

Product Overview

- Introduction to Cisco Spaces: Detect and Locate, on page 1

Introduction to Cisco Spaces: Detect and Locate

Cisco Spaces: Detect and Locate enables you to view the current and historic location of Wi-Fi devices in your deployment.

Using Cisco Spaces: Detect and Locate, you can view the fixed physical layout of the buildings in your network and the Wi-Fi access points (APs) deployed in the building. You can see other fixed components such as GPS markers and Exclusion or Inclusion Zone for location calculation. Cisco Spaces: Detect and Locate also allows you to see the dynamic nature of the Wi-Fi devices in your network. You can view the calculated location of the following devices:

- Associated clients: Represented by a green dot . Includes information about the device from the Cisco AireOS Wireless Controller such as IP address and Manufacturer (when available). The history of when these devices were seen is also maintained.
- Unassociated clients: The location of these types of devices and their number is calculated on a best-effort basis and displayed.
- Tags: Active Radio-Frequency Identification (RFID) Wi-Fi tags. This information is displayed to help troubleshoot applications that use RFID tag data.
- BLE Tags: Bluetooth low energy data. This information is displayed to help troubleshoot applications that use the BLE tag data.
- Rogue Access Points: These are APs that the wireless controller detected and labeled as Rogue. The AP MAC address is displayed along with the estimated location.
- Rogue Clients: These are Wi-Fi clients that the wireless controller has detected and labeled as Rogue. The client MAC address is displayed along with the estimated location.
- Interferers: Any device that is not an AP or a wireless client, but still generate a radio frequency (RF) signal. For more information, see Detecting Interferers

Warning Web GL browser functionality is necessary to render maps on Cisco Spaces: Detect and Locate, and is enabled by default. Do not manually disable the Web GL functionality on your browser as this will prevent maps from rendering accurately.

Note These devices can change their MAC address and do not have a valid location history as long as they are not associated with the network.

Detect and Locate dashboard

Cisco Spaces tracks only active devices, defined as those sending a Wi-Fi probe packet at intervals of five minutes or less. The frequency of probe sending is determined by the device, making it unpredictable.

You cannot directly compare client counts (both associated and probing) between Cisco Spaces and the Wireless Controller due to differences in their designs. Both the Wireless Controller and Catalyst Center consider associated devices as active. Associated devices are devices that are merely associated to the network. Since Catalyst Center relies on Cisco Spaces for device locations, it shows such devices as un-positioned.

Linking of a Cisco CMX device to Cisco Spaces is a design that should be used to help a customer transition to Cisco Spaces(Tethering). This allows a customer an initial view of how devices are displayed on Cisco Spaces. However, device counts on Cisco CMX andCisco Spaces should not be compared. For tethered devices, perform accuracy troubleshooting on Cisco CMX.

The Wireless Controller does not require active devices to probe continuously. In contrast, Cisco Spaces requires a probe frequency of five minutes or less. Therefore, devices shown as active on the Wireless Controller might not appear on Cisco Spaces. These are termed non-locatable devices.

Devices may be listed as missing on Cisco Spaces for the following reasons:

- The device is reported by an AP that is not placed on the map. If many APs connected to the Wireless Controller are not on the map, the devices they report will be missing
- Associated clients probe less frequently to conserve battery, affecting the accuracy of location. They do not probe when in ultra-power reserve mode (sleeping mode and screen blanked out). Cisco Spaces cannot locate devices in this inactive state. Once the user activates the device (unlocks screen, starts streaming), it resumes sending probes to the network.
- Cisco Spaces expects Wi-Fi devices to send regular Wi-Fi probe packet updates to ensure that the device status is active. However, some devices are considered active by the Wireless Controller although they are not sending Wi-Fi probes, and such devices are considered as non-locatable devices
- Cisco Spaces requires regular Wi-Fi probe updates to maintain active device status. Some devices may be considered active by the wireless controller even without sending Wi-Fi probes, making them non-locatable on Cisco Spaces.

For more information about the open source used in Cisco Spaces: Detect and Locate, see:

Open Source Documentation.