Create baselines

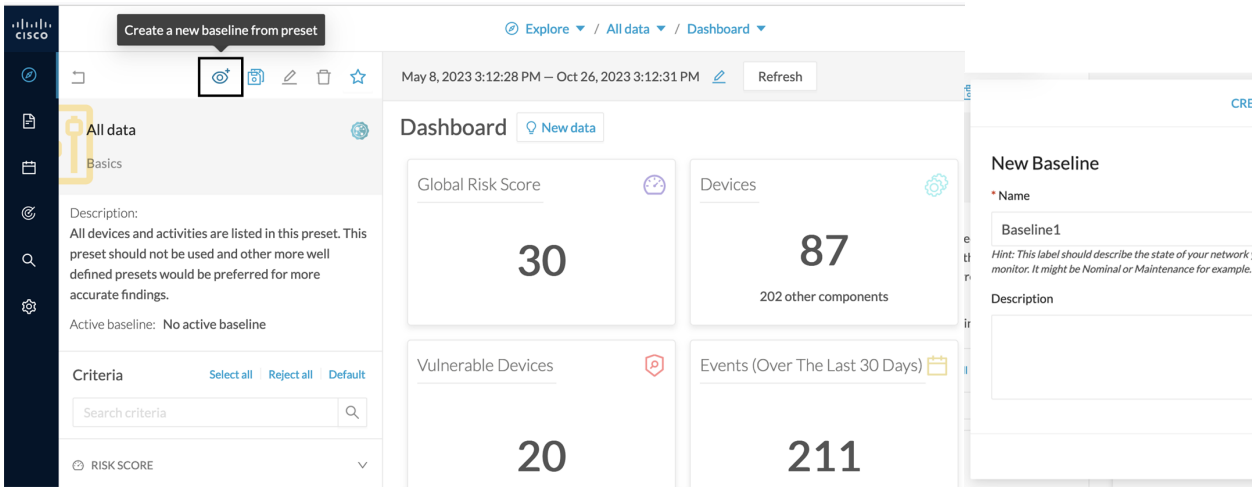
Create and setup a baseline

Procedure

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

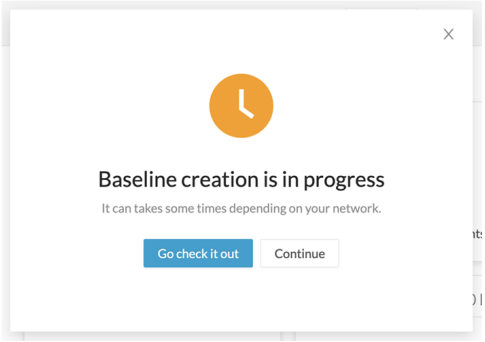
Step 2 Click **Basics**, click the **All data** preset.

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



Step 4 Type in **Name**.

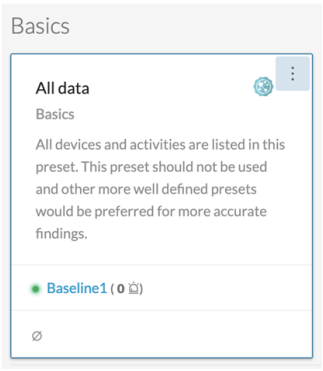
Step 5 Click **Create**. The Baseline creation window appears.



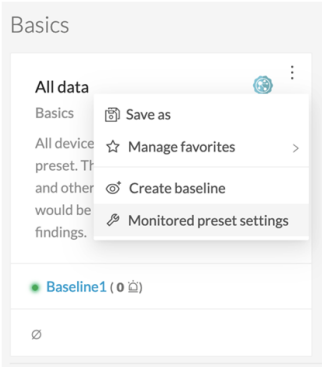
Step 6 Click **Continue**.

Step 7 Access the **Monitor** page.

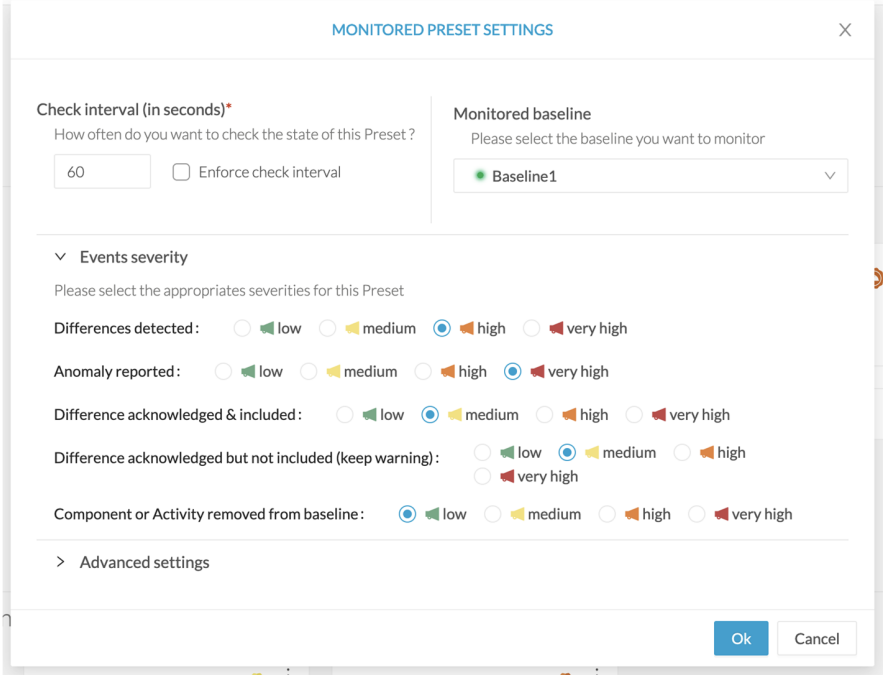
On the All data preset, the new baseline appears.



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



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



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

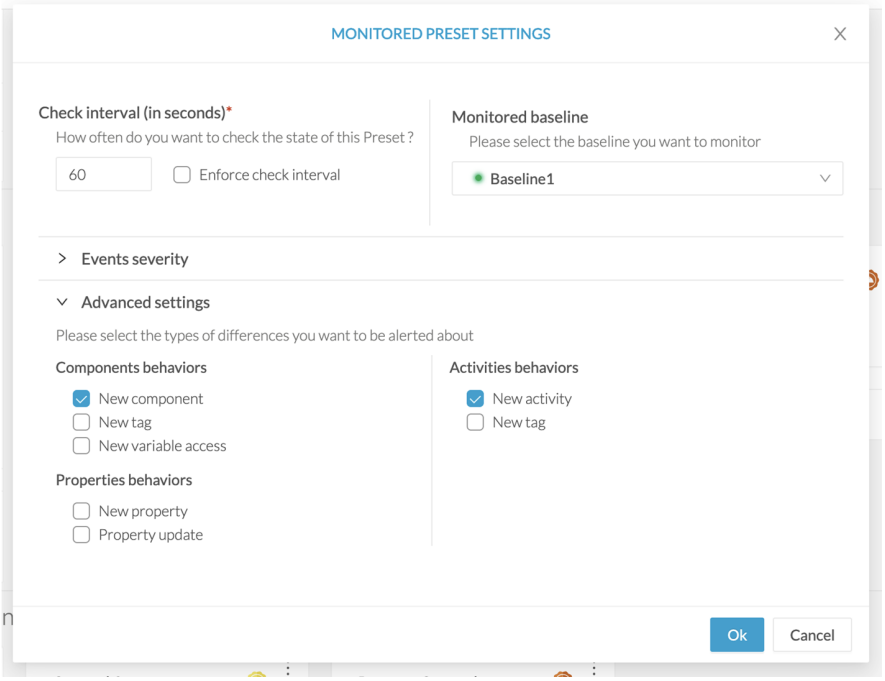
- Drastically reduce the number of differences found to facilitate results treatment.

  Refer to Review differences.

- 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.



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

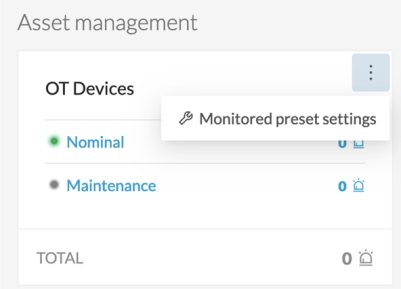
happen at the same time on a preset. Enable the proper baseline as the network enters a new operating phase. When you enable a baseline on a preset, the active one is automatically disabled.

To enable a baseline:

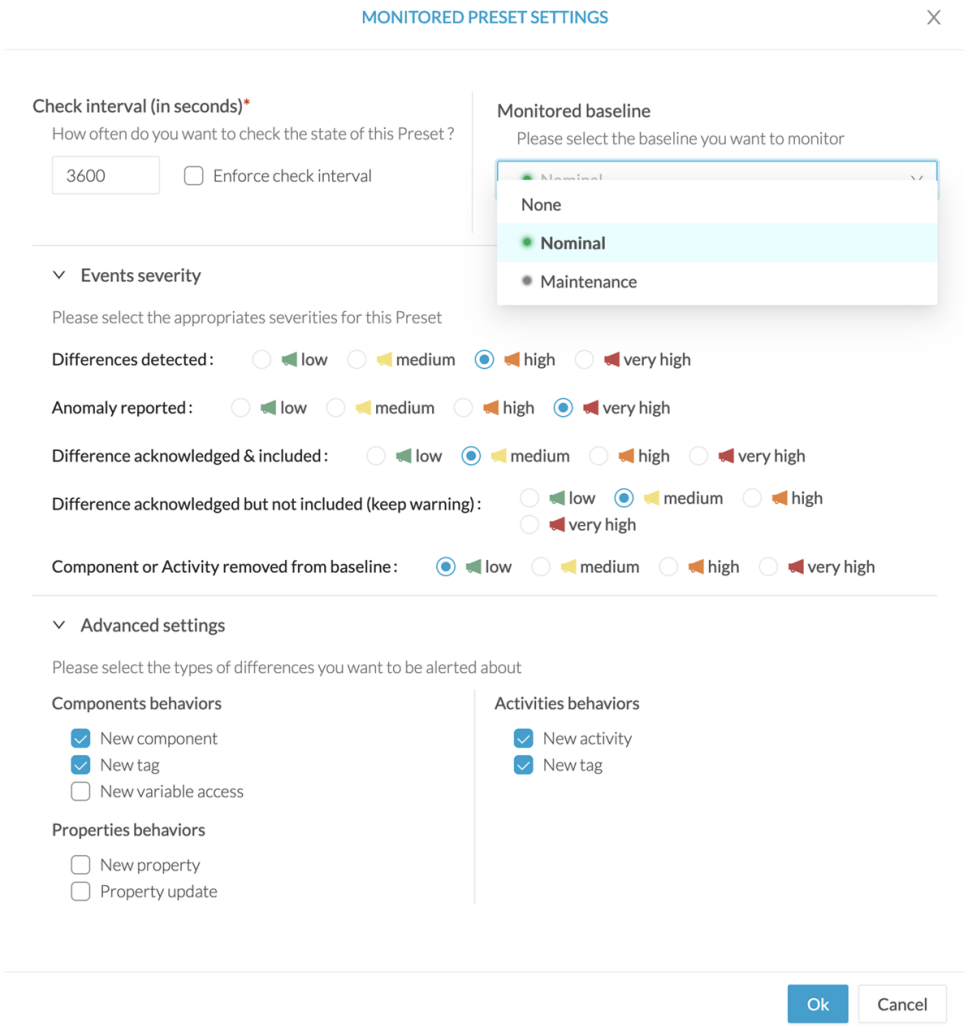
Procedure

Step 1 Access the **Monitor** page.

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



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



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.