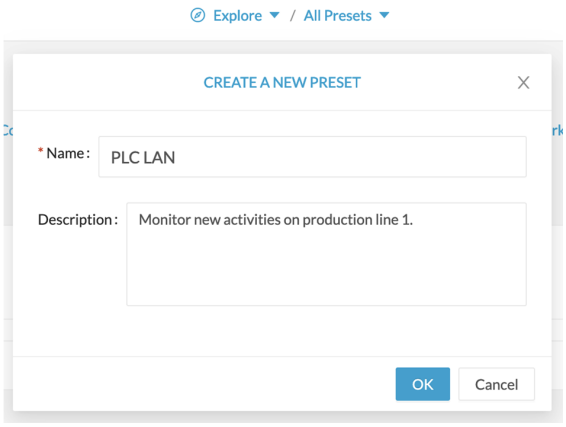
Use cases

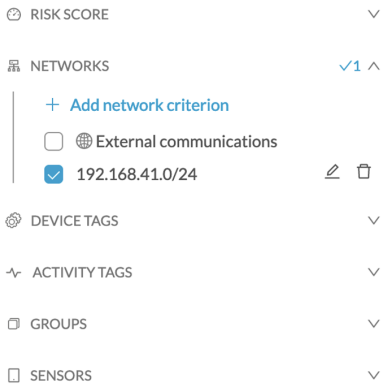
New activity detected on a set of critical equipment

Production lines are the most central and critical part of an industrial network. Good practice is to monitor the set of PLCs which manages these production lines. Ensure notification if a new activity happens on the network.

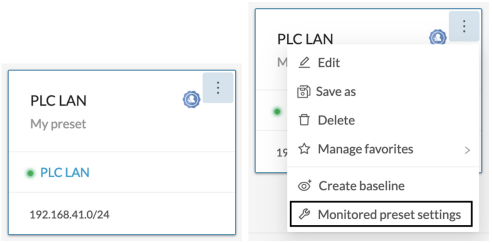
To monitor, access the **Explore** page and create a new PLC LAN **preset**.



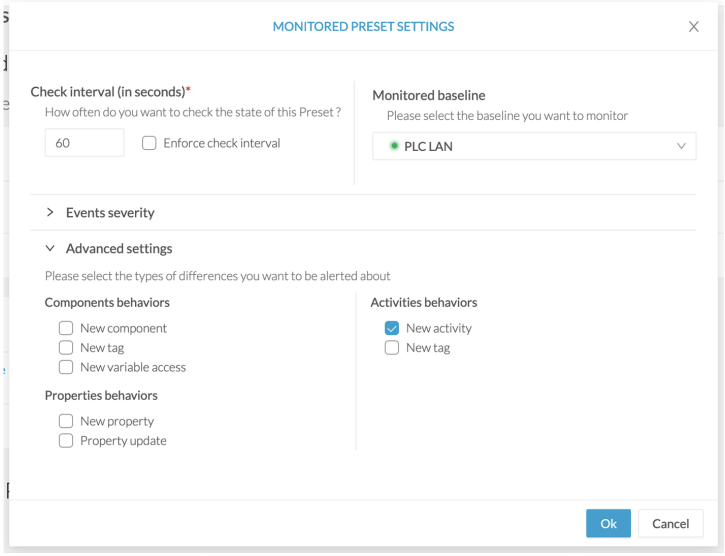
In **Networks**, select the subnetwork corresponding to the production line.



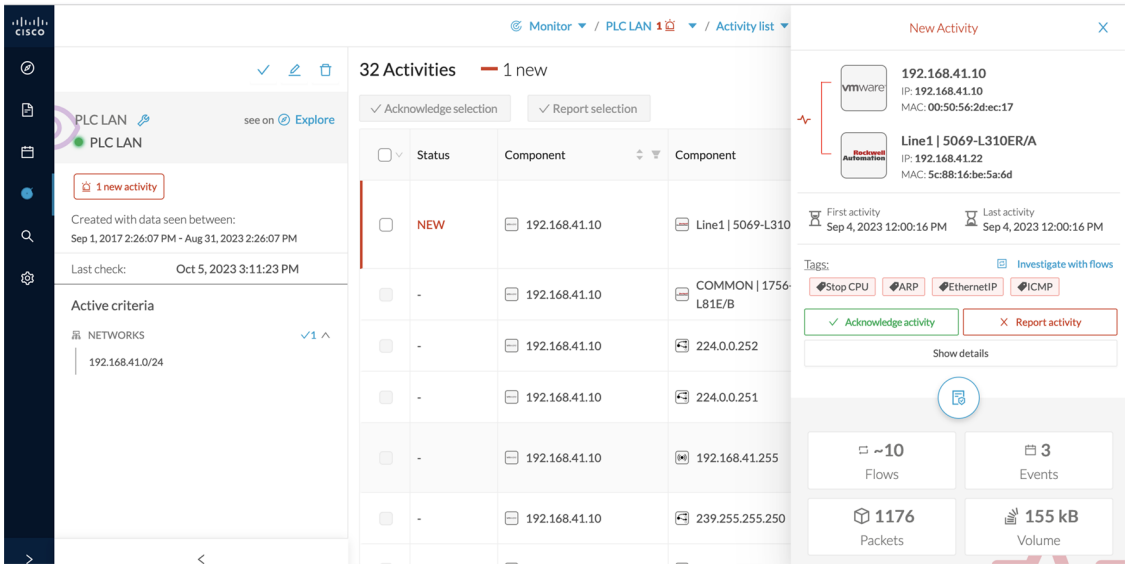
Click the **Monitor page > Monitor preset settings**.



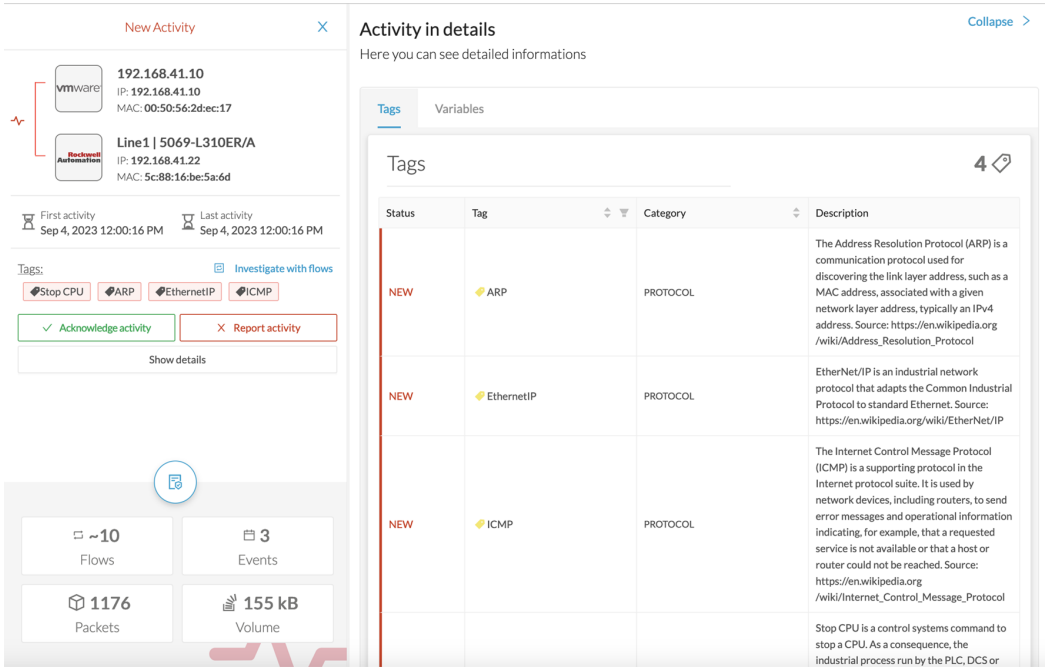
Click **Advanced settings > New activity > Ok**.



An alert appears when a new activity comes in. See the example below:



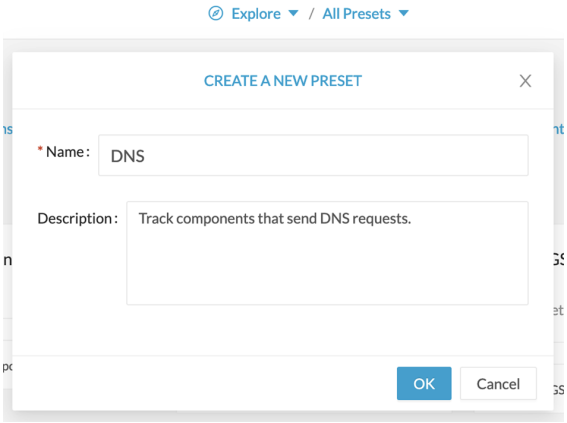
For more information about the activity of tags and their definition, click **Technical sheet**.



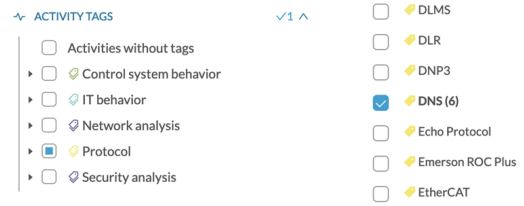
Tracking components that send DNS requests

Monitor components that send DNS requests on a network, in case a distant server, a service, or a URL established communication with the monitored network. You get alerts with information, such as the IP address of the component.

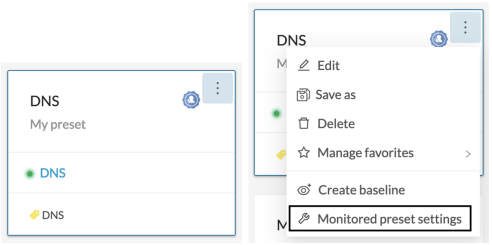
On the **Explore page > Create a new preset**.



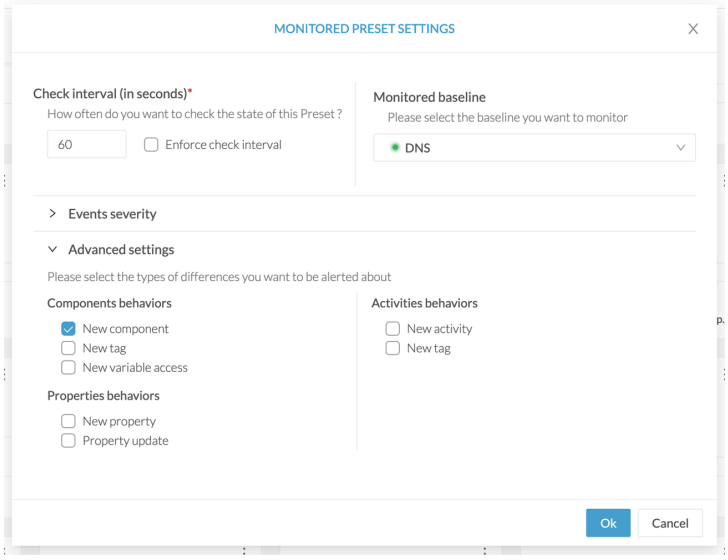
In the **Activity tags** filter > select **protocol DNS** .



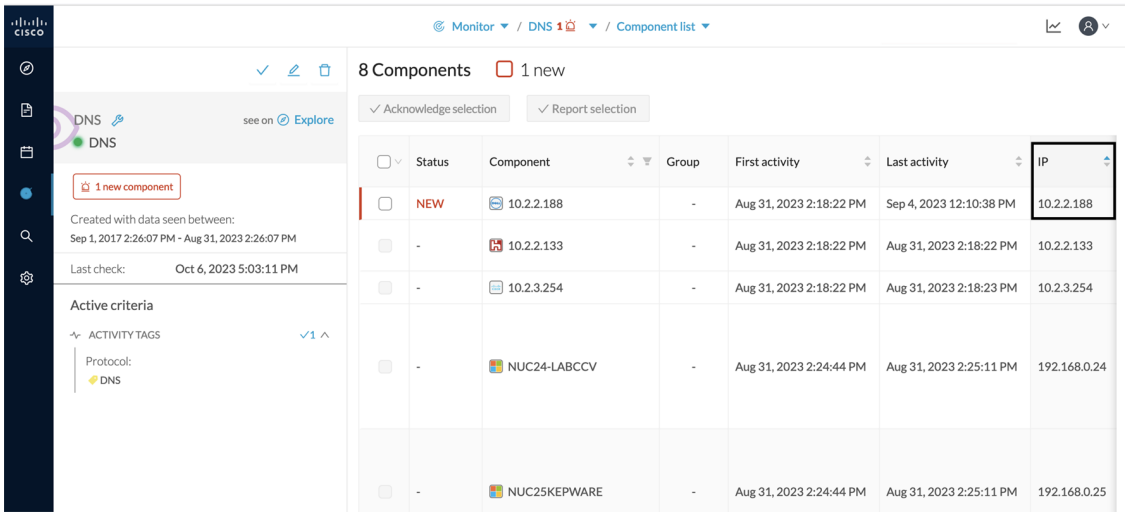
In the **Monitor page > Monitor preset settings**.



In **Advanced settings**, click **New component > Ok**.



An alert appears when a new component using the DNS protocol comes in. See the example below.



The IP address of the component is displayed under the IP column.

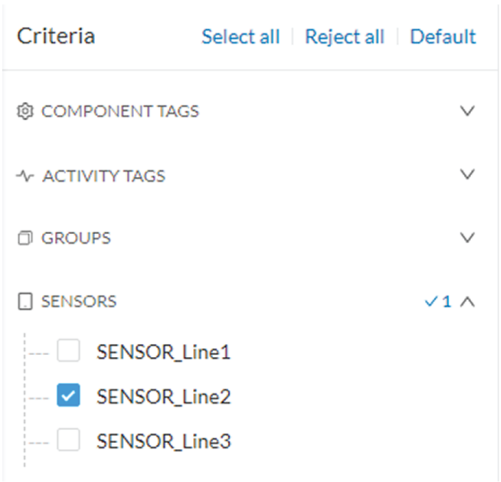
Detection of assets newly connected to the network

Detecting when new equipment connects to the industrial network is a very basic use case. Good practice: organize components in an intelligible way, for example, according to the network topology per production chain. A network can be divided into several areas, such as several production chains with different criticality levels. Place a Cisco Cyber Vision Sensor to capture and monitor its traffic. Create groups which represent a production chain and contain its components to reflect that topology. Cisco Cyber Vision detects a new component and its related activities within a specific area to see if a component connects with this production chain. Its related activities are also highlighted in **Monitor mode**.

Key Differences: New components and their related activities on the network.

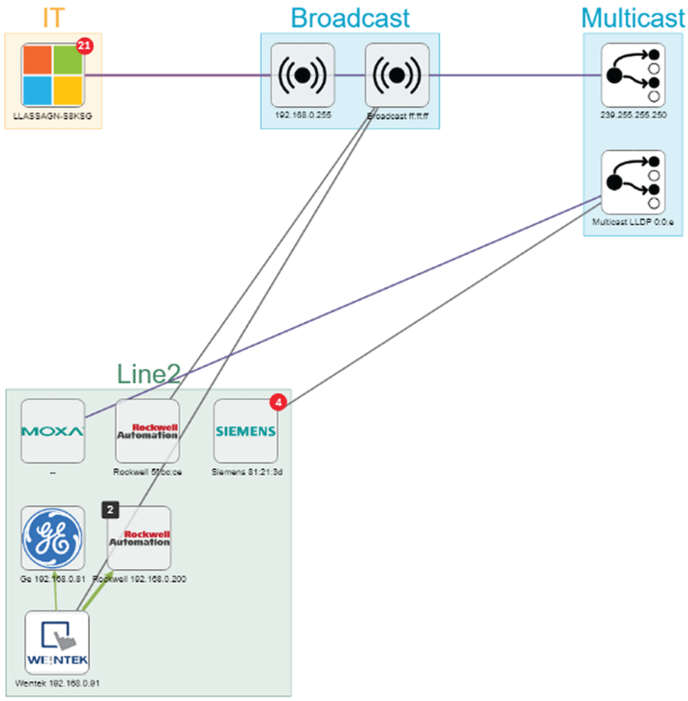
Aim: Monitor the production line 2 of the industrial network.

Place a sensor on each production chain. Use the sensor filter to display each production chain. In the industrial network example below, we are monitoring has three production lines on which we have positioned a sensor. We want to see and monitor what is happening on production line 2. In **Explore** mode access the **Preset All data**. Select the filter SENSOR_Line2 (it is possible to rename sensors to identify which area of the network they are monitoring) so only traffic captured on Production Line 2 appears.



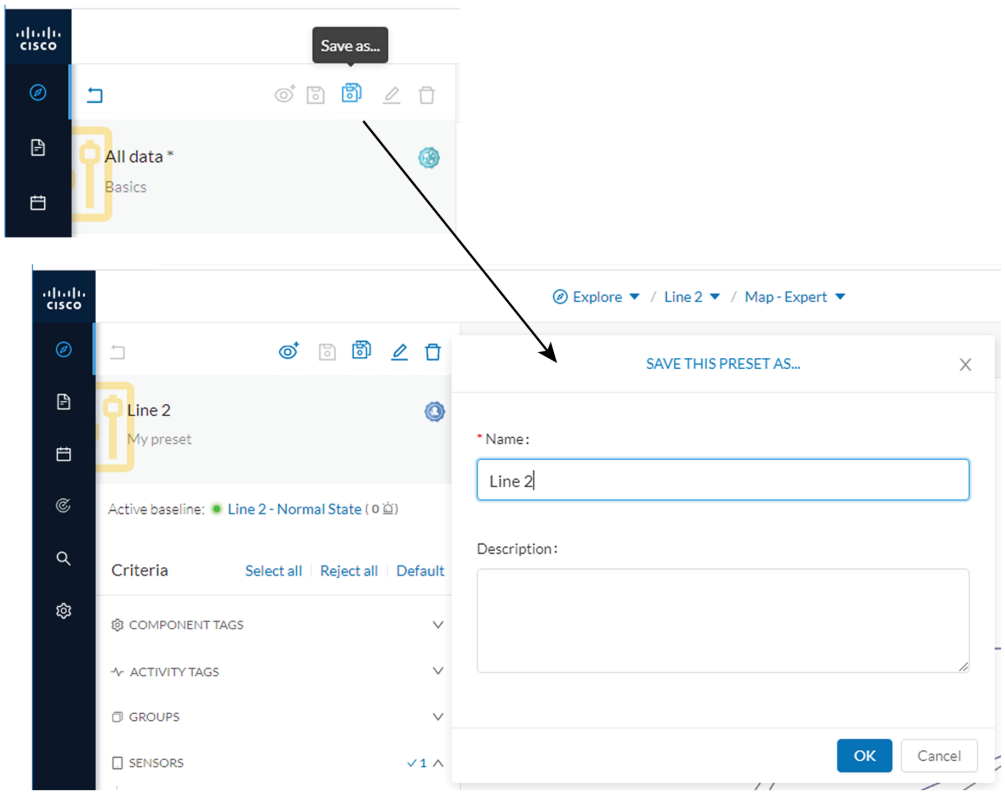
Organize the components into groups, per function:

- PLCs in Line 2
- IT
- Broadcast
- Multicast

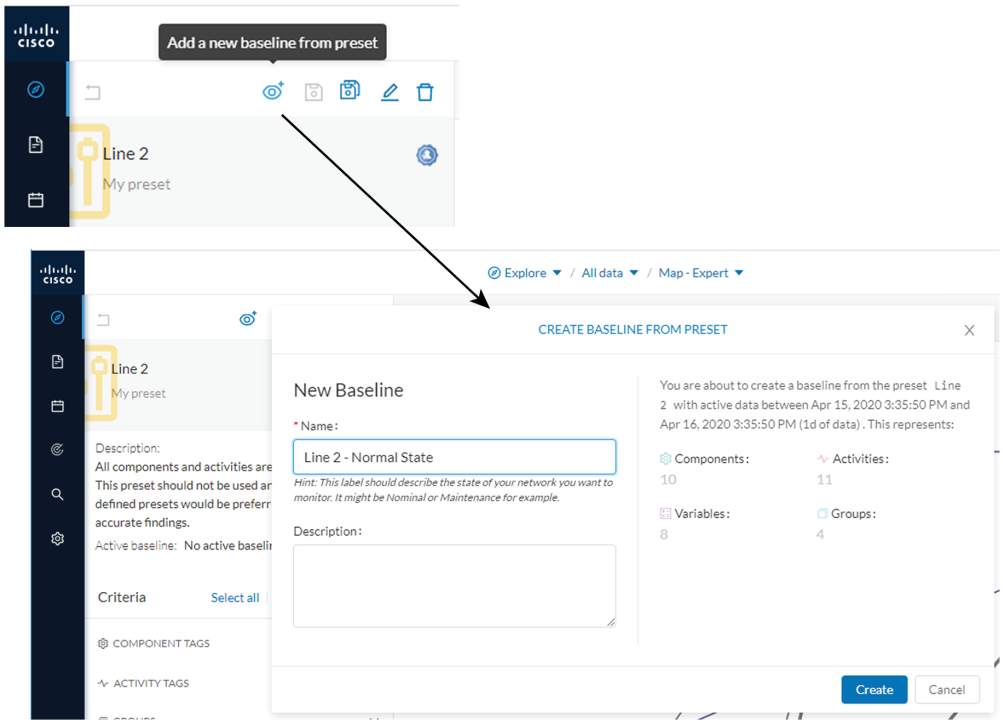


Result: A filtered and organized view of production chain 2.

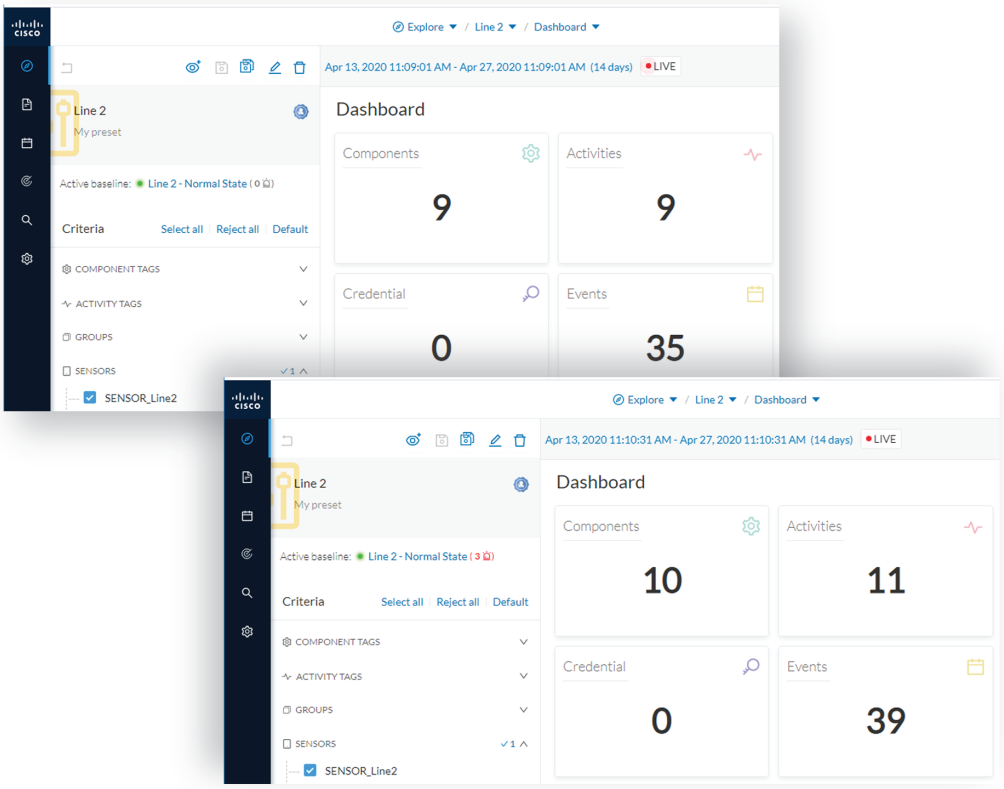
Save the filtered and grouped network data selection as a new preset. Name it **Line 2.**



The preset **Line 2** contains components and activities that are interacting in a normal way. Production line 2 is in normal operating state. Save the normal state of the preset as a baseline. Name it **Line 2 - Normal State**.



Check Production Line 2. In **Explore** mode, we see 10 components instead of 9. Number of activities and events has increased, too. The baseline **Line 2 - Normal State** reports 3 alerts.

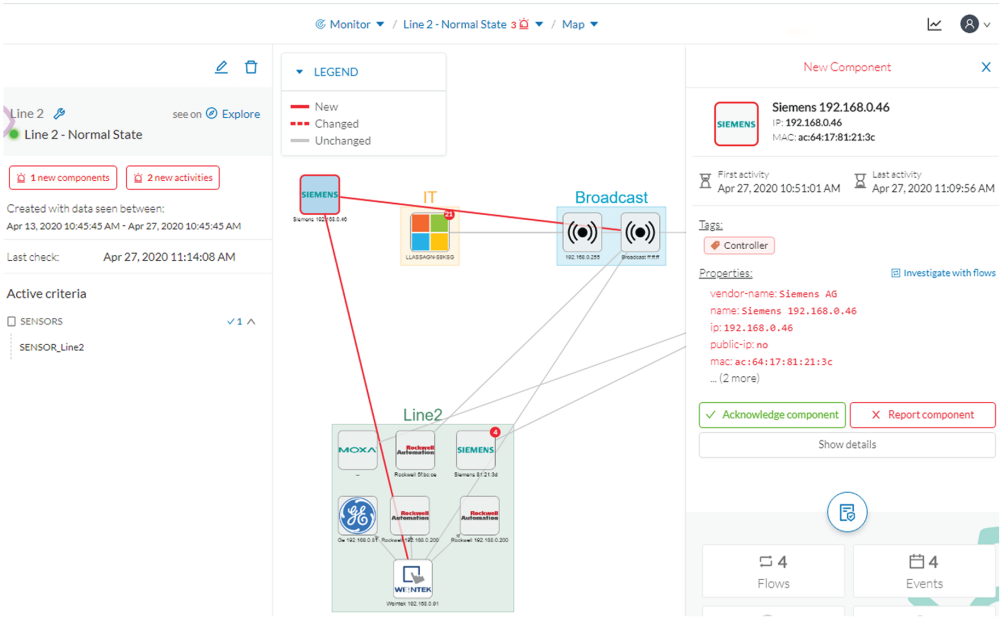


To understand exactly what happened, go to **Monitor mode**.

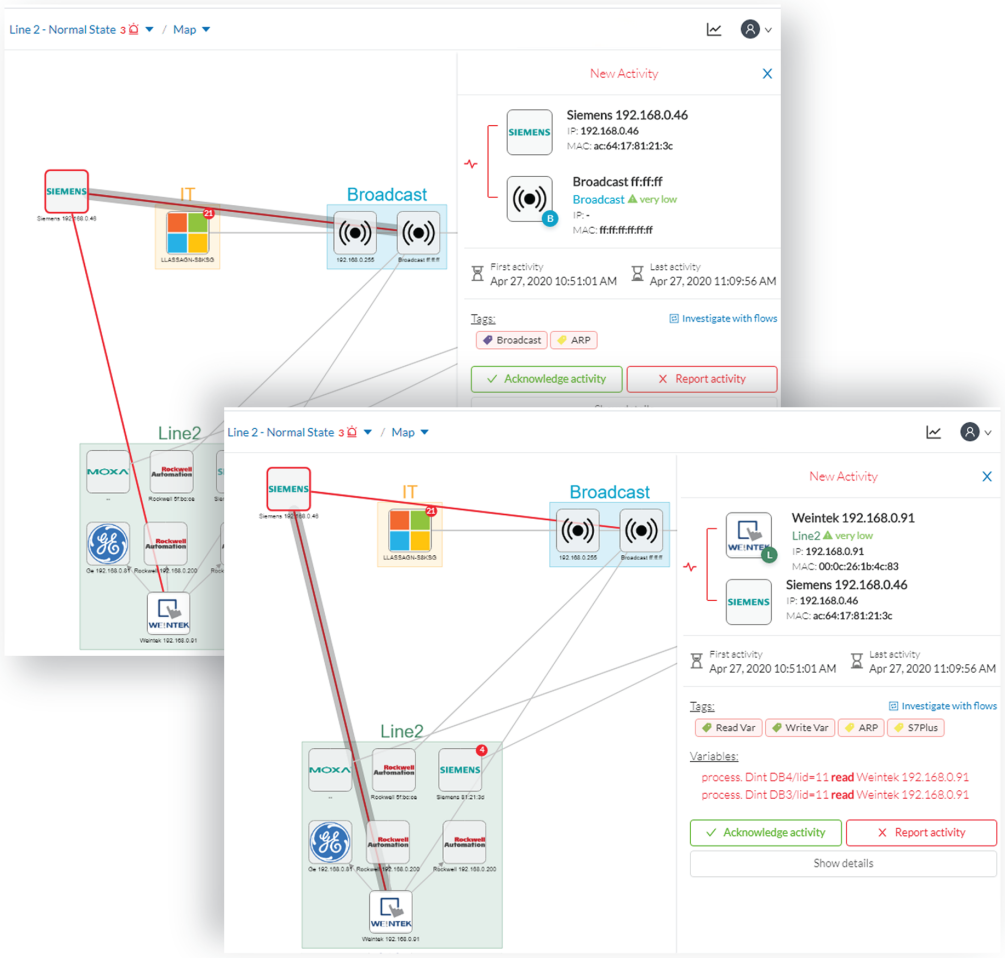
The left panel shows 1 new component and 2 new activities have been found.

Click the new component. The right side panel opens with the detailed properties of the component.

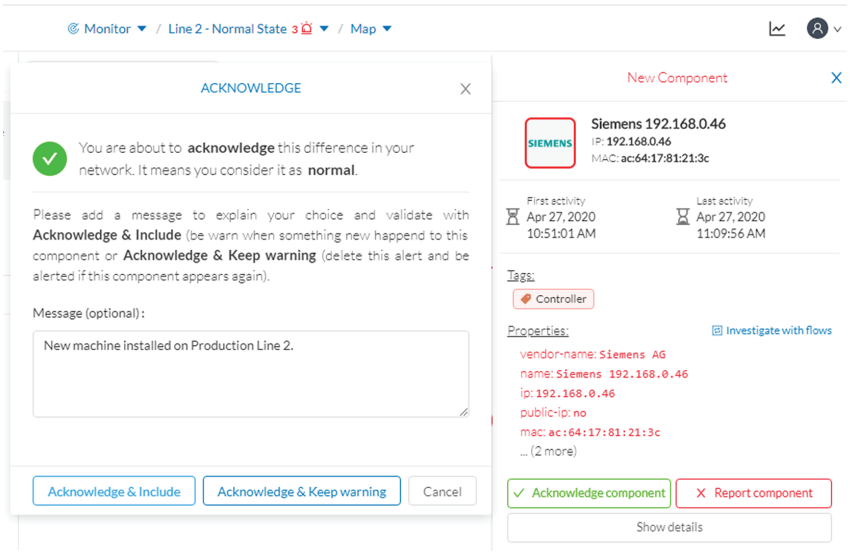
The component details show it is a controller with similar properties to other component characteristics. After visually confirming, we discover that a new PLC was connected to the network to enlarge Production Line 2.



This new component behaves normally, looking at its activities. It has been identified because it has sent a broadcast packet (probably ARP) and then has connected to the Weintek machine using a legitimate protocol. Actions like **Read variable** accesses look normal, too.

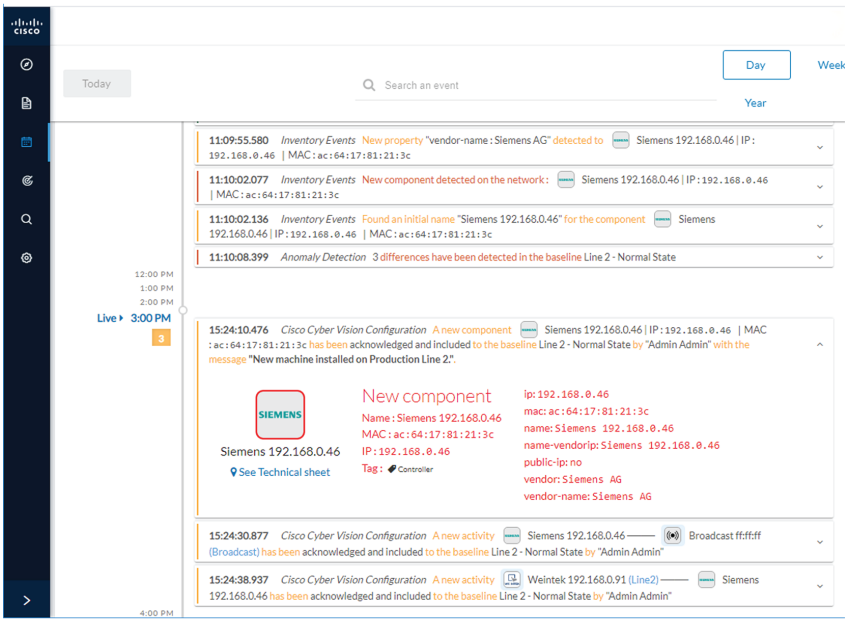


Since the component and activities are part of the normal operating process of Production Line 2, you can acknowledge and include the baseline differences, if any change occurs.



Go to **Explore** mode and add the component into the Line 2 group.

Go to the **Events** page and see that all previous actions are reported here: the detection of a new component, activities on the network, and adding the component into the group Line 2.



Tracking sensitive assets properties

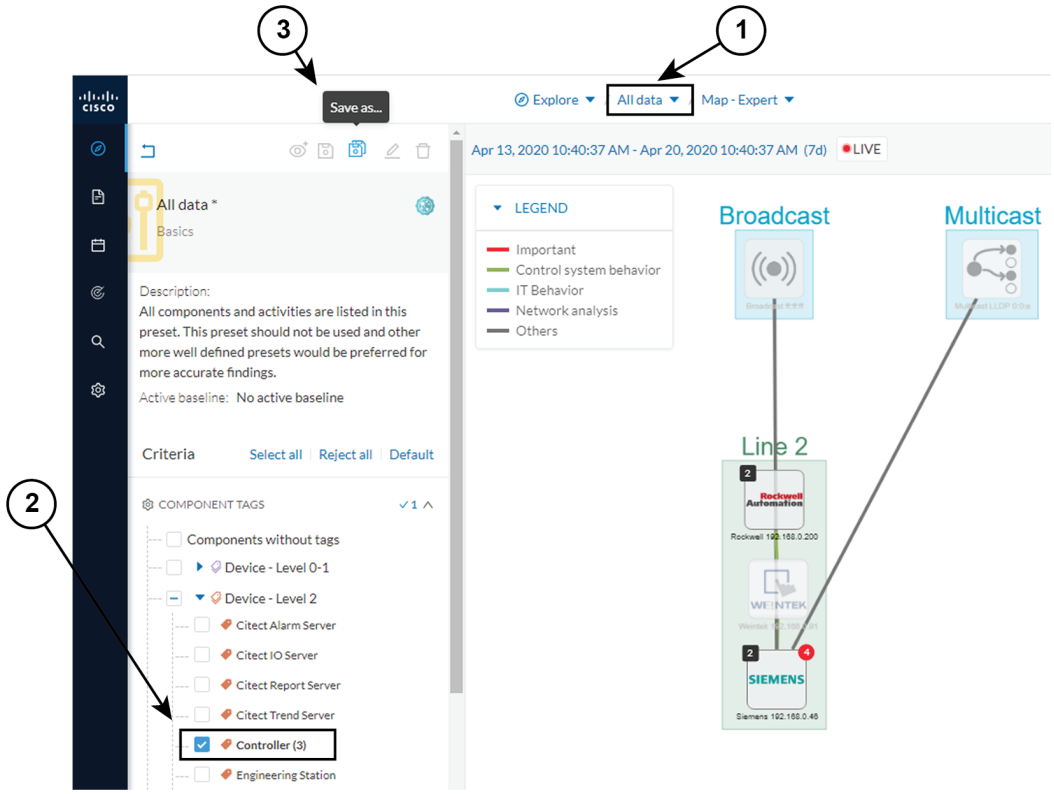
To ensure To ensure the security of the network, monitor its critical assets closely. Usually, critical assets are controllers which ensure the plant's operation. To monitor them, check the properties of the controllers. Typically, programs and firmware versions changes are properties that might cause malfunctions or even stop a production line.

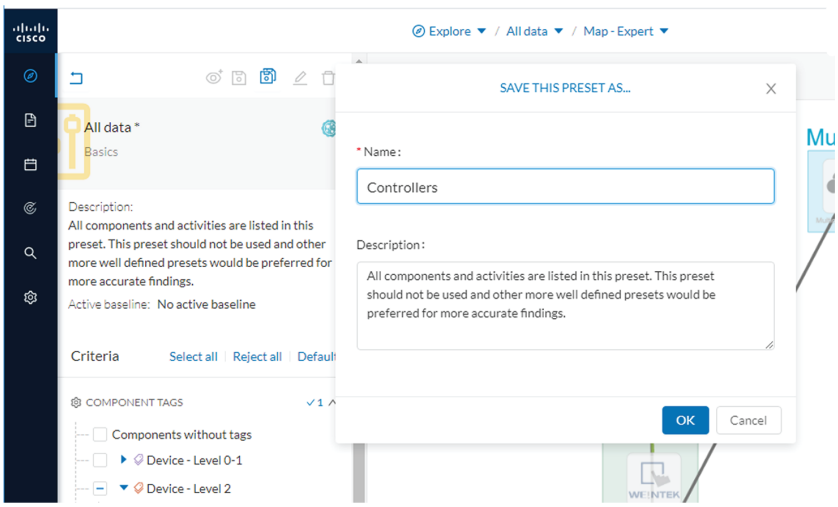
Preset definition: Preset needs to be defined per group or multiple groups.

Key differences: New properties or changed properties on components.

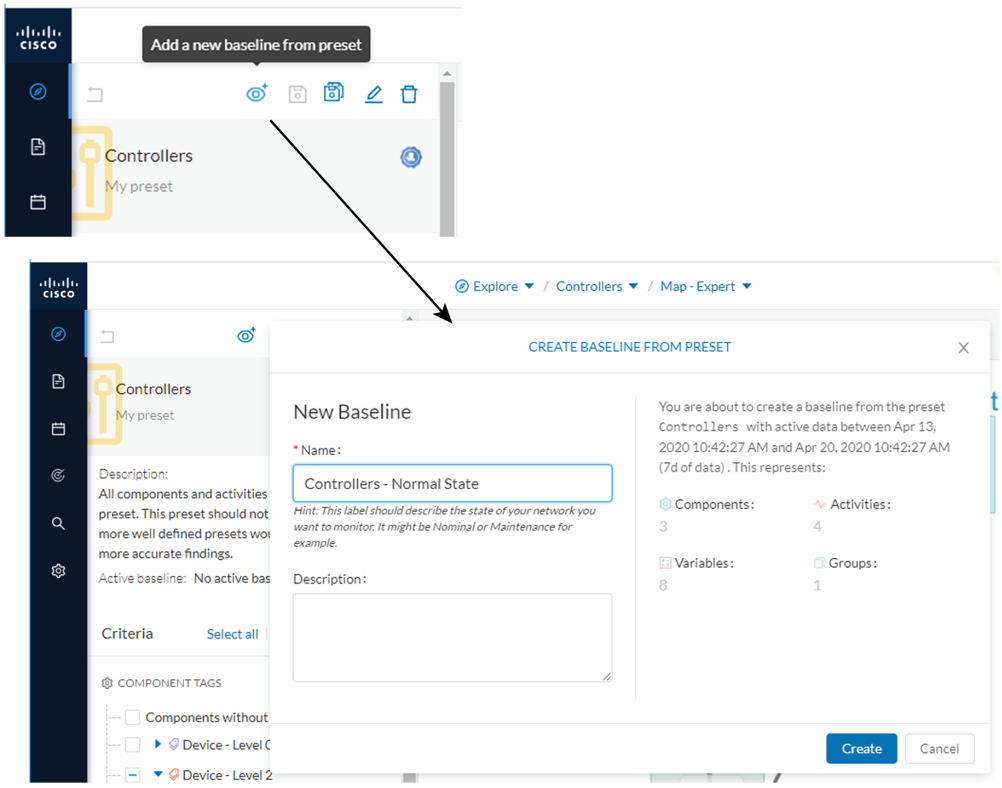
In **Explore** mode, click **All data (1)**. Group the components per function (Broadcast, Multicast, Production Line 2) to organize our data. Select the Controllers component filter **(2)**, so only the components marked with the **Controller** tag, their activities, and related components display. The network data is filtered and grouped.

Save the selection as a new preset **(3)**. Name it **Controllers**.



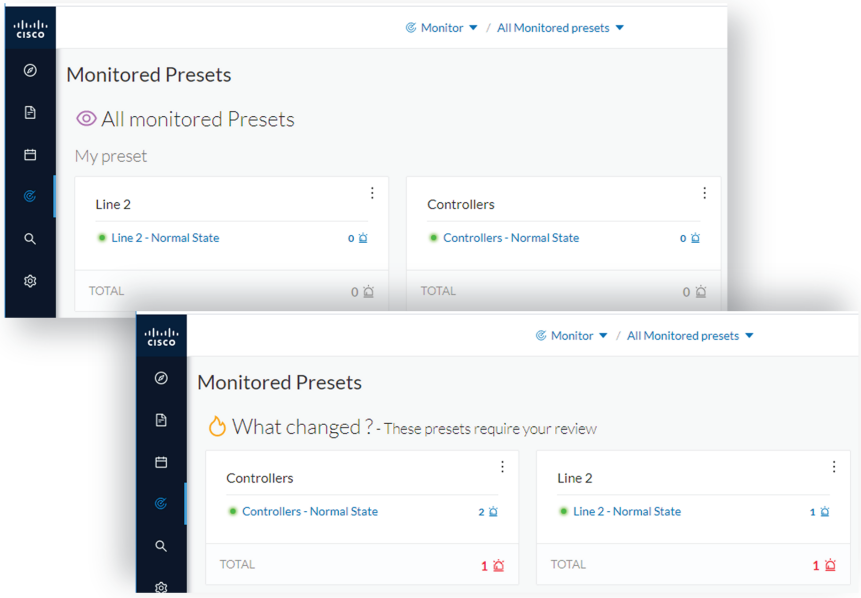


The preset Controllers contain components and activities operating in a normal way. Save the normal state of the preset as a baseline. Name it **Controllers - Normal State**.



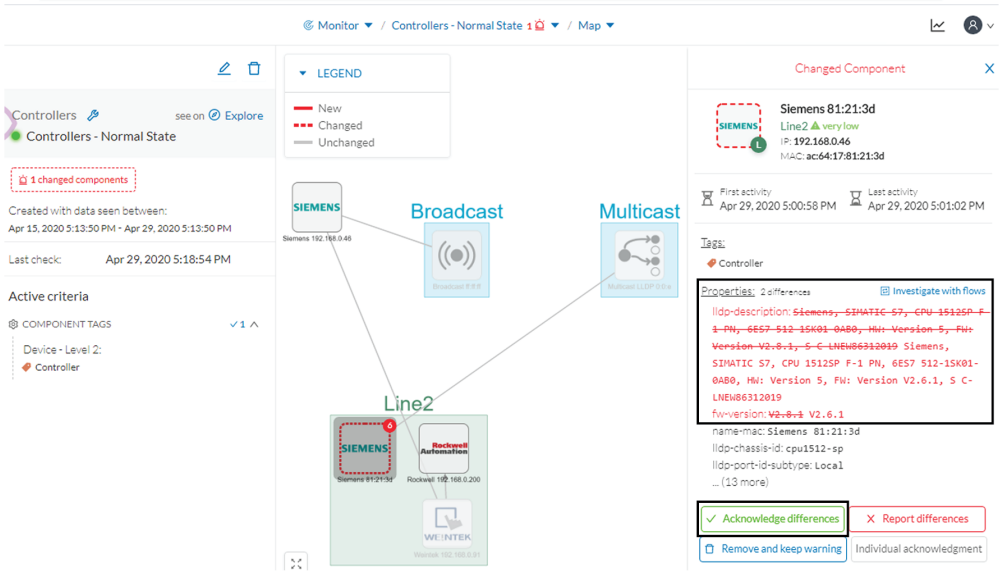
Go to **Monitor mode**. The new baseline **Controllers - Normal State** displays.

Soon, two alerts are reported in the Controllers preset. Access the baseline to investigate.



The left panel reports that one component and one activity have changed in the scope of the preset.

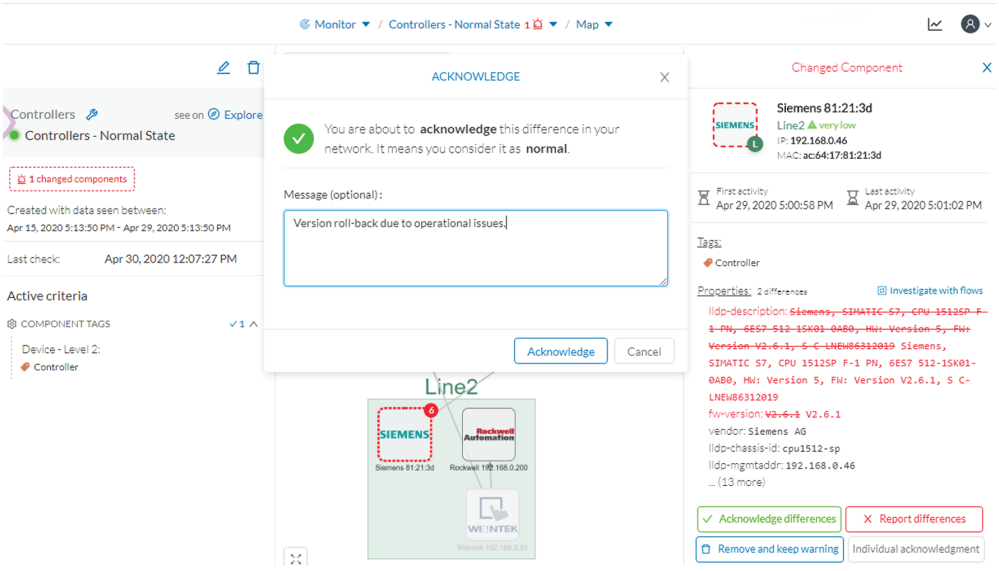
Click on the changed component in the map. A right side panel opens with more information. Changes appear in red. The tag indicates that it is a controller. The properties lldp-description and firmware version have changed and the former version is crossed off.



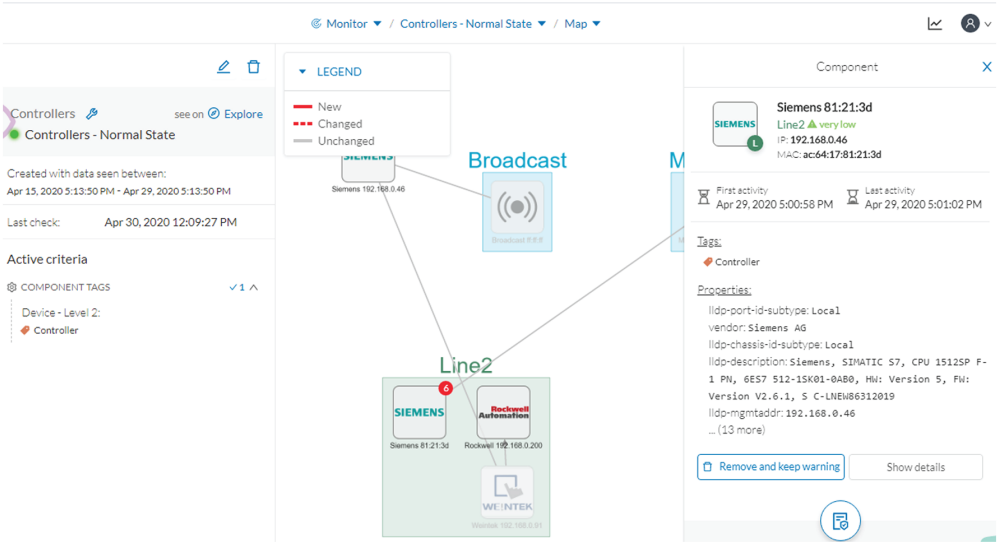
Issue: no activity on the network seems to explain why the firmware version of the SIEMENS component rolled back.

Diagnosis: meet with the technical operator in charge of the production line. The operator says that the latest version was causing several issues on the network. A maintenance operator performed a rollback to solve this, until a new fix is available.

Conclusion: this was part of a normal maintenance act and we acknowledge the differences.



Once you acknowledge differences, they are considered **normal** and do not appear in red anymore. If a new change happens such as the version update, the component appears as changed again in **Monitor mode**.



Monitor mode generates an event, showing the previous behaviors that happened on preset Controllers and actions.