# 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.

In RAM2 you can perform the following tasks

* Manage the production floor in operational terms by creating a hierarchical structure of entities in the factory, with shops, cells & assets
* Collect information about physical factory assets & assign them to shops and cells in the factory
* Regularly collect updated and critical changed information about assets
* Perform intelligent risk prioritization to better handle factory threats: calculate the Risk Level for each asset, cell, and shop, based on the vulnerabilities discovered in the assets, and the impact levels
* Automatically generate alerts when abnormal events and vulnerabilities are found in assets
* Easily view KPIs and detailed information about the factory network and its components

## Main Features

### Factory Management

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

RAM2 manages the factory by dividing it hierarchically into the following entities:

**Factory** – a single business or industrial unit, but can be distributed over several geographical locations

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

**Cell** – a production unit in a shop

**Asset** – a single machine or device in a cell

In RAM2, the first step is to define the shops and cells in the factory and after this assign the asset into cells.

RAM2 receives information about assets in the factory from different Asset Collectors. Using this, it builds an asset inventory. This inventory is updated regularly, based on updated information from the Asset Collectors. The information includes details about the device type, location, impact level, and the firmware/software installed on it.

Newly discovered assets are not automatically assigned to cells. RAM2 notifies you when new assets are found, and you assign them to cells.

### Risk Assessment

RAM2 calculates a Risk Level for each cell, based on the information it receives about the assets from Asset Collectors, and using an internal threat intel database of known vulnerabilities. It then calculates the Risk Level for cells and shops, ~~based on the Risk Levels of the component assets~~.

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

### Alerts

RAM2 generates automatically alerts for security issues discovered in assets ~~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 vulnerabilities or asset change.

~~You can acknowledge an alert for a specific asset. This removes the alert from the list.~~Once you acknowledge an alert, it reduces the risk, and the alert removed from the filtered view. you can filter the view for reviewing the whole list with both statuses (new and acknowledged)

### Manage 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, alerts will not be generated for them.  
RAM2 assesses the risk level for an asset using a vulnerabilities database compiled by the Otorio threat intelligence research team.

You can disable (and re-enable) specific vulnerabilities, in which case, alerts will not be generated for them.

By default, all the vulnerabilities are active.

## Key Indicators

The top of the Dashboard shows key indicators for the factory.



Figure 5 Key Factory Indicators

These are:

* The number of shops
* The number of cells
* The total number of assets

# Get Started

## Login to RAM2

Connect to RAM2 from a browser, with the URL for your RAM2 server.

Enter your username and password.

Once you are logged in, the Dashhoard view will open.

### First steps

The first time you login into RAM2, there are no shops or cells. If assets have been discovered, there will be a list of Unassigned Assets.

Your first steps at this point will be to create shops, and cells, and, after this, to assign assets to cells. These steps are described in the next section.

## The Dashboard

The Dashboard view shows summary information for the shops in your factory, as well as key summary information for the factory as whole.

The left side shows the shops in the factory. Select one of the shops, to see information for it.

* The overall Risk Level for the shop
* The number of production cells in the shop
* The number of assets in the shop (with distribution by cells and types)
* The number of alerts that have been triggered for the shop (with distribution by the cells and types)

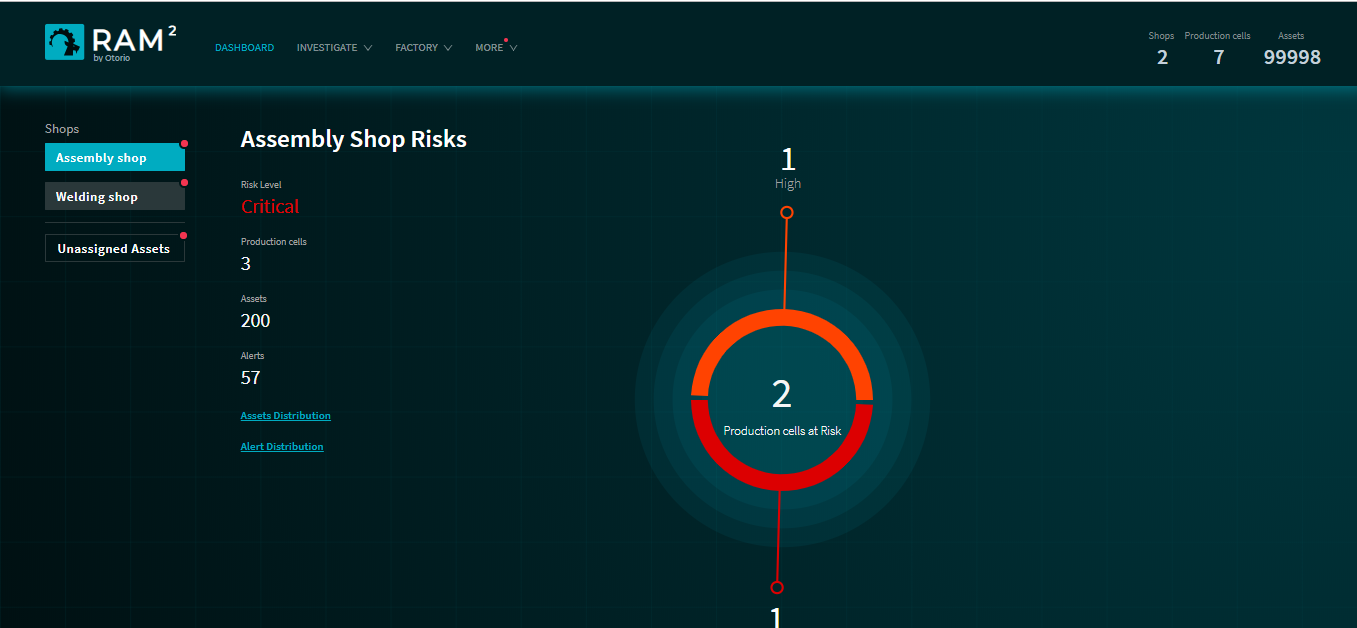


Figure 1 Dashboard view

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



Figure 2 Cell Risk Level pie-chart distribution

There are four different Risk Levels: Critical, High, Medium, and Low.

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 in the pie-chart, to show more detail. This is shown on the right. In the example below the cell at High Risk has 7 assets affected by risk, with 10 alerts generated.

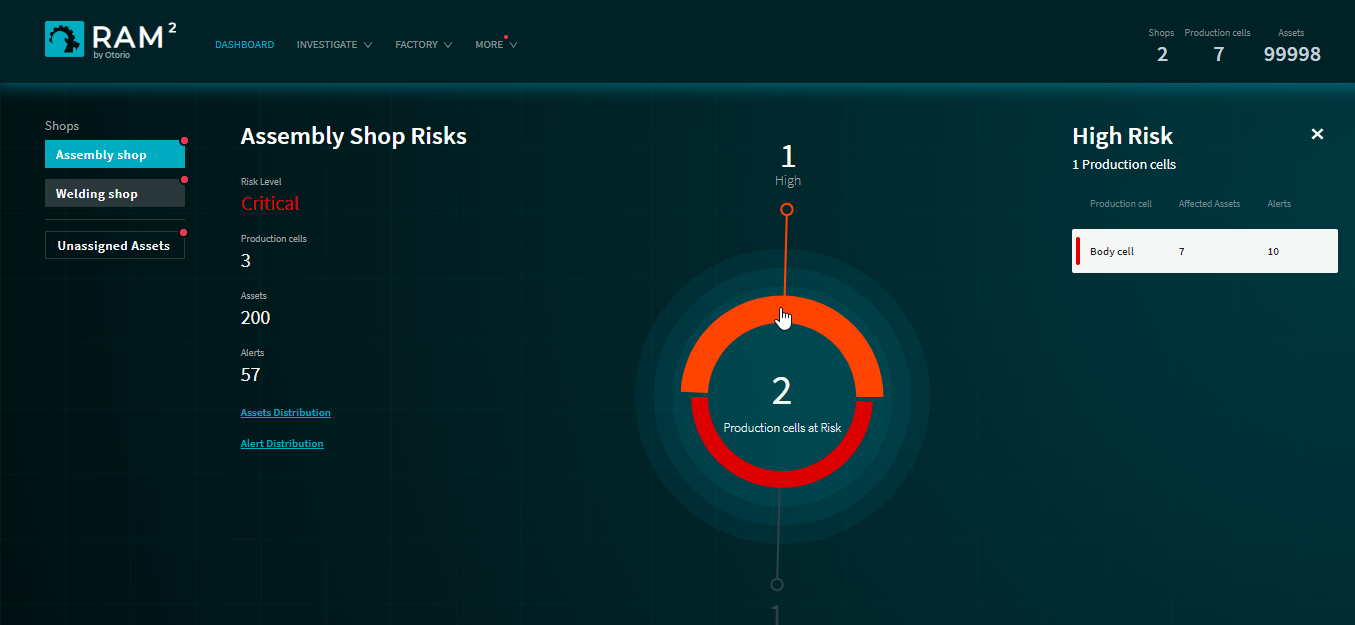


Figure 3 At-risk production cell details

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

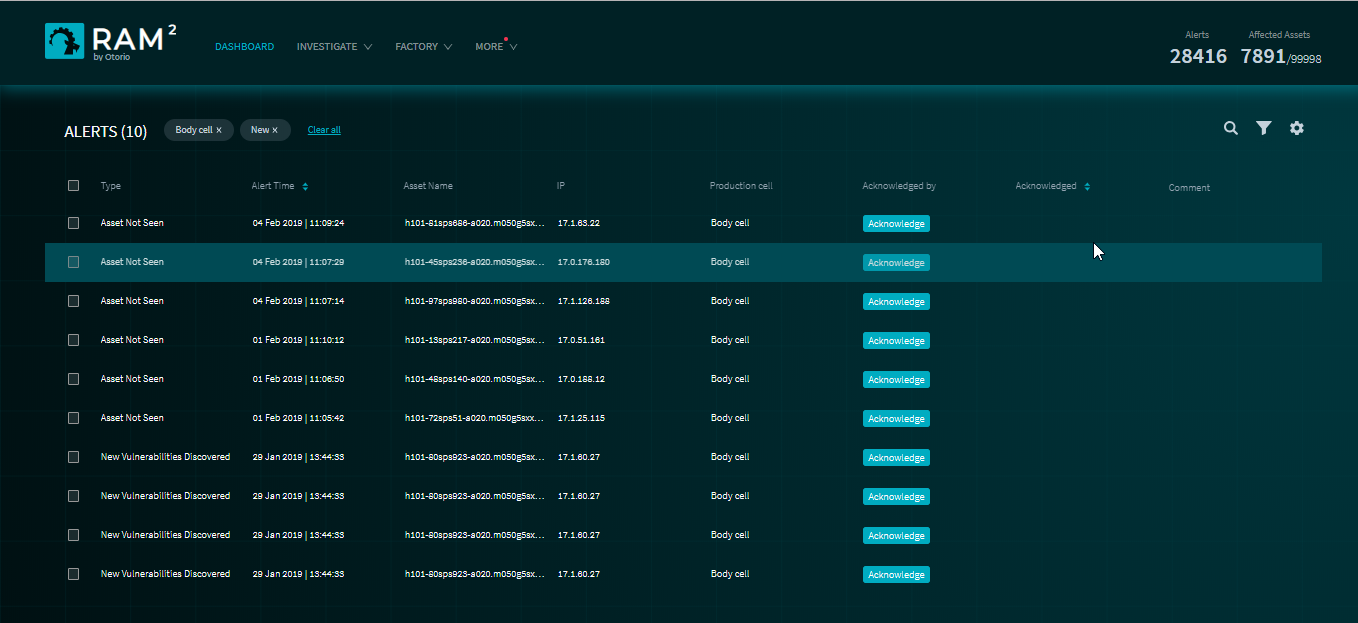


Figure 4 Alerts for Production Cell

A shop marked with a red dot indicates there are alerts for one or more assets in the shop.



### Asset Distribution

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

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

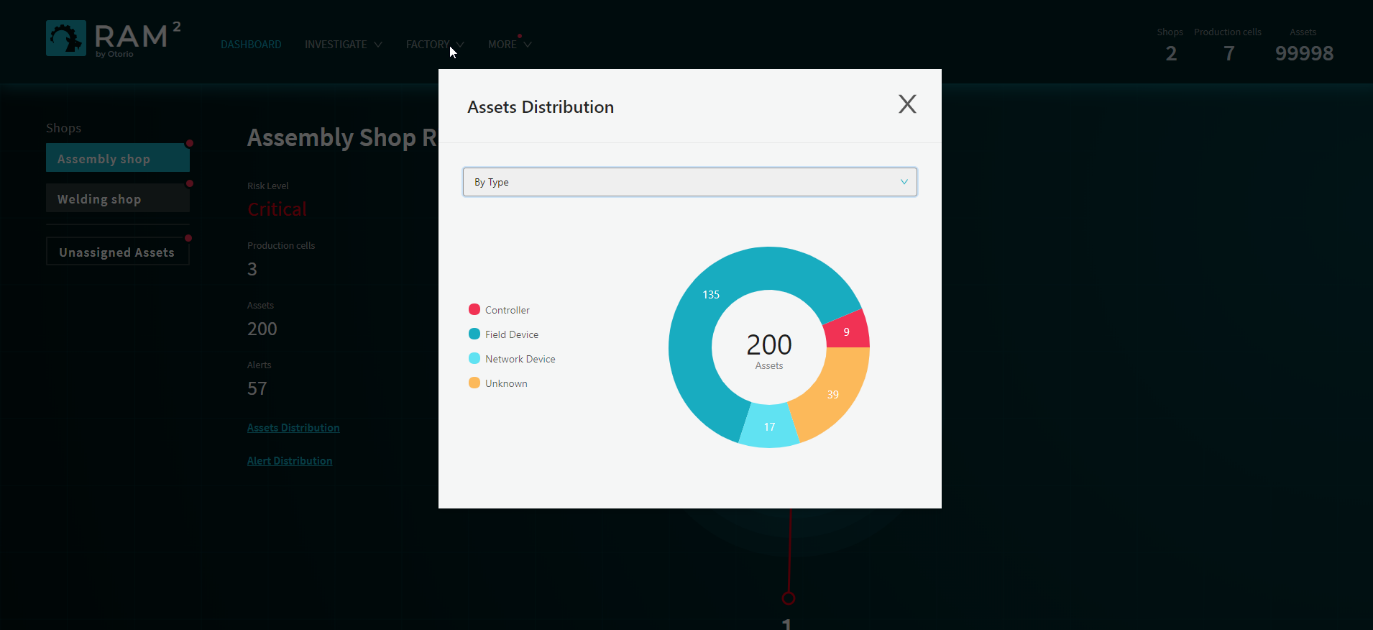


Figure 5 Asset Distribution by Asset Type

### Alert Distribution

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

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

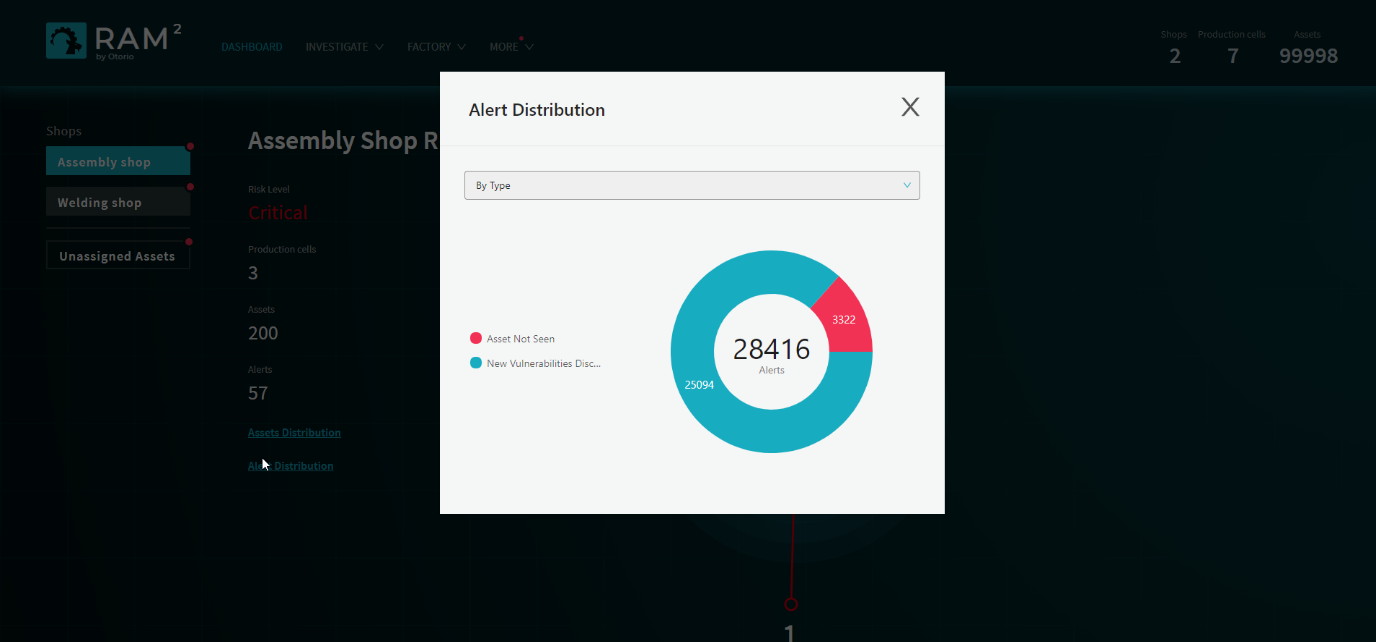


Figure 6 Alert Distribution by Alert Type

### Unassigned Assets

Click Unassigned Assets in the list of shops, in the Dashboard on the left, to see a list of unassigned assets (assets that are not assigned to any production cell) In this view, there is no overall Risk Level.

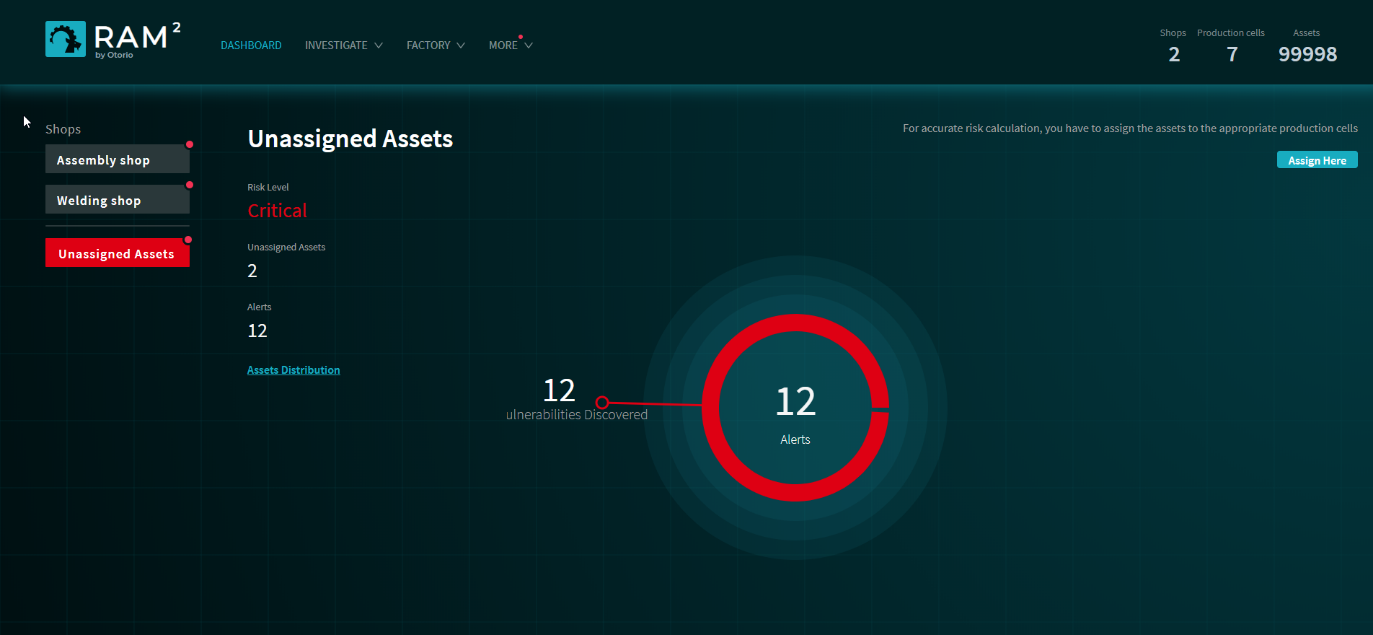


Figure 7 Unassigned Assets

Click , on the right, to open the list of Unassigned Assets. From there, you can view details for the assets, and assign them to production cells.

### Navigation from the Dashboard

At the top of every page, including the Dashboard, is the top-level menu-bar.



Use these menus to navigate to different pages in RAM2, to perform the actions discussed in later sections.

Dashboard – navigate to the Dashboard

Investigate –navigate to the Alerts page

Factory –navigate to the Shops, Production Cells, and Assets pages

More – navigate to the Settings, Language, and Troubleshooting pages

You can also click  to return to the Dashboard from any other page.

# Factory Management

RAM2 manages the factory by dividing it hierarchically into two operational layers, shops, and cells.

RAM2 builds an asset inventory automatically, based on information received from Asset Collectors in the network.

Once shops and cells are defined, you can assign cells to shops, and then assets to cells.

## Shops

Shops are the highest-level entity in a factory. Shops contain production cells.

### Shop view

Select Shops from the Factory menu to see the shops you have defined for the factory. Each shop in the view is shown as a ‘card’.

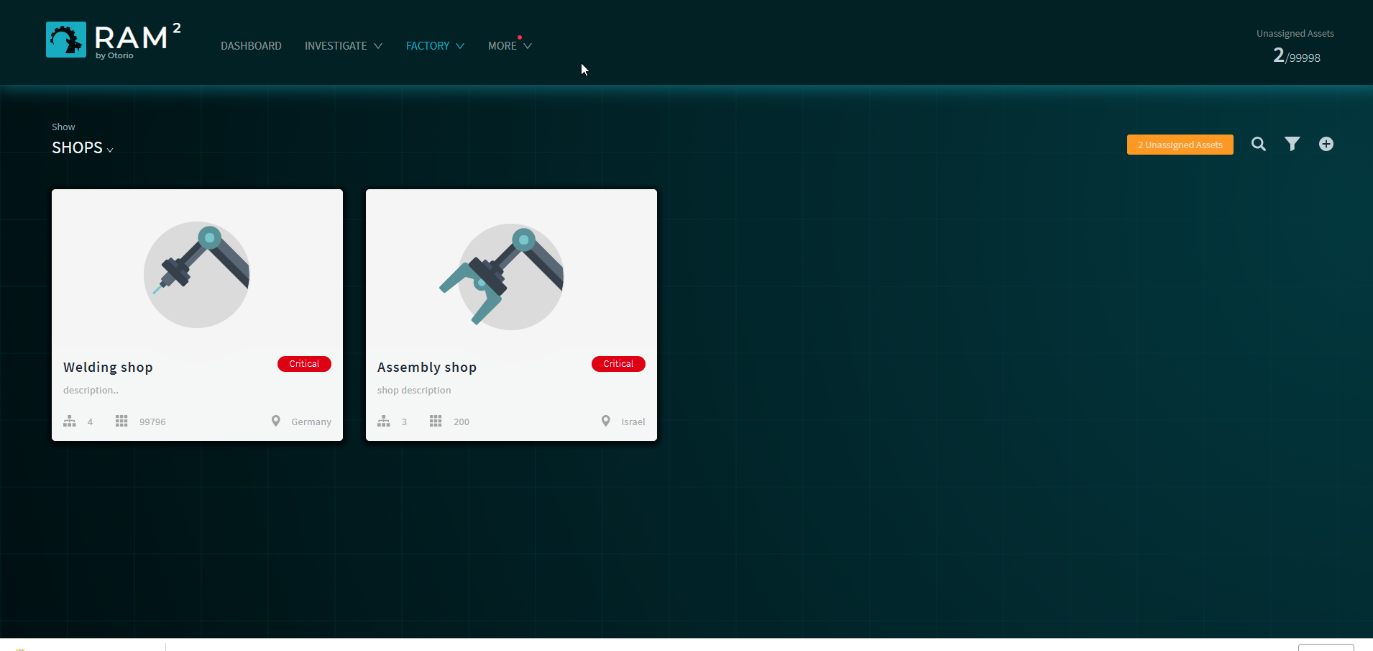


Figure 8 Shops

Each card in this view shows the following information for the shop:

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

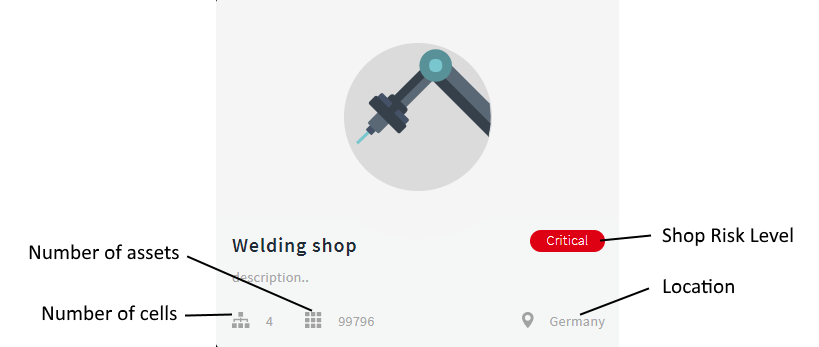


Figure 10 Shop card

### Create a shop

To add a new shop:

1. Select Shops from the top-level Factory menu.
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 card

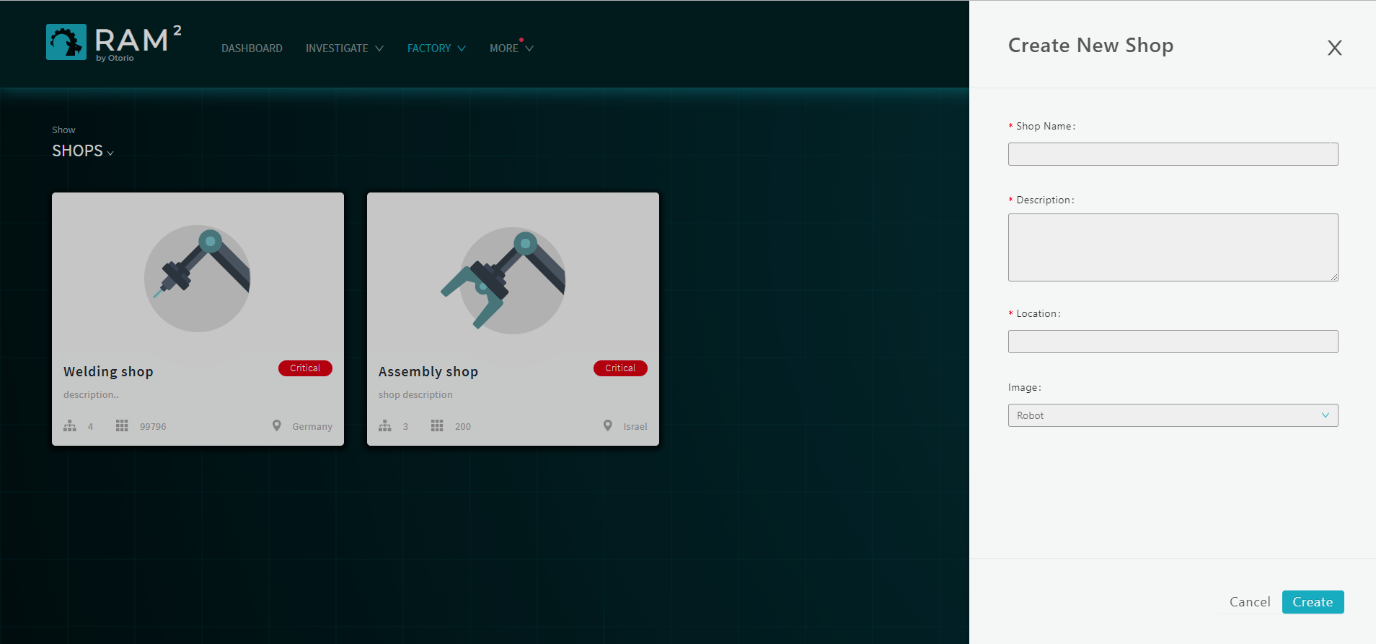


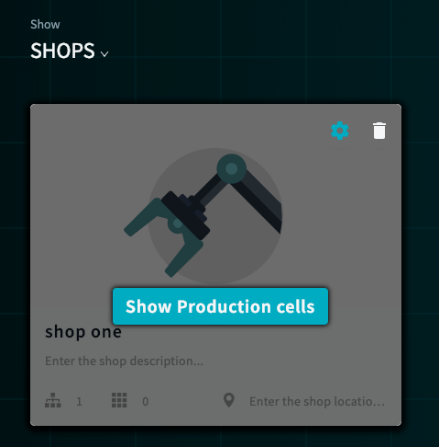
Figure 13 Create new shop

1. Click Create.

A shop card for new shop will appear on the page.

To modify details for a shop:

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



1. Click .

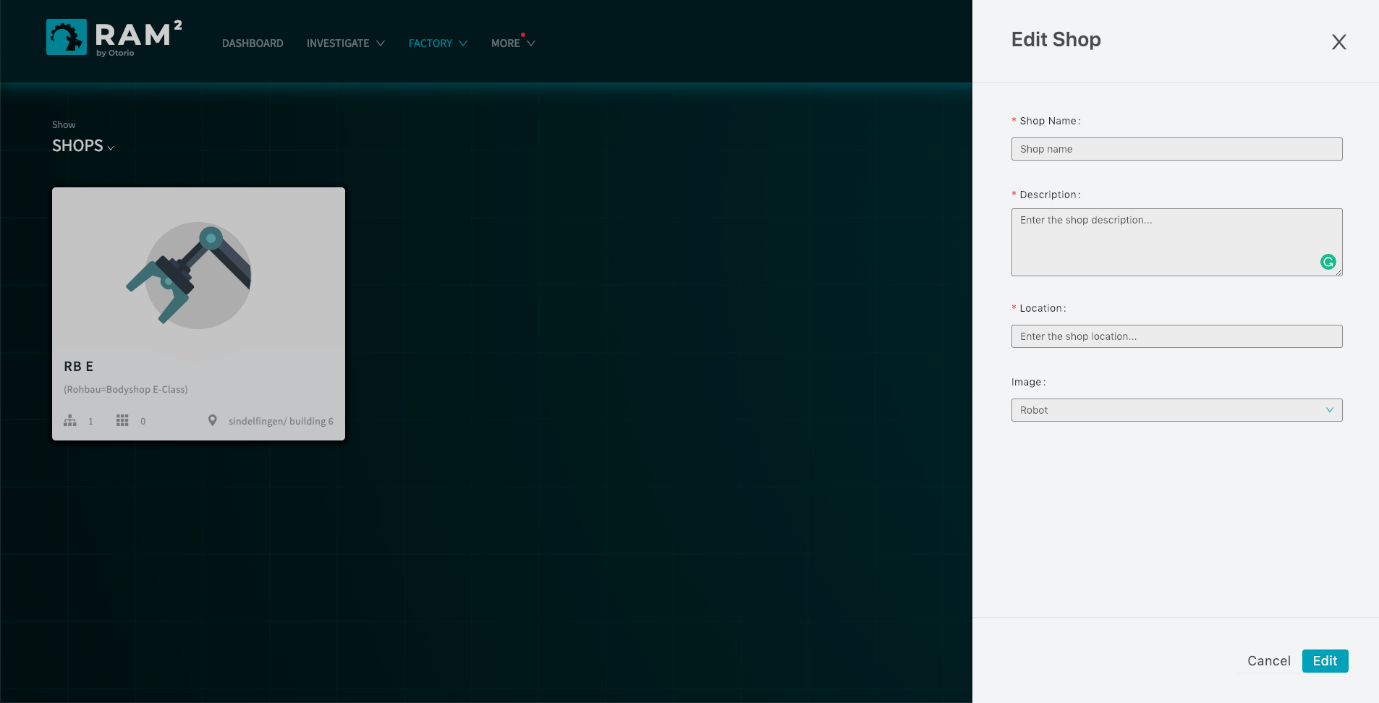


Figure 14 Edit shop

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

### Filter or search for shops

You can filter or search for specific shops in the Shop view.

Click  to select the filter for the view. You can filter according to the name or location of the shop.

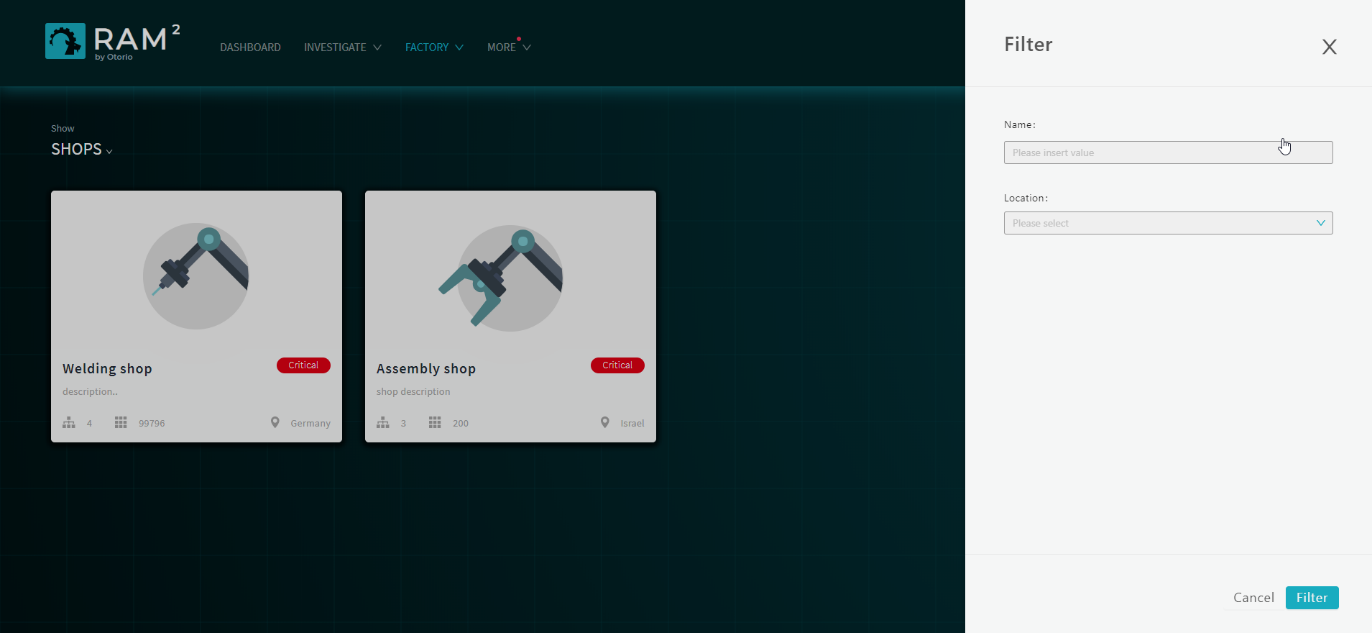
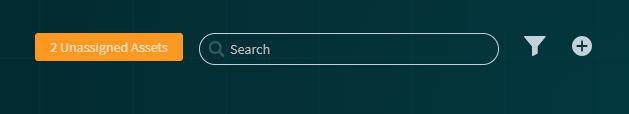


Figure 12 – Filter

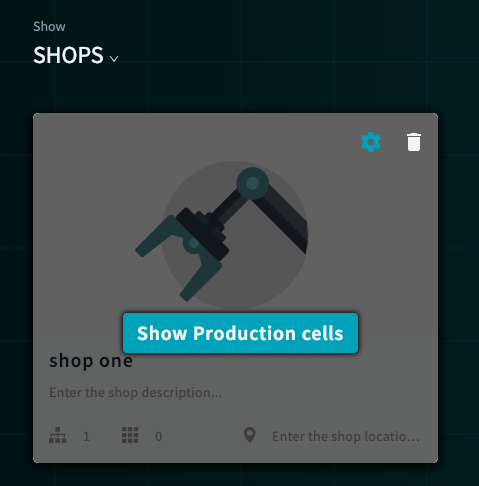
Click  to search for a specific shop by name.



### Delete a shop

### Navigation from the Shop view

Hover over a shop card, and then click Show Production cells.



This will open a Cell view, filtered to show the cells for the shop.

Click  in the upper right, to show a list of Unassigned Assets From this list, you can manage your unassigned assets, and assign them to the cells.

## Cells

Production Cells are entities within shops. Cells contain assets. A cell can be assigned to a single shop, but can have any number of assets assigned to it.

### Cells view

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

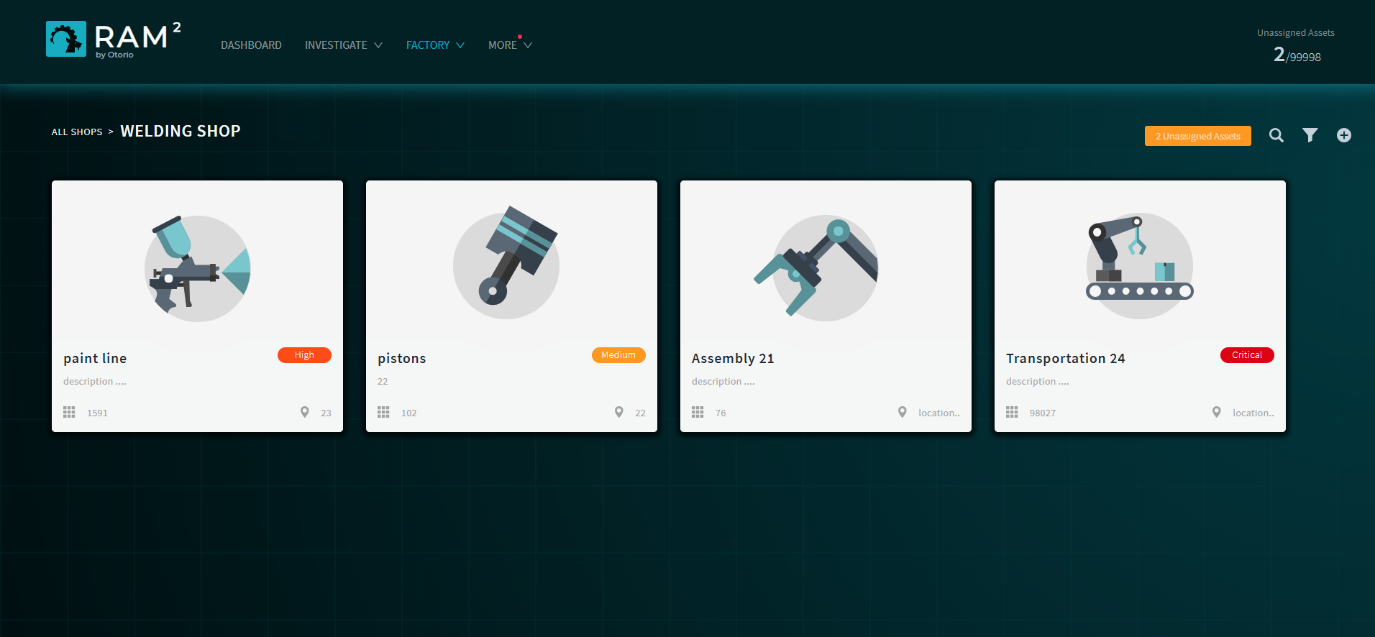


Figure 9 Shop cells

Cells are shown as ‘cards’. Each card shows this information:

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

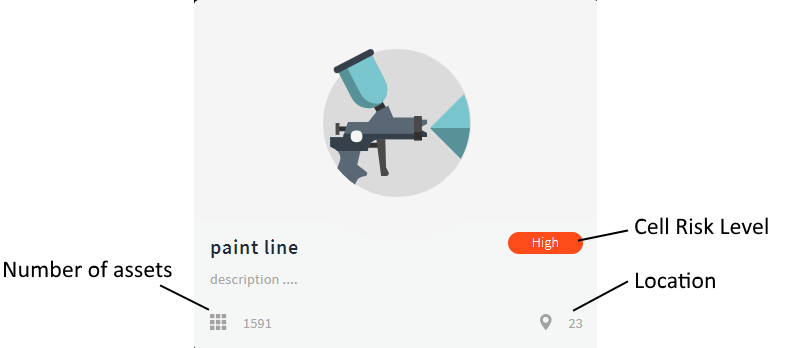


Figure 15 Cell card

### Create a cell

Add or modify cells in the Production Cells page. 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, is assigned to this shop.

To create a cell:

1. Select Production Cells from the top-level Factory menu. The cell cards for the factory are shown.
2. Click .in the upper right.
3. In the Create New Production cell panel, enter the following details for the cell:
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

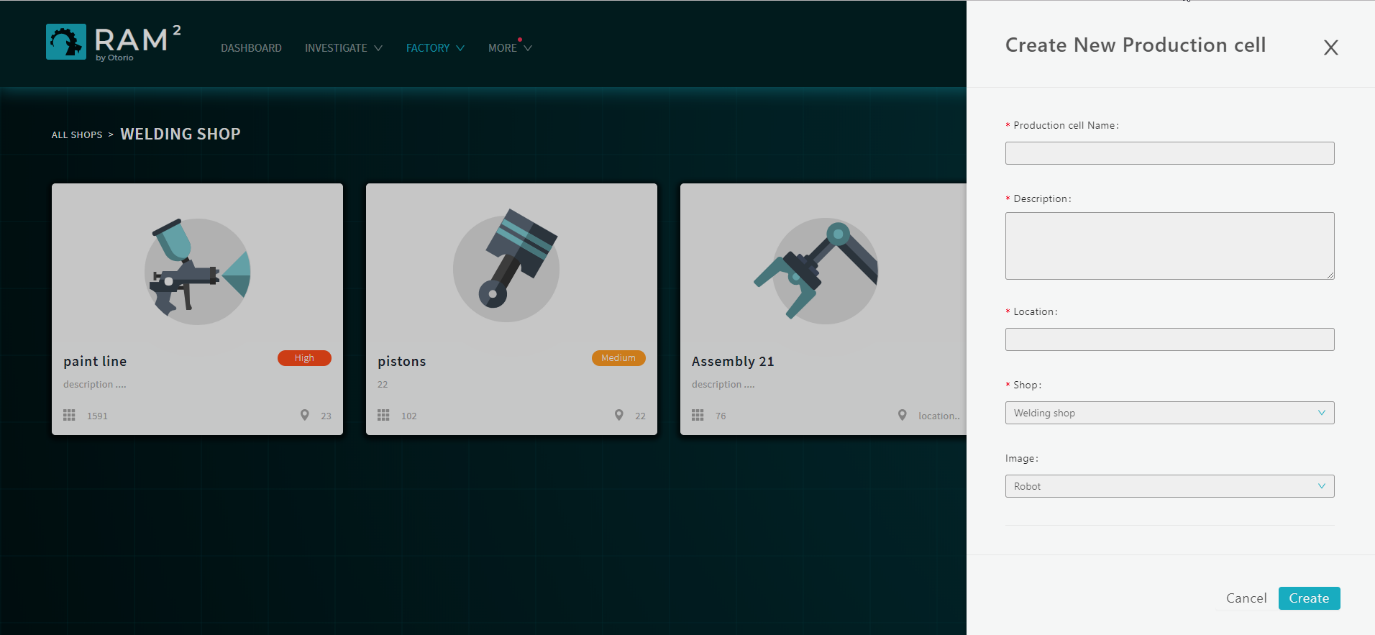


Figure 15 Create production cell

1. Scroll down, and enter values for the **Impact Level** of the cell. These indicate the impact the loss of the cell would have. For each of the parameters here, select the level from Insignificant, Minor, Moderate, Major, or Catastrophic.

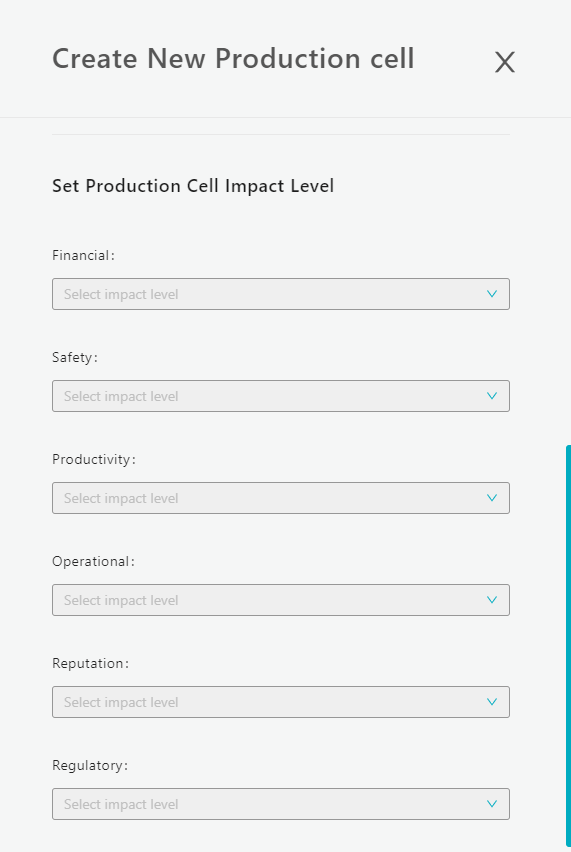


Figure 17 Cell impact level

1. Click Create.

A card for the cell will appear on the Production Cells page.

To create a cell in a specific shop:

1. In the Shops page, select the shop to which the cell will be added. Cards for the current cells for the 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. (optional) Image – upload an image for the cell
7. (optional) Select the Impact Levels for the cell
8. Click Create.

A card for the new cell will appear in the page for the shop.

### Edit cells

You can modify details for a cell, including the shop assignment.

To edit a cell:

1. Select Production Cells from the top-level Factory menu.
2. Hover over the cell to be modified and click .
3. In the Edit Production Cell panel, change details as necessary.
4. Click Edit to save the changes.

### Filter or search for cells

You can filter or search for specific cells in the Cell view.

Click  in the upper right to filter for cells. You can filter according to the name or location of the cell.

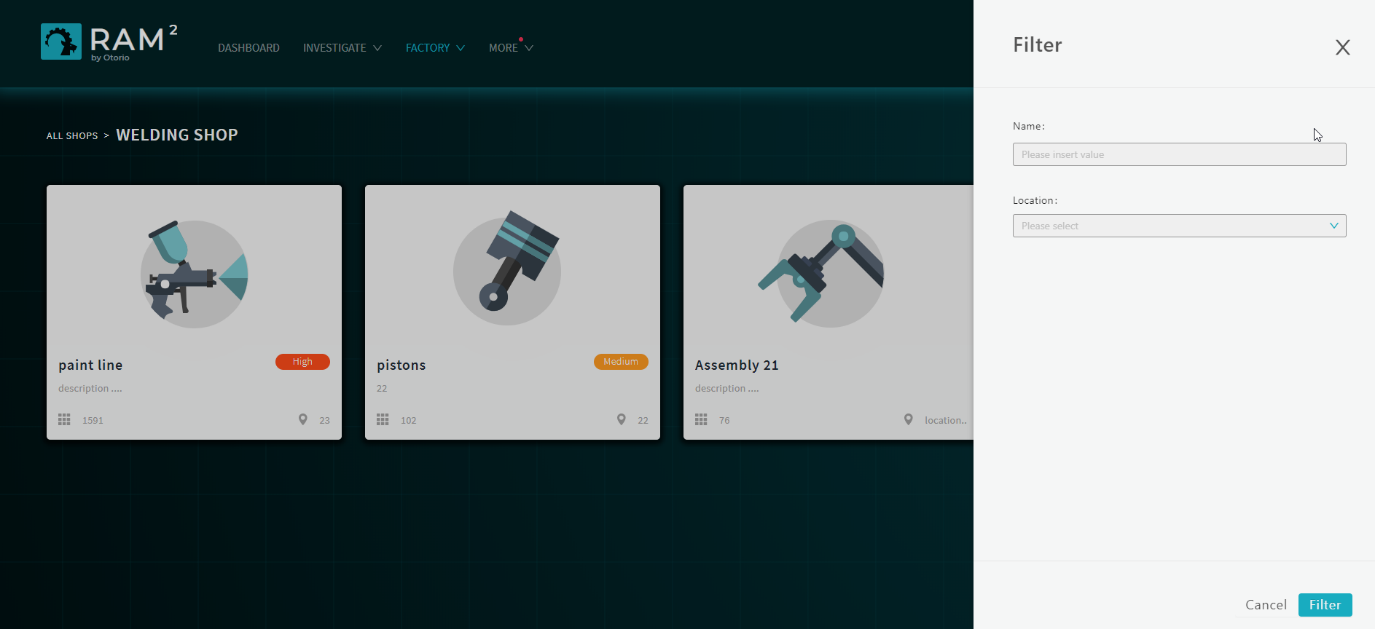
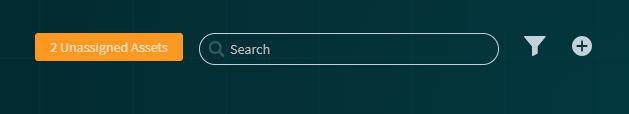


Figure 18 Filter cells

.

Click  to search for a specific cell by name.



### Delete a cell

### Navigation from the Cell view

You can navigate from a Cell view to the list of assets for the cell, or to the list of Unassigned Assets.

Hover over a cell card, and then click  to show a list of the assets for the Cell.

Click  in the upper right, to show a list of Unassigned Assets.

## Assets

Assets are individual shop-floor devices. They are discovered automatically by Asset Collectors in the ~~factory and reported to the RAM~~~~2~~. A production floor machine could represent several assets.

You can assign assets to production cells once they are discovered, or move them to different cells.

Once assets are included in RAM2, a Risk Level is calculated for them.

Once assets are assigned to a cell, their issues contribute to the overall Risk Level of the assigned cell and shop.

### Assets view

Hover over a cell card, and then click  to show the assets in it. Alternatively, select Assets from the top-level Factory menu, to show all the assets in the factory, or click  from the Cell or Shop views to show Unassigned Assets.

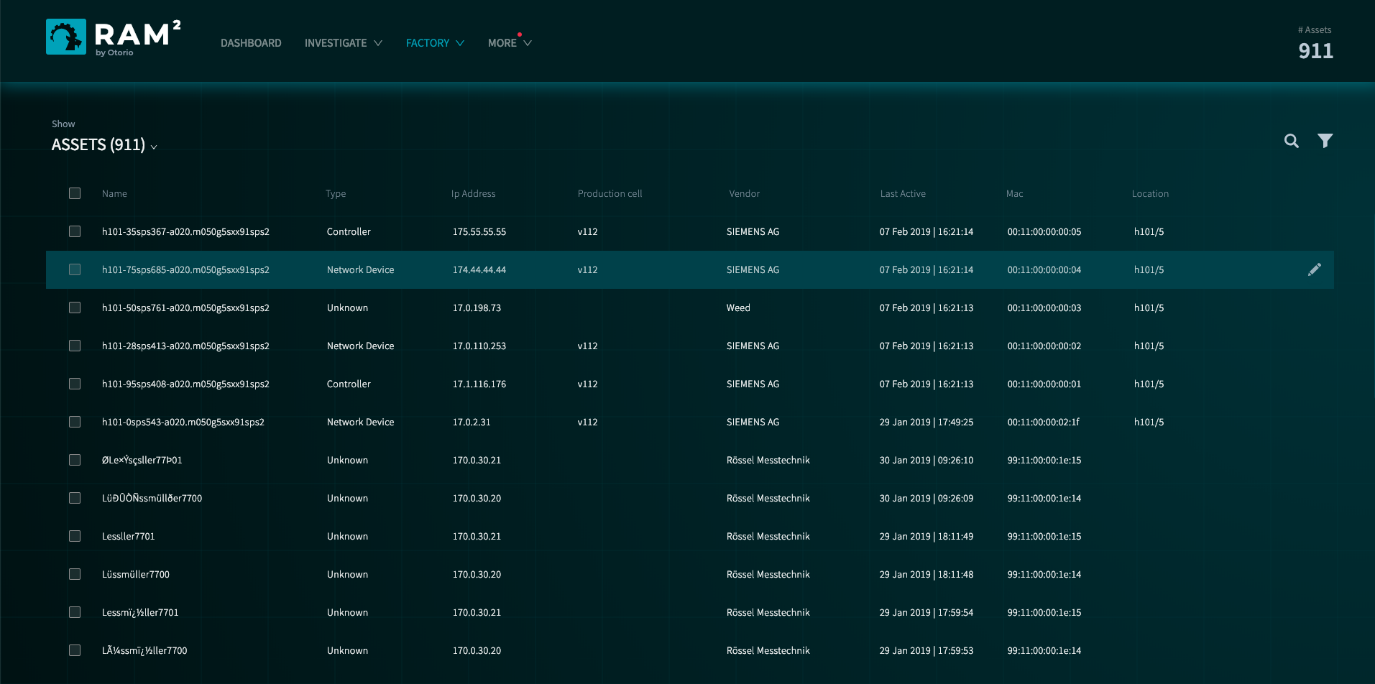


Figure 10 Factory assets

The list 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

Click on an asset in the list to show more detail. This shows the following:

* General asset details – the shop, cell, location, and current state
* IP and Firmware details
* Impact Level

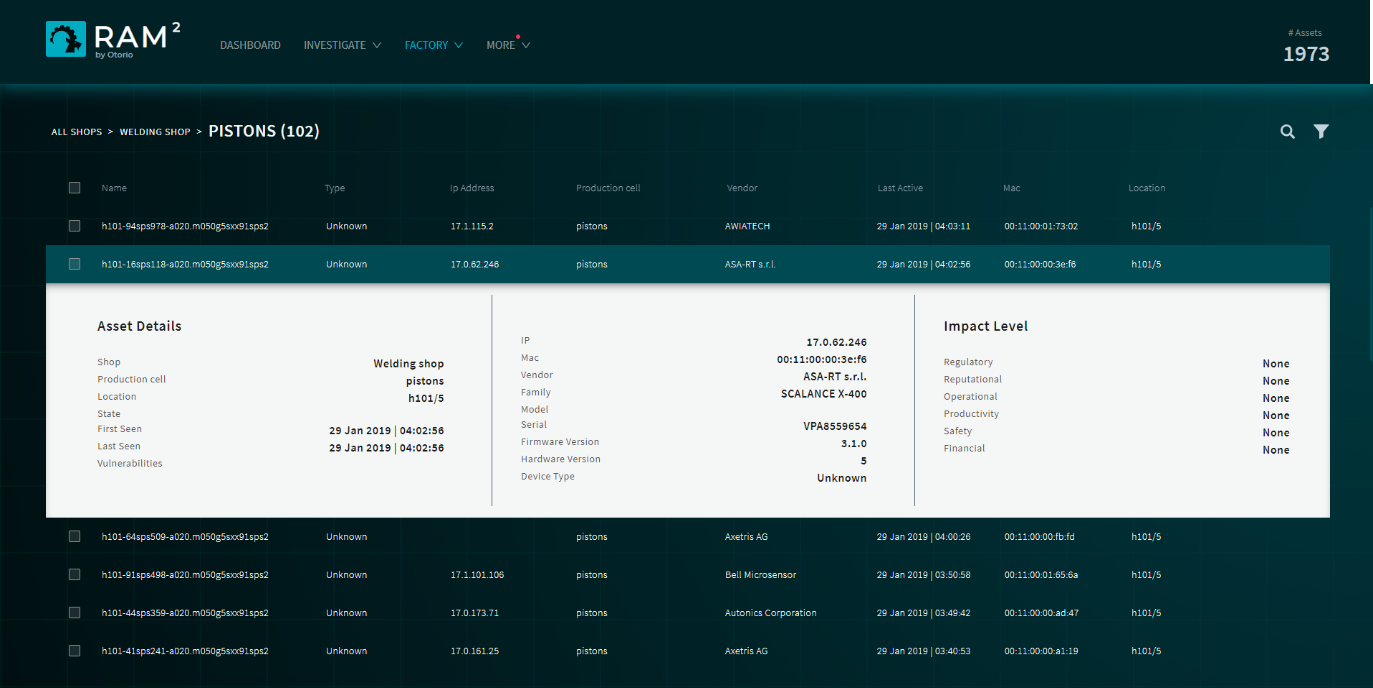


Figure 20 Asset detail

### Assign assets to cells

You can assign assets to cells from the Assets list view.

To assign a single asset to a cell:

1. Hover over the asset in the list.

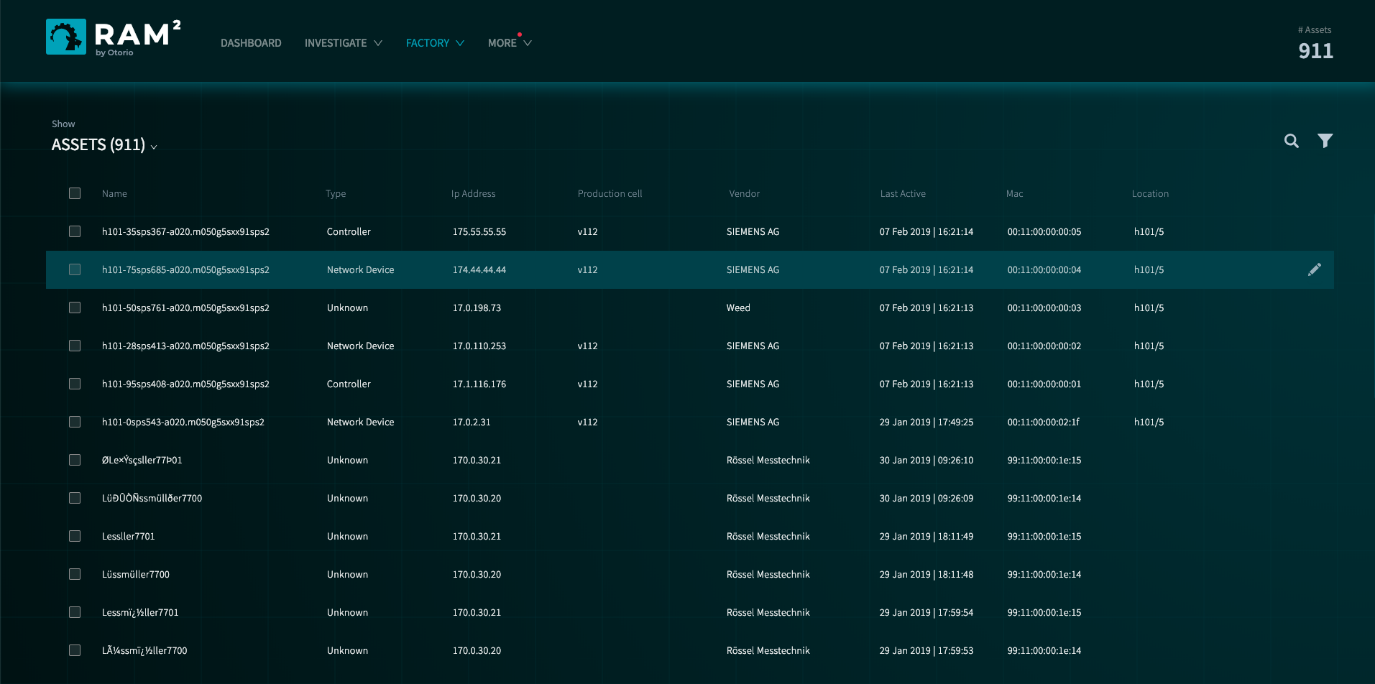


Figure 16 Select an asset to assign

1. Click  (on the right side).

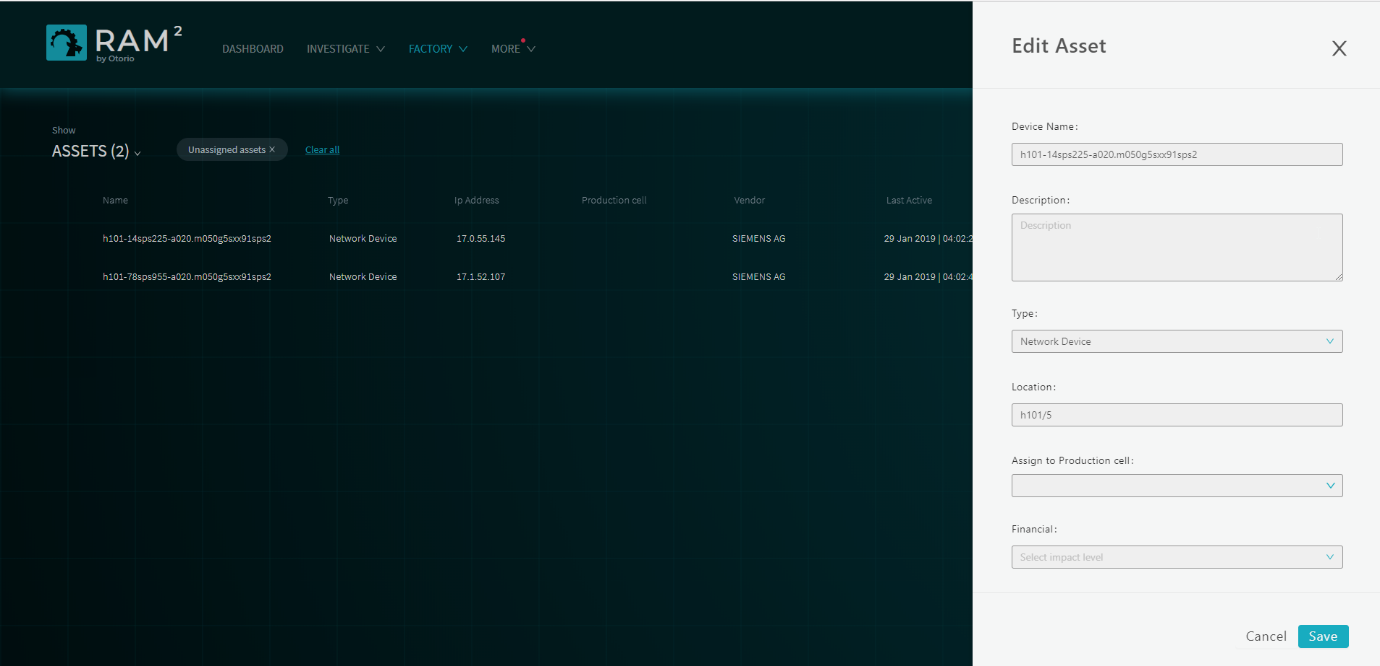


Figure 17 Assign an asset to a cell

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

### Bulk assign assets to cells

To asset a number of assets to a production cell:

1. Select the assets in the list, and then click  in the upper right.

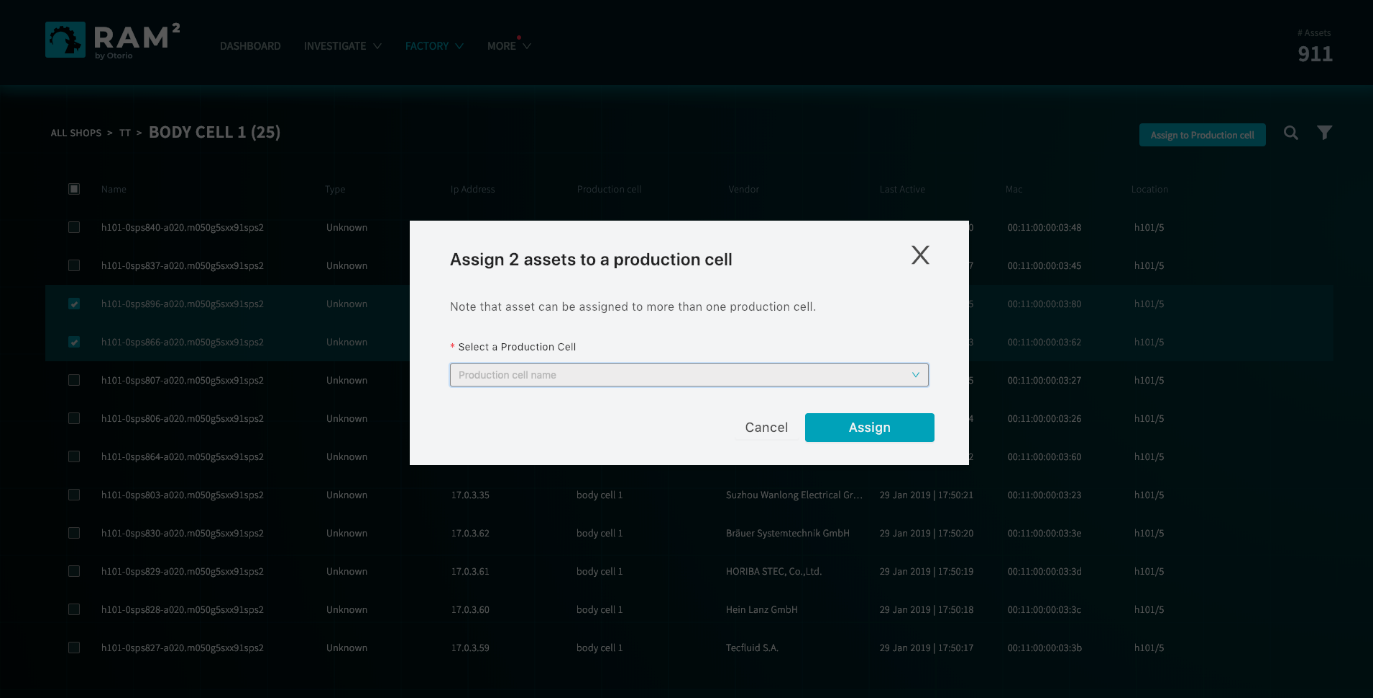


Figure 18 Assign multiple assets to a cell

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

### Filter or search for assets

You can filter or search for specific assets in the Asset list view.

Click  in the upper right to filter for assets. You can filter according to the name, location, vendor, cell, and IP address of the asset.

Click  to search for a specific asset by name. The search is progressive: this list of matching assets is updated as you enter more text for the name.

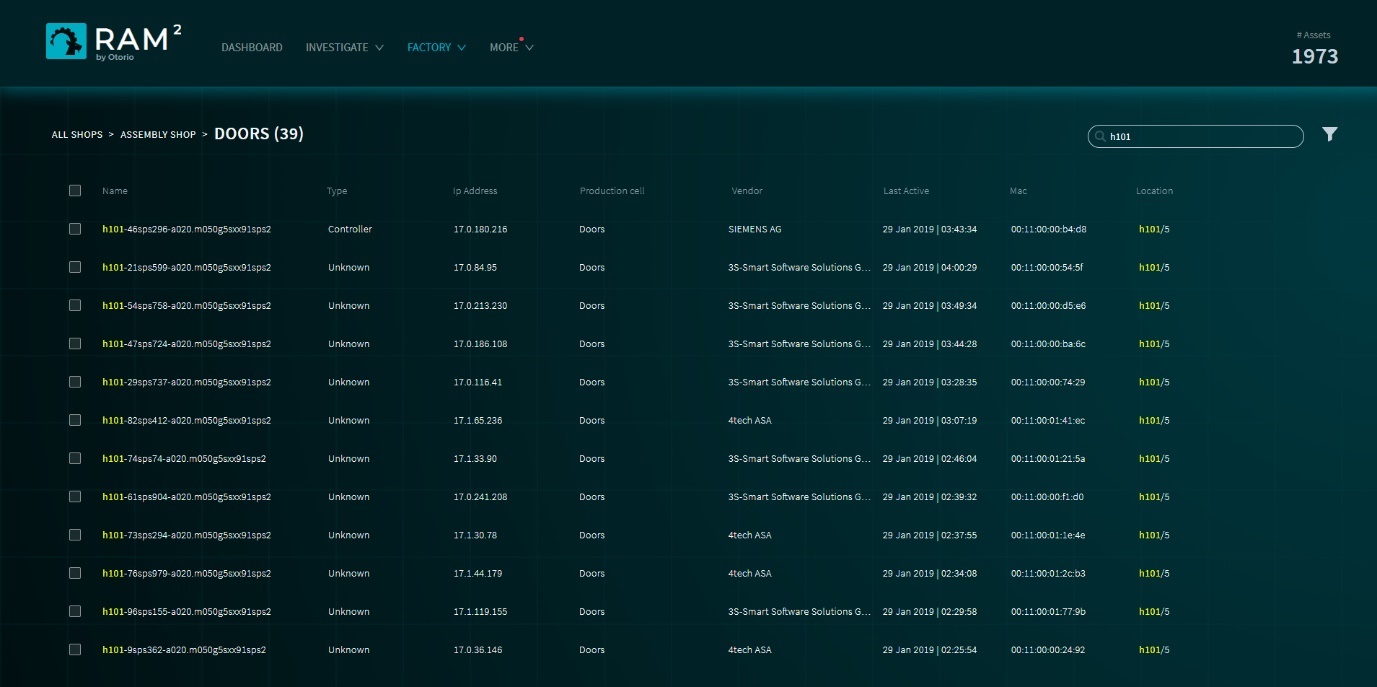


Figure 24 Asset search

# Investigation - 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 generating alerts.

## Alerts view

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

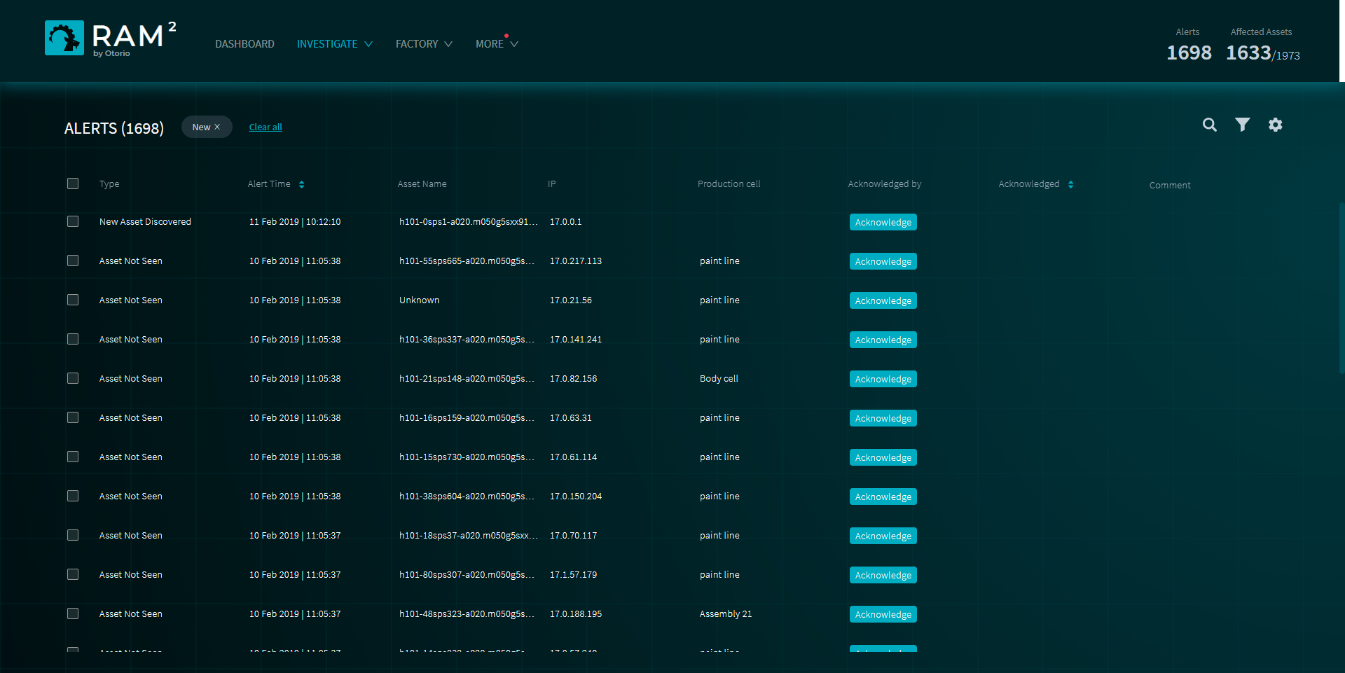
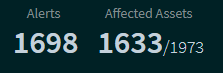


Figure 11 Alerts view

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 button to acknowledge the alert
* **Acknowledged** – indicates the alert was acknowledged (blank, if not)

The top right of the view shows the total number of unacknowledged alerts, and the number of factory assets affected by 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 certainty.
* **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
* **Firmware version changed** – the firmware version on an asset has changed; it does mean that there is a security issue certainty.
* **IP address changed** – the IP address for an asset has been changed
* **State changed** – an asset state has changed. Assets can be in one of these states: Running, Stopped, Test, Fault, No Config, Unknown

## Acknowledge alerts

You can acknowledge an alert. The Alerts page will indicate the alert is acknowledged in the Acknowledged column.

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).

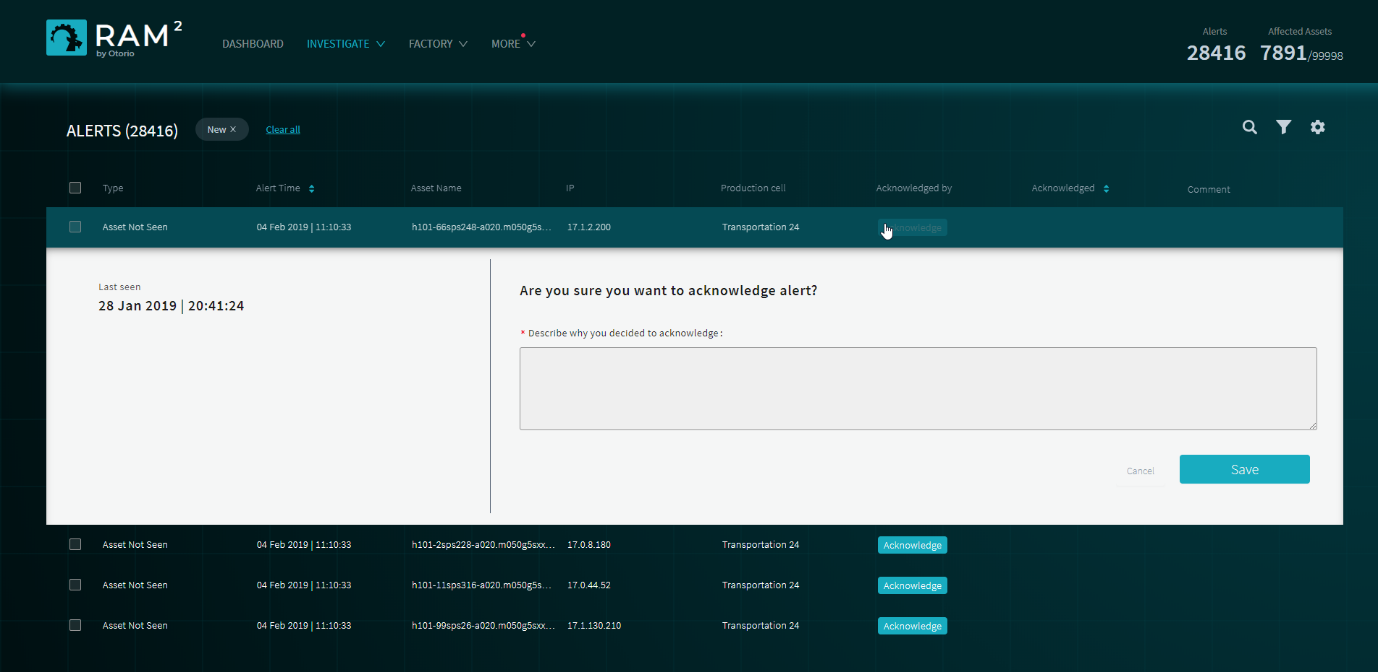


Figure 19 Acknowledge an alert

1. Click Save.

To acknowledge a number of alerts:

1. On the Alerts page, select the alerts to acknowledge

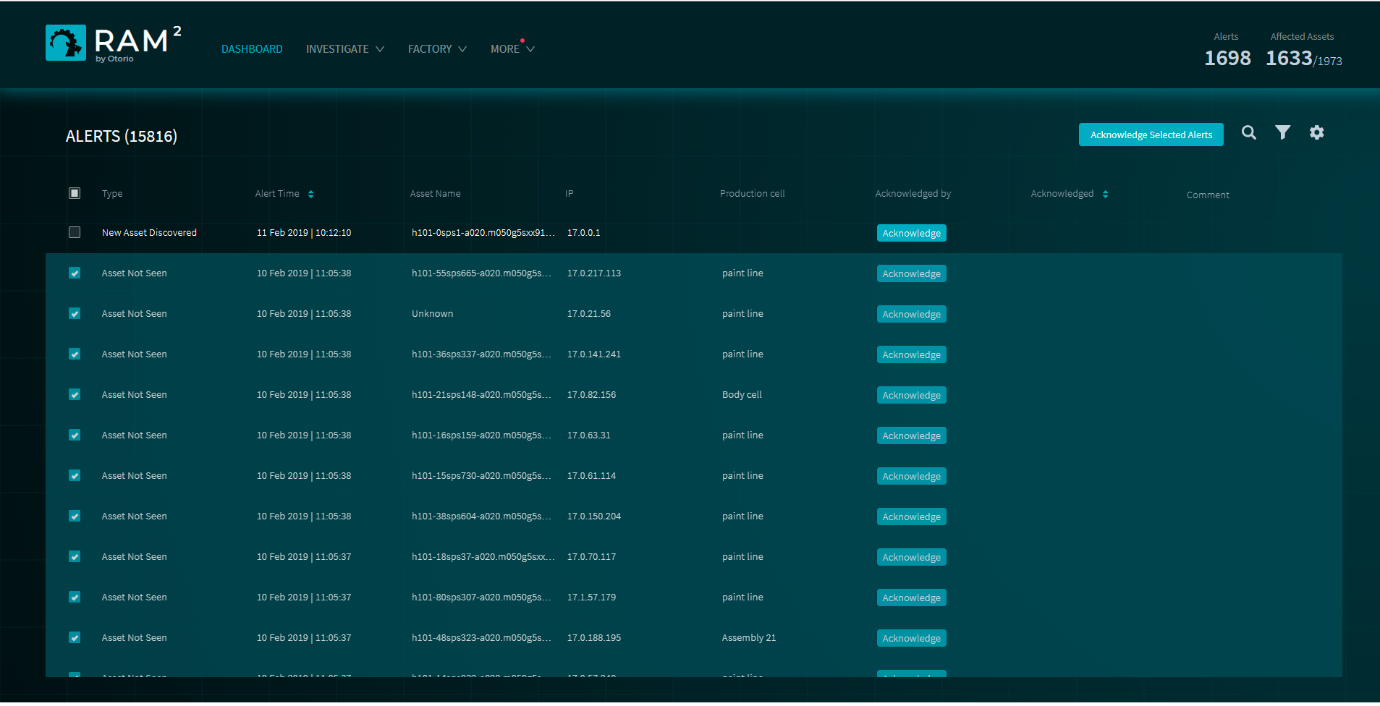


Figure 27 Alert bulk select

1. Click  at the top of the page.
2. Enter an explanation why the alerts are being acknowledged.
3. Click Acknowledge all.

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

## Filter or search alerts

Click  in the upper right to filter alerts. You can filter according to the alert type, status, time, cell, vulnerability type, or severity. You can also filter for new or acknowledged alerts.

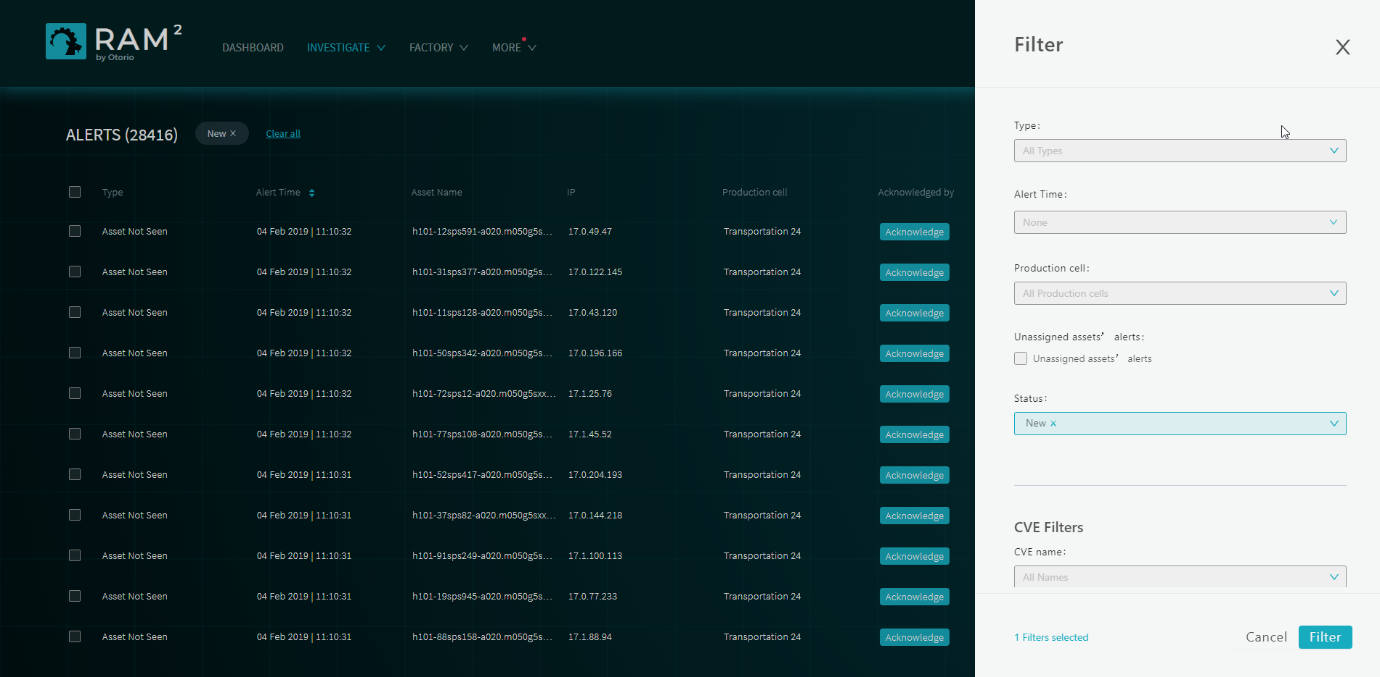


Figure 28 Filter alerts

Click  to search for alerts.

## View alert distribution

Click on the summary of alerts and affected assets in the upper right of the Alerts view to see a distribution of alerts according to type or production cell.

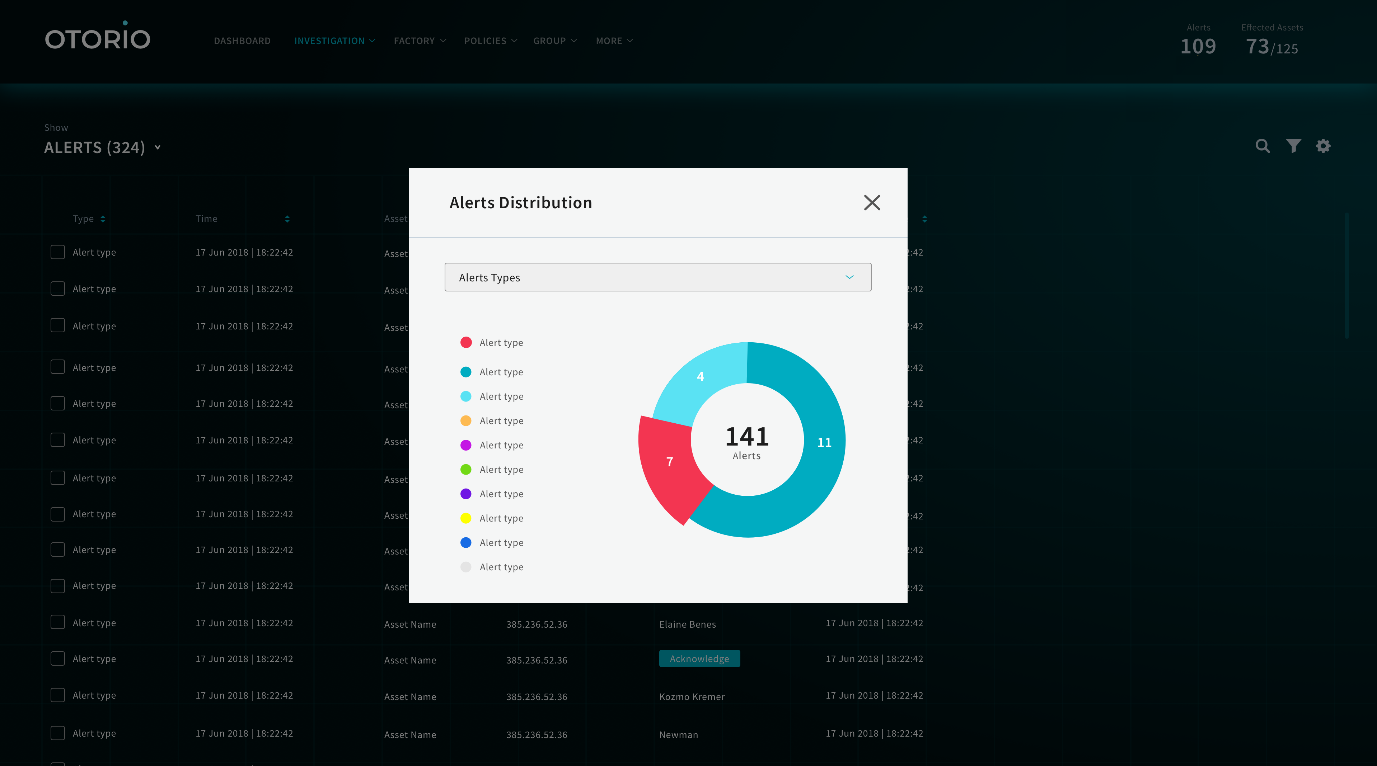


Figure 29 Alert distribution by type

## Disable vulnerabilities

You can disable (and re-enable) specific vulnerabilities, in which case, alerts will not be generated for them. In addition, when you disable a vulnerability, all alerts issued for that vulnerability (that appear in the Alerts page) are acknowledged

By default, all the vulnerabilities are active.

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.

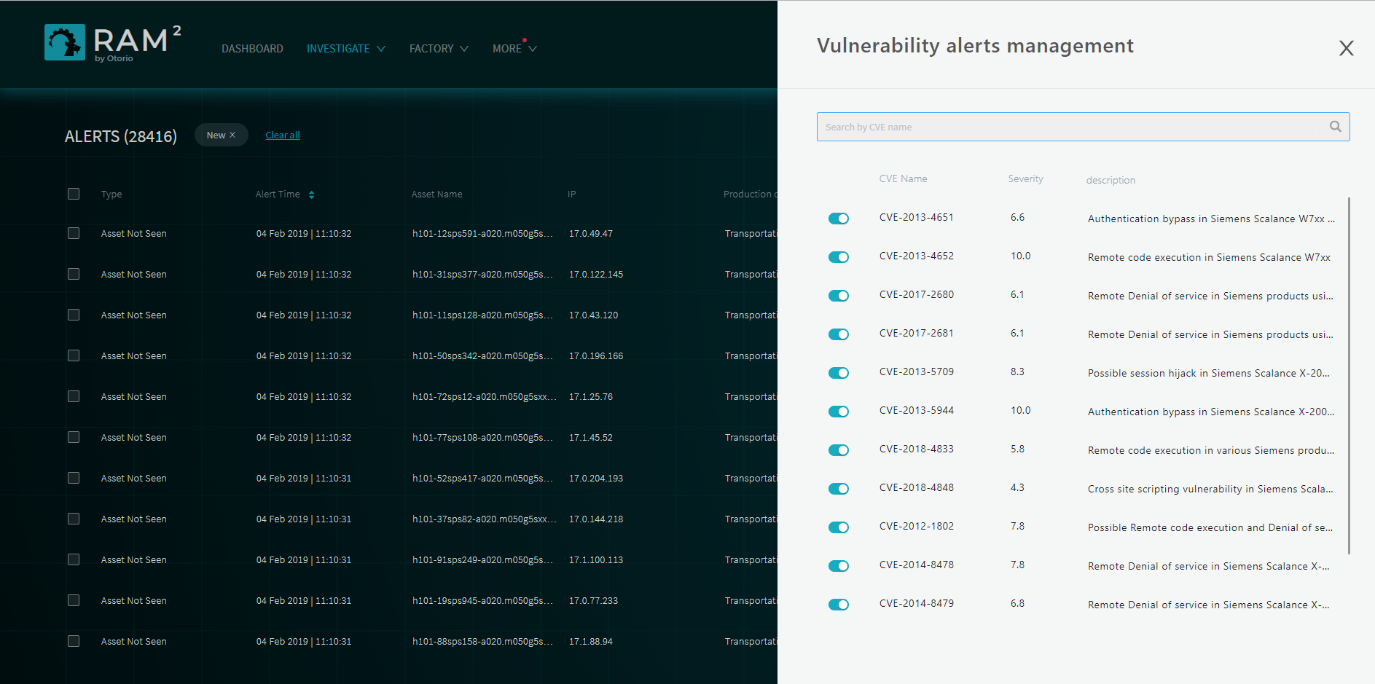


Figure 29 Vulnerabilities

You can re-enable a disabled vulnerability in the same way. Once a vulnerability is enabled, future alerts for it will be issued, and will appear in the Alerts page.

# Users

To use RAM2, you must login with a username and password.

Admin users of RAM2 can create users.

## User roles

RAM2 has different roles, that can be assigned to users. These are:

**Admin** – this user can access all pages in RAM2, including the configuration and user management pages (can changes settings, and add users). Admin users can add or modify shops and cells.

**Board** – this user can view any page, define cells and shops, and acknowledge alerts. This user cannot access the configuration pages, or add/modify users.

**Security** – same as Board

**Operations** – same as Board

## Add users

To add a user:

1. Select Configuration from the top-level More menu.
2. Select USER MANAGEMENT from the drop-down list in the upper left. A list of all RAM2 users is shown and, for each, the user role.

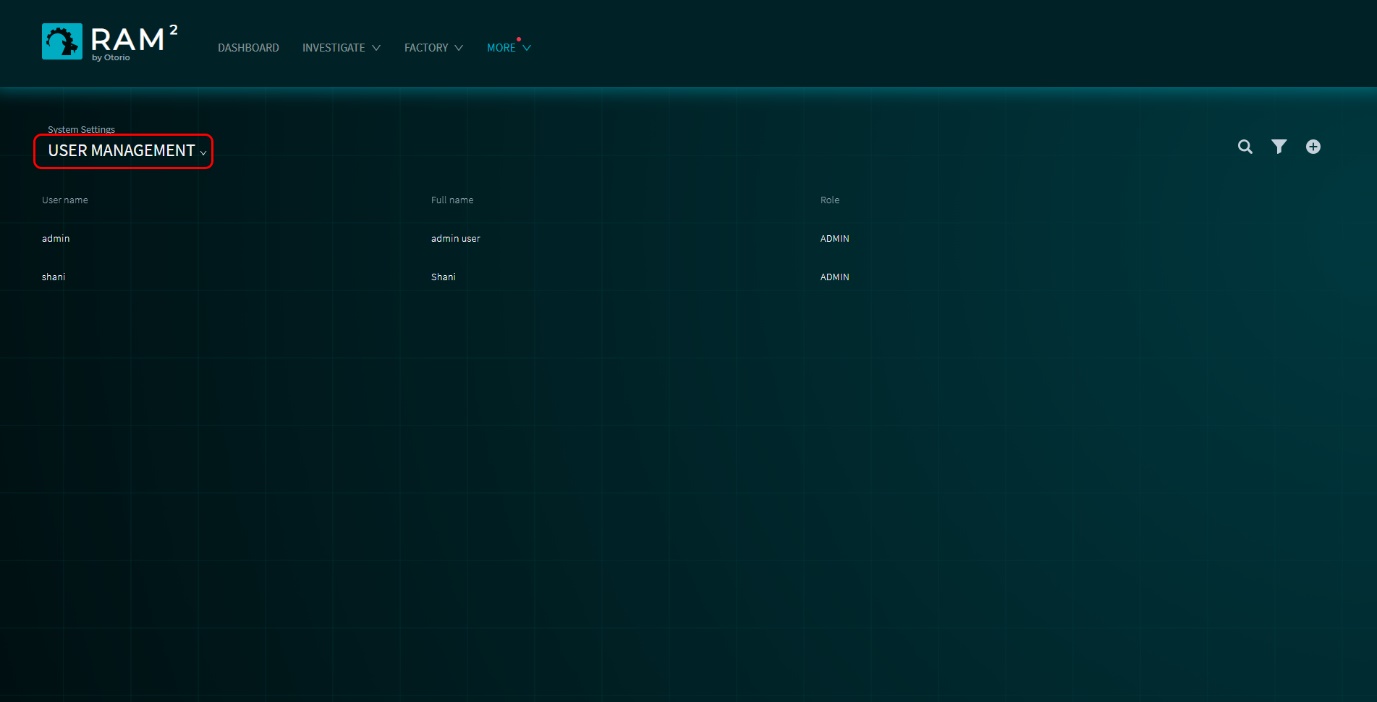


Figure 31 User management

1. Click  in the upper right.
2. Enter details for the new user, and select the role.

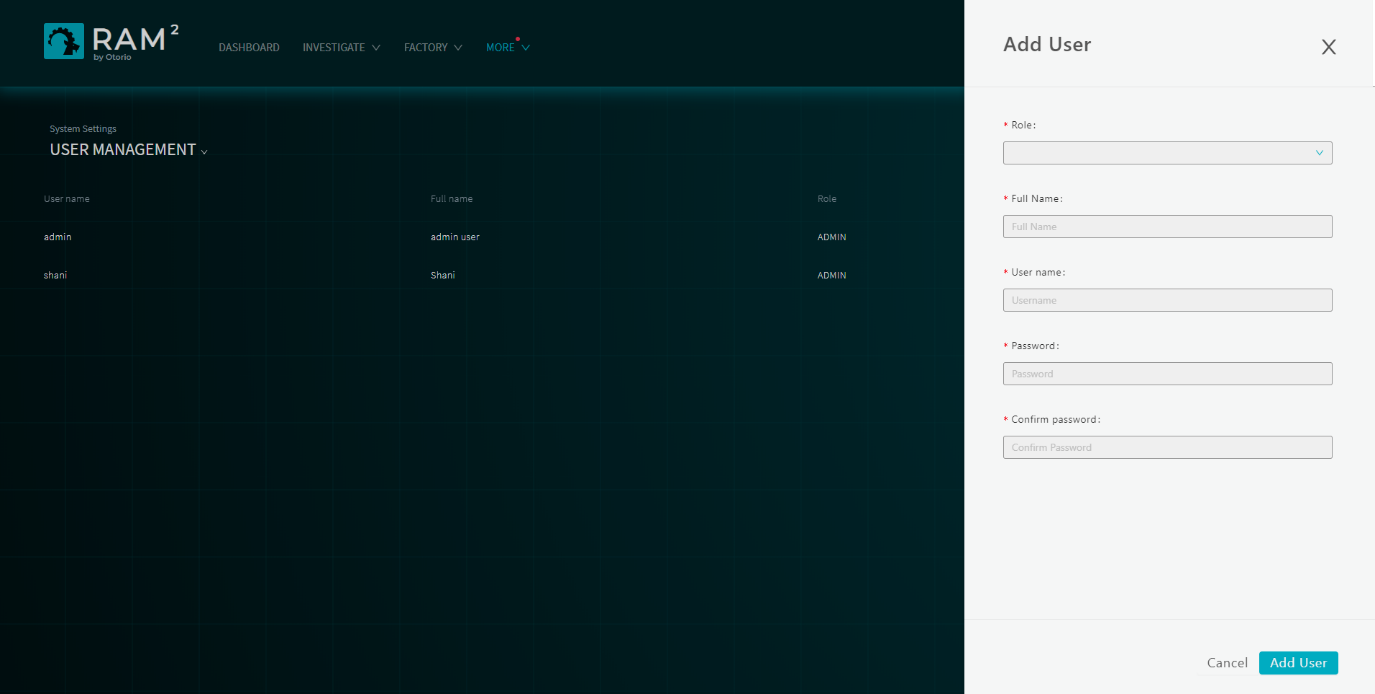


Figure 32 Add user

1. Click Add User.

# Configuration

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

## Network config

To configure the RAM network settings:

1. In the Configurations page, select the Network Configuration tab.

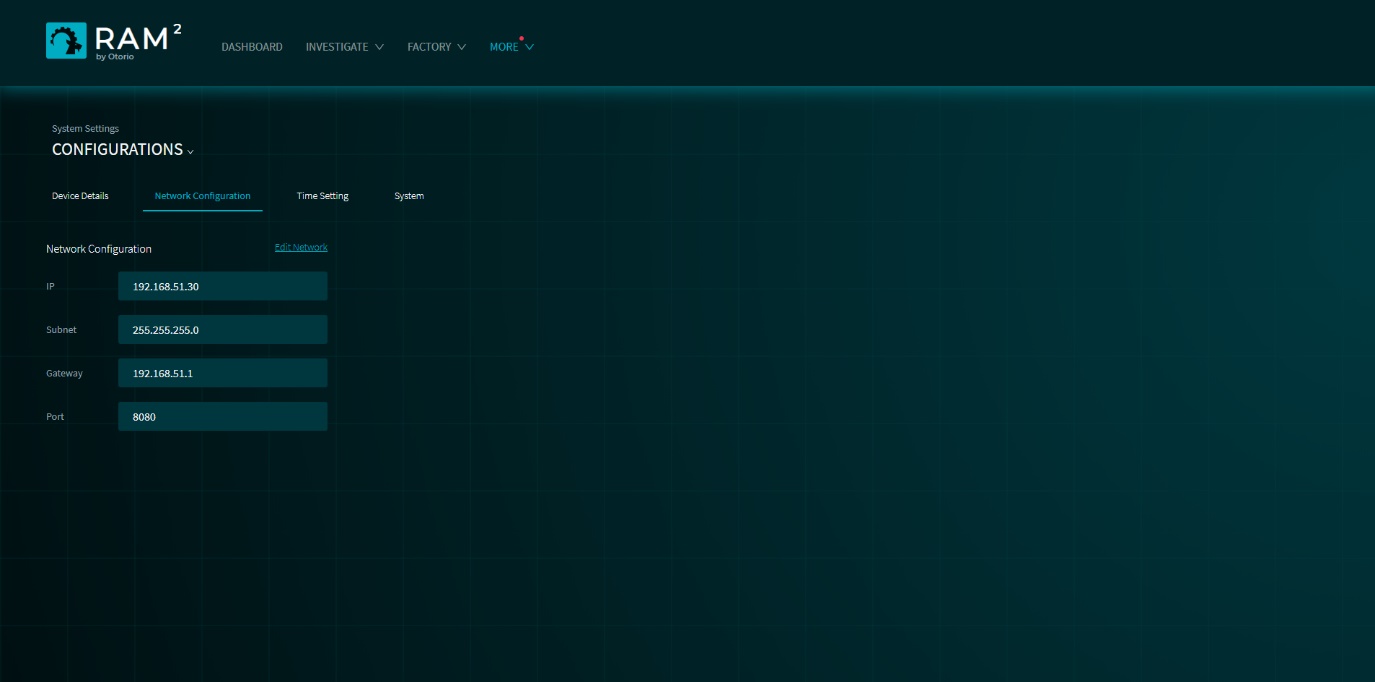


Figure 33 Network configuration

1. Set these values:
2. IP - an IPv4 value, in the form 0.0.0.0
3. Subnet – the subnet mast, in the form 255.255.255.255
4. Gateway – the IP address of the gateway
5. Port – the port

## Time

To configure the RAM2 time setting:

1. In the Configurations page, select the Time Setting tab.

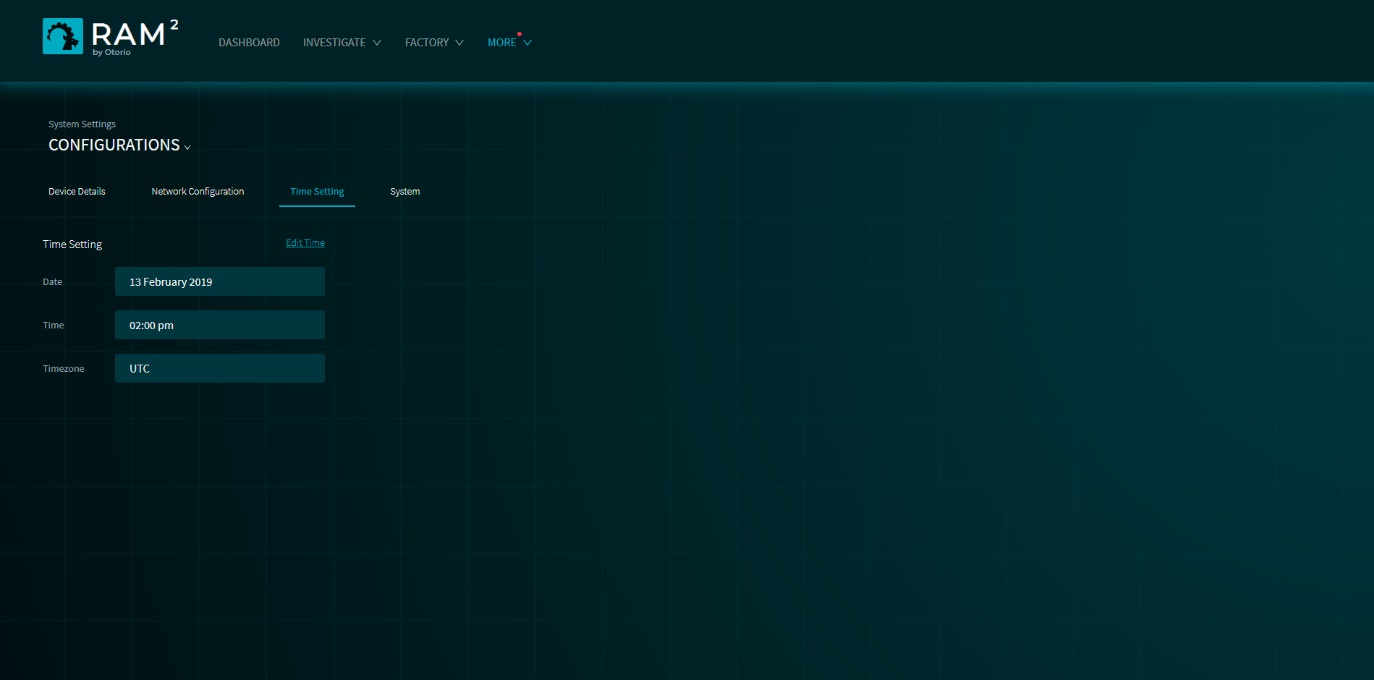


Figure 34 Set time

1. Enter the system time (local time).

## Deployment mode

You can set RAM2 to ignore all alerts from assets. Use this option when RAM2 is started, to ignored alerts from assets as they are discovered (in particular, alerts indicating ‘New Asset Discovered’). Once RAM2 is running, and all assets have been discovered, you can re-enable alerts.

This control is the Deployment Mode. Set the deployment mode in the System Settings page.

In the Configurations page, select the System tab.

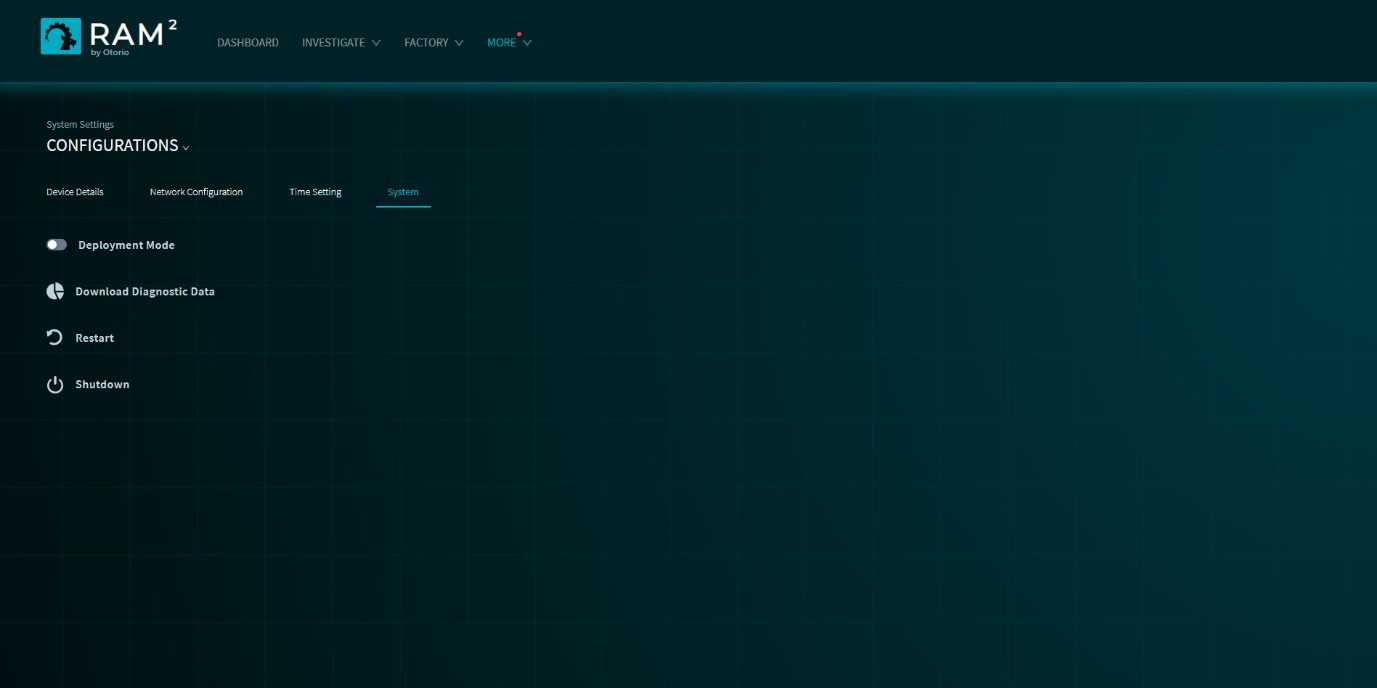


Figure 35 System settings

## Start & Shutdown

Restart or shutdown RAM2 from the Systems tab of the Configurations page.

Click  to restart RAM2 or  to shut it down.

# Troubleshooting

The troubleshooting page shows errors and other events that occurred in RAM2 (such as loss of connectivity to RAM2 components). It does not show alert or other event information for factory entities; this is shown in the Alerts page.

Select Troubleshooting from the top-level More menu.

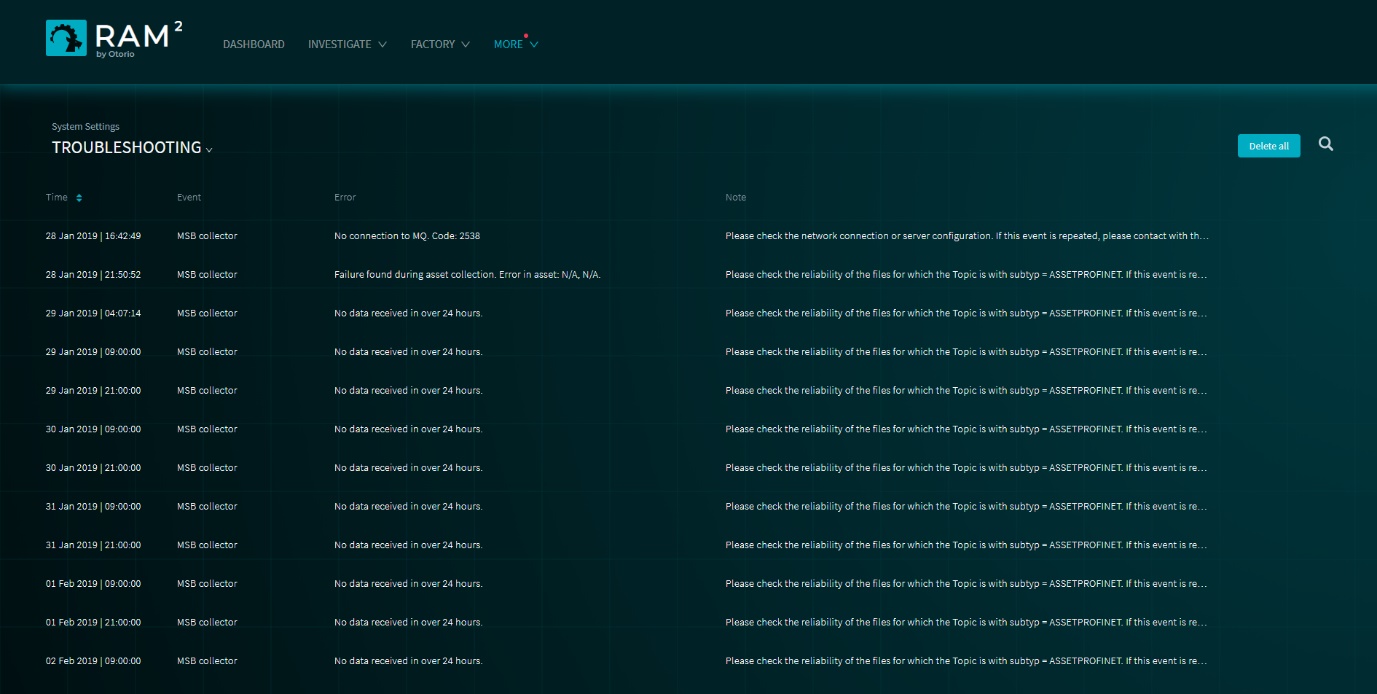


Figure 36 Troubleshooting

You can filter the list for specific errors or events.

Click  to remove all entries in the list.