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.