



Overview

- [Monitor mode, on page 1](#)
- [Monitor mode's views, on page 2](#)
- [New and changed differences, on page 5](#)

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

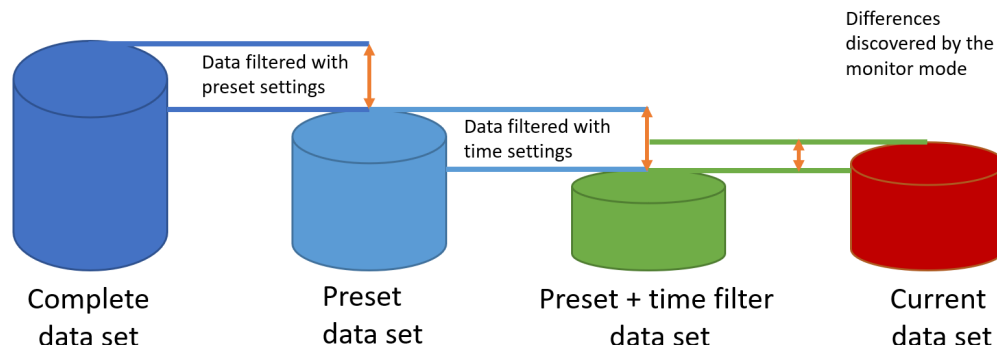
A Preset is a set of criteria which shows a detailed fragment of a network. To monitor a network, set a preset, and define what would be its normal, stable state. This represents the baseline of the preset. A state relies on a period because a network fragment is subject to several states. It is possible 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.

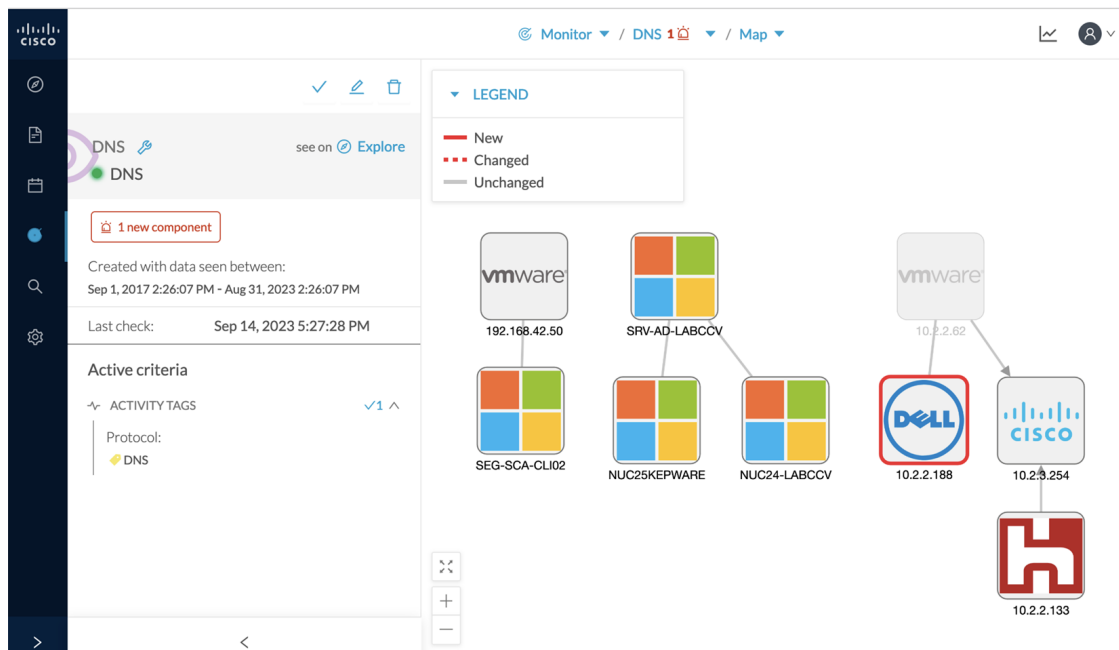


Monitor mode's views

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



Component List View

Monitor / DNS 1 / Component list

8 Components 1 new

✓ Acknowledge selection ✓ Report selection

<input type="checkbox"/>	Status	Component	First activity	Last activity	IP	MAC	Tags	Flows	Vuln
<input type="checkbox"/>	NEW	10.2.2.188	Aug 31, 2023 2:18:22 PM	Sep 4, 2023 12:10:38 PM	10.2.2.188	4cd9:8f:79:fd:fa	No tags	-10	
<input type="checkbox"/>	-	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	
<input type="checkbox"/>	-	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	
<input type="checkbox"/>	-	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	
<input type="checkbox"/>	-	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

Monitor / DNS 1 / Activity list

6 Activities

✓ Acknowledge selection ✓ Report selection

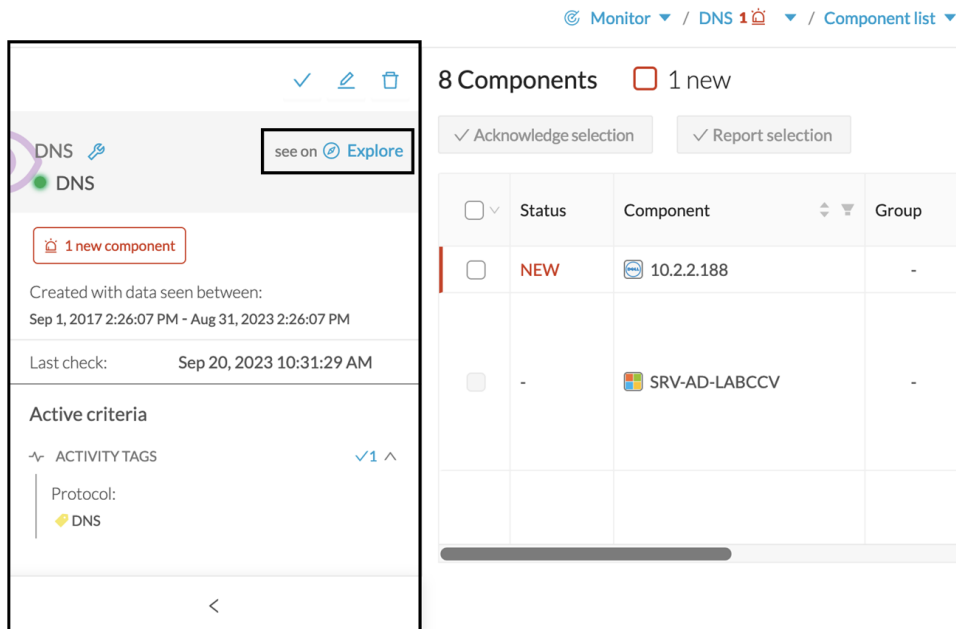
<input type="checkbox"/>	Status	Component	Component	First activity	Last activity	Tags	Flows	Packets	Volume	Events
<input type="checkbox"/>	-	10.2.2.62	10.2.3.254	Sep 4, 2023 12:06:44 PM	Sep 4, 2023 12:06:44 PM	DNS	-200	442	55.2 kB	0
<input type="checkbox"/>	-	10.2.2.62	10.2.2.188	Sep 4, 2023 12:06:44 PM	Sep 4, 2023 12:06:44 PM	ARP, DNS	-10	4	390 B	0
<input type="checkbox"/>	-	SRV-AD-LABCCV	NUC24-LABCCV	Aug 31, 2023 2:25:11 PM	Aug 31, 2023 2:25:11 PM	Admin, Authentication, Procedure Ca, Low Volume, ARP, DCE-RPC, DNS, SMB	-30	85	10.6 kB	0
<input type="checkbox"/>	-	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
<input type="checkbox"/>	-	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

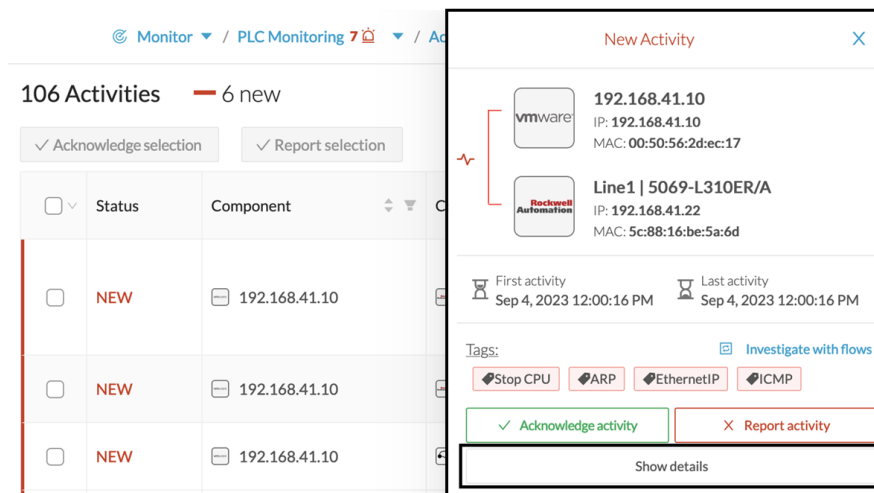
- The last time this baseline was checked
- The preset it belongs to and the list of criteria selected

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

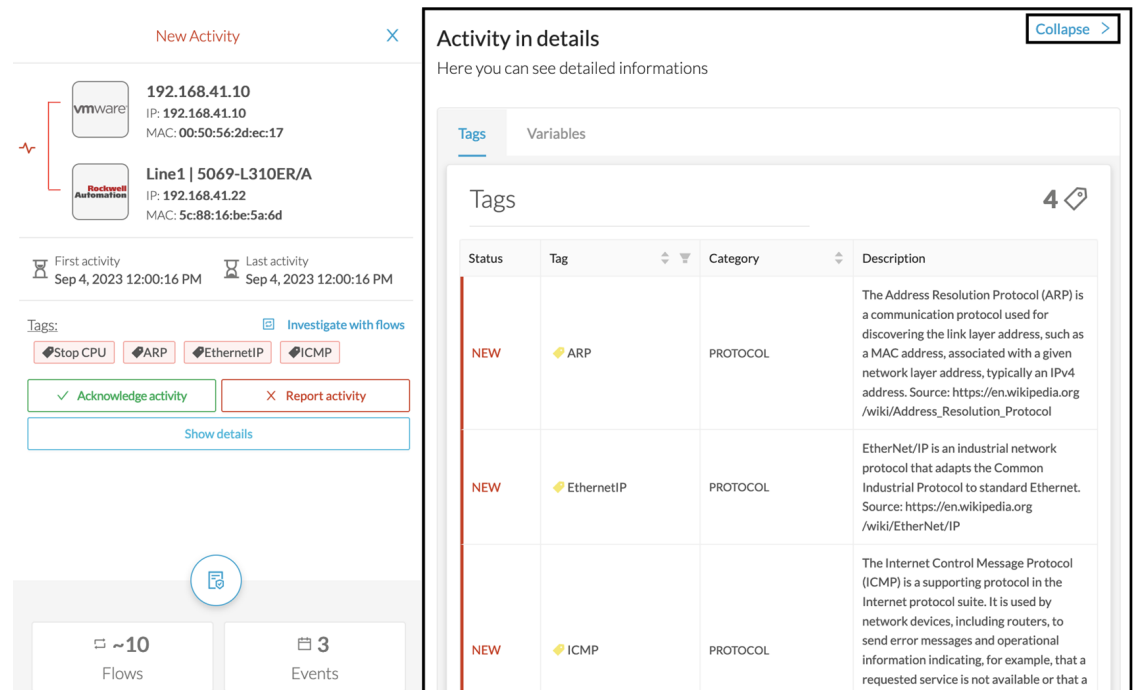


Check one of the elements marked as new in the **Activity List View** to see the following:

- 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 actions](#).



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



New Activity ✕

vmware 192.168.41.10
IP: 192.168.41.10
MAC: 00:50:56:2dec:17

Rockwell Automation 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: Investigate with flows

Stop CPU ARP EthernetIP ICMP

Acknowledge activity Report activity

Show details

~10 Flows 3 Events

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

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

[Investigate with flows](#)

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:



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](#).