April 2021

What's New in this Release

Captive Runtime

Social Authentication using Facebook: Cisco Spaces now supports the removal of publicly available user data such as the first name, last name, gender, and email ID that is stored in the Cisco Spaces backend during the authentication process.

To enable removal of publicly available user data from Cisco Spaces, configure the **Data Deletion Callback URL** for that app in your Facebook Developer account. The format for the **Data Deletion Callback URL** is **`https://<live_domain>/p/<customerName>/fb_revoke`**. For example, https://splash.dnaspaces.io/p/ciscotest/fb_revoke. For the detailed procedure, see the Working with the Captive Portal App chapter in the *Cisco Spaces Configuration Guide*.

To remove user data from Cisco Spaces, the app user must do the following on their Facebook profile settings page:

1. Remove the signed-in app by clicking **Settings & Privacy** > **Settings** > **Apps and Websites** > **Active**.

2. Send a data delete request by clicking **Settings & Privacy** > **Settings** > **Apps and Websites** > **Removed**.

Dashboard

Role-based access control is introduced for the following apps in the Cisco Spaces Dashboard:

- Engagements
- Location Personas
- OpenRoaming

By default, Cisco Spaces Dashboard administrators have access to these apps. Using the **User Management** option for each of these apps, the Dashboard administrators can manage user access to the individual apps.

What's Changed in this Release

Map service

The timezone of a location is now obtained from the corresponding latitude and longitude values present in the source map file. This timezone value is saved to the Cisco Spaces back-end during map import.

The timezone is shown on the **Location Info** page corresponding to that location, under **Location Hierarchy**. The location's address, based on the information present in the imported source map file, is also displayed on the **Location Info** page.

Caveats

Caveats describe unexpected behavior in the Cisco Spaces application. The Resolved Caveats and Open Caveats sections list the caveats in this release.

The following information is provided for each caveat:

- Identifier: Each caveat is assigned a unique identifier (ID) with a pattern of CSC*xxNNNNN*, where *x* is any letter (a-z) and *N* is any number (0-9). These IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices, and other Cisco support documents. Cisco Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific caveat.
- Description: A description of what is observed when the caveat occurs.

This section contains the following topics:

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Open Caveats

This section lists the open caveats in this release of Cisco Spaces.

Table 1: Cisco Spaces Open Caveats

Caveat Identifier	Caveat Description
CSCvu98859	Telemetry such as **Button Click** and **Movement** data gets reset to 18+ hours when applying new configuration
CSCvv16880	During gateway deployment workflow, the AP is sometimes erroneously categorized as `needs config mode` due to timing issues.

Resolved Caveats

There are no fixed bugs in this release of Cisco Spaces.