Active Discovery

Active Discovery

Active Discovery is a feature to enforce data enrichment on the network. As opposed to passive traffic capture principles on which Cisco Cyber Vision is relying on and was originally built around, Active Discovery is an optional feature that explores traffic in an active way. The reason is, some components are sometimes not found by Cisco Cyber Vision because those devices haven't been communicating from the moment the solution started to run on the network. Moreover, some information like firmware version can be difficult to obtain because they are not exchanged often between components.

With Active Discovery enabled on selected presets, broadcast messages will be sent to the targeted subnetwork through the sensors to speed up network discovery. Then, returned responses will be analyzed through Deep Packet Inspection and tagged as Active Discovery and additional information. Thus, components and activities will be clarified with additional and more reliable information than what is usually found through passive DPI.

Active Discovery's jobs are launched every 10 minutes. In case Active Directory is enabled on several presets that use the same sensor, the job is executed only once to avoid traffic load. You can also choose which broadcast protocol will be active on the subnetwork.

Active Discovery supports three broadcast protocols, which are EtherNet/IP (Rockwell), and Profinet and S7 Discovery (Siemens).

Active Discovery is available on:

- Cisco Catalyst 9300 Series Switches.
- Cisco Catalyst IE3400 Rugged Series Switches.
- Cisco Catalyst IE3300 10G Rugged Series Switches.
- Cisco IC3000 Industrial Compute Gateway.

To use Active Discovery, you must first perform a few configurations:

Procedure

Step 1 Enable the feature on a sensor, and set the subnetwork to be monitored.

Step 2 Enable Active Discovery on a preset using the sensor set with Active Discovery and choose which protocols to be broadcasted on the subnetwork.

To enable Active Discovery on sensors:

Step 3 On Cisco Cyber Vision, navigate to Admin > Sensors.

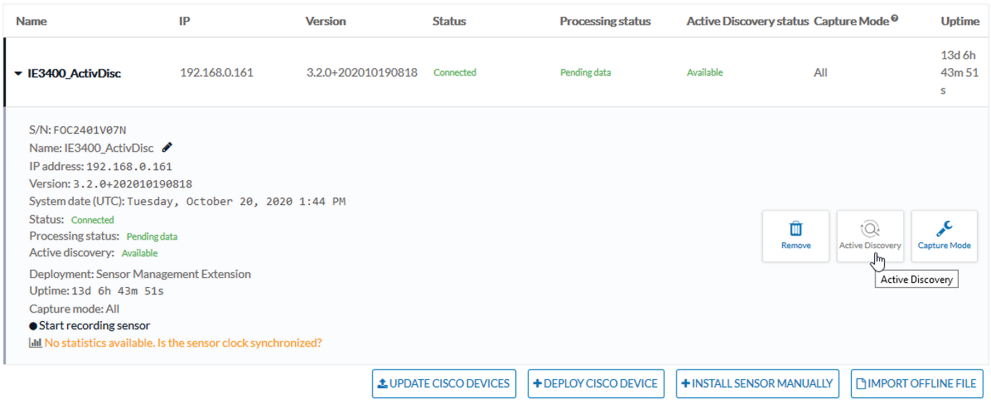
The sensors list displays.

Step 4 Check the sensors' Active Discovery status:

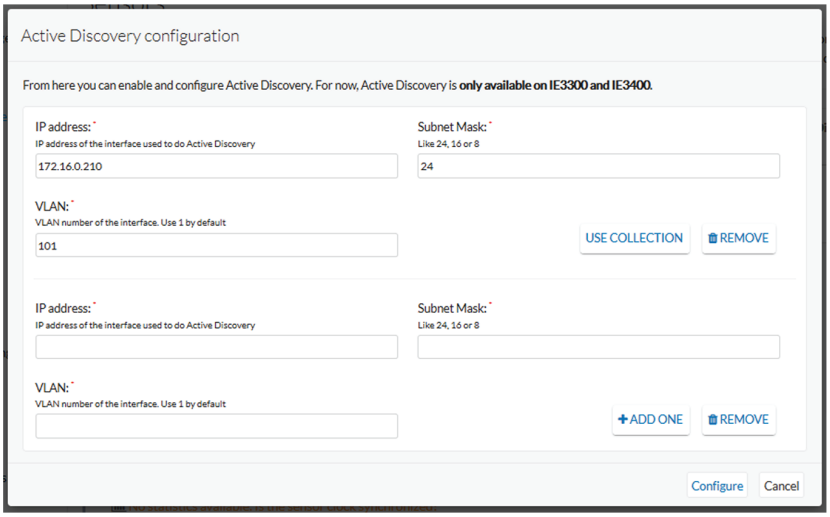
- Unavailable: This sensor model does not support Active Discovery (i.e. Cisco IR1101 Integrated Services Router Rugged); The Cisco Cyber Vision IOx Application is not up-to-date on the device (version must be 3.2.0 or newer); The IOx Application installed does not include Active Discovery (two packages are available, one includes Active Discovery, the other does not). For more information, refer to the relevant Cisco Cyber Vision Network Sensor Installation Guide.
- Available: IOx app's version is up-to-date on the device and using Active Discovery is possible.
- Running: The sensor is scanning the network sending broadcast et the moment.

  The sensor's Active Discovery status must be in Available to continue the procedure.

Step 5 Click the Active Discovery button.



The Active Discovery configuration window pops up.



Step 6 Set the interface corresponding to a subnetwork monitored by the sensor filling the following information:

- The subnetwork IP address.
- The subnet mask.
- The VLAN.

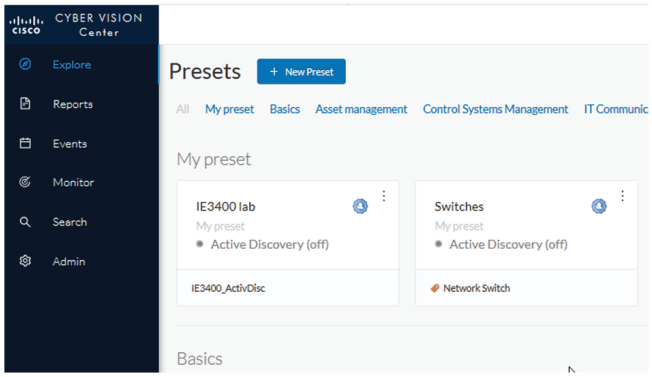
You can set as many interfaces as subnetworks monitored by the sensor.

Step 7 Click Configure.

To enable Active Discovery and set protocol scanning on a preset:

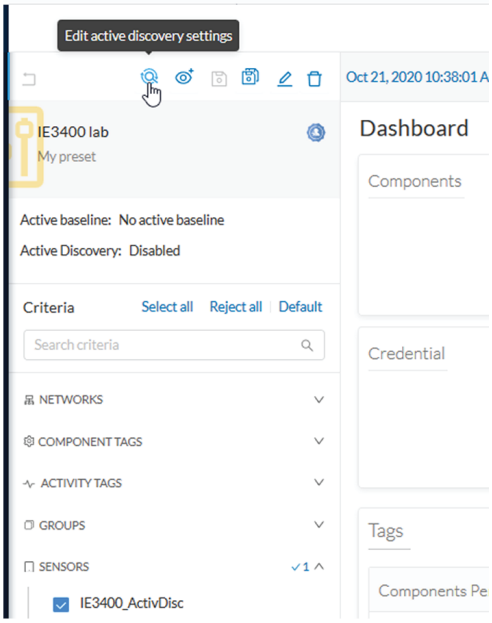
Active Discovery is not available on default presets (under Basics). To use it, you must use a custom preset (under My Presets) or create a new preset. You can create it from a default preset.

Step 8 Access or create a custom preset in the Explore menu.

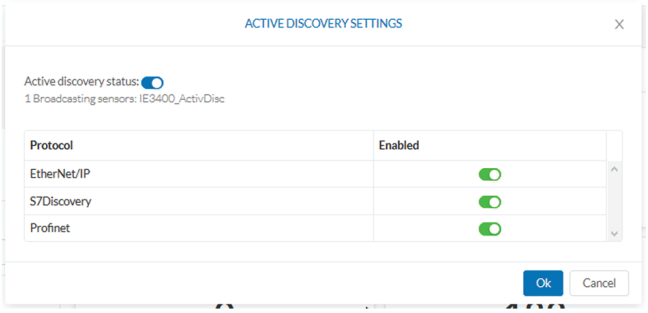


In the example, we use the IE3400 lab preset that we created with the sensor filter selected, previously configured with Active Discovery.

Step 9 Click the Edit Active Discovery settings button on the top left corner.



The Active Discovery settings window pops up.



Step 10 Use the toggle button to enable Active Discovery.

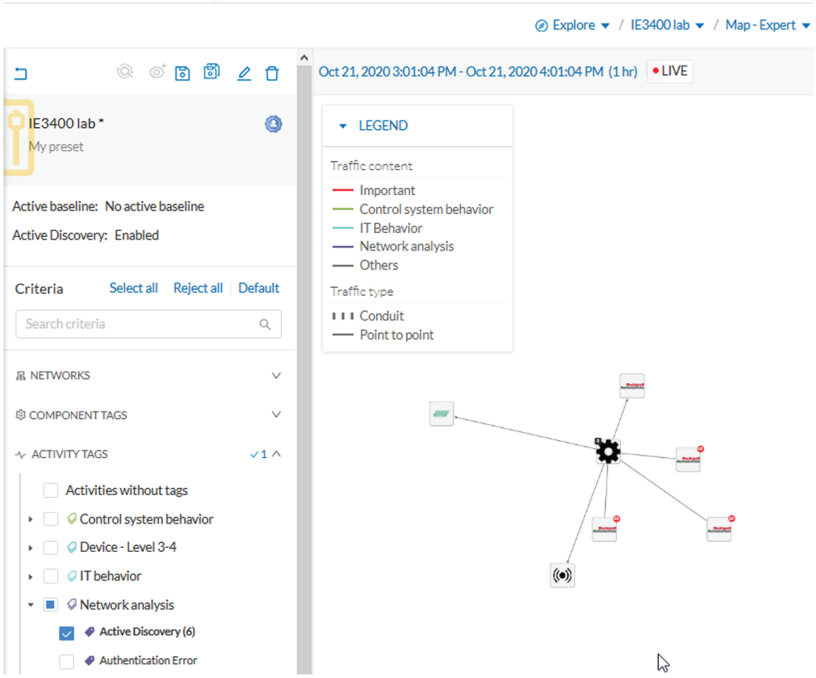
Step 11 Use the toggle buttons to enable the protocols you want the subnetwork to be scanned with.

To identify elements detected by Active Discovery:

Step 12 In the criteria area > Activity tags > Network Analysis, select the Active Discovery tag.

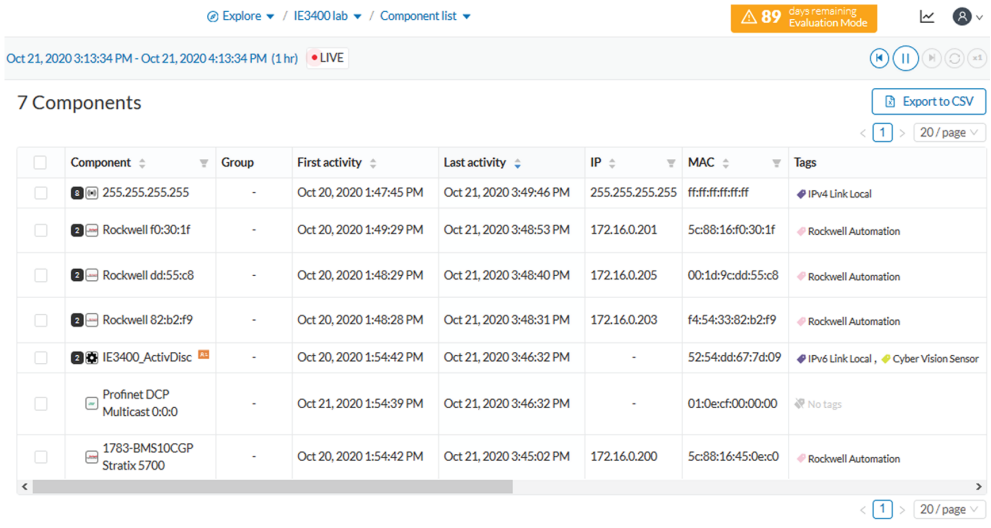
All components and activity tagged as Active Discovery, and so detected thanks to the feature, display.

Elements found and other related elements detected by Active Discovery in the Map - Expert view:



Components, activities and sensors detected by Active Discovery are tagged as Active Discovery.

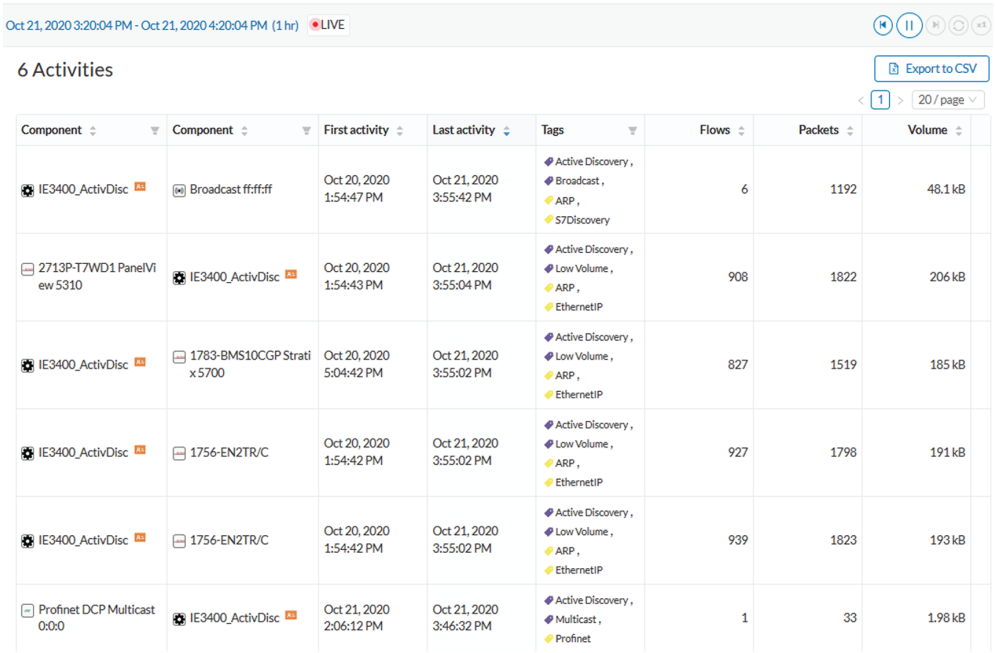
Components related to Active Discovery scanning in the Component list view:



Step 13

- Components discovered thanks to Active Discovery are tagged as Active Discovery. This is not the case here because these components had already been detected thanks to passive traffic capture. However, they are shown here because their activities have been detected through Active Discovery.
- Sensors are in passive traffic capture often tagged as Engineering Station or Scada Station, which is incorrect. With Active Discovery, these tags are removed and the sensor is tagged as Cisco Cyber Vision Sensor.

Activities related to Active Discovery scanning in the Activity list view:



Component	Component	First activity	Last activity	Tags	Flows	Packets	Volume
IE3400_ActivDisc	Broadcast ff:ff:ff	Oct 20, 2020 1:54:47 PM	Oct 21, 2020 3:55:42 PM	Active Discovery, Broadcast, ARP, S7Discovery	6	1192	48.1 kB
2713P-T7WD1 PanelView 5310	IE3400_ActivDisc	Oct 20, 2020 1:54:43 PM	Oct 21, 2020 3:55:04 PM	Active Discovery, Low Volume, ARP, EthernetIP	908	1822	206 kB
IE3400_ActivDisc	1783-BMS10CGP Stratix 5700	Oct 20, 2020 5:04:42 PM	Oct 21, 2020 3:55:02 PM	Active Discovery, Low Volume, ARP, EthernetIP	827	1519	185 kB
IE3400_ActivDisc	1756-EN2TR/C	Oct 20, 2020 1:54:42 PM	Oct 21, 2020 3:55:02 PM	Active Discovery, Low Volume, ARP, EthernetIP	927	1798	191 kB
IE3400_ActivDisc	1756-EN2TR/C	Oct 20, 2020 1:54:42 PM	Oct 21, 2020 3:55:02 PM	Active Discovery, Low Volume, ARP, EthernetIP	939	1823	193 kB
Profinet DCP Multicast 0:0:0	IE3400_ActivDisc	Oct 21, 2020 2:06:12 PM	Oct 21, 2020 3:46:32 PM	Active Discovery, Multicast, Profinet	1	33	1.98 kB

Activities detected by Active Discovery, which is meant to enrich data, are tagged as Active Discovery and as S7 Discovery, EtherNet/IP or Profinet in addition to other tags detected by passive traffic capture.

Tip: Register this selection as a preset to be informed about any new Active Discovery's elements found on the subnetwork.

Tip: You can see all Active Discovery effects on the network consulting the Active Discovery Activities preset. You will see activities tagged as Active Discovery, the components involved, and the sensors.