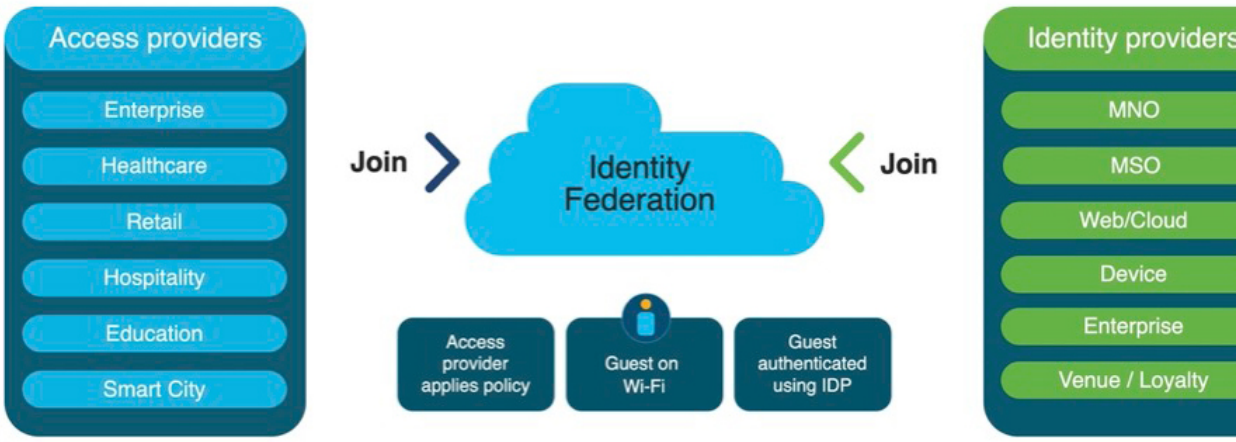
Overview of OpenRoaming

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.

Prior to the introduction of OpenRoaming, many mobile device users preferred to stay connected to their personal cellular network because it was more convenient and provided a more secure internet connection. Their internet usage was dependent on their cellular coverage and mobile data plan.

OpenRoaming enables secure, seamless, and automatic network connectivity by eliminating tedious Wi-Fi guest onboarding processes and the risk of connecting to rogue SSIDs. This is especially helpful for a mobile device user trying to access the internet because OpenRoaming removes the need to choose between multiple SSIDs, or enter insecure, shared credentials on poorly designed captive portals. With OpenRoaming, user mobility is enhanced by enabling users to connect to the guest network by signing in using a trusted identity provider.

Figure 1: OpenRoaming Federation



The OpenRoaming Federation consists of access providers and identity providers. Access providers provide the wireless networks that customers will automatically connect to. Access providers include retailers, airports,

hotels, large enterprises, and public venues. Identity providers allow users to access the network after verifying if they are valid customers. Identity providers include service providers (based on SIM card validity), device and cloud providers (such as Google and Apple), and internet Wi-Fi providers.

OpenRoaming leverages Hotspot 2.0 and enables guest users to roam freely across Wi-Fi and cellular networks. The Wi-Fi connection is secured using industry-standard Wi-Fi Protected Access 2 (WPA2) and Wi-Fi Protected Access 3 (WPA3) protocols and encrypted authentication.

As a retail or other public-access location operator, you can accelerate your guest Wi-Fi attach rate, with the click of a button. The amount of data you can gather about the usage of your physical space can be leveraged with Cisco Spaces, which help you better understand and identify your consumers' behavior patterns. This leads to an improved and engaged experience for your customers at your location while delivering your business outcomes.

This chapter contains the following sections:

- Benefits of OpenRoaming, on page 2
- Prerequisites for OpenRoaming, on page 2

Benefits of OpenRoaming

- Simplified Wi-Fi guest access for your customers on site
- Increased Wi-Fi attach rate
- Improved customer onboarding with seamless and secure Wi-Fi connection
- Easy sign-up and network configuration for OpenRoaming through your Cisco Spaces account
- Access to insights and analytics on visitors and customers
- Improved engagement with your customers through Wi-Fi, Cisco Spaces, and your loyalty app
- Reduced operational expenses because of traffic offload from cellular to Wi-Fi networks

Prerequisites for OpenRoaming

To use OpenRoaming through Cisco Spaces, your network must meet the following prerequisites:

- You need an active Cisco Spaces account.
- You need a Cisco wireless network. Both controller-based (Cisco AireOS or Cisco Catalyst wireless controller) and cloud-based (Cisco Meraki) networks are supported.
- You need to add the wireless network to your Cisco Spaces account.
  - For controller-based architecture, the Cisco Spaces Connector must be used. For information on downloading and configuring a Cisco Spaces Connector, see the *Cisco Spaces Connector Configuration Guide*.
  - For Cisco Meraki networks, you need to add the Cisco Meraki account to your Cisco Spaces account.