all the cells in the plant.

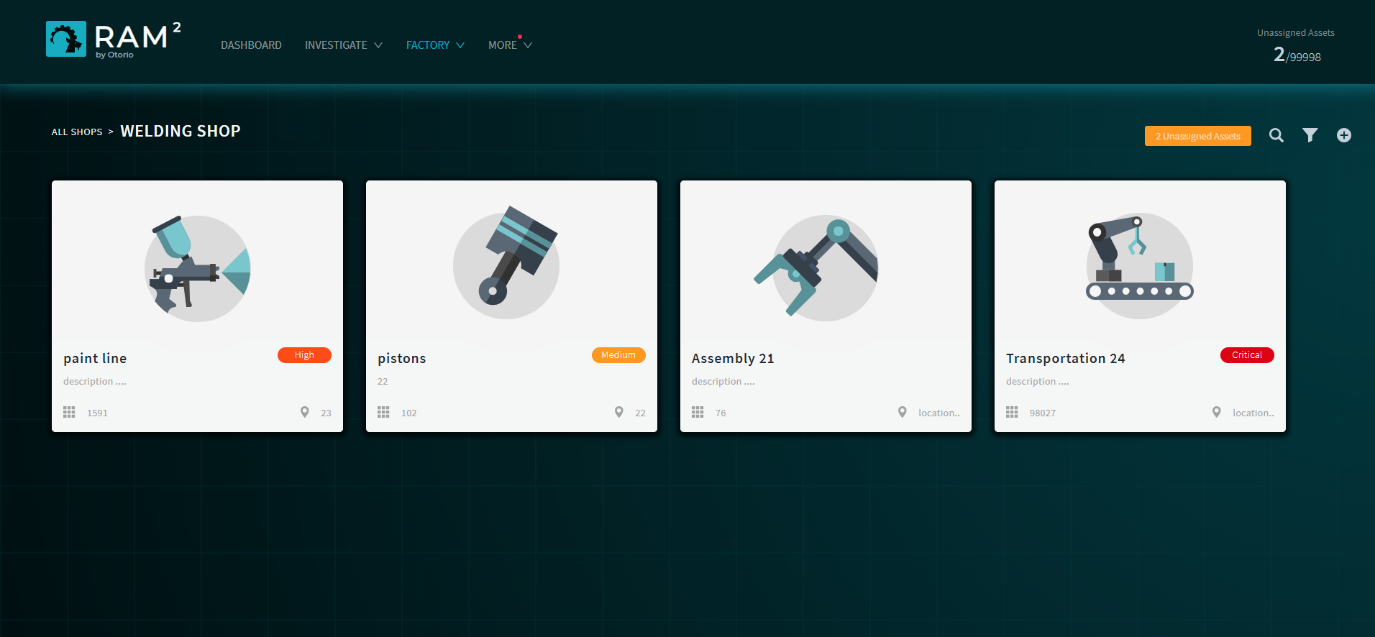


Figure 9 Shop cells

Each image in this view represents a production cell, and shows this information:

* the overall Risk Level for the cell
* the number of assets
* the location of the cell

### Assets view

Click on a cell to show the assets in it. Alternatively, select Assets from the top-level Factory menu, to show all the assets in the plant.

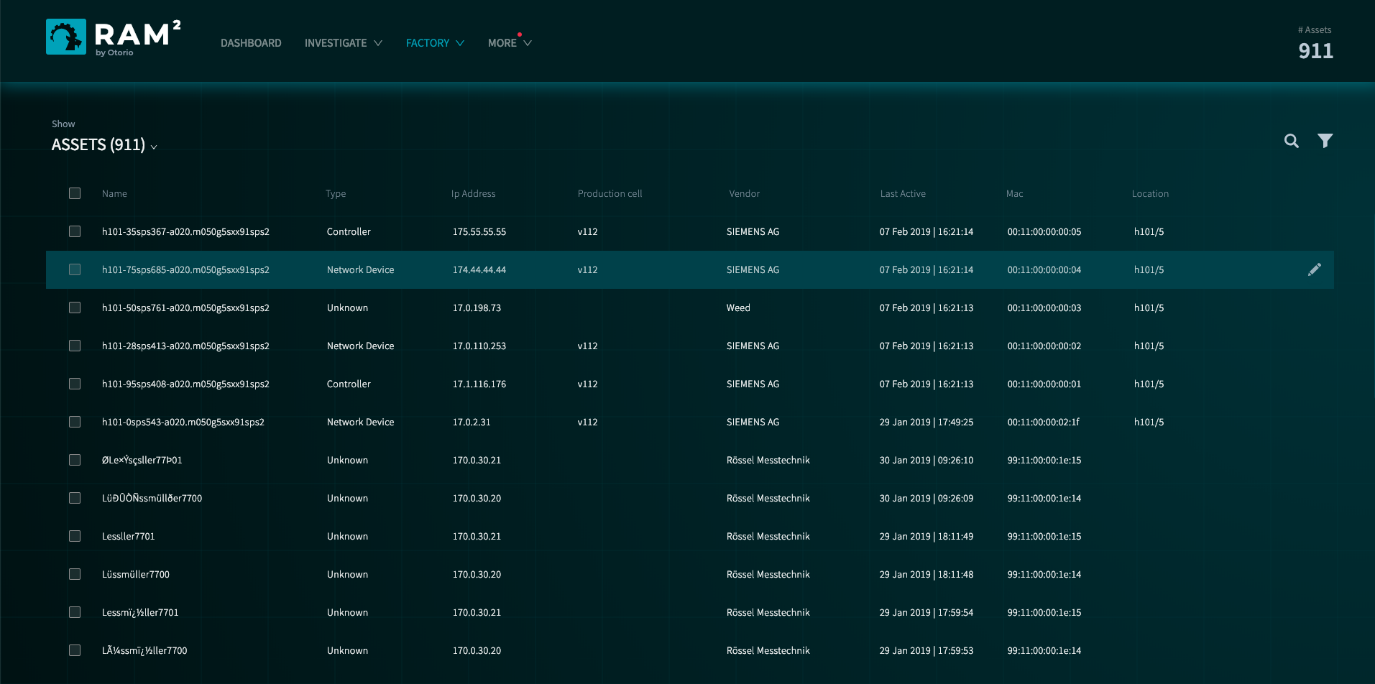


Figure 10 Factory assets

The table of assets shows this information:

* Asset name
* Asset type – Controller, Network Device,
* Asset IP address
* Production cell to which the asset is assigned
* Vendor
* Time asset was last active
* MAC address
* Location

## Alerts

You can view alerts that have been generated by RAM2 in the alert view. Select this from the top-level Investigate menu.

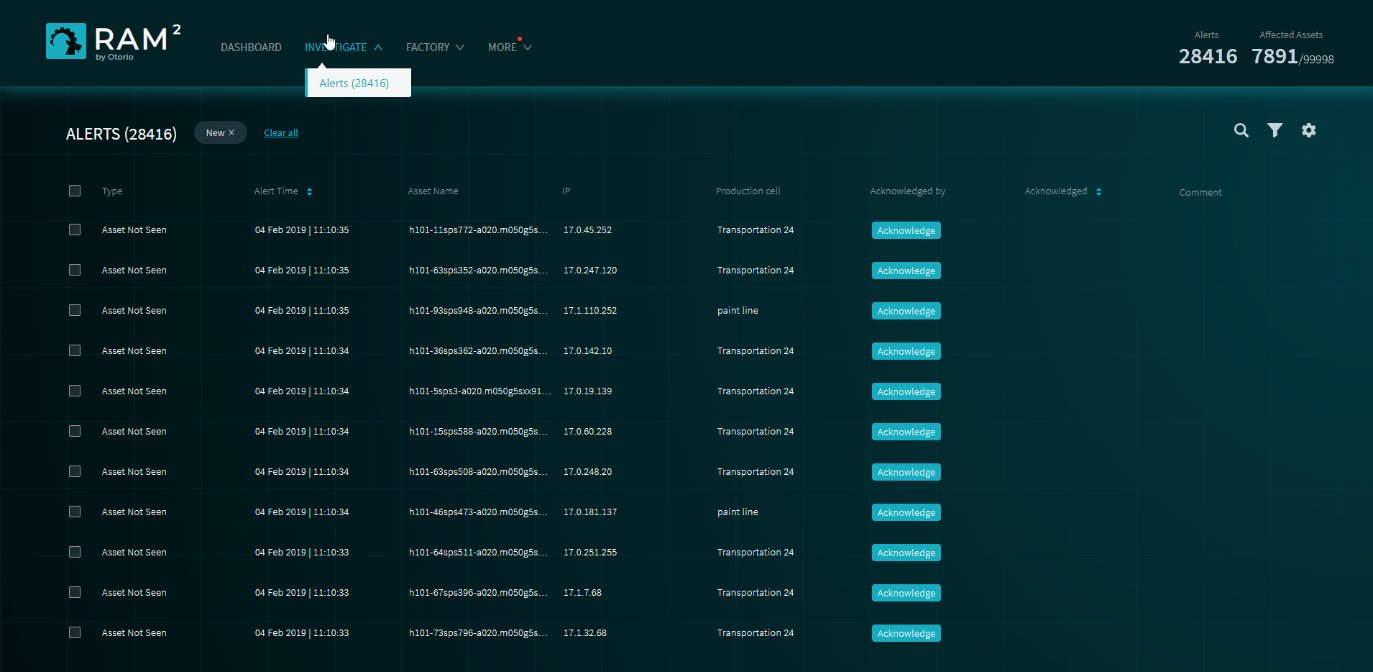


Figure 11 Alerts view

This view shows following details for each alert

* **Alert type** – from a list of pre-defined alert types
* **Alert time** – the time the alert occurred
* **Asset name** – the asset on which the alert occurred
* **Asset IP** – the IP address of the asset
* **Production cell** – the cell containing the affected asset
* **Acknowledged by** – if the alert was acknowledged, the name of the person who acknowledged it, otherwise a link to acknowledge the alert.
* **Acknowledged** – indicates the alert was acknowledged (blank, if not)

## Filters

You can filter the views in RAM2 to select specific items of interest.

Click  to select the filter for the view. The options vary according to the view, but the filter panel on the right is common.

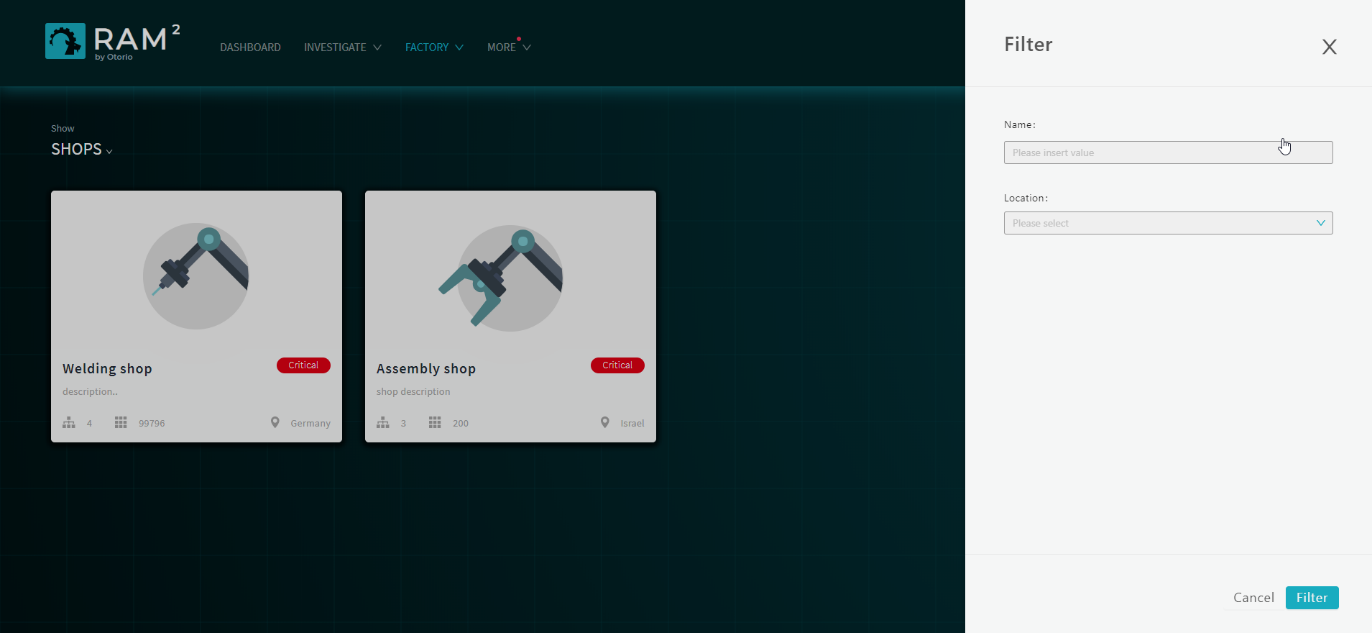


Figure 12 - Filter

# Factory Management

In RAM2 you can define shops and production cells for your factory. RAM2 discovers factory-floor assets itself directly from the MSB.

You can associate cells to shops, and assets to cells.

## Shops

Shops are the highest-level entity in a factory.

### Create Shops

Add or modify shops in the factory, in the Shops page.

To add a new shop:

1. Select Shops from the top-level Factory menu. A list of all shops in the factory is shown.
2. Click .
3. In the Create New Shop panel, enter the following:
4. **Shop name & description** – the name for the shop in RAM2, and a description of it; this is free text
5. **Location** – the geographic location of the shop
6. **Image** – (optional) upload an image for the shop.

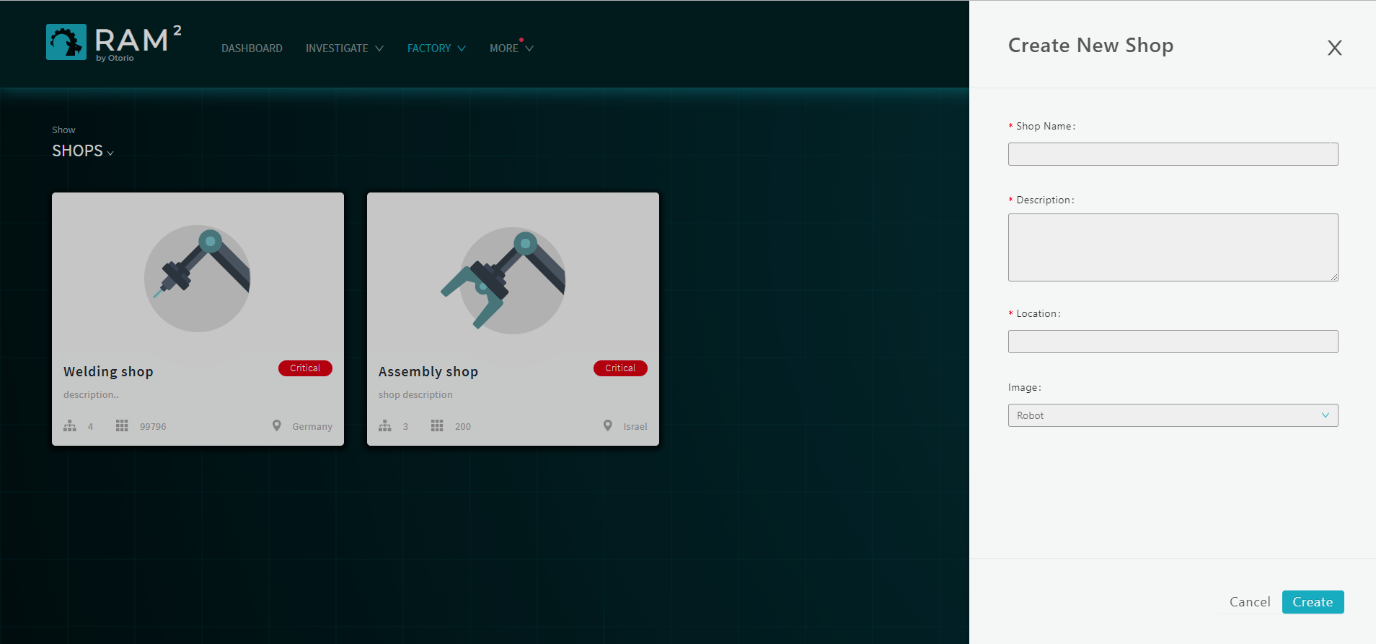


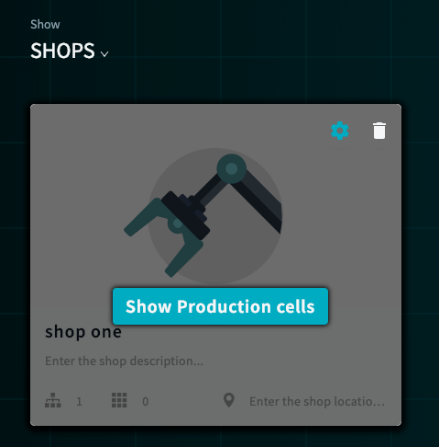
Figure 13 Create new shop

1. Click Create.

The new shop will appear on the page.

To modify details for a shop:

1. In the Shops page, hover over the image of the shop to be modified.



1. Click .

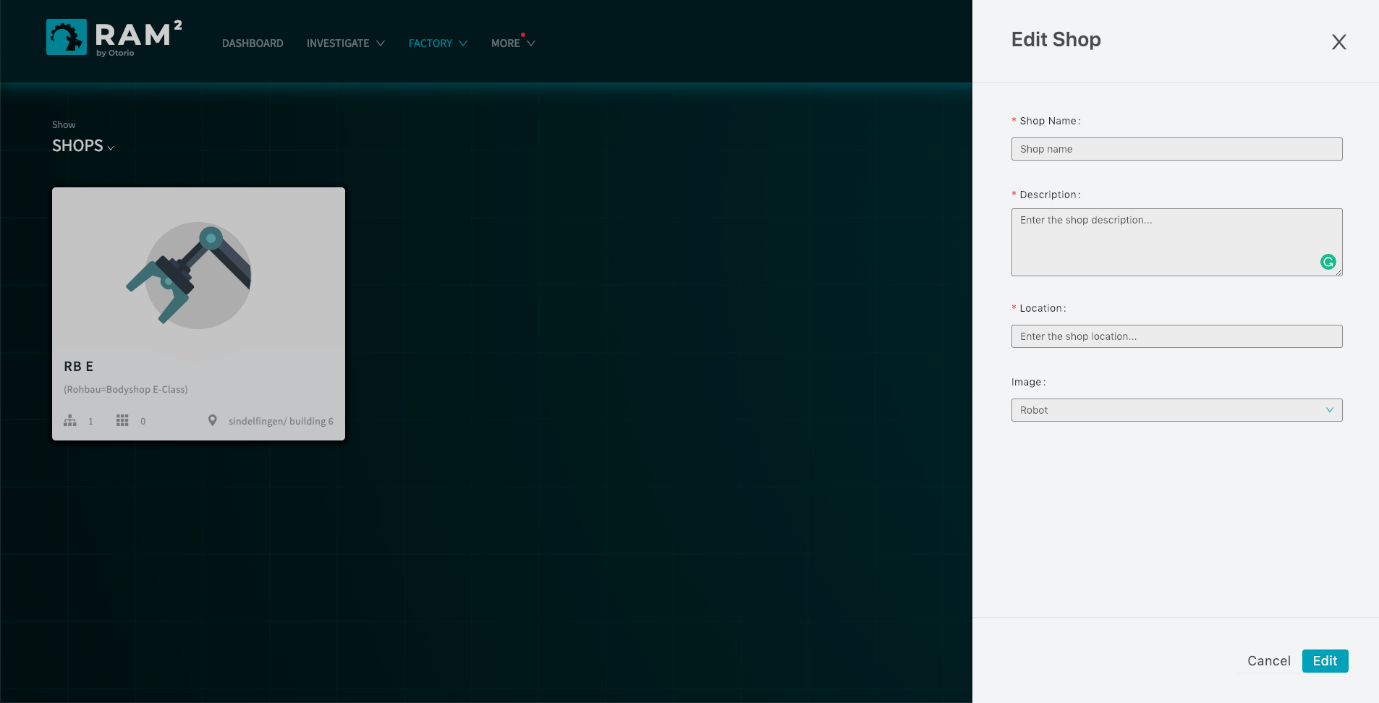


Figure 14 Edit shop

1. In the Edit Shop panel, make changes to the shop details, as necessary, and then click Edit.

## Cells

Production Cells are entities within shops. A cell can be assigned to a single shop.

### Create Cells

Add or modify cells in the Production Cells page. Select Production Cells from the top-level Factory menu. When you create the cell, you assign it to a shop. Alternatively, you can add a cell from the Shops page for a specific shop, in which case the cell, once created, is assigned to this shop.

To create a cell:

1. Select Production Cells from the top-level Factory menu. A list of all cells in the factory is shown.
2. Click .
3. In the Create New Production cell panel, enter the following:
4. **Cell name & description** - the name for the cell in RAM2, and a description of it; this is free text
5. **Location** - the geographic location of the cell
6. **Shop** – the shop with which the cell will be associated (from a list)
7. **Image** – upload an image for the cell

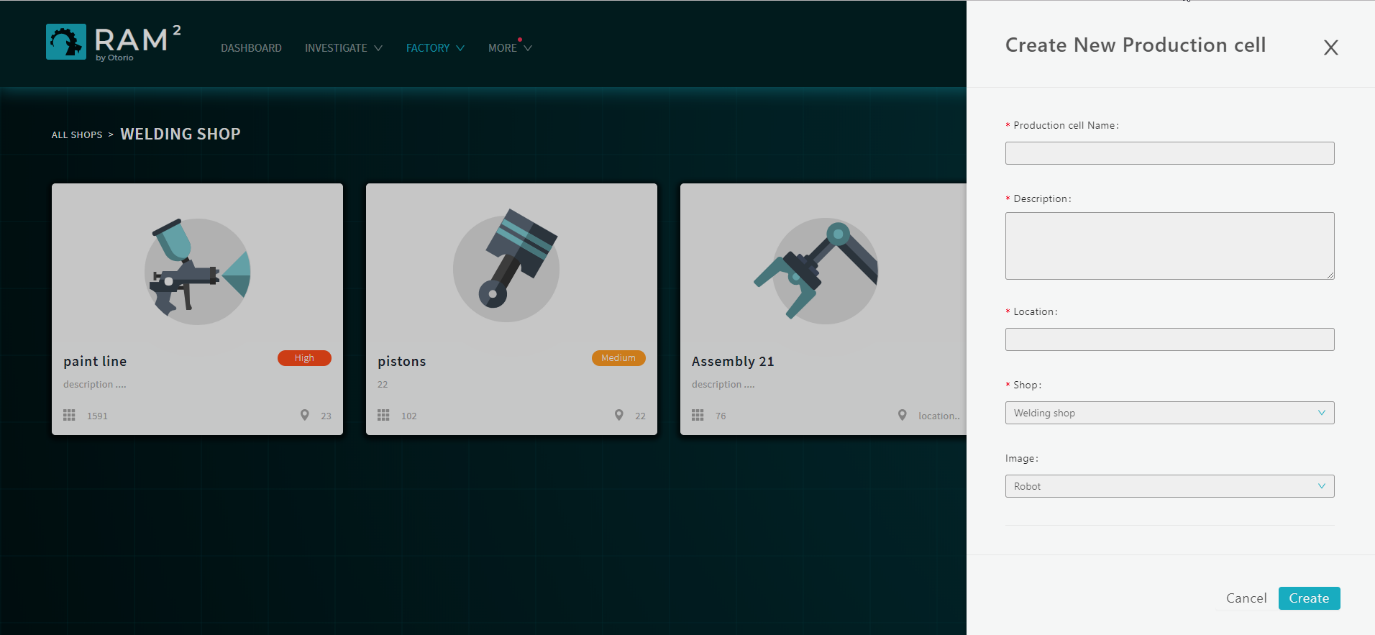


Figure 15 Create production cell

1. Click Create.

The cell will appear on the Production Cells page, and also as one of the cells in the Shops page to which it was assigned.

To create a cell in a shop:

1. In the Shops page, select the shop to which the cell will be added. The current cells for this shop will be shown.
2. Click .
3. In the Create New Production cell panel, enter the following
4. Cell name & description - the name for the cell in RAM2, and a description for it
5. Location - the geographic location of the cell
6. Image – upload an image for the cell
7. Click Create.

The cell will appear in the page for the cell.

### Change the Shop for a Cell

When you create a cell, it is assigned to a shop. You can change the shop to which it is assigned by editing the cell details.

To change the Shop for a Cell:

1. Select the Shops page for the shop containing the cell.
2. Hover over the cell to be moved, and click .
3. In the Edit Production Cell panel, select the new Shop from the list.
4. Click Edit.

## Assets

Assets are individual shop-floor machines. They are discovered automatically (for example, using the MSB). You can assign them to production cells once they are discovered, or move them to different cells.

Once discovered, RAM2 assesses a Risk Level for them.

Once they are assigned to a cell, their Risk Level contributes to the overall Risk Level of their assigned cell and shop.

### Assign Assets to Cells

You can assign an asset to a cell from the Assets page. Select Assets from the top-level Factory menu. This will show a list of all the assets in the factory (assigned and unassigned). Filter or search for the assets to assign to a cell. For example, to assign newly discovered unassigned assets, filter for Unassigned assets.

To assign a single asset to a cell:

1. Hover over the asset in the list.

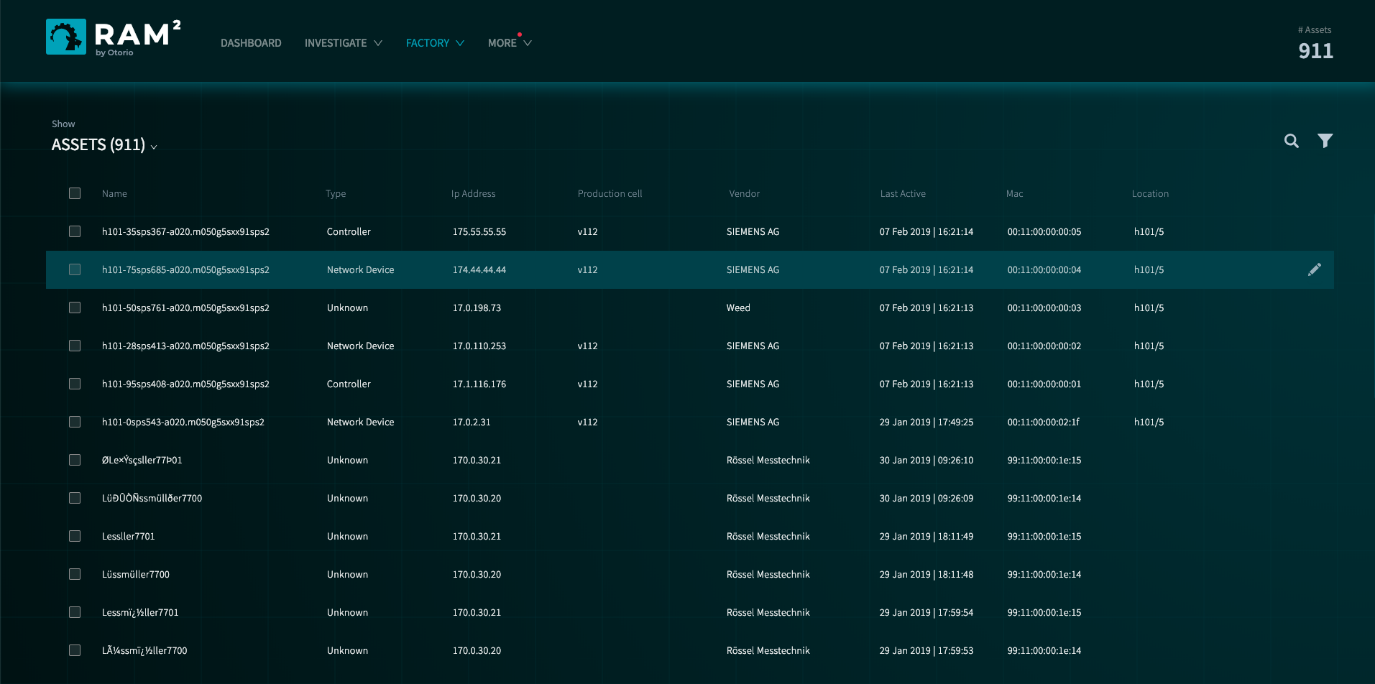


Figure Select an asset to assign

1. Click  (on the right side).

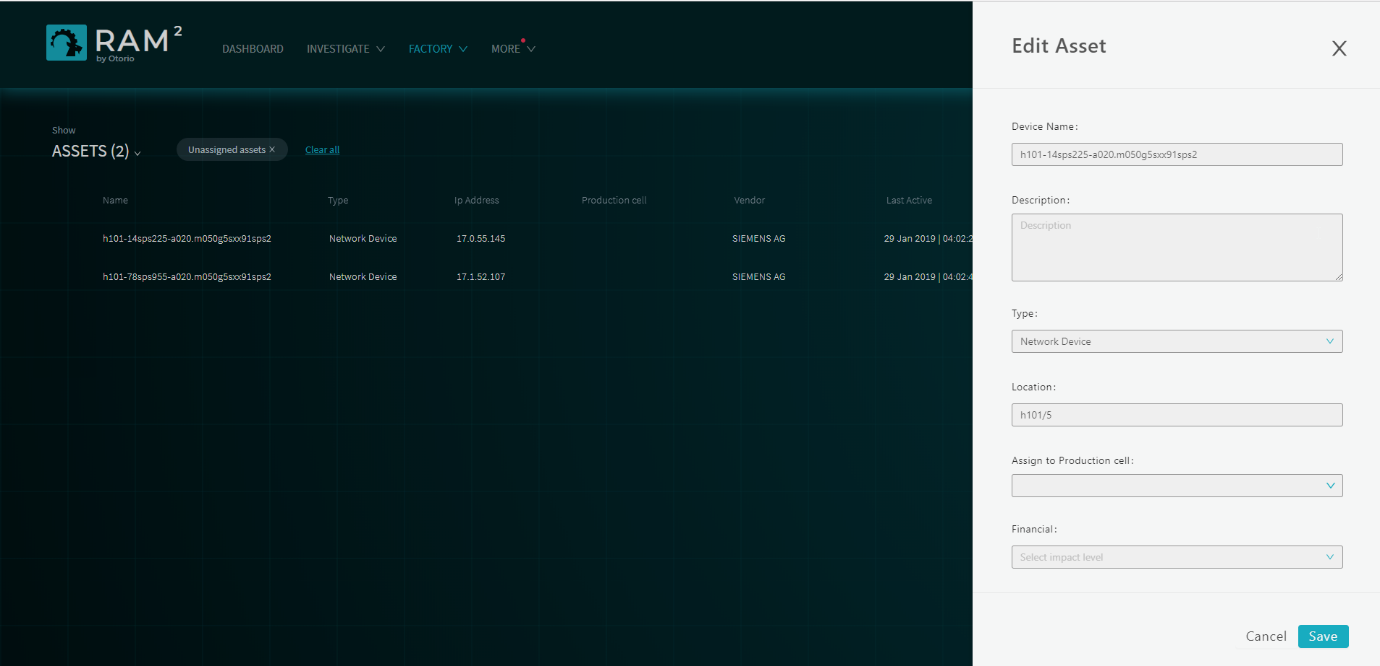


Figure Assign an asset to a cell

1. In the Edit Asset panel, select the production cell from the list.
2. Click Save.

To asset a number of assets at once:

1. Select the assets in the list, and then .

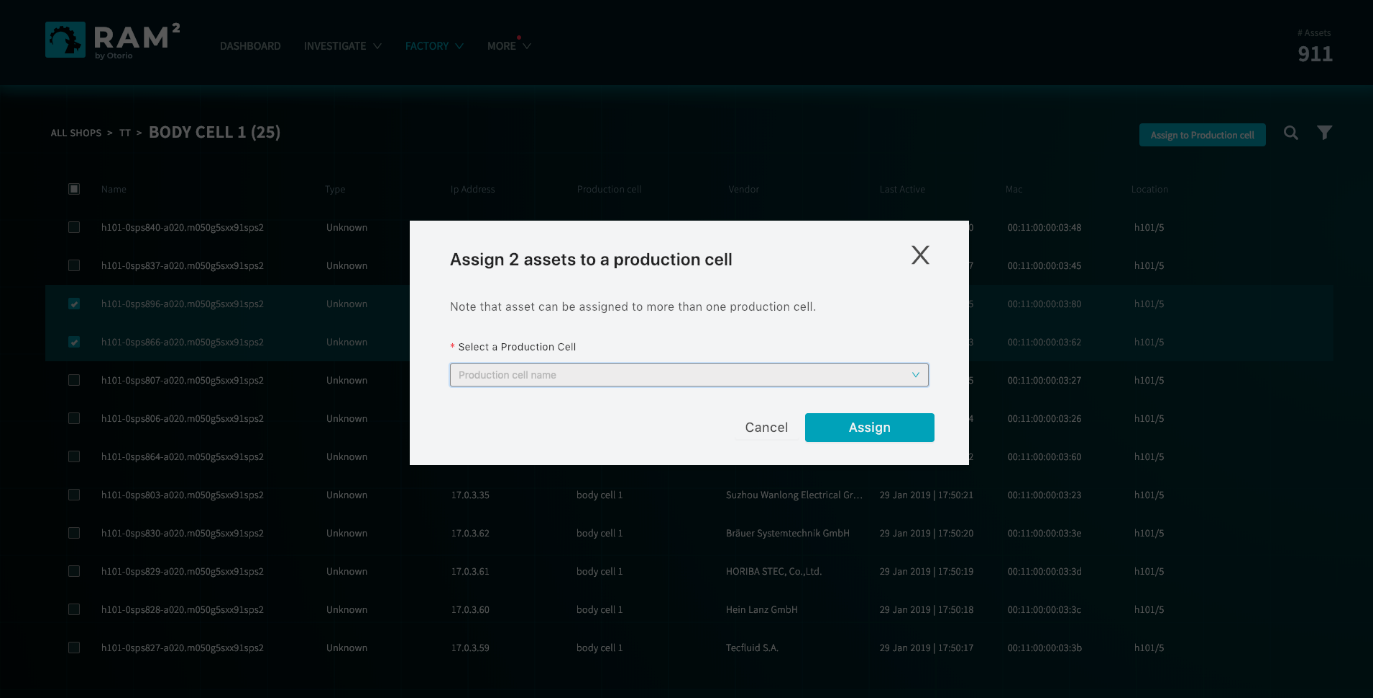


Figure Assign multiple assets to a cell

1. Select the production cell from the list.
2. Click Assign.

# Alerts

RAM2 generates alerts when security issues are discovered in assets after they are scanned. These alerts are shown in the Alerts view.

You can perform the following actions on alerts, from the Alerts page.

* View details for the alert, and the asset affected.
* View the distribution of alerts according to alert type or production cell.
* Acknowledge the issue in the alert
* Disable specific vulnerabilities from being reported in future alerts.

## Alert types

Alerts are classified into these types:

* New asset discovered – new asset has been discovered by RAM2; it does not mean there is a security issue.
* Asset not seen – an asset has not been detected on the network for 72 hrs (this time is configurable)
* New vulnerability discovered – a new vulnerability has been detected for a specific asset; the alert includes details of the vulnerability
* FW version changed – the firmware version on an asset has changed; it does necessary mean that there is a security issue.
* IP address changed – the IP address for an asset has changed
* State changed – an asset state has changed; assets can be in one of these states: Running, Stopped, Test, Fault, No Config, Unknown

## View alert details

## View alert distribution

## Acknowledge alerts

You can acknowledge an alert for a specific asset. The Alerts page will indicate the alert is acknowledged in the Acknowledged column. Once an alert is acknowledged, future alerts of this type for this asset will not be shown. This can help to declutter the display.

To acknowledge an alert:

1. On the Alerts page, select the alert.
2. Click  opposite the alert
3. Enter an explanation why the alert is being acknowledged. This text will be saved with the alert, and visible to others (for example, in reports).

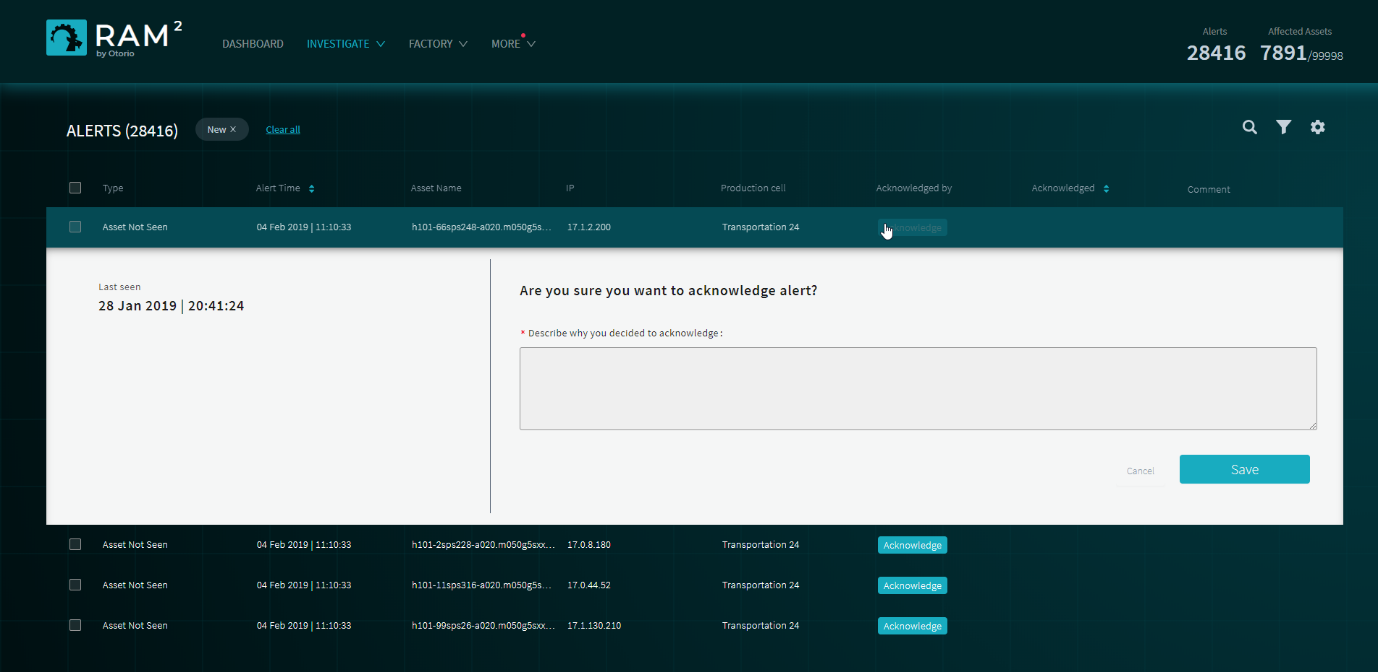


Figure Acknowledge an alert

1. Click Save.

To acknowledge a number of alerts:

1. On the Alerts page, select the alerts to acknowledge
2. Click  at the top of the page.
3. Enter an explanation why the alerts are being acknowledged.
4. Click Save.

Acknowledged alerts will show the name of the user who acknowledged them, on the Alerts page.

## Disable vulnerabilities (manage CVE policy)

You can manage the list of vulnerabilities that the RAM2 maintains, and select which ones will generate alerts, and which will be ignores. This applies to all assets.

When you disable a vulnerability, all alerts issued for that vulnerability (that appear in the Alerts page) are acknowledged.

To disable a vulnerability:

1. In the Alerts page, click .
2. In the Vulnerability alerts management panel, disable alerts for which you do not want to receive alerts.

You can enable a disabled vulnerability in the same way. Once a vulnerability is enabled, alerts for it will be issued.

## Examples

### View alerts by Asset, Cell or Shop

### View by Vulnerability (CVE)

### View details (KPI)

### Acknowledge an alert

### Investigate alerts

### Disable a vulnerability

# Users

## User types

## Add users

# Configuration

You can configure the RAM2 server settings in the System Settings page. Select this from the top-level More menu.

## Network config

To configure the RAM network settings:

1. Select System Settings from the top-level More menu
2. Select the Network Configuration tab
3. Set these values:
4. IP - an IPv4 value, in the form 0.0.0.0
5. Subnet – the subnet mast, in the form 255.255.255.255
6. Gateway – the IP address of the gateway
7. Port – the port

## Time

To configure the RAM2 time setting:

1. In the System Settings page, select the Time Setting tab
2. Enter the system time (local time).

## Deployment mode

Turn on the deployment mode switch when RAM2 is started up. When this switch is on, RAM2 will ignore all alerts from assets as they are being discovered (in particular, alerts indicating ‘New Asset Discovered’). Once all the assets have been discovered and scanned, turn off the switch, and RAM2 will accept new alerts from assets.

## Start & Shutdown

### Startup RAM2

### Shutdown RAM2

### Export/Import settings

### Backup

### Factory Reset

# Troubleshooting