



Release Notes for the Cisco Enterprise Mobility Services Platform Release 2.2

Release Month: November, 2015

Contents

This document describes the system requirements, new features, enhancements, and known issues for the Cisco Enterprise Mobility Services Platform (EMSP). Use this document in conjunction with the documents listed in the [“Support” section on page 9](#).

- [Introduction to the EMSP, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 2](#)
- [Enhancements, page 5](#)
- [Known Issues, page 8](#)
- [Support, page 9](#)

Introduction to the EMSP

The EMSP is a mobile-application platform that enables rapid delivery of context-aware mobile experiences to meet the business requirements and customer expectations. The platform includes a cloud-based application server that combines the Cisco network infrastructure capabilities with the enterprise and open-cloud systems.

The EMSP comprises several applications that you can install and subscribe to, such as WiFi Engage, EMSP App Builder, EMSP Studio, EMSP SDK, and EMSP API. These applications enable you to access the various features of the EMSP.



[Send documentation comments to emsp-docfeedback@cisco.com](mailto:emsp-docfeedback@cisco.com)

System Requirements

This section lists the hardware requirements, operating systems, software requirements, and browsers for the EMSP.

Table 1 *System Requirements for the EMSP (WiFi Engage, EMSP App Builder, EMSP Studio, EMSP SDK, and EMSP API)*

Item	Supported Requirements
Hardware	<ul style="list-style-type: none"> 1 GHz processor 1 GB RAM 16 GB hard disk
API Network (For WiFi Engage)	<ul style="list-style-type: none"> MSE 7.1 or later
Operating System	<ul style="list-style-type: none"> Microsoft® Windows® XP or later Mac OS X 10.6 or later
Browser	<p>Windows OS</p> <ul style="list-style-type: none"> Internet Explorer version 9 or later Firefox version 30 or later Chrome version 34 or later Safari version 5.1.7 or later <p>Mac OS</p> <ul style="list-style-type: none"> 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
Mobile SDK	iPhone OS 6.0 or later, Android 2.3 or later

New Features

EMSP Dashboard

- [New User Interface for the EMSP Home Page and the EMSP Dashboard, page 3](#)
- [Do Not Track List, page 3](#)

EMSP Module

- [Multi-Building and Multi-Floor Support for the Micello Wayfinding Module, page 3](#)

WiFi Engage

- [WiFi-MX Re-branded, Redesigned, and Merged with the EMSP, page 4](#)
- [Third-Party Vendor Support for SMS Gateway, page 4](#)
- [Third-Party Vendor Devices Support, page 4](#)

Send documentation comments to emsp-docfeedback@cisco.com

- [SMS Verification Password: Auto-Generated and Custom](#), page 4

EMSP Dashboard

The following new features are available in the EMSP dashboard:

New User Interface for the EMSP Home Page and the EMSP Dashboard

The user interface of the EMSP home page and the EMSP dashboard are changed. The following links are added to the EMSP home page that appears when you access <https://emsp.cisco.com>:

- **What's New**— This link leads to the What's New section of the EMSP.
- **Learn EMSP**—This link leads you to the EMSP documentation.
- **Sales Resources**—This link leads you to sales-related information of the EMSP.
- **Features and Products**—The Features and Products sections are integrated to form a single section. The content for this section is updated with the latest modifications.

Do Not Track List

A new icon, Add MAC Address to Do Not Track List, is added to the EMSP dashboard. This option enables you to specify the MAC addresses of the mobile devices that are not to be tracked. The end users can inform you through an e-mail if their actions in a portal are not be tracked. You can enter the MAC address of the mobile of such users whose actions are not to be tracked.

EMSP Module

The following new features are available in the EMSP Module:

Multi-Building and Multi-Floor Support for the Micello Wayfinding Module

The Micello Wayfinding module is updated to provide multi-building and multi-floor support. This is applicable only for Cisco Unified Wireless Network (CUWN). Even though this functionality was available in the earlier version, it was not functioning as expected.

To use this feature, you need to create the Micello Wayfinding feed with the appropriate map details. You can obtain the map details from the Micello. You can use the Feed Editor icon in the EMSP dashboard to create the feed for the Micello Wayfinding.

If the feed details match with the EMSP API configuration, then the map of the floor where the user is currently presently is shown. If there is a mismatch, the default map is shown.

Send documentation comments to emsp-docfeedback@cisco.com

WiFi Engage

The following new features are available in the WiFi Engage:

WiFi-MX Re-branded, Redesigned, and Merged with the EMSP

The WiFi-MX is now branded as WiFi Engage and the WiFi Engage user interface is redesigned. All of the modules related to the WiFi Engage are accordingly renamed.

The WiFi Engage is now merged with the EMSP. When you click the Go to WiFi Engage icon in the EMSP dashboard, the WiFi Engage dashboard appears as a part of the EMSP. The new URL that appears for the WiFi Engage is emsp.cisco.com/wifiengage. The incoming requests to cisco.wifi-mx.com are redirected to emsp.cisco.com/wifiengage.

The Switch Account button label is removed. When you click the icon for Settings, the Settings window appears with a Connect Account button. You can switch your account using this button.

The Microsite option that was available in the earlier version of the WiFi Engage (WiFi-MX) is removed.

Third-Party Vendor Support for SMS Gateway

The WiFi Engage now supports the SMS gateway of third-party vendors. You can configure the customized SMS gateway in the Settings option.

Third-Party Vendor Devices Support

The WiFi Engage now supports the following third-party wireless network providers: Motorola, Xirrus, and Ruckus. The entire WiFi Engage functionality is extended for these networks.

SMS Verification Password: Auto-Generated and Custom

The WiFi Engage now lets you configure either a custom password or an auto-generated password for an SMS Gateway. Additional fields such as Default Country Code, SMS Gateway, and Password Type are added to the SMS verification option under the Authentication module to support this feature.

Send documentation comments to emsp-docfeedback@cisco.com

Enhancements

EMSP Studio

- [Unified EMSP Studio Installer, page 5](#)
- [Adobe Flash Player Dependency Removal, page 5](#)

EMSP App Builder

- [Unified App Builder Installer, page 6](#)
- [Adobe Flash Player Dependency Removal, page 6](#)

WiFi Engage

- [Get Invite Window, page 6](#)
- [Social and SMS Authentication Now to Allow Customer's Own App, page 6](#)
- [Advanced Configuration for Radius Server and Captive Portal, page 7](#)
- [Search By MAC Address, page 7](#)

EMSP Studio

The following enhancements are made to the EMSP Studio:

Unified EMSP Studio Installer

The EMSP Live Studio, EMSP Sandbox Studio, and WiFi Engage Studio installers are unified, and a single EMSP Studio installer is provided for all of the environments. You can download the unified EMSP Studio installer from the EMSP main window that appears when you log in to <https://emsp.cisco.com>. During the initial launch of the EMSP Studio, all of the environments are installed on your computer. A single client icon appears on your desktop for the Cisco EMSP Studio. When you click this icon, an environment window appears from which you can choose the required environment to which you need to log in. The EMSP Studio icon in the EMSP main window always redirects you to the Live environment. The following environments are available:

- Live—The environment for the admin users and portal developers.
- Development Cloud—The environment for the developers who create custom modules.
- Developer—The environment for the internal developers.

Adobe Flash Player Dependency Removal

The Cisco EMPS Studio is enhanced to work without the Adobe Flash Player. You do not have to install the Adobe Flash Player now to launch the EMSP Studio. The prerequisites for the EMSP Studio installation are Java and Adobe Air plug-in.

Send documentation comments to emsp-docfeedback@cisco.com

EMSP App Builder

The following enhancements are made to the EMSP App Builder:

Unified App Builder Installer

The EMSP Live App Builder and EMSP Sandbox App Builder installers are unified and a single EMSP App Builder installer is provided for both the environments. You can download the unified EMSP App Builder installer from the EMSP main window that appears when you log in to <https://emsp.cisco.com>. During the initial launch of the EMSP App Builder, both these environments are installed on your computer. A single client icon appears on your desktop for the Cisco EMSP App Builder. When you click this icon, an environment window appears from which you can choose the required environment to which you need to log in. The EMSP App Builder icon in the EMSP main window always redirects you to the Live environment. The following environments are available:

- Live—The environment for the end users such as app builders.
- Development Cloud—The environment for the developers who create customized modules.

Adobe Flash Player Dependency Removal

The Cisco EMSP App Builder is enhanced to work without the Adobe Flash Player. You do not have to install the Adobe Flash Player now to launch the EMSP Add Builder. The prerequisites for the EMSP App Builder installation are Java and Adobe Air plug-in.

WiFi Engage

The following enhancements are made to the WiFi Engage:

Get Invite Window

In the Get Invite window, two new fields are added to specify the company name and designation of the user. This Get Invite window is used to send an invite to the users to enable them to access their WiFi Engage account.

Social and SMS Authentication Now to Allow Customer's Own App

The WiFi Engage now lets the customer configure their own social apps.

A new option, Settings, is available in the WiFi Engage. Click the Accounts icon in the WiFi Engage dashboard to view the Settings option. This option enables you to configure the customer-specific social apps and SMS gateway. You can configure the following in the Settings window:

- SMS Gateway—You can configure your customized SMS gateway using this option.
- Facebook App—You can configure your customized Facebook app through this option. You require this app, so that users can sign in to Facebook from your captive portal.
- Google App—You can configure your customized Google app through this option. You require this app, so that users can sign in to Google plus from your captive portal.
- Twitter App—You can configure your customized Twitter app through this option. You require this app, so that users can sign in to Twitter from your captive portal.
- Linked In App—You can configure your customized Linked In app through this option. You require this app, so that users can sign in to Linked In from your captive portal.

Send documentation comments to emsp-docfeedback@cisco.com

If you need to use any social sign-in feature in your portal that requires authentication, then you need to configure the respective social app in the Settings option. You can configure the apps of Facebook, Google, Twitter, and Linked In.

To integrate the app with a captive portal, in the Authentication module in **Create> Portals**, specify the required app.

Advanced Configuration for Radius Server and Captive Portal

The WiFi Engage is enhanced to show whether a radius server from the EMSP or a captive portal created using the EMSP Studio is configured for an SSID. If either of these, or both of these are configured for an SSID, then an Advanced Configuration With Meraki message appears against that SSID in the Actions column of the SSID window.

In addition, for the radius server configuration, the Radius Server Configuration message appears in the Remarks column. Similarly, for an EMSP Studio portal configuration, the details of the EMSP Studio Portal configuration appear in the Remarks column of the SSID. A green indicator is shown for each of these configurations.

If the Radius server or captive portal configured is not of the EMSP, the sync option appears in red.

You can revert the advanced configurations for an SSID by clicking the corresponding Revert to Basic Config button. Then, the WiFi Engage captive portal gets configured for that SSID.

Search By MAC Address

The WiFi Engage now lets you search for a location based on the MAC address of the access points. You can specify the MAC address of an access point in the search option that is available in the Locations window.

[Send documentation comments to emsp-docfeedback@cisco.com](mailto:emsp-docfeedback@cisco.com)

Known Issues

Table 2 *Known Issues in the EMSP*

Description
<p>The email ID entered in the Forward Password window is not deleted—In the WiFi Engage login window, when you click the Forgot your password? link, a Cisco WiFi Engage window appears where you can enter the email ID. The link to create the new password is sent to this ID. After entering the email ID, if you click the Back to Login button to go back to the Login window, and then click the Forgot your password? link again, the email ID specified earlier is shown.</p> <p>Workaround: None.</p>
<p>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.</p> <p>Workaround: After making changes in the Meraki, re-login to the WiFi Engage, and synchronize.</p>
<p>Read More links in the EMSP Dashboard—The Read More links in the EMSP dashboard are not linked to the appropriate pages.</p> <p>Workaround: None.</p>
<p>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.</p> <p>Workaround: None.</p>

Send documentation comments to emsp-docfeedback@cisco.com

Table 2 ***Known Issues in the EMSP***

Description

Repeated Installer file download for the EMSP Studio and EMSP App Builder—The following browsers have issues when launching the EMSP Studio or the EMSP App Builder in the Mac operating systems:

Safari—After logging in to the EMSP Studio, if the user tries to launch the EMSP Studio again from the EMSP dashboard, the user is prompted to download the installer. The same issue occurs for the EMSP App Builder.

Google Chrome or Mozilla Firefox—After logging in to the EMSP Studio, if the user tries to launch the EMSP Studio again from the EMSP dashboard, the user is not taken to the opened EMSP Studio window. For Google Chrome, an alert message is shown in the Status Bar when downloading the installer. The same issue occurs for the EMSP App Builder.

Workaround: None.

Re-login after updating the installer patches—When you launch the EMSP Studio or App Builder, the EMSP asks you update the installer patches, if any. After installing the patches, you need to re-login to launch the EMSP Studio or the EMSP App builder.

Workaround: None.

Support

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