Introduction

Note **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

Getting Started with Cisco Spaces: Proximity Reporting App

The Cisco Spaces: Proximity Reporting app helps workplace administrators of enterprise networks to create a safe environment for employees who are returning to work after a pandemic. The app collects data from one or more wireless devices belonging to a person. The wireless device must be associated to the wireless networks and mapped to physical locations. The Proximity Reporting app works to track the movement of a person reporting as tested positive.

Some of the key capabilities of the Proximity Reporting app are as follows:

- It helps you understand which physical spaces an affected person was during a configurable period (usually 14-28 days).
- A list of other people who were in the same location as a affected person.
- A timeline of when an affected person entered and exited a physical space.

Creating a Report

This section describes how you can look up a person who has reported in as being positive. The section takes you through a typical workflow of the Proximity Reporting app and shows you how to generate a report. The workflow requires that employees report themselves to the company, revealing that they may be positive. This employee is henceforth called the reporting person. A reporting person reveals the IEEE 802.1x user ID, the MAC address of devices used, and the estimated date on which the employee last visited the campus.

Before you begin

Some of the prerequisites and assumptions made for this workflow are:

- You have an active subscription to Cisco Spaces ACT license and Cisco Spaces: Detect and Locate.
- Your network is equipped with Cisco Catalyst Access Points.

.

- An employee of your company might be using more than one wireless device to associate with the enterprise network. An employee might also have more than one IEEE 802.1x user IDs to associate with the wireless network of your company campus.
- An employee has granted you permission to access location information for troubleshooting of devices or safety.

SUMMARY STEPS

1. Log in to the Cisco Spaces: Proximity Reporting app and click **Create Report**.
2. In the **Search User Name or Mac Address** field, enter one of the following:
   - IEEE 802.1x User ID of a reporting person (Figure 1)
   - MAC address of this person's device (Figure 2)
3. Click **Lookup**.
4. Depending on what you entered in Step 2:
   - Check up to two IEEE 802.1x userIDs.
   - Check the MAC addresses of the associated devices.
5. Click **OK**.
6. Check the **Device Type** of your choice. This filters the final report of devices that are in proximity of the reporting device, based on the selected **Device Type**.
7. Drag the **Report Level** controls to set the proximity to the reporting device. Only user names or MAC addresses of devices that are in the chosen proximity level of the reporting device are shown in the final report.
8. (Optional) Uncheck the **Filter noisy data** check box.
9. To create a report, enter a **Start Date** and an **End Date**. Ensure that the range is within 28 days.
10. Click **Generate Report.**

DETAILED STEPS

Step 1 Log in to the Cisco Spaces: Proximity Reporting app and click **Create Report**.

Step 2 In the **Search User Name or Mac Address** field, enter one of the following:

- IEEE 802.1x User ID of a reporting person (Figure 1)
- MAC address of this person's device (Figure 2)

Step 3 Click **Lookup**.

Step 4 Depending on what you entered in Step 2:

- Check up to two IEEE 802.1x userIDs.
- Check the MAC addresses of the associated devices.

Note
- The Proximity Reporting app auto selects the displayed results based on the number of results. If the results display up to two IEEE user IDs or up to three MAC addresses, the system auto selects these results for you.
- You can manually select only up to two IEEE 802.1x user IDs.
- You can manually select any number of MAC addresses.

Step 5 Click **OK**.
A high-level **Lookup Summary** is displayed.

Step 6 Check the **Device Type** of your choice. This filters the final report of devices that are in proximity of the reporting device, based on the selected **Device Type**.

Note At least one device type should be selected.

Step 7 Drag the **Report Level** controls to set the proximity to the reporting device. Only user names or MAC addresses of devices that are in the chosen proximity level of the reporting device are shown in the final report.

The number of columns in the proximity tables of your generated report may increase or decrease based on this proximity report level.

Step 8 (Optional) Uncheck the **Filter noisy data** check box.

By default, this filter is selected. Data is considered noisy if many devices transition across different floors too frequently, during a selected time range. If this happens, you no longer see the results at the floor level and instead see the results at the larger location level, for example, at the building level.

Note Currently, this filter is only applied to Meraki data.

If unchecked, the displayed report shows data at actual location levels regardless of how noisy the data is.

Step 9 To create a report, enter a **Start Date** and an **End Date**. Ensure that the range is within 28 days.

Step 10 Click **Generate Report.**

The generated detailed report is displayd. You can export this report as a PDF or a CSV file.

What to do next

- Using the detailed report, you can inform the persons who are at risk because of their contact with the reporting person.

Note The list of people in the report is not exhaustive and cannot be considered complete.

- You can also choose to shut down the facilities of campus for intensive cleaning.

The rest of this document describes the various parts of this detailed report.