Release Notes for the Cisco Enterprise Mobility Services Platform Release 3.1.6

Release Month: February, 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 7.

- Introduction to the Enterprise Mobility Services Platform, page 1
- System Requirements, page 2
- New Features, page 3
- Enhancements, page 5
- Known Issues, page 7
- Support, page 7

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

- Retry Limit for Access Codes, page 3
- Time Zones for Locations, page 3
- Location-Specific Portals, page 3
- Managing Internet Provisioning through Captive Portal Rule, page 4

EMSP Studio

- App On-Boarding, page 4

EMSP Runtime

- Captive Portal Support for Ruckus, page 4
- Captive Portal Support for Extreme Networks, page 5

WiFi Engage Dashboard

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

Retry Limit for Access Codes

To control the internet access through access codes, maximum retry limit is introduced for the access codes. You can now define the maximum number of times a customer can access the internet using a particular access code. A new field, **No: of times access code can be used**, is added to the Access Code window where you can specify the maximum number of times the customer can access the internet through an access code.Only successful internet provisioning with the particular access code will be counted.

Time Zones for Locations

In the location hierarchy, you can now configure the time zone for various locations. In the Locations page, a new option, Time Zone, is added to the drop-down list for each location. The default time zone will be GMT + 00:00(UTC). If you are not configuring a time zone for a location, the default time zone is applied for that location.

Location-Specific Portals

You can now create portals that are location-specific. In the Portal window for creating portals, the locations will be listed so that you can select the locations for which the portal must be available. A “This portal is available in all locations” check box is also provided so that you can make this portal available for all the locations.

When creating a captive portal rule, a portal will be available for selection only if you select a location that is configured for the portal. However, the portals created using the earlier versions of the WiFi Engage will be available for selection for all the captive portal rules.

To edit the locations for a portal, an Edit Locations button is provided for each portal listed in the Portals page.

Managing Internet Provisioning through Captive Portal Rule

The Captive Portal rule is enhanced to manage the internet provisioning to the customers connecting to the SSID configured for the rule.

In the Action area, the following additional options are provided:

- **Seamlessly Provision Internet:** Provides direct access to the internet, when a customer filtered for the captive portal rule connects to the configured SSID. The customer does not have to undergo any authentication steps to access the internet.
- **Deny Internet**: Internet is not provisioned to a customer who is filtered for the captive portal rule connects to the configured SSID.

EMSP Studio

The following new features are introduced in the EMSP Studio:

App On-Boarding

When the customers connect to your SSID, you can now provide direct internet access to them, provided an app that is integrated with the EMSP SDK is installed on customer's device.After internet provisioning the app will be opened in the device. This feature is currently available only for the iOS devices.

When connecting to an SSID from an iOS device, a "I have an App" button will be shown. When a customer, who has an app that is integrated with EMSP SDK installed on the device, click this button, internet is provisioned immediately and the app gets opened in the device.When a customer, who does not have an app that is integrated with EMSP SDK installed on the device, click this button, internet is provisioned for some time, but will get disconnected after detecting that the app is not installed.

A new module "WiFi Engage App Launcher, is added to the WiFi Engage v3 module group in the EMSP Studio to provide the "I have an App" button in the portal. The WiF Engage App Launcher is a custom module.

EMSP Run Time

The following new features are introduced in the EMSP Run time:

Captive Portal Support for Ruckus

The EMSP provides captive portal support for the Ruckus network.You can now configure captive portals, and execute the captive portal rules if you are having a Ruckus network.

As of now you cannot do the network configurations from the WiFi Engage dashboard. You have to do it from the back end.

Captive Portal Support for Extreme Networks

The EMSP provides captive portal support for the wireless network, “External Networks”.You can now configure captive portals, and execute the captive portal rules if you are having the wireless network, “External Networks”.

As of now you cannot do the network configurations from the WiFi Engage dashboard. You have to do it from the back end.

Enhancements

WiFi Engage Dashboard

- Access Code Manager, page 5
- Security Appliance Changes, page 5
- Custom 404 Page Implementation, page 6
- SMS Gateway, page 6
- Reports, page 6

EMSP Run time

- SMS Gateway Support, page 6
- E-mail Input Inline Validation, page 7
- Country Name Derived from Country Codes, page 7

WiFi Engage Dashboard

The following enhancements are made to the WiFi Engage Dashboard:

Access Code Manager

You can now reuse the access code values of the expired access codes. All the access codes that are expired will be listed in the Access Code page under the area “Expired Access codes”, with its access codes values.

When you reuse an expired access code value, in the Expired Access Codes area, the access code value will be renamed as “[access code value]-expired”. For example, if 5463 is an access code value of an expired access code “A”, and if you are allocating this value to an active access code, then in the Expired Access Codes area, for the access code “A”, the access code value will appear as “5463-expired”.

Security Appliance Changes

A network in Meraki may have both security appliances and access points. When you are adding a network to the WiFi Engage dashboard or during network synchronization, now a single network name only will be available for selection for this network. When you add that network, both the security appliances and the access points with that network name are imported.

Previously, for networks having both access points and security appliances, same network name used to appear twice, one for access points, and the other for security appliances. You had to add both separately to the WiFi Engage dashboard.

Custom 404 Page Implementation

A custom 404 error page is developed to display when the requested page is not found. In the WiFi Engage dashboard, if you are accessing an URL that is not valid or if any error occurs during accessing a page, the custom 404 error page will be shown. Earlier, the default 404 page used to appear in such cases.

SMS Gateway

The WiFi Engage is enhanced to support the following SMS Gateways from the WiFi Engage dashboard.

- DataMetrix
- Mgage
- Panacea Mobile
- Reason8
- Twilio
- Waterfall

In the SMS Gateway tab, a drop-down list “SMS Gateway Type” is added that lists all the preceding SMS gateways.

The SMS gateway you specify here will be available in the following sections:

- For SMS authentication in the portals
- For Via SMS notifications in the Engagement Rule

Reports

The following enhancements are made to the Report feature in the WiFi Engage:

- In the Customer Acquisition tab, in the User Profile section, a pie chart is added, which displays the percentage of the tagged and untagged users among the total users. The percentage of the tagged users is shown in the middle of the pie chart.
- Shows the report only for those locations for which you have access rights. When you choose the Reports option in the WiFi Engage dashboard, the report shows the data only for the locations for which you have access rights.

EMSP Runtime

The following enhancements are made to the EMSP Runtime:

SMS Gateway Support

The EMSP runtime now supports the Hard SMS and Soft SMS authentication through the following SMS Gateways:

- DataMetrix
- Mgage
- Panacea Mobile

- Reason8
- Twilio
- Waterfall

E-mail Input Inline Validation

The Inline validation support is added to validate the e-mail ID entered by the customer for 'Email Authentication'. The inline validation support is also provided for validating the e-mail ID entered in the Data Capture form. Now the e-mail ID validation happens immediately after the customer enters the e-mail ID. Previously, the e-mail ID was validated after clicking the **Submit** button.

Country Name Derived from Country Codes

Now when a customer enters the phone number for Hard SMS authentication or in the Data Capture form, the EMSP runtime derives the country names from the country codes specified. The derived country name will be added as business tags in the User Subscriber system.

Known Issues

Table 2 Known Issues in the Enterprise Mobility Services Platform

Description
The SMS gateway configured is not listed immediately in the SMS Gateway grid. The "successfully saved" message is also not shown. Need to refresh to view the record.
In the portals, in the Data Capture module, you can save a business tag without providing the business tag options.
In the Proximity Rules such as Captive portal Rule, the radio buttons to select the locations are not displaying consistently in the Choose Location window.

Support

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