Release Notes for the Cisco CMX Engage Release 3.2.10

Release Month: March, 2018

Contents

This document describes the enhancements, resolved issues, and open issues for the Cisco CMX Engage Release 3.2.10. Use this document in conjunction with the documents listed in the "Support" section on page 4.

- Introduction to the CMX Engage, page 1
- New Features, page 2
- Enhancements, page 2
- Resolved Issues, page 4
- Open Issues, page 4
- Support, page 4

Introduction to the CMX Engage

The CMX Engage is a location intelligence, digital customer acquisition and multi-channel engagement platform that enables companies to connect, know, and engage with visitors at their physical business locations.

The major features of the CMX Engage 3.2.10 release are as follows:

- Optimized the synchronization process by limiting the synchronization only for the updated floors.
- Provision to restrict adding Meraki APs and security appliances based on the license limit for the customer.
- For CUWN-WLC, optimized the AP updation process by defining stale duration for APs.
- Support to configure bandwidth and session expiry period in the Captive Portal Rule.

Cisco Systems, Inc.
www.cisco.com

- Provision to add custom variables for Trigger API parameters.
- Provision to remove invalid Meraki credentials from the CMX Engage.
- {Link} made optional for the “SMS with Password Verification” authentication.

New Features

CMX Engage Dashboard

- Network Synchronization for Floor, page 2
- Support for License Limit Check, page 2

CMX Engage Dashboard

The following new features are added to the CMX Engage dashboard:

Network Synchronization for Floor

The CMX Engage is now enhanced to synchronize the Meraki floors based on the updates in the Meraki. The subsequent synchronization for a floor is carried out only if that Meraki floor is updated. This increases the efficiency of the synchronization process.

Support for License Limit Check

For Meraki, during network synchronization, the CMX Engage now checks whether the APs/Security Appliances in the Meraki exceeds the CMX Engage license limit for that customer. If the license limit exceeds, then new APs/Security Appliances will not be added and synchronized to the CMX Engage.

Enhancements

CMX Engage Dashboard

- Optimized AP Updation Process, page 3
- Support to Define Bandwidth and Session Expiry, page 3
- Custom Variables for Trigger API Parameters, page 3
- Support to Remove Outdated Meraki Credentials, page 3
- SMS with Password Verification, page 4

CMX Engage Dashboard

The following enhancements are made to the CMX Engage Dashboard:

Optimized AP Updation Process

For the wireless network, CUWN-WLC, the AP updation process is optimized by defining a stale duration for each AP. If the WLC APs are not updated within the stale duration, those APs are considered as stale. Currently the time interval to get updates for an AP is 2 hours. Now, when CMX Engage gets new set of APs, it removes the APs that crossed the stale duration, updates other existing APs, and appends new APs, if any. Previously, the CMX Engage used to replace the existing APs with new set of APs without any verification.

Support to Define Bandwidth and Session Expiry

The CMX Engage dashboard now supports configuring bandwidth and session expiry for the captive portals in the Captive Portal Rules.

In the “Create Captive Portal Rule” window, in the Actions area, under the “Show Portals” section, the following fields are added to support this feature.

- Session Duration
- Bandwidth Limit

You can configure the session duration in minutes, hours, or days. You can specify a bandwidth between the range 1kbps-1 tbps.

This bandwidth and session expiry configurations will override the configurations in the wireless network such as Meraki or CUWN. In addition, you can configure more session duration than the one that you can configure in the wireless network. For example, if the maximum session duration that you can specify in Meraki is 90 days, you can configure more than 90 days as session duration using this feature.

Custom Variables for Trigger API Parameters

For the Trigger API methods, “Get”, “Post Form”, and “Post JSON”, you can now add custom variables for the Key parameters. To add the custom variables, a “Add Custom Variable” button is displayed at the bottom of the variable list, which appears when you click the “Add Variable” button. To know the list of custom variables that you can add, contact the CMX Engage support team.

Support to Remove Outdated Meraki Credentials

The CMX Engage is now enhanced to remove the outdated Meraki credentials from the CMX Engage. This helps to avoid the Meraki accounts getting locked due to login attempts from the CMX Engage dashboard using outdated credentials. This issue occurs when the Meraki credentials are updated in the Meraki system.

If the credentials for a Meraki account is updated in the Meraki system, you cannot execute a CMX Engage activity that needs a connection to the Meraki network. For example, Importing the SSIDs. In addition, when you click the “Wi-Fi” icon in the left pane of the CMX Engage dashboard, a label “Disconnected” is displayed for the Meraki network. When you click the Meraki Network, the “Meraki Account Settings” window appears with a description “Click here to remove your Meraki Credentials from CMX Engage” at the bottom of the window. You can remove the outdated Meraki credentials by clicking the “Click here” link. You can then connect to the Meraki network by specifying the updated credentials in the “Meraki Account Settings” window.

SMS with Password Verification

For the “Hard SMS with Password Verification” authentication, the {link} that appears in the “SMS Text” box is now made optional. You can create the portal for “SMS with Password Verification” authentication, even if you remove the {link} in the “SMS Text” box. However, if you remove the {link}, the SMS sent will not have the link to access the captive portal.

Resolved Issues

Table 1 Resolved Issues in the CMX Engage 3.2.10

Description
CMX Engage Dashboard
In the “Right Now” reports, in the “Current visitors by their locations” section, the child locations are having more visitor count than the parent location.
CMX Engage Runtime
The Facebook authentication was failing due to ‘Strict URI Matching” enabled in the Facebook API.
CMX Engage Studio
For the portals enhanced using the Form Modules group or CMX Engage V3 module group, when reconnecting to the SSID, the customer is not redirected to the same screen the customer was in when got disconnected (for example, the Data Capture screen or OTP screen),

Open Issues

Table 2 Open Issues in the CMX Engage 3.2.10

Description
There are no open issues for this release.

Support

You can access the support documentation using the Help button in the CMX Engage Dashboard.