Release Notes for the Cisco Enterprise Mobility Services Platform Release 2.3

Release Month: February, 2016

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 8.

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, App Builder, 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

Enterprise Mobility Services Platform Studio

WiFi Engage

Enterprise Mobility Services Platform Studio

Support for the SMS and Social Authentication

The Enterprise Mobility Services Platform Studio now enables you to enhance the captive portals with SMS or social authentication.

A new OOB module group, WiFi Engage v2, is added to the Enterprise Mobility Services Platform Studio to support the captive portals with the SMS or social authentication. You can create the captive portal with SMS or social authentication in the WiFi Engage. Then, you can modify that captive portal using the Enterprise Mobility Services Platform Studio using the modules in the WiFi Engage v2 group. In addition, you can add other OOB modules to the portal to enhance the captive portal.

The OOB modules such as Context Aware Container requires social-authentication if configured for age, gender, or social targeting.

WiFi Engage

The following new features are available in the WiFi Engage:

Auto-Provisioning of the Location IDs for the CUWN or Meraki

When you connect to the Meraki or the CUWN account through the WiFi Engage main window, the WiFi Engage is enabled to do the following functions automatically:

- Generate the location ID.
- Associate the location ID to the connected CUWN or Meraki account.

The auto-generated location ID is displayed in the Location window in the WiFi Engage. For CUWN, the location is created based on the CUWN IP address. For Meraki, the location ID is created for a Meraki network.

Now, to use the modules such as Micello Wayfinding, Context Aware Container, and so on that requires device location details, you can generate the location ID, and associate the location ID to your CUWN or Meraki network yourself. You don't have to send the request to the Cisco support as done earlier.

For CUWN, the location ID is generated and associated to the CUWN account, when you connect the Enterprise Mobility services Platform to your CUWN account using the WiFi Engage. For Meraki, the location ID is generated and associated to the Meraki account, when you add an access point in a Meraki network to a location in the Enterprise Mobility services Platform using the WiFi Engage.

The previously mentioned functions were done manually by an Enterprise Mobility Services Platform Administrator. The user had to sent request to the Cisco support team to add the CUWN or Meraki account to the Enterprise Mobility Services Platform and to create the location ID.

New Role "Read Only Access"

A new user role "Read Only Access" is added to the Invite User window in the WiFi Engage.

You can invite a user by assigning the "Read Only Access" role.

The user with the "read only" access can view the WiFi Engage dashboard, but cannot edit any WiFi Engage configurations.

Instructions to Configure the Radius Server

The radius server details along with the instructions to configure it in the Meraki or CUWN are provided in the WiFi Engage.

- For Meraki, the instructions are specified in the Configure SSIDs manually tab that you can access from the SSIDs window.
- For CUWN, the instructions are specified in the Configuration Instructions tab that you can access from the SSIDs window.

SMPP Support for SMS Gateway

The WiFi Engage now supports the SMPP gateways.

The Account > Settings option in the WiFi Engage main window is updated to choose the SMS Gateway Type as HTTP or SMPP.

You can specify the following information for the SMPP Gateway:

- SMS Gateway Name
- Host
- Port
- System Id
- SMS Gateway Password
- Source Address

Enhancements

Enterprise Mobility Services Platform Studio

WiFi Engage

Enterprise Mobility Services Platform Studio

The following enhancements are made to the Enterprise Mobility Services Platform Studio:

Context Aware Container and Micello Wayfinding Support for the Meraki

The Context Aware Container and Micello Wayfinding modules now function for the Meraki network. The multi-building and multi-floor feature in the Micello Wayfinding module is not supported for the Meraki network.

Beacon Trigger Container Support on Meraki MR32

The Beacon Trigger Container module is now enabled to support the Meraki MR32.

In the Beacon Trigger Container module, the Proximity field is removed. Now, when a beacon detects a device with an app that has a Beacon Trigger Container module configured with the same UUID, Minor number and Major number of the beacon, it shows or hides the content in the Beacon Trigger Container module.

Enhancements for the Micello Wayfinding Module

The following enhancements are done to the Micello Wayfinding module:

- The Micello Wayfinding module is enhanced to display the maps faster as the Enterprise Mobility Services Platform location API call is moved to AJAX.
- A check box “Show User Location” is added for this module. The way to the destination is shown from the user’s current location only if you select this check box. Other wise, the map is displayed without a way pointer.
- The Micello Wayfinidng module now supports the search option provided in the maps by the Micello. The Micello provides a search option in the map that enables the users to search for stores and locations. The searched store or location is displayed in the map.
- The Micello Wayfinding module is enhanced to display the map centering the user’s current location. If the user is moving from a location, the map is centered based on the user’s latest location and displays the way to the destination from the user’s latest location.

WiFi Engage

The following enhancements are made to the WiFi Engage.

Meraki MX 64 Support

The WiFi Engage now supports the captive portals with the Meraki MX64 security appliance.

Social Authentication Support for the CUWN

The WiFi Engage is enhanced to provide the social-authentication support for the CUWN. You can restrict to provide the access to a portal only after authenticating through the specified social networking sites.

Radius-Authentication Support for the SMS and Social Authentications

The WiFi Engage is enhanced to enable the radius server support for the SMS and social authentications. The radius server configuration provides an additional layer of security for your portals. If configured for the radius-authentication, the internet is provisioned only after validating the user credentials with the radius server configurations.

Location Search by Access Point Name

The WiFi Engage now enables you to search for a WiFi Engage location based on the name of the access points associated with that location.

You can search for a location by specifying the access point name in the Search text field in the Locations window.

Delete SSIDs Marked "Removed/Renamed SSID"

The WiFi Engage now enables you to delete the SSIDs that are marked as "Removed/Renamed SSID" in the SSIDs window, provided the SSID is not associated with any experience zone.

The "Removed/Renamed SSID" mark denotes that the SSID is removed or renamed in the Meraki.

Engagement Report to Show Recent Users

The Engagement report is now enhanced to display the number of the users who have visited the portal at least 10 minutes before the report is generated.

SEULA in Activation Mail

When you invite a user to the Enterprise Mobility Services Platform using the Invite User button in the Manage Users> Users window, the user receives an activation e-mail.

The activation e-mail is now enhanced to have the Supplement End User License Agreement (SEULA) as attachment. Also, a link is provided in the e-mail to the Enterprise Mobility Services Platform service description offer.

Captive Portal Footer

The captive portals created using the WiFi Engage are now labeled "Enabled by Cisco Enterprise Mobility Services Platform" in the footer.

Known Issues

Table 2 Known Issues in the Enterprise Mobility Services Platform

Description
SSID configurations made in the Meraki are overwritten with the configurations made in the WiFi Engage—The SSID configurations made in the Meraki are synchronized by the WiFi Engage immediately after you log in to the WiFi Engage. After logging in to the WiFi Engage, if you make any changes to the SSID configuration in the Meraki, and then clicks the Sync button in the WiFi Engage, the WiFi Engage overwrites the configurations made in the Meraki. **Workaround**: After making changes in the Meraki, re-login to the WiFi Engage, and synchronize.
Read More links in the Enterprise Mobility Services Platform Dashboard—The Read More links in the Enterprise Mobility Services Platform dashboard are not linked to the appropriate pages. **Workaround**: None.
Font not as expected in the My Account window—After saving the password changes in the My Account window, the font of the text entered changes. **Workaround**: None.
Re-login after updating the installer patches—When you launch the Enterprise Mobility Services Platform Studio or App Builder, you are asked to update the installer patches, if any. After installing the patches, you need to re-login to launch the Enterprise Mobility Services Platform Studio or the Enterprise Mobility Services Platform App builder. **Workaround**: None.

Support

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