Cisco Cyber Vision GUI Monitor Mode User Guide, Release 4.3.0

First Published: 2023-09-20

Last Modified: 2023-12-13

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

About this documentation

Document purpose

This user guide describes the **Monitor mode** of the GUI for Cisco Cyber Vision and how to use it.

It requires the highest license level (Advantage). You must have **Admin** and **Product user** roles.

This manual is applicable to **system version 4.3.0**.

Warnings and notices

To ensure your personal safety and to prevent damage to property, observe the following: Warnings and notices and Safety Alert symbols. These notices are graded according to the degree of danger.

Warning Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.

Important Indicates risks that could involve property or Cisco equipment damage and minor personal injury if proper precautions are not taken.

Note Indicates important information on the product described in the documentation to which attention should be paid.

CHAPTER 1

Overview

Monitor mode

Cisco Cyber Vision provides **Monitor mode**, a monitoring tool that detects changes inside industrial networks. Because a network architecture (PLC, switch, SCADA) is constant and its behaviors tend to be stable over time, an established and configured network is predictable. However, some behaviors are unpredictable and can even compromise a network's operation and security. **Monitor mode** shows the evolution of the behaviors of a network, predicted or not, based on presets. Behavior changes are noted as differences in **Monitor mode**. Using **Monitor mode** is particularly convenient for large networks, as a preset shows a network fragment and changes are highlighted and managed separately in the views of **Monitor mode**.

Baselines as Preset's normal states

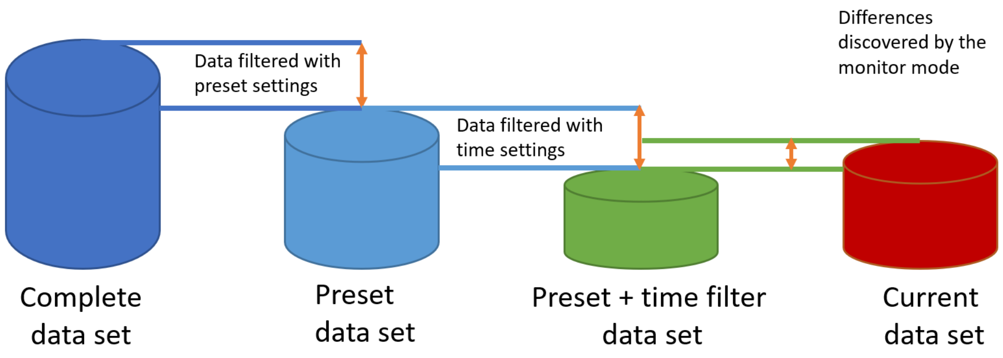
A Preset is a set of criteria which shows a detailed fragment of a network. To monitor a network, set a preset, and define what would be its normal, stable state. This represents the baseline of the preset. A state relies on a period because a network fragment is subject to several states. It is possible to create several, planned, controlled and time-framed baselines per preset and to monitor the whole network. For example, a normal state of the network can be a typical weekday operating mode, in which numerous processes are performed iteratively. During weekends, these processes may be slowed down, different, or even stopped. Save any network phase as a baseline by selecting the time span in which it occurs and is monitored. Other examples of baselines are: a regular maintenance period, a degraded mode, a weekend and night mode. Create a baseline by "framing" a normal operating process in which all network behaviors (components, activities, properties, tags, variable accesses) are considered.

Review and assignment of differences

A **difference** is defined as a new or changed behavior happening within a fragment of a network. **Monitor mode** detects and highlights any differences. **Monitor mode** contains the following three views:

- Map View
- Component List View
- Activity List View

You can report or acknowledge these view issues, depending on whether you consider them as normal or not, and their level of criticality. You can include these changes into your baseline if it is part of a normal network development process, or take action, in case of suspicious behavior. Therefore, each baseline gets refined bit by bit over time and become more compliant with your needs.

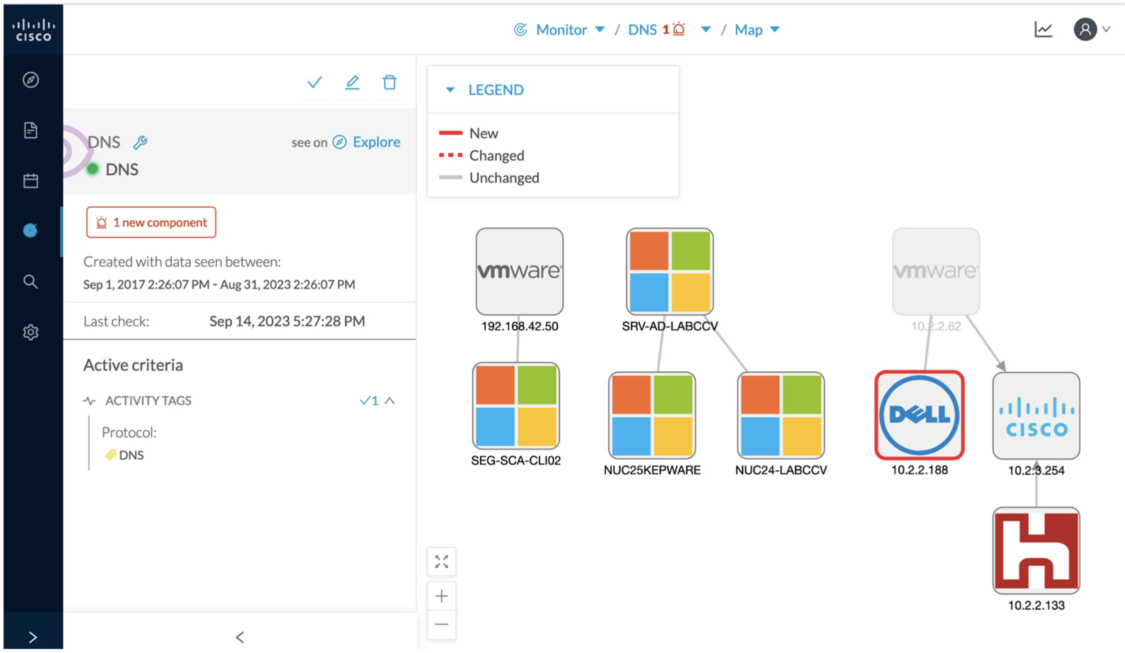

Differences discovered by the monitor mode
Data filtered with preset settings
Data filtered with time settings
Complete data set
Preset data set
Preset + time filter data set
Current data set

Monitor mode's views

Like in **Explore** mode, **Monitor mode** offers several views of data so you can see them through different representations. In **Monitor mode**, new and changed detected elements are highlighted in red.

For more information about the views listed below, refer to the **Explore** chapter.

Map View



DNS
see on Explore
DNS

1 new component

Created with data seen between:
Sep 1, 2017 2:26:07 PM - Aug 31, 2023 2:26:07 PM

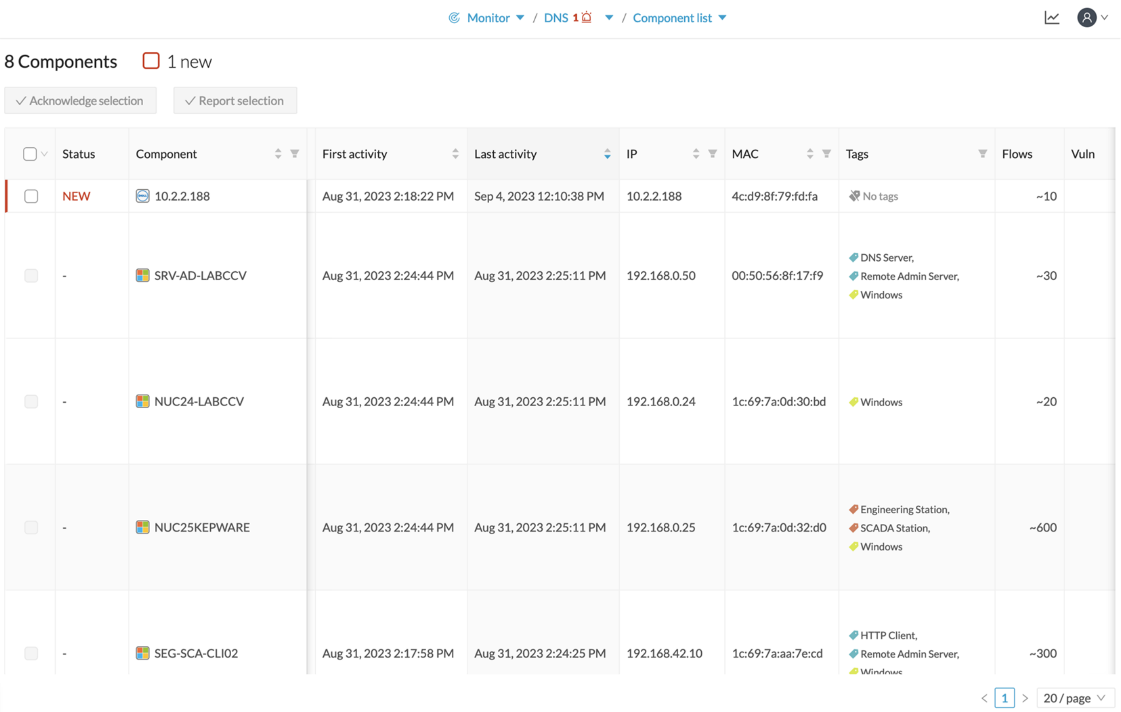
Last check: Sep 14, 2023 5:27:28 PM

Active criteria

ACTIVITY TAGS ✓1

Protocol:
DNS

Component List View



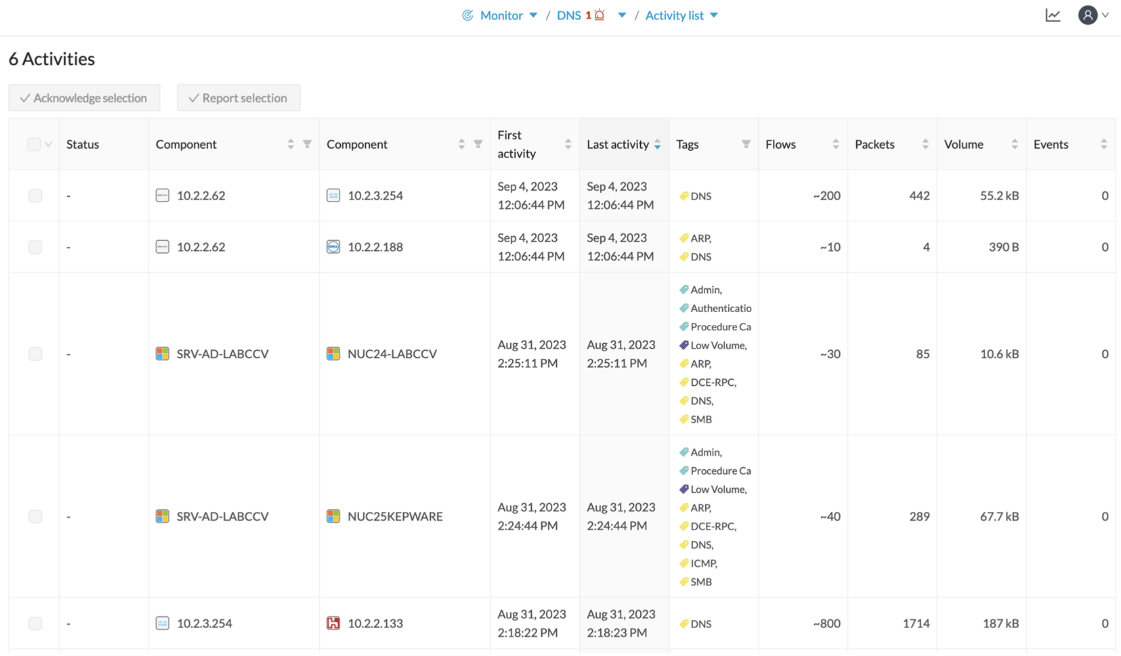
8 Components □ 1 new

✓ Acknowledge selection ✓ Report selection

□	Status	Component	First activity	Last activity	IP	MAC	Tags	Flows	Vuln
□	NEW	10.2.2.188	Aug 31, 2023 2:18:22 PM	Sep 4, 2023 12:10:38 PM	10.2.2.188	4c:d9:8f:79:fd:fa	No tags	~10	
□	-	SRV-AD-LABCCV	Aug 31, 2023 2:24:44 PM	Aug 31, 2023 2:25:11 PM	192.168.0.50	00:50:56:8f:17:f9	DNS Server, Remote Admin Server, Windows	~30	
□	-	NUC24-LABCCV	Aug 31, 2023 2:24:44 PM	Aug 31, 2023 2:25:11 PM	192.168.0.24	1c:69:7a:0d:30:bd	Windows	~20	
□	-	NUC25KEPWARE	Aug 31, 2023 2:24:44 PM	Aug 31, 2023 2:25:11 PM	192.168.0.25	1c:69:7a:0d:32:d0	Engineering Station, SCADA Station, Windows	~600	
□	-	SEG-SCA-CLI02	Aug 31, 2023 2:17:58 PM	Aug 31, 2023 2:24:25 PM	192.168.42.10	1c:69:7a:aa:7e:cd	HTTP Client, Remote Admin Server, Windows	~300	

< 1 > 20 / page

Activity List View



6 Activities

✓ Acknowledge selection ✓ Report selection

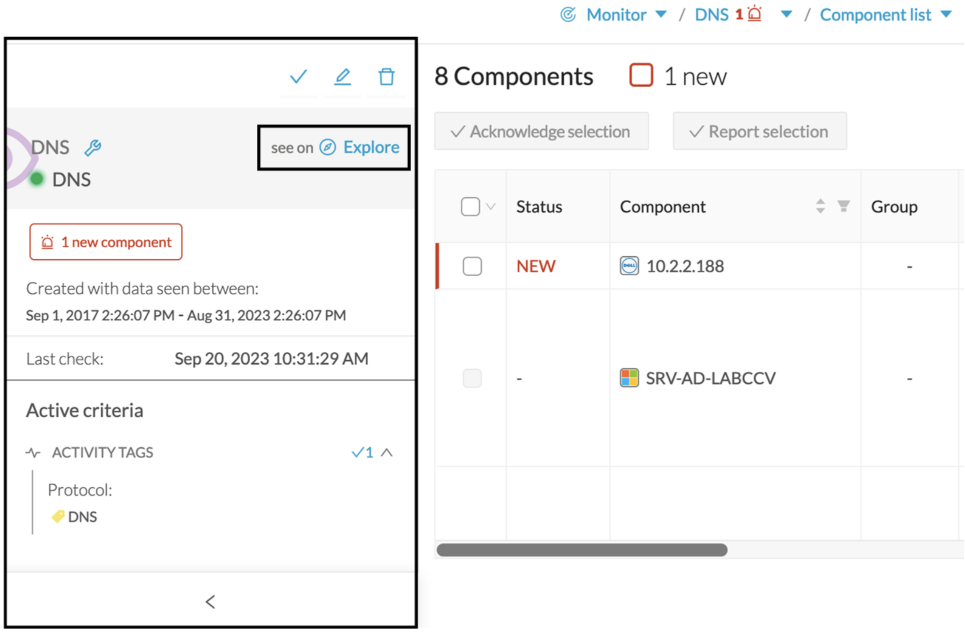
□	Status	Component	Component	First activity	Last activity	Tags	Flows	Packets	Volume	Events
□	-	10.2.2.62	10.2.3.254	Sep 4, 2023 12:06:44 PM	Sep 4, 2023 12:06:44 PM	DNS	~200	442	55.2 kB	0
□	-	10.2.2.62	10.2.2.188	Sep 4, 2023 12:06:44 PM	Sep 4, 2023 12:06:44 PM	ARP, DNS	~10	4	390 B	0
□	-	SRV-AD-LABCCV	NUC24-LABCCV	Aug 31, 2023 2:25:11 PM	Aug 31, 2023 2:25:11 PM	Admin, Authenticatio Procedure Ca Low Volume, ARP, DCE-RPC, DNS, SMB	~30	85	10.6 kB	0
□	-	SRV-AD-LABCCV	NUC25KEPWARE	Aug 31, 2023 2:24:44 PM	Aug 31, 2023 2:24:44 PM	Admin, Procedure Ca Low Volume, ARP, DCE-RPC, DNS, ICMP, SMB	~40	289	67.7 kB	0
□	-	10.2.3.254	10.2.2.133	Aug 31, 2023 2:18:22 PM	Aug 31, 2023 2:18:23 PM	DNS	~800	1714	187 kB	0

Each view contains the following:

- Panel with a summary of the detected elements in **Monitor mode**
- The time period of the baseline

- The last time this baseline was checked
- The preset it belongs to and the list of criteria selected

Modify the baseline settings using the **Explore** button that redirects you to the corresponding preset in **Explore** mode.



DNS

Created with data seen between:
Sep 1, 2017 2:26:07 PM - Aug 31, 2023 2:26:07 PM

Last check: Sep 20, 2023 10:31:29 AM

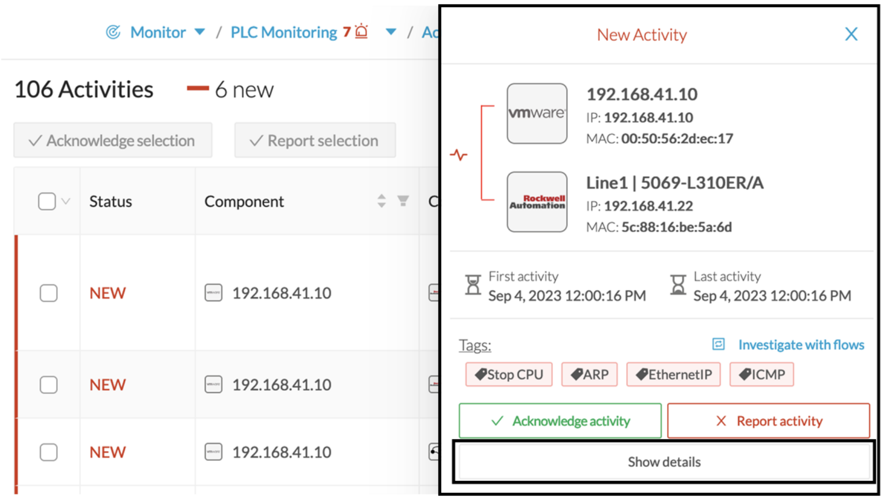
Protocol:
DNS

8 Components 1 new

□	Status	Component	Group
□	NEW	10.2.2.188	-
□	-	SRV-AD-LABCCV	-

Check one of the elements marked as new in the **Activity List View** to see the following:

- Information about the activity, such as the two components it belongs to
- The date of the first and the last activity
- Its tags
- Buttons to perform several actions. See Review differences.



106 Activities 6 new

□	Status	Component	C
□	NEW	192.168.41.10	
□	NEW	192.168.41.10	
□	NEW	192.168.41.10	

192.168.41.10
IP: 192.168.41.10
MAC: 00:50:56:2d:ec:17

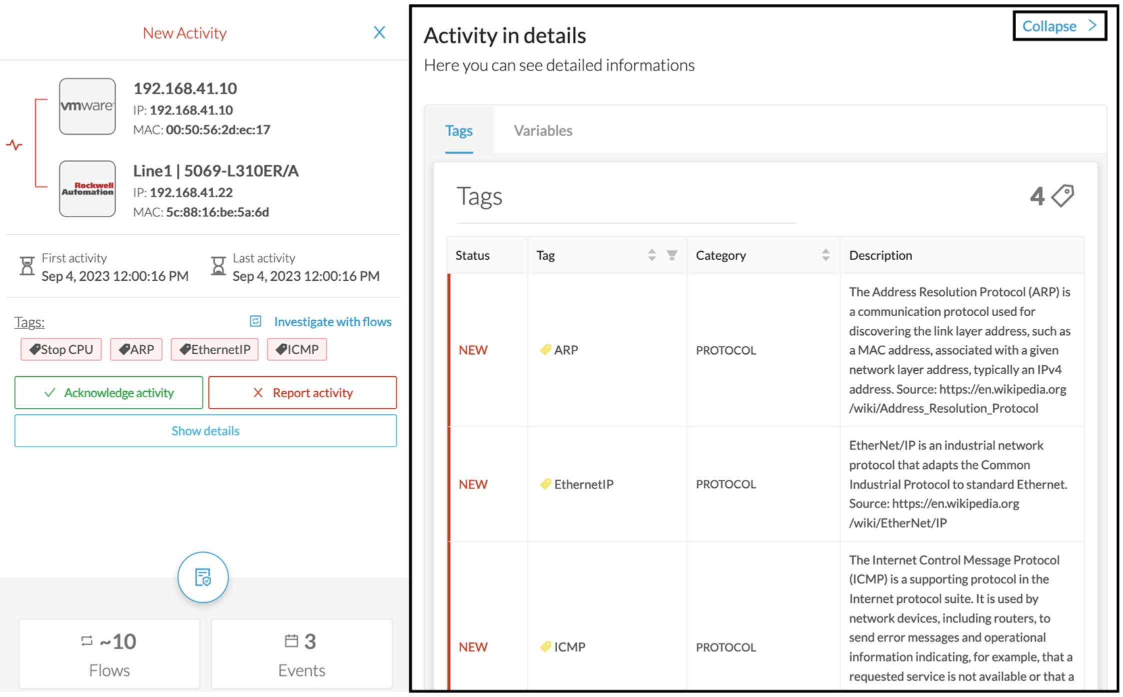
Line1 | 5069-L310ER/A
IP: 192.168.41.22
MAC: 5c:88:16:be:5a:6d

First activity
Sep 4, 2023 12:00:16 PM

Last activity
Sep 4, 2023 12:00:16 PM

Tags:
Stop CPU
ARP
EthernetIP
ICMP

Click **Show details** for more information. The example below shows the activity tags with the category they belong to and their description.



New Activity

192.168.41.10
IP: 192.168.41.10
MAC: 00:50:56:2d:ec:17

Line1 | 5069-L310ER/A
IP: 192.168.41.22
MAC: 5c:88:16:be:5a:6d

First activity
Sep 4, 2023 12:00:16 PM

Last activity
Sep 4, 2023 12:00:16 PM

Tags: Stop CPU, ARP, EthernetIP, ICMP

Investigate with flows

✓ Acknowledge activity | ✕ Report activity

Show details

~10 Flows | 3 Events

Activity in details

Here you can see detailed informations

Collapse >

Tags | Variables

Tags 4

Status	Tag	Category	Description
NEW	ARP	PROTOCOL	The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given network layer address, typically an IPv4 address. Source: https://en.wikipedia.org /wiki/Address_Resolution_Protocol
NEW	EthernetIP	PROTOCOL	EtherNet/IP is an industrial network protocol that adapts the Common Industrial Protocol to standard Ethernet. Source: https://en.wikipedia.org /wiki/EtherNet/IP
NEW	ICMP	PROTOCOL	The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a

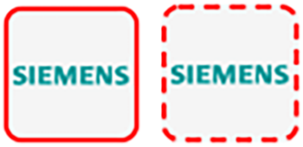
Click **Collapse** to return to the initial view.

To deeply analyze, click Investigate with flows.

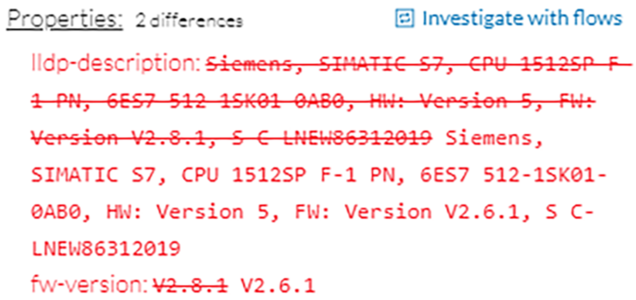
New and changed differences

When **Monitor mode** detects a difference, it appears in red. There are two types of differences: new and changed. A component, an activity, a tag, a property, and a variable access can appear (new) or evolve (change). Below are a few examples of how **Monitor mode** represents differences.

A new component (plain red) and a changed component (hyphenated red)



Changed properties of a component, with the former crossed out property

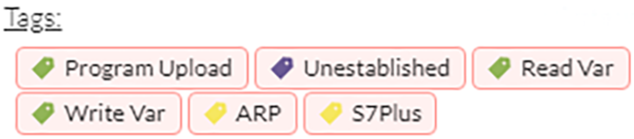


Properties: 2 differences

lldp-description: ~~Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512 1SK01 0AB0, HW: Version 5, FW: Version V2.8.1, S C-LNEW86312019~~ Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019

fw-version: ~~V2.8.1~~ V2.6.1

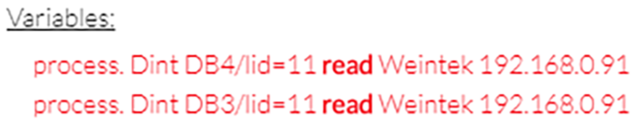
New and changed component and activity tags



Tags:

Program Upload | Unestablished | Read Var | Write Var | ARP | S7Plus

New and changed variable access of the activity list



Variables:

process. Dint DB4/lid=11 **read** Weintek 192.168.0.91

process. Dint DB3/lid=11 **read** Weintek 192.168.0.91

Review each difference to identify a potential threat and refine the baseline. Refer to the section Review differences, on page 15.

CHAPTER 2

Create baselines

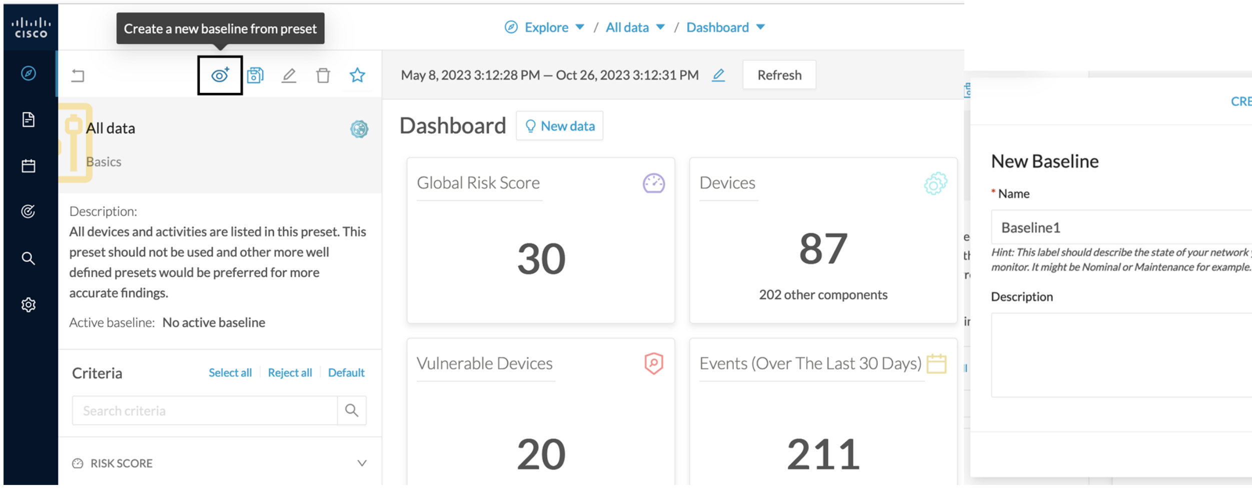
Create and setup a baseline

Procedure

Step 1 Click **Explore** from the left panel.

Step 2 Click **Basics**, click the **All data** preset.

Step 3 Click the **Create a new baseline from preset** button.



Description:
All devices and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline

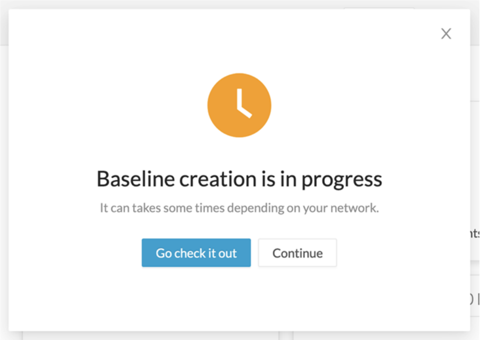
* Name: Baseline1

Hint: This label should describe the state of your network monitor. It might be Nominal or Maintenance for example.

Description

Step 4 Type in **Name**.

Step 5 Click **Create**. The Baseline creation window appears.



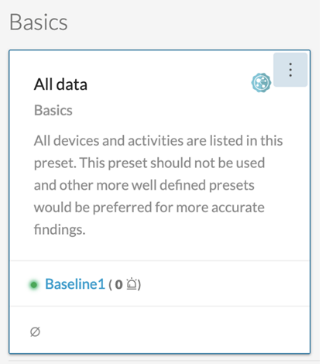
Baseline creation is in progress

It can takes some times depending on your network.

Step 6 Click **Continue**.

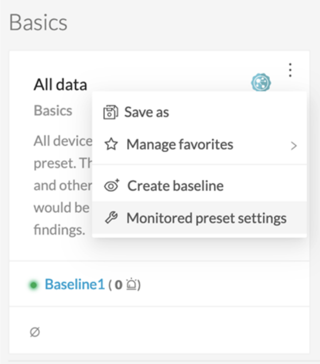
Step 7 Access the **Monitor** page.

On the All data preset, the new baseline appears.

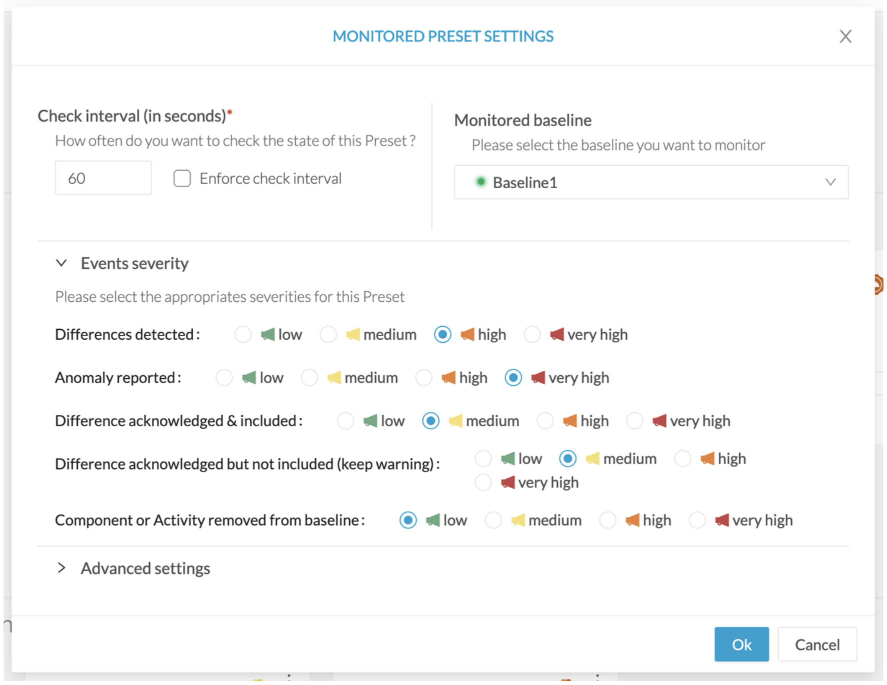


All devices and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Step 8 Click **three dots icon** > **Monitor preset settings**.



Change the **Check Interval** frequency and the **Events severity** preset state, if necessary.



MONITORED PRESET SETTINGS

Check interval (in seconds)*

How often do you want to check the state of this Preset ?

60 □ Enforce check interval

Monitored baseline

Please select the baseline you want to monitor

● Baseline1

Events severity

Please select the appropriates severities for this Preset

Differences detected : ○ low ○ medium ● high ○ very high

Anomaly reported : ○ low ○ medium ○ high ● very high

Difference acknowledged & included : ○ low ● medium ○ high ○ very high

Difference acknowledged but not included (keep warning) : ○ low ● medium ○ high ○ very high

Component or Activity removed from baseline : ● low ○ medium ○ high ○ very high

Advanced settings

In **Advanced settings**, select the type of differences about which you want to be alerted. This is useful to:

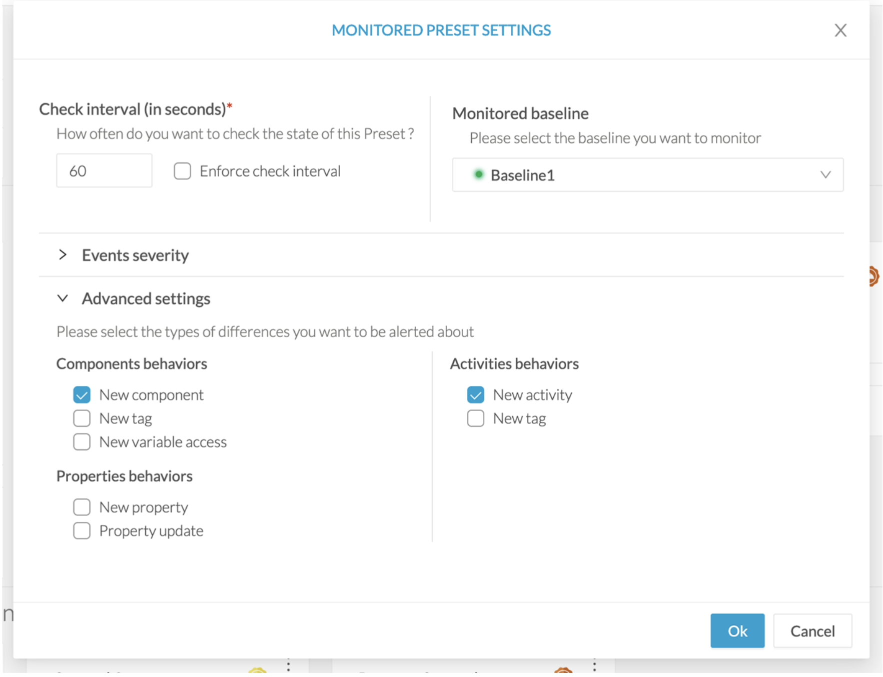
- Drastically reduce the number of differences found to facilitate results treatment.

  Refer to Review differences, on page 15.

- Target the type of information that are really relevant to your organization.

  For each behavior type, select the type of information to be checked: components, activities, tags, variable access, and properties. For more information about these concepts, refer to the Cisco Cyber Vision GUI User Guide.

- Set up a preset monitoring with a more advanced approach. Refer to the use case Tracking sensitive assets properties, on page 31.



MONITORED PRESET SETTINGS

Check interval (in seconds)*
How often do you want to check the state of this Preset ?
60 □ Enforce check interval

Monitored baseline
Please select the baseline you want to monitor
● Baseline1

> Events severity

∨ Advanced settings

Please select the types of differences you want to be alerted about

Components behaviors
☑ New component
□ New tag
□ New variable access

Properties behaviors
□ New property
□ Property update

Activities behaviors
☑ New activity
□ New tag

Step 9 Click **Ok**.

Create a baseline from a default preset

Procedure

Step 1 Access the **Explore** page.

Step 2 In **Basics**, click the **Essential data** preset.

Step 3 Click **Add a new baseline from preset**.

Step 4 Click **Go check it out**.

Step 5 All elements display. Some components and activities may already appear in red as new or changed.

Create a baseline from a group

To create groups:

Procedure

Step 1 Access the **All data preset**.

Step 2 Create two groups of components.

Example:

Create a group HMI and a group PLC.

To create presets from groups:

Step 3 In criteria, access the groups filter and select the first one of the group you created.

Example:

Select the HMI group in the filter.

The HMI group displays in the map with its related activities.

Step 4 Create a preset from this view.

Step 5 Click **Save as** and name the preset HMI.

Step 6 Repeat the previous steps for the PLC group.

Step 7 Go to **All Presets**. You will see your two new presets.

To create a baseline from presets:

Step 8 Access the **HMI preset**.

Step 9 Click **Add a new baseline from preset**.

Step 10 Name it HMI.

Step 11 Repeat the previous steps for the PLC preset.

Step 12 Access **Monitor mode**. You will see your two new baselines.

Create a weekend baseline

Create a baseline to monitor the network during weekends.

Procedure

Step 1 Access **All data preset**.

Step 2 Set the period for the weekend. For example, from Friday 5 p.m. to Monday 4 a.m.

Step 3 Click **Add a new baseline from preset**.

Step 4 Name the baseline "All data weekend" and add the description "Must be active from Friday 5 p.m. until Monday 4 a.m."

Enable a baseline monitoring

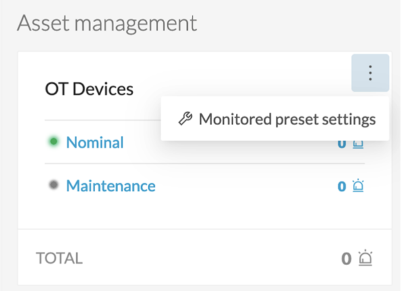
To use **Monitor mode** effectively, create several baselines per preset. However, only one baseline can be active at a time per preset. This is because a baseline monitors a well-defined network process during a specific period of time (e.g., baselines Normal operating mode, Maintenance, Week-end, Night). Two baselines cannot happen at the same time on a preset. Enable the proper baseline as the network enters a new operating phase. When you enable a baseline on a preset, the active one is automatically disabled.

To enable a baseline:

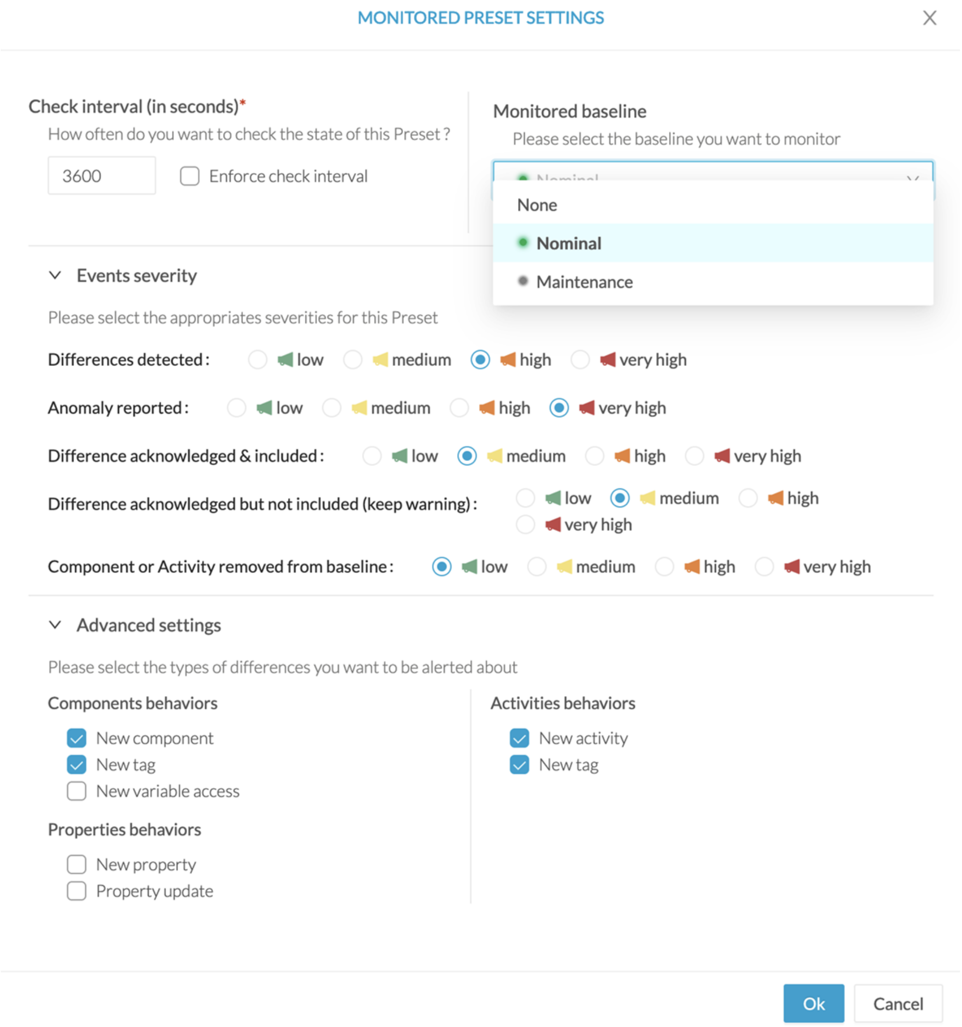
Procedure

Step 1 Access the **Monitor** page.

Step 2 Select the preset. Click **monitored preset settings**.



Step 3 In **Monitored baseline**, select the baseline.



MONITORED PRESET SETTINGS

Check interval (in seconds)*

How often do you want to check the state of this Preset ?

3600 □ Enforce check interval

Monitored baseline

Please select the baseline you want to monitor

- None
- Nominal
- Maintenance

Events severity

Please select the appropriates severities for this Preset

Differences detected : ○ low ○ medium ● high ○ very high

Anomaly reported : ○ low ○ medium ○ high ● very high

Difference acknowledged & included : ○ low ● medium ○ high ○ very high

Difference acknowledged but not included (keep warning) : ○ low ● medium ○ high ○ very high

Component or Activity removed from baseline : ● low ○ medium ○ high ○ very high

Advanced settings

Please select the types of differences you want to be alerted about

Components behaviors

- ☑ New component
- ☑ New tag
- □ New variable access

Properties behaviors

- □ New property
- □ Property update

Activities behaviors

- ☑ New activity
- ☑ New tag

For difference types, only new components, component tags, activity and activity tags are enabled by default.

You can disable some of these differences to focus the monitoring or enable other options, if needed.

Step 4 Click **Ok**.

The selected baseline turns green and is enabled.

CHAPTER 3

Review differences

Acknowledge differences

Acknowledge in the Monitor mode

Use the **Acknowledge** action to indicate that determined behaviors or differences are safe and normal and are included in the baseline. You can acknowledge differences on any element of **Monitor mode**: tags, properties, variable accesses, components, activities, and baselines.

Acknowledge a component or an activity

If the behavior is notified as changed, **Acknowledge** displays in the UI. If the behavior of a component or an activity is **new**, determine if the behavior is exceptional or part of an iterative process.

- **Acknowledge & Include**

  Use this action for a behavior which is part of a normal process and happens regularly, over time. This action includes this behavior into the current baseline. If the component or the activity changes, for example if a new tag is detected, **Monitor mode** alerts you. The item changes to red and hyphenated. This action is useful to refine a baseline as it evolves over time.

  Ex: Perform this action on a new machine installed in the network, or a new activity due to a new supported protocol.

- **Acknowledge & Keep Warning**

  Use this action when a behavior is punctual and not part of a process. Consider these behaviors as unusual, but not abnormal because they do not have a bad impact on the network. **Acknowledge & Keep Warning** acknowledges and clears the behavior, but the behaviors are not included into the baseline. If the behavior happens again, you'll be notified of a new behavior in the monitored baseline.

  Ex: Perform this action on a new component and a new activity due to an exceptional maintenance act.

Report differences

Use this action on a difference that is an anomaly, a behavior that is abnormal and may compromise the operating capability and security of the network. Before reporting the anomaly, investigate and resolve it, if possible. When reporting an anomaly, supply the incident response or acknowledgment (incident details, potential threats, or how it has been fixed). Once an anomaly is reported, it is cleared and not included in the baseline, and an event is generated with a default severity level higher than the acknowledge action. If the incident happens again, you are alerted in **Monitor mode**.

Remove and keep warning

Use this action to remove the component or activity from the current baseline so you do not see it anymore. You are alerted if the component or activity returns. The difference will appear as **new**. This action is also available on variable accesses through Individual acknowledgment.

Note If a difference keeps returning in a baseline and you don't want to see it, modify the preset.

Individual acknowledgment

Cisco Cyber Vision has **Advanced Settings** which includes **Individual acknowledgment**. This feature is available on changed components and activities, or elements already included in a baseline. It allows you to access their details to perform a deep behavior review by Acknowledge differences and Remove and keep warning. The differences on the network are detected one by one. **Individual acknowledgment** is available on the properties and tags of the components and on the tags and variable accesses of the activities.

- **Component properties**

  New and changed properties display in red. For changed properties, the former one is crossed out and the new one displays next to it. They display in red, unless you acknowledge them.

- **Component and activity tags**

  New and changed tags display in red. They clear when you acknowledge or report them. They are no longer displayed in red.

- **Activity variable accesses**

  New and changed variable accesses display in red. A variable access can be acknowledged, reported, and deleted (use "**Remove and keep warning**"). Delete a variable access when it should not be part of the current baseline and you don't want to see it. It gets removed from the baseline and disappears. If the variable access happens again, you are alerted and it displays in red.

Once you review all component or elements of the activities (acknowledged, reported, or removed), the entity they belong to is cleared. The component or activity is no longer displayed in red. Any action performed in **Monitor mode** appear in the **Event** page.

Investigate with flows

This button is not an action but an option to get more information and context about the differences detected on the network. In fact, each difference found, since it belongs to a component or an activity, is related to a flow. This view allows you to perform forensic analysis and may give you some clues to understand what happened.

Ex: You can search from which flow exactly a tag comes from.

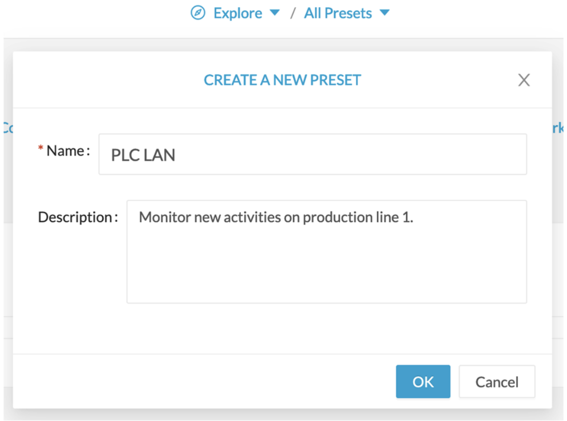
CHAPTER 4

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.

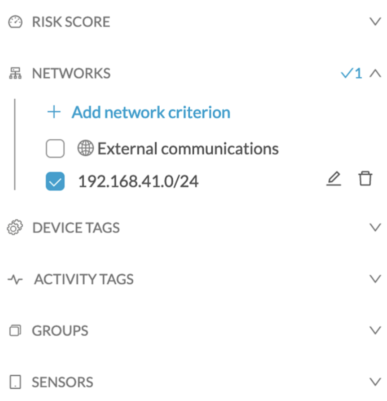
To monitor, access the **Explore** page and create a new PLC LAN **preset**.



*Name: PLC LAN

Description: Monitor new activities on production line 1.

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



RISK SCORE

NETWORKS ✓1

+ Add network criterion

□ External communications

☑ 192.168.41.0/24

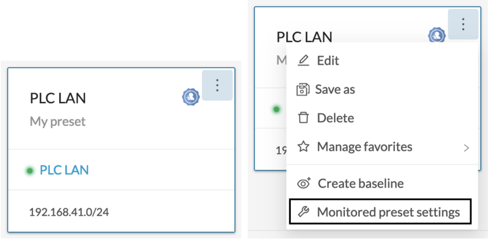
DEVICE TAGS

ACTIVITY TAGS

GROUPS

SENSORS

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



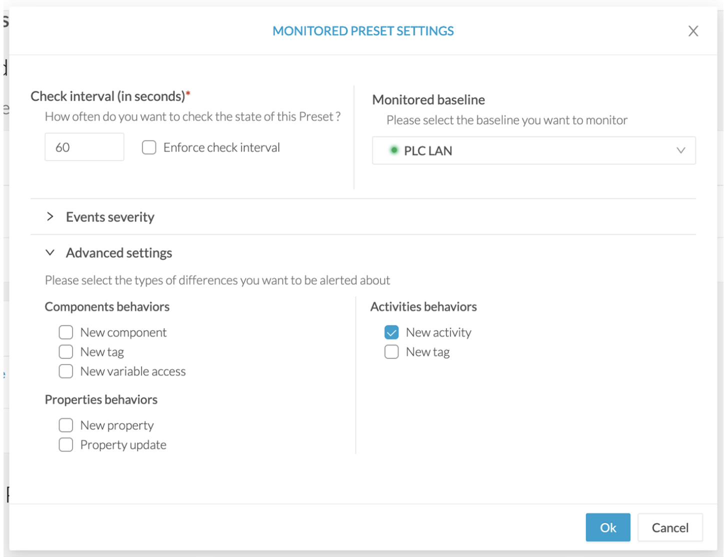
PLC LAN

My preset

● PLC LAN

192.168.41.0/24

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



MONITORED PRESET SETTINGS

Check interval (in seconds)*

How often do you want to check the state of this Preset ?

60 □ Enforce check interval

Monitored baseline

Please select the baseline you want to monitor

● PLC LAN

Events severity

Advanced settings

Please select the types of differences you want to be alerted about

Components behaviors

□ New component

□ New tag

□ New variable access

Properties behaviors

□ New property

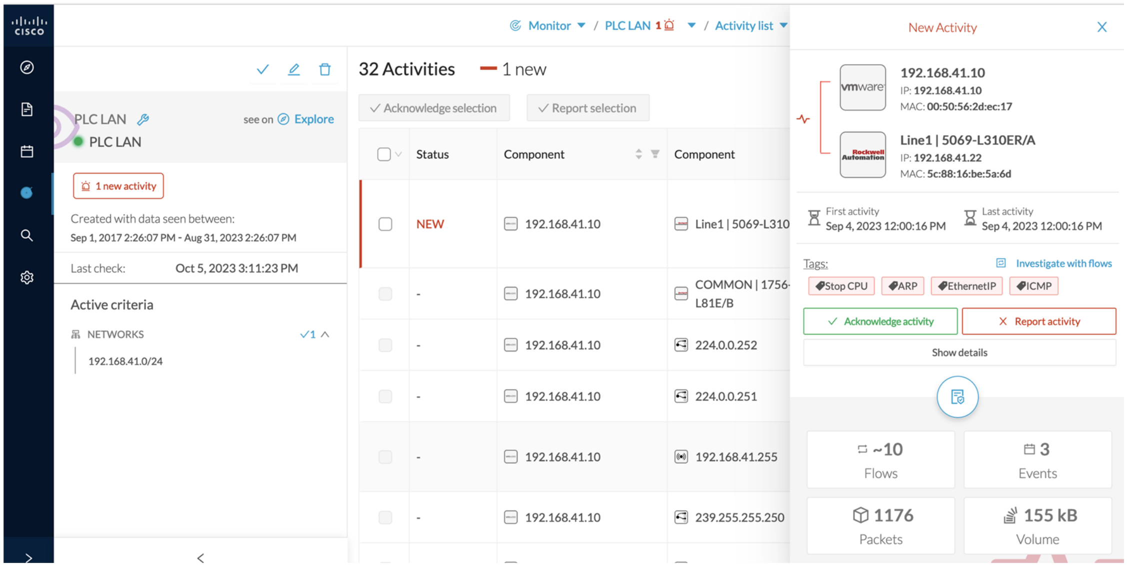
□ Property update

Activities behaviors

☑ New activity

□ New tag

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



Monitor / PLC LAN 1 / Activity list

PLC LAN — see on Explore

PLC LAN

1 new activity

Created with data seen between:
Sep 1, 2017 2:26:07 PM - Aug 31, 2023 2:26:07 PM

Last check: Oct 5, 2023 3:11:23 PM

Active criteria

NETWORKS ✓1
192.168.41.0/24

32 Activities — 1 new

✓ Acknowledge selection ✓ Report selection

□	Status	Component	Component
□	NEW	192.168.41.10	Line1 | 5069-L310
□	-	192.168.41.10	COMMON | 1756-L81E/B
□	-	192.168.41.10	224.0.0.252
□	-	192.168.41.10	224.0.0.251
□	-	192.168.41.10	192.168.41.255
□	-	192.168.41.10	239.255.255.250

New Activity

192.168.41.10
IP: 192.168.41.10
MAC: 00:50:56:2d:ec:17

Line1 | 5069-L310ER/A
IP: 192.168.41.22
MAC: 5c:88:16:be:5a:6d

First activity: Sep 4, 2023 12:00:16 PM
Last activity: Sep 4, 2023 12:00:16 PM

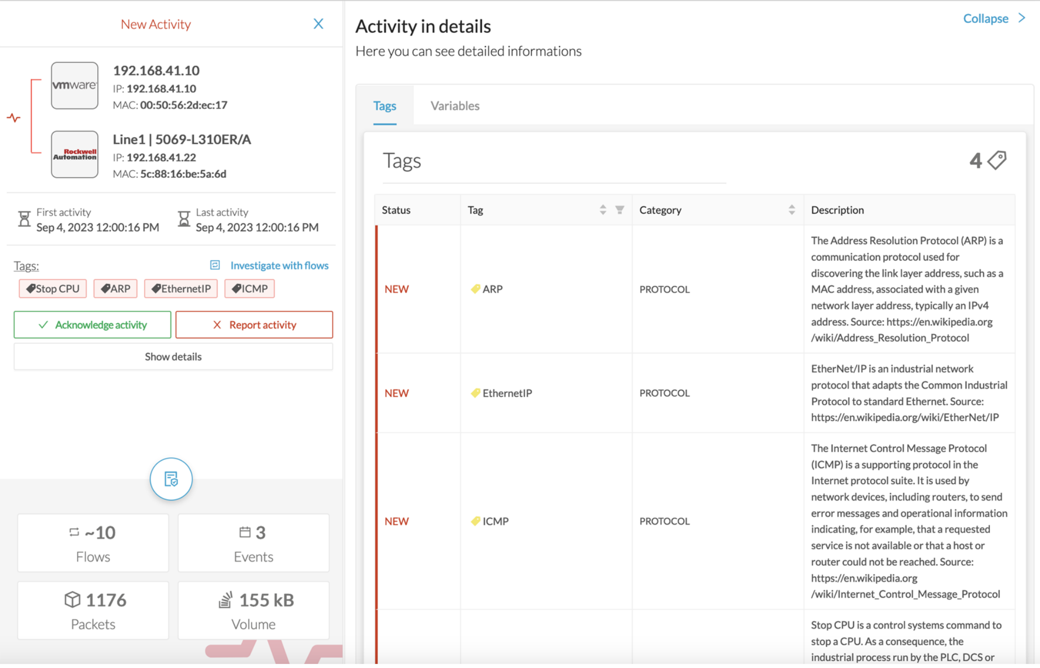
Tags: Stop CPU, ARP, EthernetIP, ICMP — Investigate with flows

✓ Acknowledge activity   X Report activity

Show details

~10 Flows | 3 Events | 1176 Packets | 155 kB Volume

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



New Activity

192.168.41.10
IP: 192.168.41.10
MAC: 00:50:56:2d:ec:17

Line1 | 5069-L310ER/A
IP: 192.168.41.22
MAC: 5c:88:16:be:5a:6d

First activity: Sep 4, 2023 12:00:16 PM
Last activity: Sep 4, 2023 12:00:16 PM

Tags: Stop CPU, ARP, EthernetIP, ICMP — Investigate with flows

✓ Acknowledge activity   X Report activity

Show details

~10 Flows | 3 Events | 1176 Packets | 155 kB Volume

Activity in details — Collapse
Here you can see detailed informations

Tags | Variables

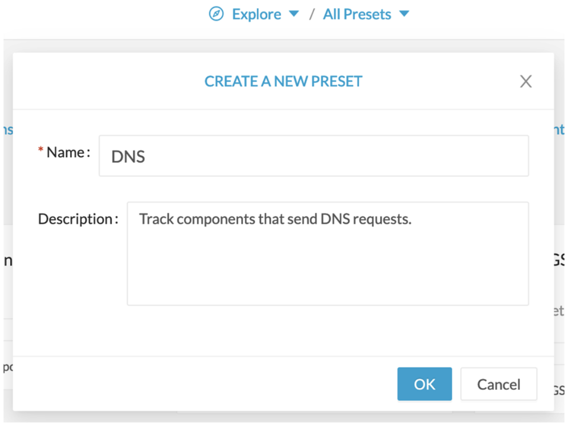
Tags — 4

Status	Tag	Category	Description
NEW	ARP	PROTOCOL	The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given network layer address, typically an IPv4 address. Source: https://en.wikipedia.org/wiki/Address_Resolution_Protocol
NEW	EthernetIP	PROTOCOL	EtherNet/IP is an industrial network protocol that adapts the Common Industrial Protocol to standard Ethernet. Source: https://en.wikipedia.org/wiki/EtherNet/IP
NEW	ICMP	PROTOCOL	The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached. Source: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
			Stop CPU is a control systems command to stop a CPU. As a consequence, the industrial process run by the PLC, DCS or

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.

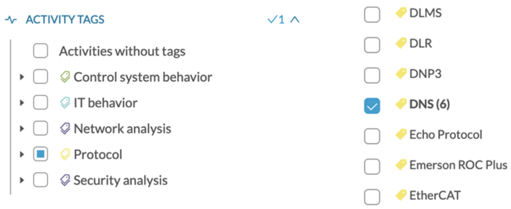
On the **Explore page** > **Create a new preset**.



* Name: DNS

Description: Track components that send DNS requests.

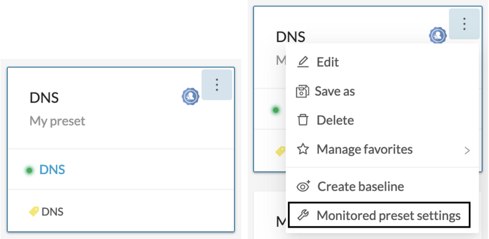
In the **Activity tags** filter > select **protocol DNS** .



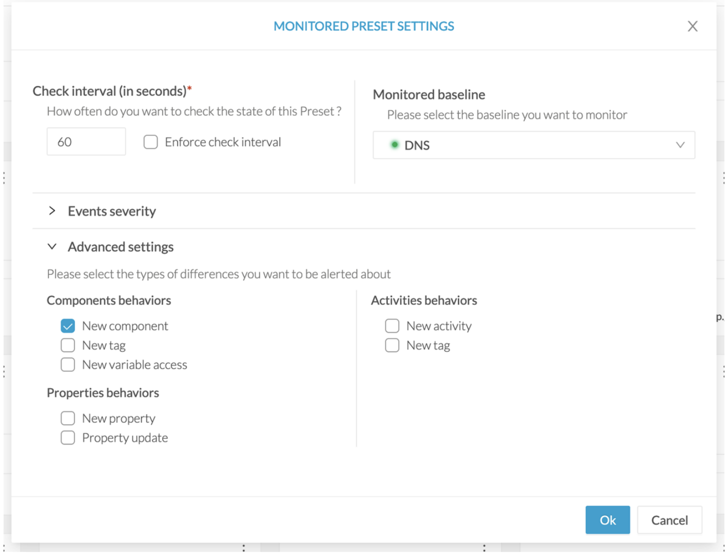
- □ Activities without tags
- □ Control system behavior
- □ IT behavior
- □ Network analysis
- ▣ Protocol
- □ Security analysis

- □ DLMS
- □ DLR
- □ DNP3
- ☑ DNS (6)
- □ Echo Protocol
- □ Emerson ROC Plus
- □ EtherCAT

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



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



MONITORED PRESET SETTINGS

Check interval (in seconds)*
How often do you want to check the state of this Preset ?
60 □ Enforce check interval

Monitored baseline
Please select the baseline you want to monitor
● DNS

› Events severity

⌄ Advanced settings

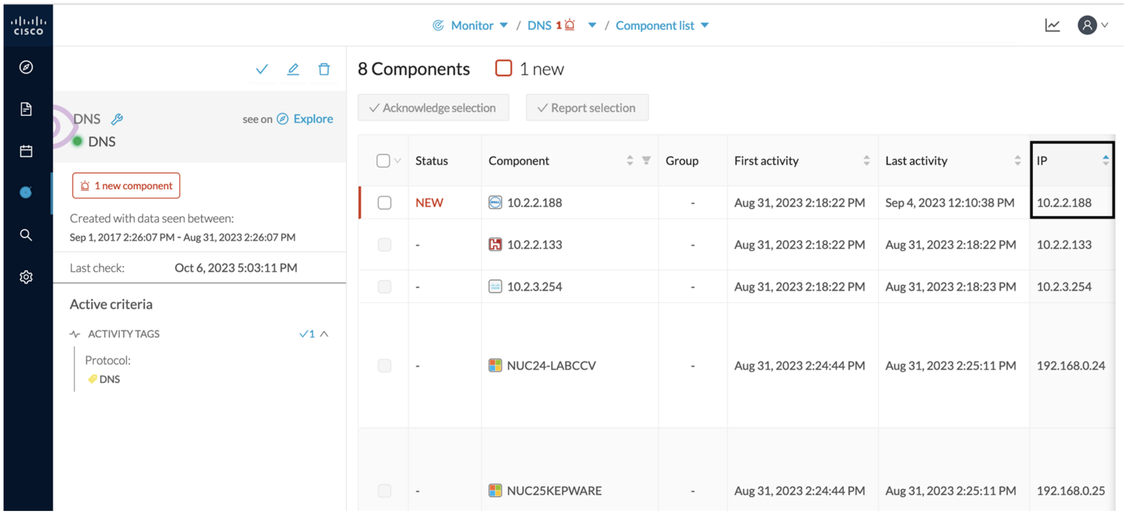
Please select the types of differences you want to be alerted about

Components behaviors
☑ New component
□ New tag
□ New variable access

Properties behaviors
□ New property
□ Property update

Activities behaviors
□ New activity
□ New tag

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



DNS
● DNS
see on Explore

1 new component

Created with data seen between:
Sep 1, 2017 2:26:07 PM - Aug 31, 2023 2:26:07 PM

Last check: Oct 6, 2023 5:03:11 PM

Active criteria
ACTIVITY TAGS ✓1
Protocol:
DNS

8 Components □ 1 new

Status	Component	Group	First activity	Last activity	IP
NEW	10.2.2.188	-	Aug 31, 2023 2:18:22 PM	Sep 4, 2023 12:10:38 PM	10.2.2.188
-	10.2.2.133	-	Aug 31, 2023 2:18:22 PM	Aug 31, 2023 2:18:22 PM	10.2.2.133
-	10.2.3.254	-	Aug 31, 2023 2:18:22 PM	Aug 31, 2023 2:18:23 PM	10.2.3.254
-	NUC24-LABCCV	-	Aug 31, 2023 2:24:44 PM	Aug 31, 2023 2:25:11 PM	192.168.0.24
-	NUC25KEPWARE	-	Aug 31, 2023 2:24:44 PM	Aug 31, 2023 2:25:11 PM	192.168.0.25

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

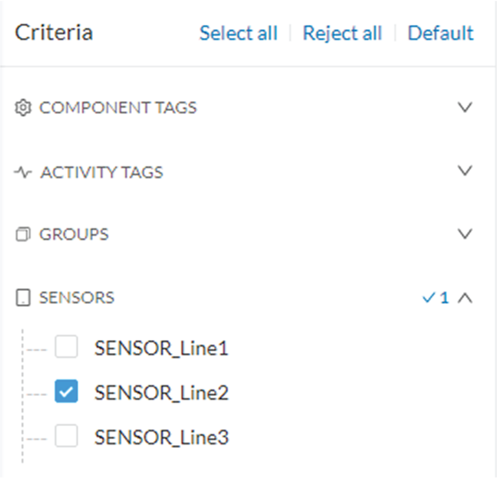
Detection of assets newly connected to the network

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.


Criteria
Select all | Reject all | Default

COMPONENT TAGS

ACTIVITY TAGS

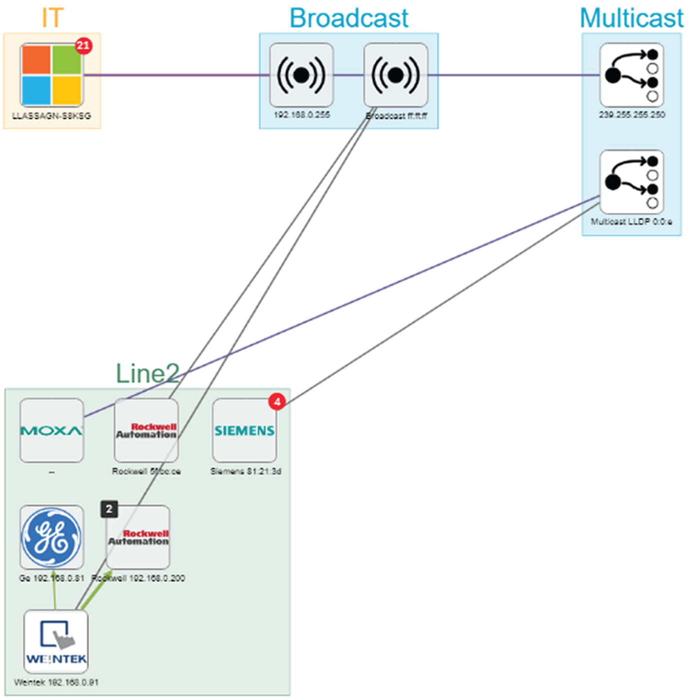
GROUPS

SENSORS ✓1

- ☐ SENSOR_Line1
- ☑ SENSOR_Line2
- ☐ SENSOR_Line3

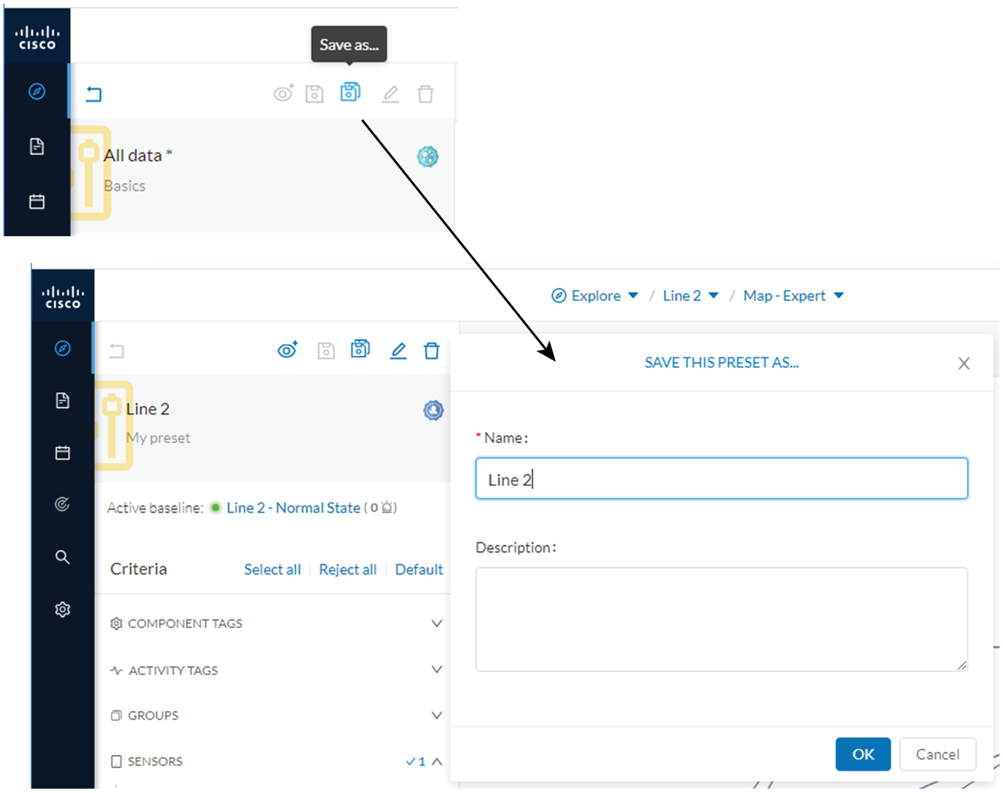
Organize the components into groups, per function:

- 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.**

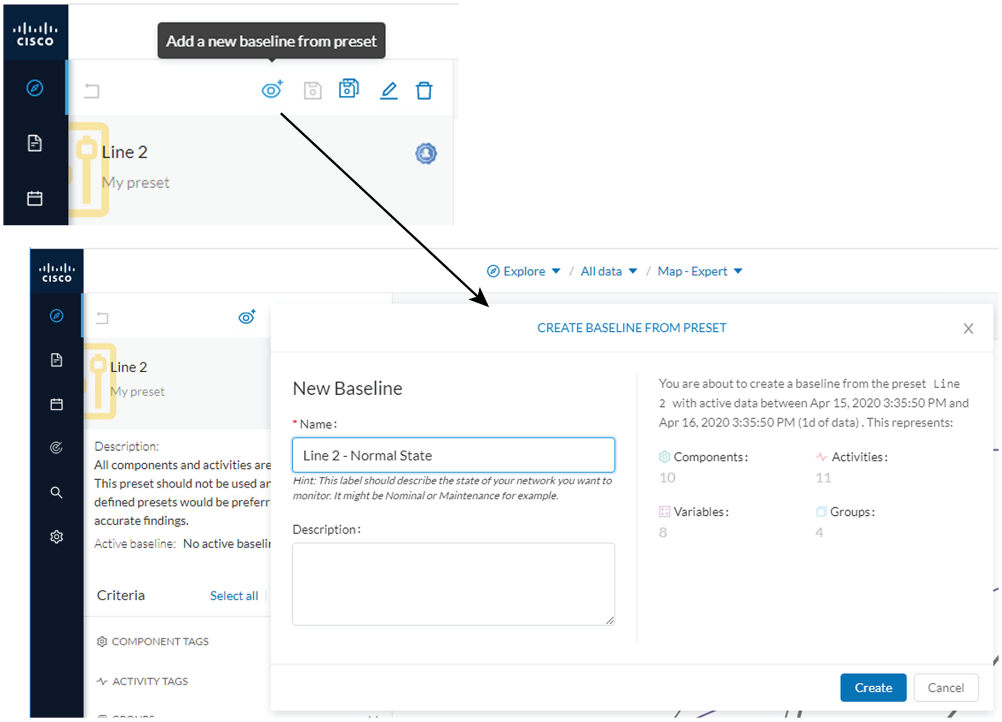


SAVE THIS PRESET AS...

* Name: Line 2

Description:

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**.


Add a new baseline from preset
Line 2
My preset
Explore / All data / Map - Expert
CREATE BASELINE FROM PRESET
Criteria
Select all
COMPONENT TAGS
ACTIVITY TAGS
Create
Cancel

Description:
All components and activities are
This preset should not be used ar
defined presets would be preferr
accurate findings.
Active baseline: No active baselir

New Baseline

* Name: Line 2 - Normal State

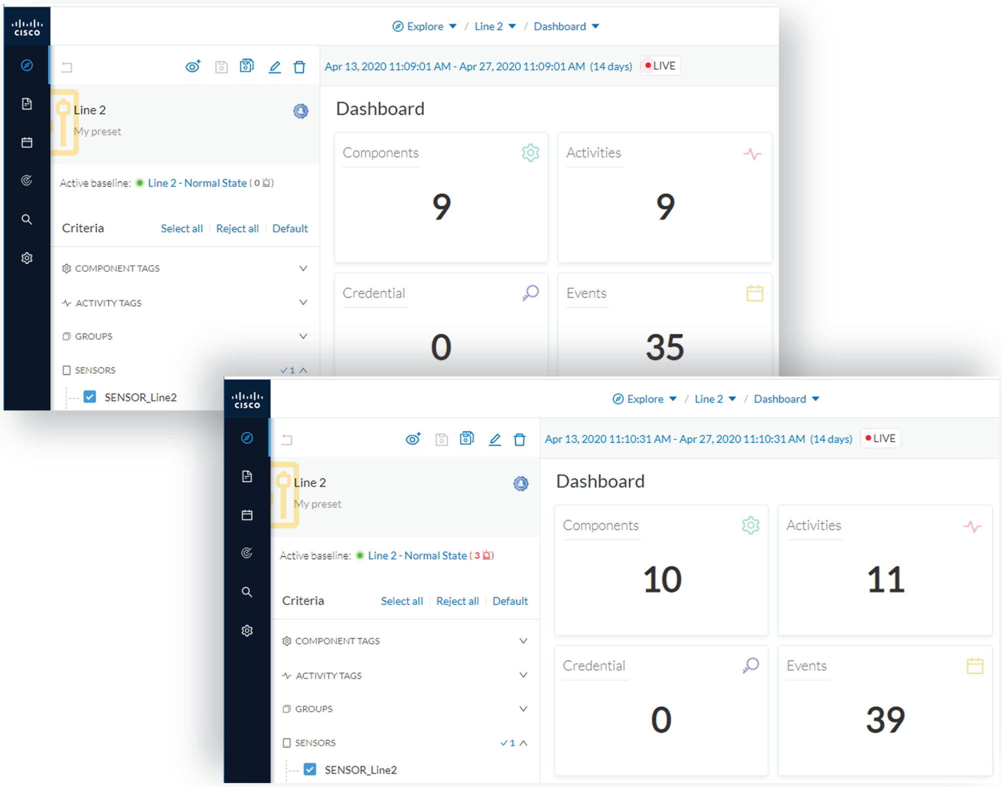
Hint: This label should describe the state of your network you want to monitor. It might be Nominal or Maintenance for example.

Description:

You are about to create a baseline from the preset Line 2 with active data between Apr 15, 2020 3:35:50 PM and Apr 16, 2020 3:35:50 PM (1d of data). This represents:

Components: 10	Activities: 11
Variables: 8	Groups: 4

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.

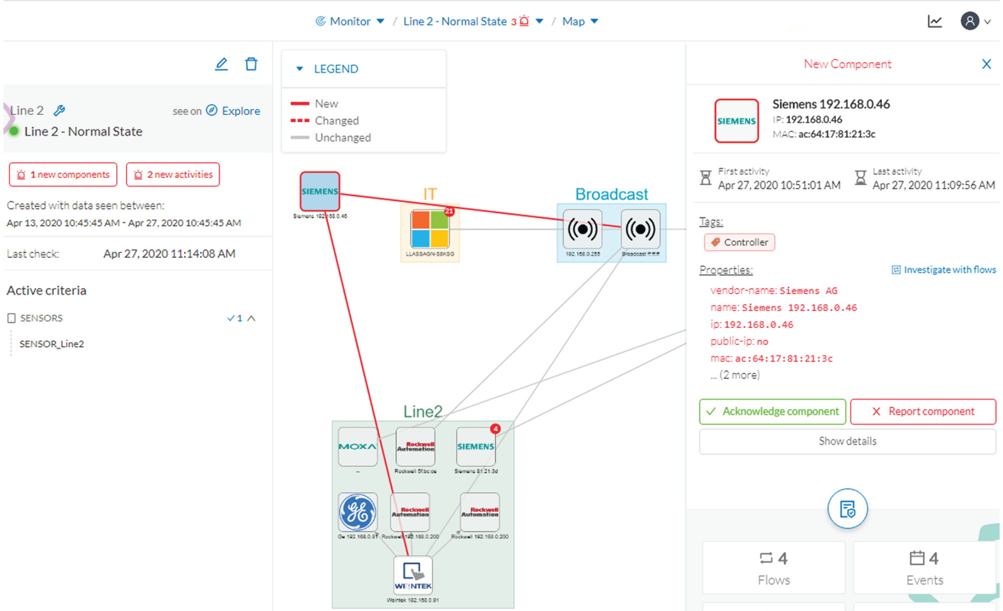

Explore / Line 2 / Dashboard
Apr 13, 2020 11:09:01 AM - Apr 27, 2020 11:09:01 AM (14 days) ● LIVE
Line 2
My preset
Active baseline: Line 2 - Normal State (0)
Criteria Select all Reject all Default
COMPONENT TAGS
ACTIVITY TAGS
GROUPS
SENSORS ✓1
☑ SENSOR_Line2
Dashboard
Components 9
Activities 9
Credential 0
Events 35
Explore / Line 2 / Dashboard
Apr 13, 2020 11:10:31 AM - Apr 27, 2020 11:10:31 AM (14 days) ● LIVE
Line 2
My preset
Active baseline: Line 2 - Normal State (3)
Criteria Select all Reject all Default
COMPONENT TAGS
ACTIVITY TAGS
GROUPS
SENSORS ✓1
☑ SENSOR_Line2
Dashboard
Components 10
Activities 11
Credential 0
Events 39

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.



Line 2
Line 2 - Normal State
see on Explore

1 new components
2 new activities

Created with data seen between:
Apr 13, 2020 10:45:45 AM - Apr 27, 2020 10:45:45 AM

Last check: Apr 27, 2020 11:14:08 AM

Active criteria

SENSORS ✓1
SENSOR_Line2

New Component

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

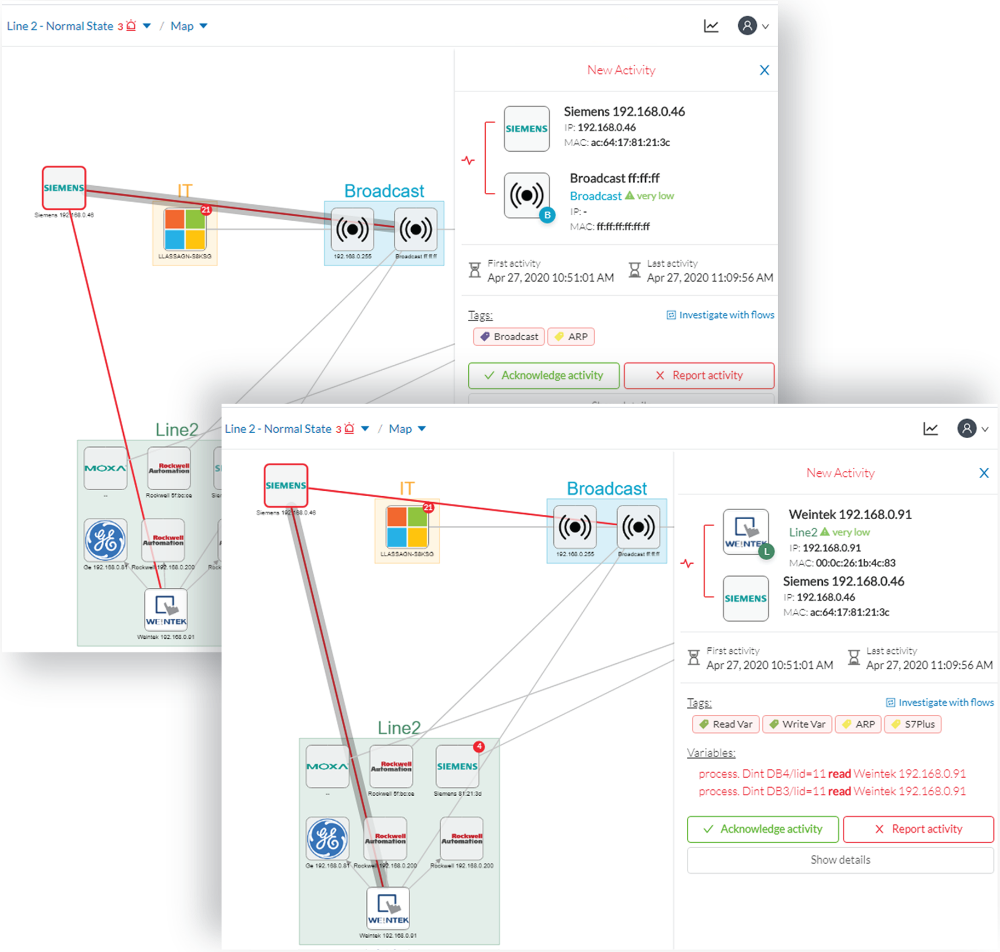
First activity Apr 27, 2020 10:51:01 AM
Last activity Apr 27, 2020 11:09:56 AM

Tags:
Controller

Properties: Investigate with flows
vendor-name: Siemens AG
name: Siemens 192.168.0.46
ip: 192.168.0.46
public-ip: no
mac: ac:64:17:81:21:3c
... (2 more)

✓ Acknowledge component
X Report component
Show details

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.



New Activity

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

Broadcast ff:ff:ff
Broadcast very low
IP: -
MAC: ff:ff:ff:ff:ff:ff

First activity
Apr 27, 2020 10:51:01 AM

Last activity
Apr 27, 2020 11:09:56 AM

Tags:
Broadcast
ARP

Investigate with flows

Acknowledge activity
Report activity

New Activity

Weintek 192.168.0.91
Line2 very low
IP: 192.168.0.91
MAC: 00:0c:26:1b:4c:83

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity
Apr 27, 2020 10:51:01 AM

Last activity
Apr 27, 2020 11:09:56 AM

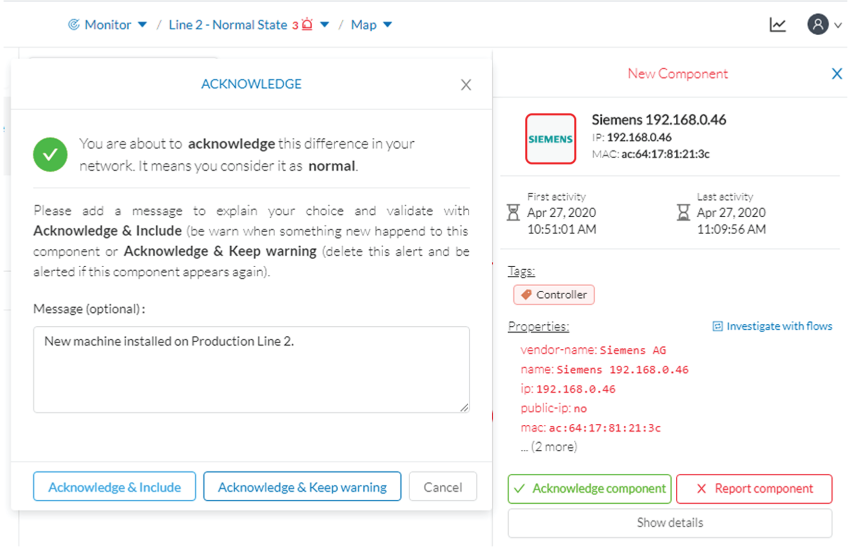
Tags:
Read Var
Write Var
ARP
S7Plus

Investigate with flows

Variables:
process. Dint DB4/lid=11 **read** Weintek 192.168.0.91
process. Dint DB3/lid=11 **read** Weintek 192.168.0.91

Acknowledge activity
Report activity
Show details

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.



You are about to **acknowledge** this difference in your network. It means you consider it as **normal**.

Please add a message to explain your choice and validate with **Acknowledge & Include** (be warn when something new happend to this component or **Acknowledge & Keep warning** (delete this alert and be alerted if this component appears again).

Message (optional) :

New machine installed on Production Line 2.

Siemens 192.168.0.46
IP: 192.168.0.46
MAC: ac:64:17:81:21:3c

First activity
Apr 27, 2020
10:51:01 AM

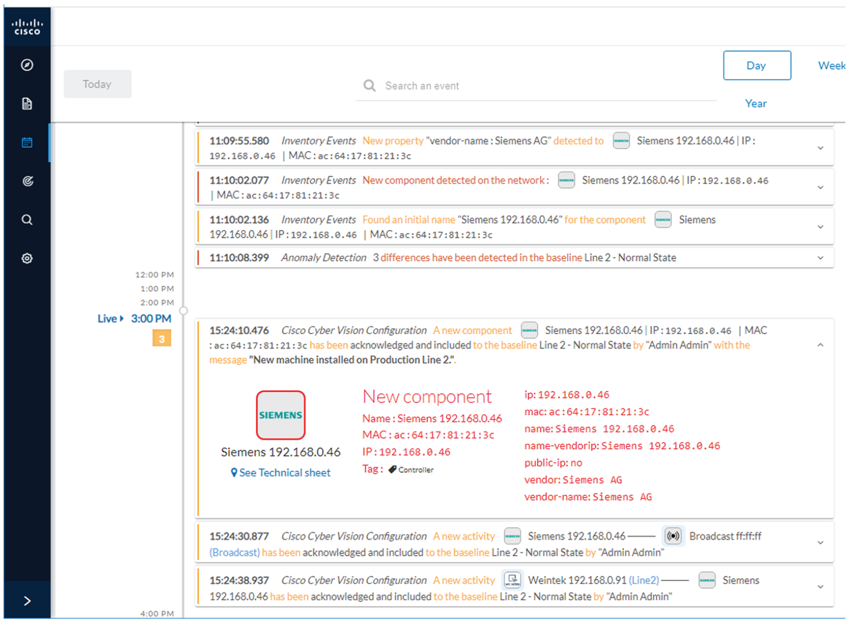
Last activity
Apr 27, 2020
11:09:56 AM

Tags:
Controller

Properties:
vendor-name: Siemens AG
name: Siemens 192.168.0.46
ip: 192.168.0.46
public-ip: no
mac: ac:64:17:81:21:3c
... (2 more)

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.



11:09:55.580 *Inventory Events* New property "vendor-name : Siemens AG" detected to Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c

11:10:02.077 *Inventory Events* New component detected on the network : Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c

11:10:02.136 *Inventory Events* Found an initial name "Siemens 192.168.0.46" for the component Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c

11:10:08.399 *Anomaly Detection* 3 differences have been detected in the baseline Line 2 - Normal State

15:24:10.476 *Cisco Cyber Vision Configuration* A new component Siemens 192.168.0.46 | IP : 192.168.0.46 | MAC : ac:64:17:81:21:3c has been acknowledged and included to the baseline Line 2 - Normal State by "Admin Admin" with the message "New machine installed on Production Line 2.".

Siemens 192.168.0.46
See Technical sheet

New component
Name : Siemens 192.168.0.46
MAC : ac:64:17:81:21:3c
IP : 192.168.0.46
Tag : Controller

ip: 192.168.0.46
mac: ac:64:17:81:21:3c
name: Siemens 192.168.0.46
name-vendorip: Siemens 192.168.0.46
public-ip: no
vendor: Siemens AG
vendor-name: Siemens AG

15:24:30.877 *Cisco Cyber Vision Configuration* A new activity Siemens 192.168.0.46 —— Broadcast ff:ff:ff (Broadcast) has been acknowledged and included to the baseline Line 2 - Normal State by "Admin Admin"

15:24:38.937 *Cisco Cyber Vision Configuration* A new activity Weintek 192.168.0.91 (Line2) —— Siemens 192.168.0.46 has been acknowledged and included to the baseline Line 2 - Normal State by "Admin Admin"

Tracking sensitive assets properties

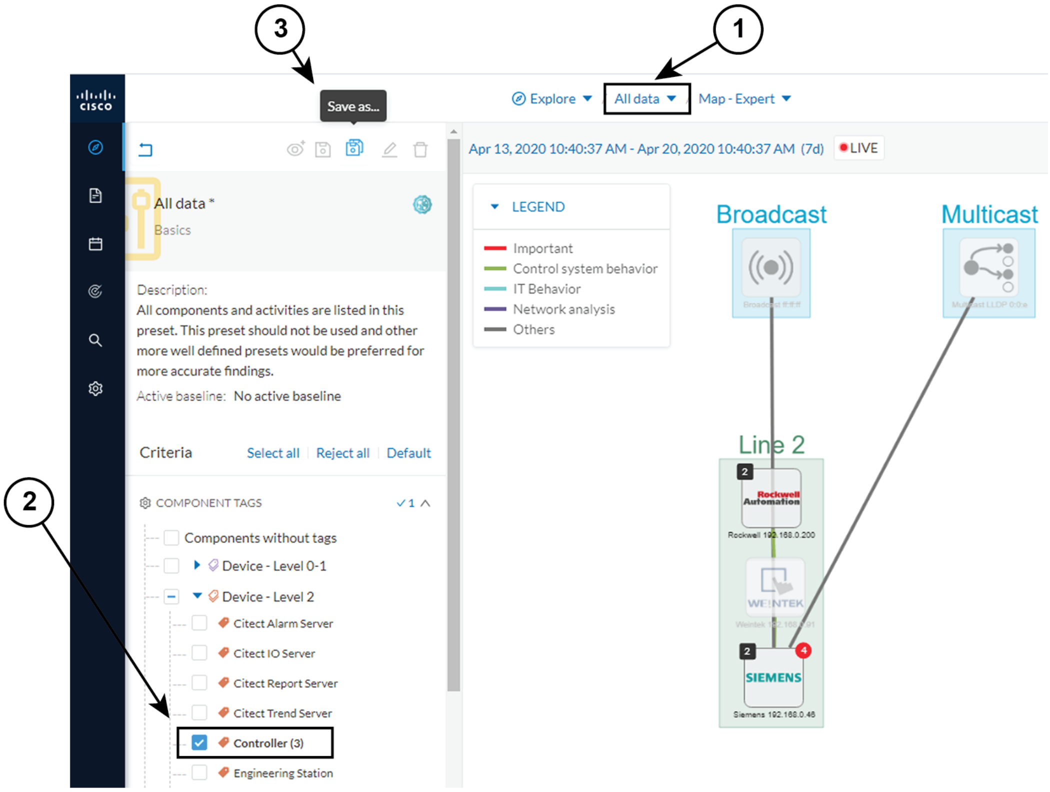
To ensure To ensure the security of the network, monitor its critical assets closely. Usually, critical assets are controllers which ensure the plant's operation. To monitor them, check the properties of the controllers. Typically, programs and firmware versions changes are properties that might cause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



Apr 13, 2020 10:40:37 AM - Apr 20, 2020 10:40:37 AM (7d) LIVE

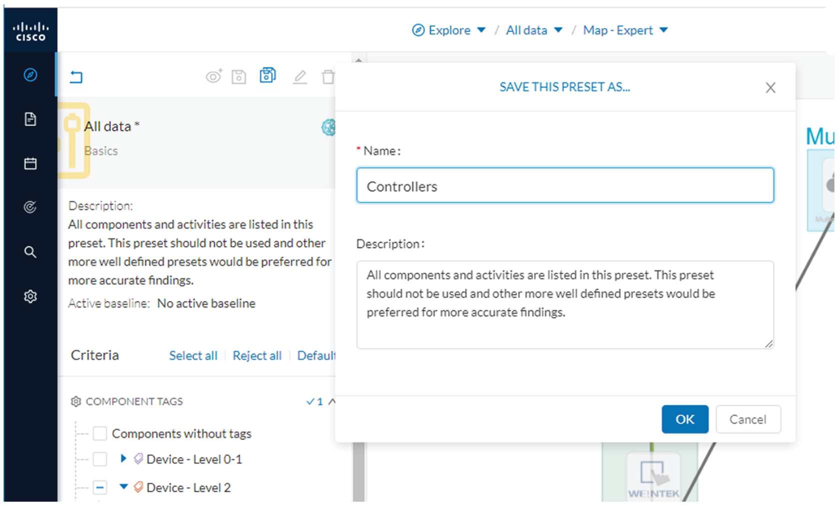
All data *
Basics

Description:
All components and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

Active baseline: No active baseline

Criteria

- □ Components without tags
- □ Device - Level 0-1
- ⊟ Device - Level 2
  - □ Citect Alarm Server
  - □ Citect IO Server
  - □ Citect Report Server
  - □ Citect Trend Server
  - ☑ Controller (3)
  - □ Engineering Station

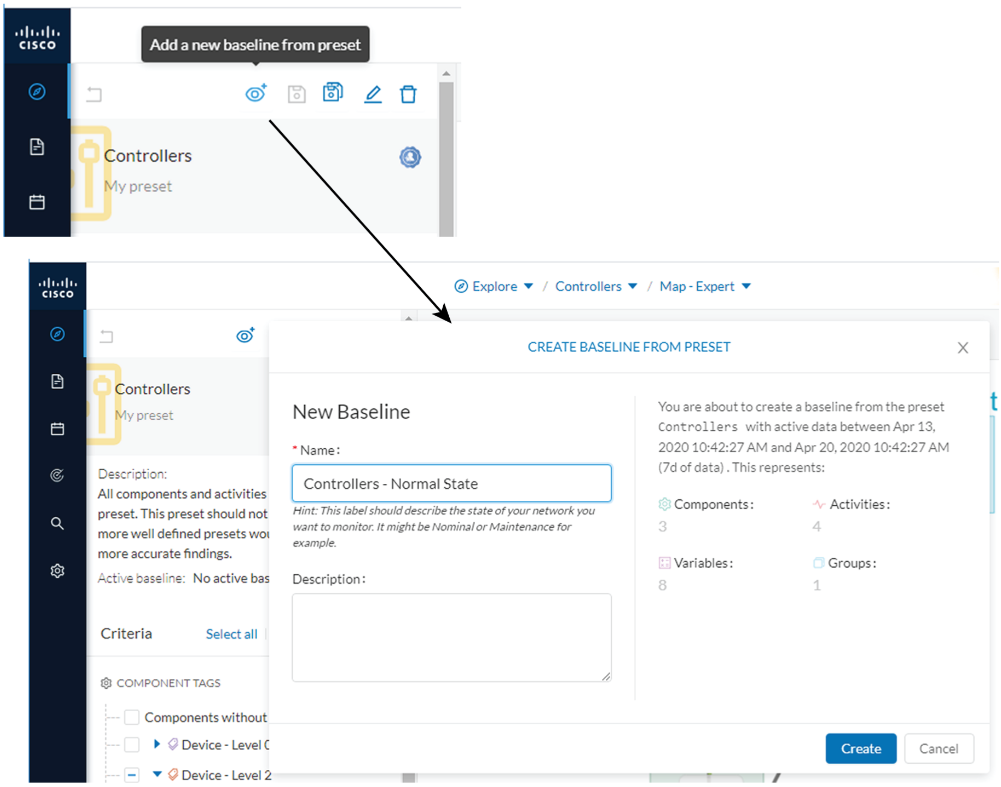


SAVE THIS PRESET AS...

* Name: Controllers

Description:
All components and activities are listed in this preset. This preset should not be used and other more well defined presets would be preferred for more accurate findings.

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**.



New Baseline

* Name: Controllers - Normal State

Hint: This label should describe the state of your network you want to monitor. It might be Nominal or Maintenance for example.

Description:

You are about to create a baseline from the preset `Controllers` with active data between Apr 13, 2020 10:42:27 AM and Apr 20, 2020 10:42:27 AM (7d of data) . This represents:

Components: 3

Activities: 4

Variables: 8

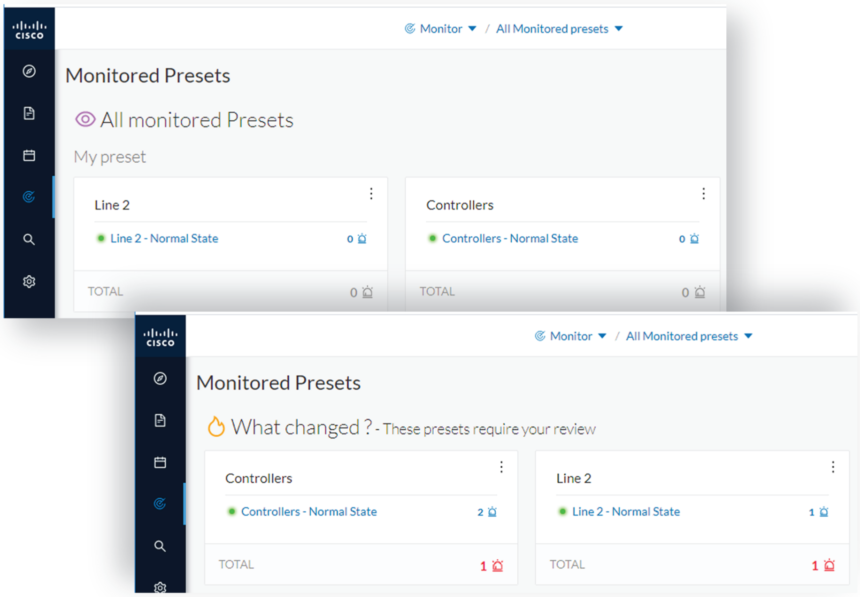
Groups: 1

Description: All components and activities preset. This preset should not more well defined presets wou more accurate findings.

Active baseline: No active bas

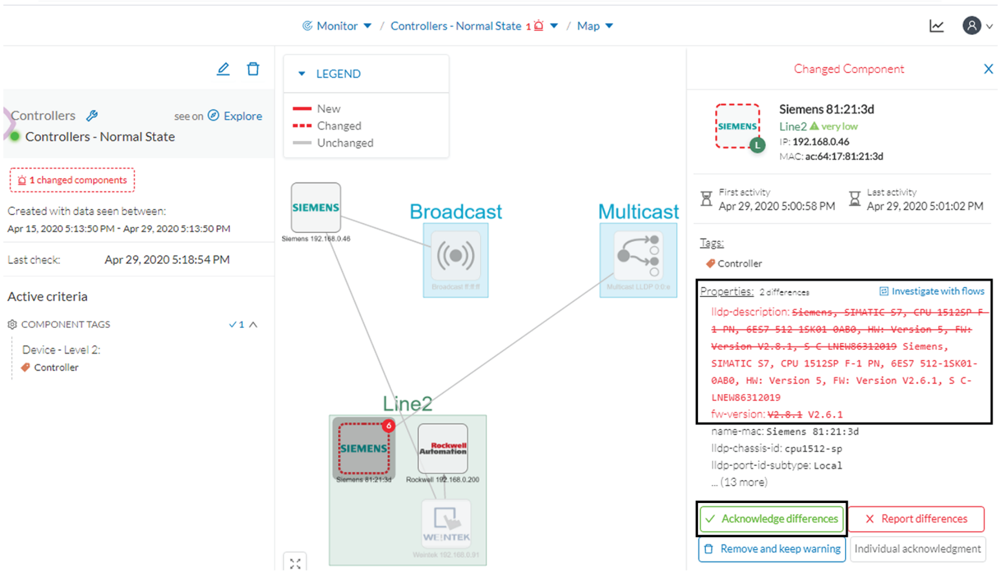
Go to **Monitor mode**. The new baseline **Controllers - Normal State** displays.

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.



1 changed components

Created with data seen between:
Apr 15, 2020 5:13:50 PM - Apr 29, 2020 5:13:50 PM

Last check: Apr 29, 2020 5:18:54 PM

Active criteria

COMPONENT TAGS ✓1

Device - Level 2:
Controller

Siemens 81:21:3d
Line2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3d

First activity Apr 29, 2020 5:00:58 PM
Last activity Apr 29, 2020 5:01:02 PM

Tags:
Controller

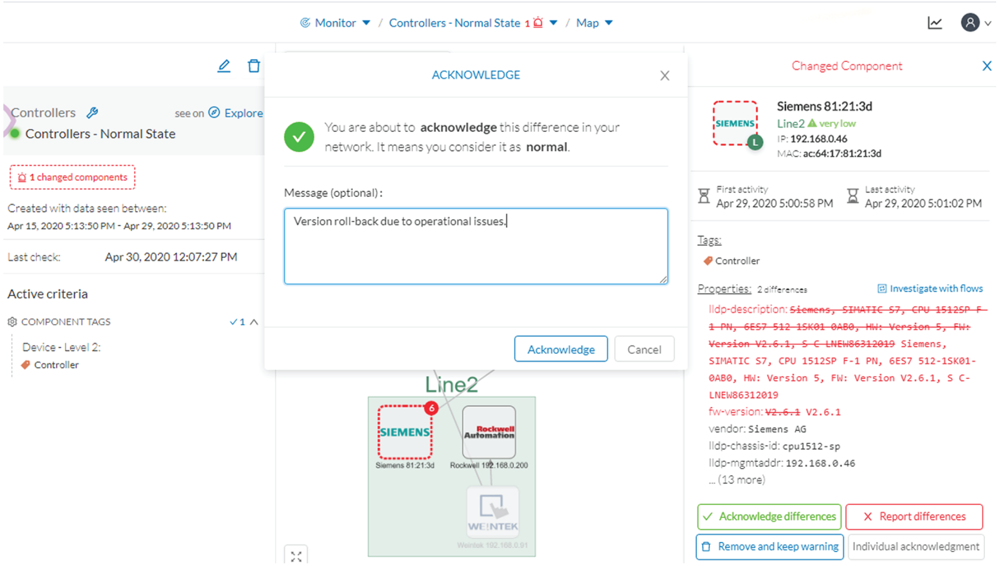
Properties: 2 differences

lldp-description: ~~Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.8.1, S C-LNEW86312019~~ Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
fw-version: ~~V2.8.1~~ V2.6.1
name-mac: Siemens 81:21:3d
lldp-chassis-id: cpu1512-sp
lldp-port-id-subtype: Local
... (13 more)

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.



Created with data seen between:
Apr 15, 2020 5:13:50 PM - Apr 29, 2020 5:13:50 PM

Last check: Apr 30, 2020 12:07:27 PM

You are about to **acknowledge** this difference in your network. It means you consider it as **normal**.

Message (optional):

Version roll-back due to operational issues.

Siemens 81:21:3d
Line2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3d

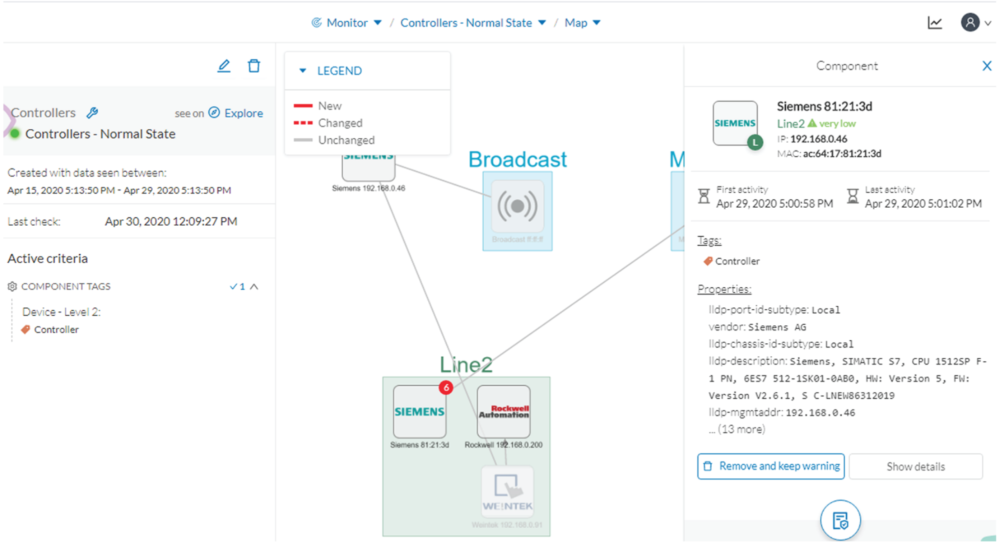
First activity Apr 29, 2020 5:00:58 PM
Last activity Apr 29, 2020 5:01:02 PM

Tags:
Controller

Properties: 2 differences

lldp-description: ~~Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512 1SK01 0AB0, HW: Version 5, FW: Version V2.6.1, S C LNEW86312019~~ Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
fw-version: ~~V2.6.1~~ V2.6.1
vendor: Siemens AG
lldp-chassis-id: cpu1512-sp
lldp-mgmtaddr: 192.168.0.46
... (13 more)

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**.



Created with data seen between:
Apr 15, 2020 5:13:50 PM - Apr 29, 2020 5:13:50 PM

Last check: Apr 30, 2020 12:09:27 PM

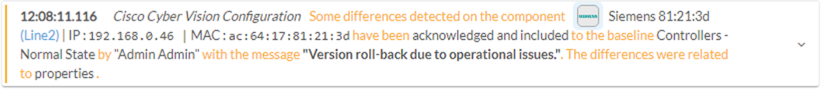
Siemens 81:21:3d
Line2 very low
IP: 192.168.0.46
MAC: ac:64:17:81:21:3d

First activity Apr 29, 2020 5:00:58 PM
Last activity Apr 29, 2020 5:01:02 PM

Tags:
Controller

Properties:
lldp-port-id-subtype: Local
vendor: Siemens AG
lldp-chassis-id-subtype: Local
lldp-description: Siemens, SIMATIC S7, CPU 1512SP F-1 PN, 6ES7 512-1SK01-0AB0, HW: Version 5, FW: Version V2.6.1, S C-LNEW86312019
lldp-mgmtaddr: 192.168.0.46
... (13 more)

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



12:08:11.116 *Cisco Cyber Vision Configuration* Some differences detected on the component Siemens 81:21:3d (Line2) | IP: 192.168.0.46 | MAC: ac:64:17:81:21:3d have been acknowledged and included to the baseline Controllers - Normal State by "Admin Admin" with the message **"Version roll-back due to operational issues."**. The differences were related to properties .