Release Notes for the Cisco Enterprise Mobility Services Platform Release 3.1.5

Release Month: January, 2017

Contents

This document describes the system requirements, new features, enhancements, and known issues for the Cisco Enterprise Mobility Services Platform. Use this document in conjunction with the documents listed in the "Support" section on page 6.

- Introduction to the Enterprise Mobility Services Platform, page 1
- System Requirements, page 2
- New Features, page 3
- Enhancements, page 5
- .Known Issues, page 6
- Support, page 6

Introduction to the Enterprise Mobility Services Platform

Cisco Enterprise Mobility Services Platform is a mobile-application platform that enables you quickly create and deploy context-aware experiences that engage people on their mobile devices. The cloud-based Enterprise Mobility Services Platform more securely integrates with your existing Cisco mobile network infrastructure. It uses context-aware data, like location and user profile information, to deliver personalized experiences that engage people on their mobile devices.

With this software platform, you can create captive portals or splash pages for guest Internet access and authentication. You can also develop native and web-based mobile apps, or add context-awareness to your existing mobile apps. Organizations can push personalized content to visitors and customers on their mobile devices to create new opportunities for engagement and revenue.

Enterprise Mobility Services Platform helps you:

Cisco Systems, Inc.
www.cisco.com

- Quickly build context-aware mobile experiences using drag-and-drop design tools.
- Simplify Internet access and authentication with custom or social Wi-Fi access.
- Send personalized notifications to visitors based on their real-time location.
- Easily integrate mobile experiences with your existing native apps using SDKs.

The platform includes adapters to interface with Cisco Meraki Cloud controllers, the Cisco Connected Mobile Experience, and Cisco wireless LAN controllers. In this way, it more securely integrates with your existing mobile network infrastructure.

System Requirements

This section lists the hardware requirements, operating systems, software requirements, and browsers for the Enterprise Mobility Services Platform.

Table 1 System Requirements for the Enterprise Mobility Services Platform (WiFi Engage, Studio, SDK, and API)

Item	Supported Requirements
Hardware	• 1 GHz processor • 1 GB RAM • 16 GB hard disk
API Network (For WiFi Engage)	• MSE 7.1 or later
Operating System	• Microsoft® Windows® XP or later • Mac OS X 10.6 or later
Browser	**Windows OS** • Internet Explorer version 9 or later • Firefox version 30 or later • Chrome version 34 or later • Safari version 5.1.7 or later **Mac OS** • Firefox version 30 or later • Chrome version 34 or later • Safari version 5.1.7 or later
Runtime Environment	Adobe Air version 3.0 or later
Java	Version 6.0
Mobile SDK	iPhone OS 6.0 or later, Android 2.3 or later

New Features

WiFi Engage Dashboard

- Support for Meraki Security Appliances, page 3
- Tags Using Captive Portal Rule, page 3
- API Trigger Notification Using Captive Portal Rule, page 3
- Engagement Rule Report, page 3

EMSP Studio

- WiFi Engage V3 Module Group, page 4

WiFi Engage Dashboard

The following new features are introduced in the WiFi Engage dashboard:

Support for Meraki Security Appliances

For Meraki, you can now import the security appliances such as MX 64 to the WiFi Engage dashboard. When you add a network with security appliances to the location hierarchy, the same network name is displayed twice, one with security appliances and other with access points. When you import the network name with access points, the access points for that network are imported. Similarly, when you import a network name with Security Appliances, the security appliances for that network are imported.

Tags Using Captive Portal Rule

The WiFi Engage now allows you create or modify tags with a captive portal rule. You can create a new tag with the customers filtered based on a Captive Portal rule. You can also add the customers to an existing tag, or remove the customers from an existing tag using a Captive Portal rule. In the Create Captive Portal Rule window, under the Actions area, a new option “Tags these users as”, is added to create or modify tags with the customers filtered based on a captive portal rule.

API Trigger Notification Using Captive Portal Rule

The WiFi Engage now allows you to send the details of the customers who have accessed the captive portal configured for a captive portal rule, to an API endpoint. When a customer accesses a captive portal configured for a captive portal rule, the customer details are captured through the Data Capture form, if configured. If the customer ignores to provide the details in the Data Capture form, only the minimum details such as device Mac address are send to the API endpoint.

Engagement Rule Report

A new report, Engagement Rule Report, is added to the WiFi Engage that is specific to each engagement rule.When you click an engagement rule that is live, the Engagement Rule report is displayed. The Engagement Report has the following sections:

Rule Activity- This section displays the details of notifications sent based on a particular engagement rule. The details include the number of notifications sent for the rule, notifications sent for each locations, the time at which the notifications are sent, the notifications sent using various notification types such as SMS, e-mail, and so on.

User Insights - This section shows the total number of customers to whom the notifications are sent based on a particular engagement rule, type of customers for whom the notifications are sent, and the behavioral pattern of the customers. The customer details include customer gender, dwelling time, repeat user engagement, number of visits made by the customers, and so on are shown.

EMSP Studio

The following new features are introduced in the EMSP Studio:

WiFi Engage V3 Module Group

A new module group, WiFi Engage V3, is added to the EMSP Studio. In addition to the features available for WiFi Engage and WiFi Engage V2 group, this module group supports the following features that a captive portal created using the WiFi Engage dashboard can have:

- **Data Capture Form-** The WiFi Engage V3 group supports the portals with a Data Capture form. The Data Capture form added for both Hard SMS with Verification Code and E-mail authentication types are supported by this group. The Data Capture form features such as adding gender information to the user subscriber tags, deriving gender from the title, and User subscriber tags having the gender and business tag selected by the customers are supported by the WiFi Engage V3 group. This group also supports the Skip option in the Data Capture form.
- **Location-specific and Repeat User Welcome Message**- The Welcome Message module in this group supports providing different messages for first time and repeat users. In addition, it supports displaying location-specific welcome messages.
- **Captive Portal Rule**- This module group supports the captive portals that are configured for a Captive Portal Rule. So, you can enhance the portals that are used in the captive portal rules using advanced EMSP Studio modules such as location-specific modules.
- **Multi Language Support**- This module group supports to display the content in languages besides English.
- **Smart Link Support**- This module group supports the smart links added in the portals.

So to enhance a portal with the following features using the EMSP Studio, use the WiFi Engage V3 group instead of WiFi Engage or WiFi Engage V2 group:

- The portal with Hard SMS with Verification Code authentication and Data Capture Form
- The Portal with E-mail Authentication and Data Capture Form
- The portal with any language other than English
- The portal configured for a Captive Portal Rule
- The portal with location-specific and repeat user welcome messages
- The portal with Smart Link URLs

Enhancements

EMSP Architecture and Back End

- Proximity Engine, page 5

WiFi Engage Dashboard

- Location-Specific Network Synchronization Status, page 5
- Displaying Reports based on License, page 5

EMSP Architecture and Back End

The following enhancements are made to the EMSP Architecture and Back End:

Proximity Engine

The Redis cache entries that were stored in the location receiver are moved to the Proximity Engine. Now, additional information of the locations such as Location Name, Location ID, and Location path are also added as Redis cache entries.

Now when sending the notifications, the Mac address of the access points through which the notifications are sent are also captured.

WiFi Engage Dashboard

The following enhancements are made to the WiFi Engage Dashboard:

Location-Specific Network Synchronization Status

In the Locations Details page that appears when you select a location in the Location Hierarchy, now the location synchronization status for that location is shown. The details such as Node Type, Network Reference, Last synchronized time, and status of the synchronization with the wireless network are displayed.

Earlier, the synchronization details of the entire location hierarchy was only displaying in the Locations page. This enhancement enables you to view the synchronization status for each location. For locations such as floors and zones, the synchronization status displayed depends on its parent location. For example, for Meraki, the network status is based on the Network and for MSE the network status is based on the Building.

Displaying Reports based on License

For the WiFi Engage license type, BASIC, the following sections will be not shown in the Reports:

- User Profile in Customer Acquisition
- User Activity Section
- Consumer Notifications, Business User Notifications, and Profile Tags in Engagement Reports.

.Known Issues

Table 2 Known Issues in the Enterprise Mobility Services Platform

Description
The locations that are not synchronized with the wireless network are also displaying the message, "In Sync".
For API Trigger Notification the following issues occur: • Post json method is not considering the json format . • The tool tip for the Request Parameters field is not displaying as expected. • After changing a Trigger API method, the details of previously selected method is not cleared.
In the Engagement rule, after inserting"$" in the message text box, the smart link variables are not listed. This error is occurring occasionally wherever the smart links are used, especially for Trigger API notification.
For a Captive Portal rule, if you go back to the previous screen using the Go back button and come back to the captive portal rule, the SSIDs are not displayed for selection properly.
In the Captive Portal rule, when you click the Show Portal drop-down list, the tool tips for portals are not displayed as expected.
For the portals with social authentication that are enhanced using the EMSP Studio, the customized message for repeat users is not shown.

Support

The support documentation is available at https://emsp.cisco.com