Offer Description for
CMX Engage

This document describes the Cisco CMX Engage Offering sold by Cisco Systems, Inc. and Cisco Authorized Resellers.

Offer Description
Upon payment of the relevant charges, Cisco shall provide CMX Engage and its associated support (together, the "Offering") described in this document (the "Offer Description"). An Offer Description may also be referred to in some documents as a "Service Description" and the Offering may also be referred to in some documents as the "Services".

Governing Agreement
This Offer Description is subject to the terms of the Cisco SaaS Agreement (or another Product, End User License, or Services Agreement agreed to between Customer and Cisco) referenced in the Order, including any applicable Supplemental End User License Agreement or other addenda associated with the Offering (the "Agreement"). If you purchased this Offering through a Cisco Authorized Reseller, this document is for informational purposes only except for Section 7, Data Privacy and its attachments which the Cisco Authorized Reseller must flow to you, and you must agree to comply with, as a condition of sale. This document is not a contract between you and Cisco. The contract, if any, governing the provision of this Offering is the one between Customer and its Cisco Authorized Reseller. Such Cisco Authorized Reseller should provide this document to Customer, or Customer can obtain a copy of this and other Cisco service descriptions and offer descriptions at www.cisco.com/go/servicedescriptions/.

Order
An "Order" means a written or electronic order to Cisco for the Offering, to be provided by Cisco under the Agreement. Such Order will reference this Offer Description and the Agreement and will detail the quantity, type, pricing, and payment terms purchased by the Customer.

Order of Precedence
Customer will have the right to use the Offering for the term specified in the Order, subject to the conditions of the Agreement and this Offer Description. If there is a conflict between the Agreement and this Offer Description, this Offer Description will take priority over the Agreement; any conflicting conditions in the Order will take precedence over both.

Defined Terms
Unless otherwise defined in the body of this Offer Description, capitalized terms used in this Offer Description are defined in the Glossary of Terms attached as Exhibit A to the CMX Engage offer description, or in the Agreement.

1. Introduction

This Offer Description describes the Cisco CMX Engage provided by Cisco to Customer including offer specific terms and conditions.

2. Cisco CMX Engage Overview

Cisco CMX Engage enables the rapid delivery of context-aware mobile experiences that exceed business and customer expectations. It integrates Cisco network infrastructure capabilities with enterprise and open cloud systems, creating ready-to-use modules for mobile, web and native applications.

Unless otherwise stated for a particular Cisco CMX Engage package, Cisco CMX Engage is consumed via a public cloud-based software platform as the standard model.

2.1. The Offering includes the features and components described below based on the specific package (package choices set forth in Section 3.8) purchased by Customer:

a. CMX Engage
d. CMX Engage Advanced

3. Components and Packages

3.1. CMX Engage is a cloud platform service that provides following services:

- **System Configuration Dashboard:** CMX Engage dashboard provides central IT Teams with oversight and control of the CMX Engage System Configurations for:
- **Wi-Fi Network configuration:** Allowing IT administrators to configure the Wi-Fi infrastructure controller admin credentials in CMX Engage to sync Wi-Fi network SSIDs as well as access points along with location hierarchy into the CMX Engage Location Manager to associate CMX Engage hierarchical tags to these locations for visitor engagements.
- **SMS & Email Notification Servers:** Allowing IT (Infrastructure Technology) administrators to configure the SMS (SMPP & HTTPS) Gateway servers and Email notification (SMTP & HTTPS) servers to be used for CMX Engage visitor LBS engagements.
- **Social Sign-in Credentials:** Allowing IT administrators to configure Facebook, Twitter, Google+, LinkedIn and Twitter business accounts that can be used for validating visitor's social credentials during on-boarding experiences as valid user ids for provisioning Guest Wi-Fi internet service and collecting personal information for references in engagement rules for delivering personalized CMX Engage LBS engagements to visitors.
- **Location Manager:** Allows IT and LoB (Line of Business) administrators to create tags on top of existing Wi-Fi network infrastructure hierarchy as well as configure BLE beacons for physical location identifications with-in CMX Engage runtime. Location Manager provides the capability to define the business physical location hierarchy for use with-in rules engines, reports & insights as well as to associate Wi-Fi captive portals to a location.
- **Portal Design Studio:** Portal Design Studio provides Web developers & designers to create pixel perfect Wi-Fi captive portals for each location defined in the location manager. It provides simple to use WYSWYG interface for non-programmers to create simple yet powerful well formatted CNA (Captive Network Assistant) web portal for creating Wi-Fi Guest Access on-boarding experiences compatible with multiple system browsers on various Android, iOS & Windows smart phones as well as tablets and computers. Portal Design Studio provides:
- **Smart Menu Items:** These systems defined portal menu items are optimized for triggering state full break away from CNA to system browser during internet provisioning on the device as well as auto formatting & positioning based on device type.
- **CSS Editor:** This online editor provides designers with enhanced capabilities to enhance the styling of the Wi-Fi portals to match the brand standards.
- **Portal Preview:** This online tool gives real-time preview of the actual portal experience on a user's device based on the configurations in the web designer. It also provides the option of emailing the preview portal URL for review by users outside the web dashboard or via scanning a QR-code that corresponds to the preview URL.
- **User Authentications:** Portal designer provides following user authentication mechanisms for authenticating a user's identity prior to provisioning the internet access on user's device:
    - **No Auth:** Simple click-through on a call-to-action button provisions the internet for the user upon successful agreement to T&Cs terms for using the free internet service.
    - **Email Auth**: User is asked to provide a valid email address along with opt-in to receive the LBS services emails and acceptance of T&Cs for using the free internet service.
    - **Ph # SMS Auth**: User is asked to provide a valid mobile phone # to receive a one-time password which user enters to successfully provision the service. User also is asked to opt-in for receiving LBS SMS-es & acceptance of T&Cs for using the free internet service.
    - **Ph # capture Auth**: User is asked to provide a valid ph # and accept T&Cs for using free internet service. (This authentication type cannot be used to receive LBS SMS).
    - **Social Sign-in Auth:** User is asked to use their social network username & password to authenticate their identity to get free internet service. User is also asked to accept T&Cs for using free internet service. Social networks supported for user validations are Facebook, Twitter, and LinkedIn.
- **Data Capture:** This form provides the capability to collect additional personal information about the user during first time or repeat visit internet service authorization on user's device. This information is used for personalized engagements as well as associating the device & log-in identity with personal information of the user. The current elements supported in the data capture form are: Title, First Name, Last Name, Gender, Email, Ph # and business tag. Business Tag is a configurable name:value pair selection that enterprises can use to capture visitor's preferences on a key service or product offered by the enterprises and use that to create personalized engagements for the visitors.
- **Captive Portal Rules:** To create new and repeat visit rules for displaying appropriate captive portal to user prior to provisioning the free internet service on user's device.
- **Reports:** Provide an up to the hourview into LBS activities across physical locations (as defined in location manager). Currently supported reports are:

  - **Customer Acquisition:** This report shows a summary & detailed view of user data acquired during free Wi-Fi internet service provisioning on a device summarized on day-by-day basis.
  - **User Activity:** These report summaries the average dwell time by users at a location, # of repeat visits, avg. time between the visits, avg. daily visits etc. capturing the user behavior snapshot at each location.
  - **Engagements:** This report shows a summary of LBS engagement success and utilization across captive portals.
- **Data Export APIs:** These APIs provide an offline post of user information captured using Wi-Fi captive portal data capture & authorization flow as a CSV or to a backend enterprise system e.g CRM or loyalty system.
- **User Manager:** This allows account administrator to invite different users in the organization and give them one of the following roles with-in CMX Engage runtime:
  - **Account Admin:** This is the super user account in CMX Engage that provides full read & write access to every configuration of the system.
  - **Admin:** This user is allowed to invite other users and has read-write access to captive portal, rules engine and reports sections.
  - **Location Manager:** This user is allowed to create, modify and delete captive portals.
  - **Read-only**: This user is allowed to view any/all configurations as well as reports.

3.2. **CMX Engage Advanced Package**

- **System Configuration Dashboard:** CMX Engage dashboard provides central IT Teams with oversight and control of the CMX Engage System Configurations for:
- **Wi-Fi Network configuration:** Allowing IT administrators to configure the Wi-Fi infrastructure controller admin credentials in CMX Engage to sync Wi-Fi network SSIDs as well as access points along with location hierarchy into the CMX Engage Location Manager to associate CMX Engage hierarchical tags to these locations for visitor engagements.
- **SMS & Email Notification Servers:** Allowing IT (Infrastructure Technology) administrators to configure the SMS (SMPP & HTTPS) Gateway servers and Email notification (SMTP & HTTPS) servers to be used for CMX Engage visitor LBS engagements.
- **Social Sign-in Credentials:** Allowing IT administrators to configure Facebook, Twitter, Google+, LinkedIn and Twitter business accounts that can be used for validating visitor's social credentials during on-boarding experiences as valid user ids for provisioning Guest Wi-Fi internet service and collecting personal information for references in engagement rules for delivering personalized CMX Engage LBS engagements to visitors.
- **Location Manager:** Allows IT and LoB (Line of Business) administrators to create tags on top of existing Wi-Fi network infrastructure hierarchy as well as configure BLE beacons for physical location identifications with-in CMX Engage runtime. Location Manager provides the capability to define the business physical location hierarchy for use with-in rules engines, reports & insights as well as to associate Wi-Fi captive portals to a location.
- **Portal Design Studio:** Portal Design Studio provides Web developers & designers to create pixel perfect Wi-Fi captive portals for each location defined in the location manager. It provides simple to use WYSWYG interface for non-programmers to create simple yet powerful well formatted CNA (Captive Network Assistant) web portal for creating Wi-Fi Guest Access on-boarding experiences compatible with multiple system browsers on various Android, iOS & Windows smart phones as well as tablets and computers. Portal Design Studio provides:
- **Smart Menu Items:** These systems defined portal menu items are optimized for triggering state full break away from CNA to system browser during internet provisioning on the device as well as auto formatting & positioning based on device type.
- **CSS Editor:** This online editor provides designers with enhanced capabilities to enhance the styling of the Wi-Fi portals to match the brand standards.
- **Portal Preview:** This online tool gives real-time preview of the actual portal experience on a user's device based on the configurations in the web designer. It also provides the option of emailing the preview portal URL for review by users outside the web dashboard or via scanning a QR-code that corresponds to the preview URL.
- **User Authentications:** Portal designer provides following user authentication mechanisms for authenticating a user's identity prior to provisioning the internet access on user's device:
  - **No Auth:** Simple click-through on a call-to-action button provisions the internet for the user upon successful agreement to T&Cs terms for using the free internet service.
  - **Email Auth**: User is asked to provide a valid email address along with opt-in to receive the LBS services emails and acceptance of T&Cs for using the free internet service.
  - **Ph # SMS Auth**: User is asked to provide a valid mobile phone # to receive a one-time password which user enters to successfully provision the service. User also is asked to opt-in for receiving LBS SMS-es & acceptance of T&Cs for using the free internet service.
  - **Ph # capture Auth**: User is asked to provide a valid ph # and accept T&Cs for using free internet service. (This authentication type cannot be used to receive LBS SMS).

    - **Social Sign-in Auth:** User is asked to use their social network username & password to authenticate their identity to get free internet service. User is also asked to accept T&Cs for using free internet service. Social networks supported for user validations are Facebook, Twitter, and LinkedIn.
- **Data Capture:** This form provides the capability to collect additional personal information about the user during first time or repeat visit internet service authorization on user's device. This information is used for personalized engagements as well as associating the device & log-in identity with personal information of the user. The current elements supported in the data capture form are: Title, First Name, Last Name, Gender, Email, Ph # and business tag. Business Tag is a configurable name:value pair selection that enterprises can use to capture visitor's preferences on a key service or product offered by the enterprises and use that to create personalized engagements for the visitors.
- **Captive Portal Rules:** To create new and repeat visit rules for displaying appropriate captive portal to user prior to provisioning the free internet service on user's device.
- **Reports:** Provide an up to the hourview into LBS activities across physical locations (as defined in location manager). Currently supported reports are:
    - **Customer Acquisition:** This report shows a summary & detailed view of user data acquired during free Wi-Fi internet service provisioning on a device summarized on day-by-day basis.
    - **User Activity:** These report summaries the average dwell time by users at a location, # of repeat visits, avg. time between the visits, avg. daily visits etc. capturing the user behavior snapshot at each location.
    - **Engagements:** This report shows a summary of LBS engagement success and utilization across captive portals.
- **Data Export APIs:** These APIs provide an offline post of user information captured using Wi-Fi captive portal data capture & authorization flow as a CSV or to a backend enterprise system e.g CRM or loyalty system.
- **User Manager:** This allows account administrator to invite different users in the organization and give them one of the following roles with-in CMX Engage runtime:
    - **Account Admin:** This is the super user account in CMX Engage that provides full read & write access to every configuration of the system.
    - **Admin:** This user is allowed to invite other users and has read-write access to captive portal, rules engine and reports sections.
    - **Location Manager:** This user is allowed to create, modify and delete captive portals.
    - **Read-only**: This user is allowed to view any/all configurations as well as reports.
- **Rule Engine Configurator:** Rule engine configurator provides a very powerful configuration for creating location specific visitor personas as well as personalized visitor LBS engagements. It provides following IFTTT (**IF T**his **T**hen **T**hat) LBS rule configurations for:
    - **Engagement Rules:** To create user engagement rules based on entry, dwell and exit from location using user persona and previous historic engagement success at location for both user facing as well as business (back-end enterprise system) facing engagement actions.
    - **Profile & Insights Rules:** To define LBS behavior persona tags and categories based on visit and duration of visit by visitors at locations captured over a period of time for use in captive portal & engagement rules as well as in reports
- CMX Engage SDK
- CMX Engage SDK provides easy access to location based user engagement, seamless WiFi connectivity, WiFi onboarding.
    - Features
        - Location Based Engagements (Using iBeacons and WiFi)
        - Seamless WiFi Connectivity
        - WiFi Onboarding through App
        - Subscriber API's for defining personas

3.8 Packaging

Features	CMX Engage	CMX Engage Advanced
Smart Location Hierarchy	Included	Included
Captive portal creation tools	Included	Included
Captive portal rules	Included	Included
Reports and analytics	Included	Included
Real –time API to integrate customer data @ onboarding	Included	Included
Export of customer data	Included	Included
Profile rules for location based personas and insights		Included
Multichannel engagement (SMS, Email, applications, API)		Included

Rules driven API post to third-party systems		Included
SDK for easy Wi-Fi on-boarding for application users		Included
Location-based application push notification with SDK		Included

4. CMX Engage Cloud Connection

4.1. To provide a quality service, and deliver as much automation as CMX Engage capabilities provide, the Offering is cloud based and Customer may need, or desire, integration with Customer's local/cloud infrastrucuture, including an IPSEC tunnel between the Customer's infrastructure/data center and CMX Engage data centers. If Customer desires or needs such integration, Customer must notify Cisco within 14 days of the Effective Date of the Offering ("Implementation Period"). If notified within the Implementation Period, Cisco will provide the Customer with the information, configurations and personnel resources reasonably necessary for Customer to effect such integration. Support is included as part of this Offering (see section 5 below) and professional services are available through Cisco Advanced Services for an additional fee; however, the need for this implementation on the Customer premise equipment is the sole responsibility of, and can only be implemented by, the Customer. The initial Subscription Term for CMX Engage will still accrue for that period of time in which the Implementation Period is in effect.

5. Support Services Included in the Offering

5.1. This Section describes Cisco CMX Engage support services which are included with CMX Engage (the "Services", together with EMPS, the "Offering"). These Services are not available for separate purchase.

5.2. Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/ : (1) the online Glossary of Terms; (2) List of Services Not Covered; and (3) Severity and Escalation Guidelines. All capitalized terms in this Section have the meaning ascribed to them in Exhibit A below, or the online Glossary of Terms; the definitions in Exhibit A below shall govern in the case of any conflicting definitions.

5.3. Direct Sale from Cisco: If you have purchased the Offering that include these Services directly from Cisco, this document is incorporated into your applicable master purchase agreement with Cisco. In the event of a conflict between this Offer Description and your applicable master purchase agreement, this Offer Description shall govern.

5.4. Sale via Cisco-Authorized Reseller. If you have purchased this Offering through a Cisco-Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Offering will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

5.5. CMX Engage Support

- Cisco Responsibilities:
  - Cisco Technical Assistance Center ("TAC") access 24 hours per day, 7 days per week to assist by telephone, fax, electronic mail or the internet with CMX Engage use, configuration and troubleshooting issues. Cisco will respond within one (1) hour for all calls received during Standard Business Hours and for Severity 1 and 2 calls received outside Standard Business Hours. For Severity 3 and 4 calls received outside Standard Business Hours, Cisco will respond no later than the next Business Day. Manage problems according to the Cisco Severity and Escalation Guideline
  - Access to Cisco.com. This system provides Customer with helpful technical and general information on Cisco Products as well as access to Cisco's on-line Software Center library. Please note that access restrictions identified by Cisco from time to time may apply.
  - Work-around solutions or patches to reported CMX Engage problems will be provided using reasonable commercial efforts. An advantage of the CMX Engage cloud based solution is any patches or Maintenance Releases/updates for CMX Engage users experiencing the problem in their subscription will be implemented automatically with little or no action on the Customer's part.
  - Minor and Maintenance Releases/Updates. All paying Customers will receive updates corresponding to the CMX Engage package to which they subscribe ("Updates"). Such Updates are limited to CMX Engage Components that have been validly licensed and paid for and that are covered under a current Term Subscription contract and whose account is in good standing order. Cisco may also release additional features or complementary services that are not included in the subscription and are available at an additional charge. Cisco may from time to time discontinue or remove some features that are deemed as depreciated or have low customer adoption. Applicable supporting Documentation for the latest production version, if available, is on Cisco.com and is limited to only the current production instance of CMX Engage.
- Customer Responsibilities:
  - Provide a severity level as described in the Cisco Severity and Escalation Guideline (http://www.cisco.com/web/about/doing_business/legal/service_descriptions/docs/Cisco_Severity_and_Escalation_Gui delines.pdf) for all interactions the Customer has with CMX Engage Support.
  - Grant Cisco reasonable access to the Product and Data and systems passwords so that problems may be diagnosed and, where possible, corrected remotely.
  - Provide thirty (30) days notice to Cisco of any requested addition(s) to Your Equipment List that may impact or require configuration changes to Offering.
  - Provide valid and applicable serial numbers for all Product problems and issues reported to Cisco or where Customer is seeking information from Cisco in connection with the Product use. Cisco may also require Customer

to provide additional information in the form of location of the Product, city location details and zip code information.

- Pay all engineering time, travel, and out-of-pocket expenses if Subscriber request performance of onsite services or services outside the scope of service options described in this document.
- Provide any Hardware required to perform fault isolation.
- Make all reasonable efforts to isolate the Offering's problem prior to requesting support from Cisco.
- Acquire, install configure and provide technical support for all:
  - Third-party Products, including upgrades required by Cisco or related services; and
  - Network infrastructure, including, but not limited to, local and wide-area data Networks and equipment required by Cisco for operation of the Offering.

6. [Reserved]

7. Data Privacy

This Section contains the terms under which each of Cisco and the Customer will protect data, including personal data, and forms an integral part of the Agreement between Customer and Cisco. Customer's adherence to this Section is a prerequisite for using the Offering. In the event of a contradiction between the Agreement, Cisco's Privacy Policy and/or this Section, this Section prevails for the subject matter indicated herein.

1. Cisco CMX Engage will collect information identifying a device and its location and certain information provided by a User through a portal that is created with the CMX Engage WiFi Engage Component ("Captive Portal"), web/browser app, or an app that is created with the CMX Engage App Builder Studio Component ("Native App") created by Customer using Cisco CMX Engage (collectively, "User Data"). The types of User Data that may be collected by Cisco CMX Engage are set out on Attachment 1 to this Data Privacy Section, directly following this Section.

a) Cisco CMX Engage will create a profile of a User by associating the User Data with a unique subscriber ID ("User Profile").

b) Prior to a User logging into a Captive Portal, web/browser app or Native App, Cisco CMX Engage will only collect device identifiers (MAC addresses) and location information and the User Profile will not include a User's name, email address, demographic information and similar personal information.

c) While a User is logged into a Captive Portal, web/browser app, or Native App, Cisco CMX Engage will collect information submitted by the User through the Captive Portal or Native App (subject to Customer's compliance with the requirements of Section 4 below).

d) Cisco CMX Engage will collect User Data when a User is located at a Customer Site and will not collect information when a User is at a location of another customer that uses Cisco CMX Engage.

e) Unless otherwise agreed by the parties in writing, User Data will be hosted by Cisco and its subcontractors and Cisco will not provide Customer with a copy of the User Profiles. Customer will be able to access User Profiles using the Cisco CMX Engage APIs.

2. Information about Users provided by third parties and other sources may be added to User Profiles as Customer and Cisco may mutually agree.

a) With the mutual agreement of Customer and Cisco, social profile information about Users who log into a Captive Portal or Native App using a social login ID will be added to the User Profile. Cisco may require Customer to license such social profile information directly from a social network or other third party.

b) Customer may request that Cisco add to the User Profiles information about Users that has been collected by Customer. Cisco will not be required to host User information the processing of which Cisco believes in its sole discretion does not comply with Section 4 or that may not be processed or stored by Cisco in compliance with applicable Privacy Laws.

c) Cisco makes no representations or warranties to Customer with respect to any social profile information or information from other sources.

3. Customer may use Cisco CMX Engage for the following purposes:

a) Personalization for visitors, including in-venue guidance and product/service finder;

b) Analytics and business intelligence for Customer;

c) Marketing by Customer on Customer's behalf, including proximity-based offers; and

d) Marketing by Customer on behalf of third parties who provide goods or services in a Customer Site.

4. Customer represents and warrants that:

a) Customer has and will maintain a privacy policy that (i) is available via a link on the landing page of the Customer's website, (ii) describes the collection and use of Customer Data under this Agreement, and (iii) discloses that Customer may track visitors using mobile device wireless information such as MAC addresses but such information will not be associated with a visitor's personal information without the visitor's consent.

b) Customer will comply with applicable app store policies regarding privacy policies and user consent for

access to location and device data with respect to any Native Apps.

c) Prior to collecting any personal information through a Captive Portal, web/browser based app, or Native App, Customer will obtain consents from a User in accordance with the CMX Engage User Experience Guidelines and otherwise as may be required and in such form as necessary to comply with applicable Privacy Laws. The User Experience Guidelines are set out in Attachment 2 to this Data Privacy Section, directly following this Section.

d) In the countries and territories in which Customer will use the Offering, Customer will comply with all applicable Privacy Laws.

e) Unless otherwise agreed by Cisco in writing, Customer will only use Cisco CMX Engage as provided in Section 3 above.

f) Notwithstanding the foregoing, Customer will not use Cisco CMX Engage for (i) delivery of third-party marketing offers that are unrelated to the Customer or a Customer Site, (ii) sharing of User Data with third parties without a User's Consent or (iii) real-time tracking of the location of Users, such as mapping individual User's location, that is unrelated to Customer's marketing or advertising to User or to otherwise enhancing User's customer experience..

5. In order to review Customer's compliance with this Section, at Cisco's request Customer will provide Cisco with a copy of its privacy policy and with access to the user screens that Customer uses to notify users of its privacy practices and obtain any consents to the collection and use of personal data.

6. Cisco represents and warrants that Cisco will process User Data in accordance with this Agreement and Cisco's privacy statement and in compliance with applicable law.

7. Customer consents to Cisco using, disclosing or otherwise processing User Data as reasonably necessary to operate Cisco CMX Engage and to provide the Offering (including sharing with suppliers Content and Submission Data necessary for such suppliers to provide CMX Engage or portions thereof to Customer, and including its suppliers collecting and using aggregate usage data that they may acquire in the ordinary course of providing all or part of the Offering, and use such data to provide, maintain, and improve the Offering), to exercise or protect Cisco's legal rights, and as required by applicable law. Cisco may use User Data on an aggregated basis for analytical purposes and disclose the results of the analysis provided that no User Data associated with specific Users is disclosed.

8. If Cisco uses a subcontractor for the provision of the Offering or the operation of CMX Engage, such subcontractor will only process User Data subject to a written agreement that complies with applicable Privacy Laws with respect to Cisco's use of subcontractors for the processing of User Data.

9. Customer agrees to indemnify, hold harmless and defend Cisco, its affiliates, directors, employees and agents from and against, and reimburse Cisco and each of such parties with respect to, any losses, damages, claims, liabilities, costs and expenses (including reasonable attorneys' fees and expenses) related to or arising out of (i) an actual or alleged violation by Customer of Privacy Laws or Customer's privacy policies, (ii) an investigation by a government agency (such a consumer protection agency, industry regulator or data protection authority) into Customer's use of the Offering, (iii) breach of any duty owed by Customer to its Users, or (iv) any breach of any representation, warranty, covenant or agreement of Customer contained in or made pursuant to this Agreement.

10. "Privacy Laws" are defined as all applicable laws and regulations relating to privacy or the collection, use, storage and other forms of and processing of personal or consumer data, including where applicable guidance and codes of practice issued by any relevant supervisory authority.

11. In the event that legislation, governmental regulations, judicial or administrative bodies' decision, or an industry self-regulatory guideline (collectively, "Restrictions") limit or prohibit the use of the Offering or Cisco CMX Engage or collection or use of any User Data, or if, in a party's counsel's reasonable judgment, use of the Offering, Cisco CMX Engage or User Data would violate any such Restrictions, or would be materially more risky than as of the Effective Date, for reasons such as an investigation by a government agency such a data protection or consumer protection agency, either party may suspend the use of the Offering or the collection and use of User Data or terminate this Agreement and the Customer shall discontinue using the Offering and the User Data from Cisco CMX Engage.

12. Additional Terms applicable to transactions with Customers in Data Protection Countries only, where "Data Protection Countries" means the European Union member states, Norway, Iceland, Liechtenstein, Switzerland and other countries and territories that have adopted legislation substantially similar to EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data:

a) The following representations and warranties will apply:

1. Cisco will not use, disclose or otherwise process User Data other than (i) as reasonably necessary to operate Cisco CMX Engage and to provide the Offering, (ii) where instructed or permitted by Customer, (iii) to exercise or protect Cisco's legal rights or (iv) as required by applicable law.

2. Cisco will process User Data in compliance with all Privacy Laws that are directly applicable to Cisco.

3. Cisco will implement and maintain appropriate technical and organization measures intended to protect User Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction.

4. Cisco will cooperate as requested by Customer in writing to enable Customer to comply with any exercise of rights by a data subject under Privacy Laws with respect to User Data processed by Cisco under this Agreement and to comply with any inquiry, notice or investigation of Customer's compliance with Privacy Laws, provided that Customer will reimburse Cisco for the costs arising from this assistance.

b) Section 7 is deleted and replaced with the following:

7. Cisco may use User Data on an aggregated basis for analytical purposes and disclose the results of the analysis provided that no User Data associated with specific Users is disclosed

c) Sections 7A and 7B are added as follows:

7A. Customer acknowledges that Cisco will use Cisco CMX Engage to process User Data as a "data processor" for Customer as such term is used in the data protection legislation of the European Economic Area member states and, where applicable, equivalent legislation in other countries and territories ((or as a Sub- processor where Customer acts as a processor of its own customer's Customer Data). Customer will be a "data controller" under the applicable data protection laws.

7B. Customer consents to the transfer of User Data to Cisco and its subsidiaries in the United States provided that Cisco maintains its certification of compliance with the U.S.-EU Privacy Shield Framework or complies with other measures required under Privacy Laws applicable to Customer with respect to transfers of personal data to countries that have not been deemed to have adequate protections for personal data.

d) Section 8 shall be amended so that if Cisco uses a subcontractor for the provision of the Offering or the operation of CMX Engage, such subcontractor will only process User Data as Cisco's sub-processor, and otherwise as set forth in Section 8.

Attachment 1 to Data Privacy Section

CMX Engage User Data Collected

Information Gathered Prior to End User Terms of Use Acceptance

Field Name	Source
Subscriber Id	Assigned from CMX Engage
User Agent Tokens	Pulled from Device
Created Date	Assigned from CMX Engage
MAC Address	Pulled from Device

Information Gathered After End User Terms of Use Acceptance

Field Name	Source
Email	Provided by User
First name	Provided by User
Last name	Provided by User
Created Date	Assigned from CMX Engage
Last Modified Date	Assigned from CMX Engage
Shared Preferences within customer and across app	Provided by User
Social Networks (List of social networks the user is associated with)	Provided by User
Gender	Provided by User
Age	Provided by User
FB ID	Provided by User
Google Plus ID	Provided by User
Twitter Profile URL	Provided by User
LinkedIn Plus ID	Provided by User
Cookie	Pulled from Device
Native Device & App UIDs (Unique Identifiers)	Pulled from Device
Custom Identities (If any)	Pulled from Device
App Ids (Apps installed by this device)	Pulled from Device

Notes:

1. Not all stated above attributes are always stored for every subscriber entry created. The fields stored are highly conditional on how the solution is implemented: app user, captive portal user, type of authentication implemented.

2. Any App related details collected here are limited to apps built on CMX Engage or apps embedded with CMX Engage SDK.

Attachment 2 to the Data Privacy Section
CMX Engage User Experience Guidelines

A. European Economic Area; Switzerland, and Other Data Protection Countries

An end-user must receive a sign-in prompt on their device in order to use the wif-fi access network. The prompt must meet the requirements described in these Guidelines.

1. The prompt will require end-user to agree to the Privacy Policy and the Terms of Use for the Internet access service by means of either:

   - a button that says “click to accept the privacy policy and terms of use for wi-fi access”, or

   - unchecked check-box that says “I accept the privacy policy and terms of use for wi-fi access”

2. The prompt must include an active link to the Privacy Policy and Terms of Use.

3. The prompt must include the statement that:

   Location information from your device will used to [personalize your experience at the stadium, give directions within the building, provide special offers while you are here and analyze how we can serve you better. See privacy policy for more information.

B. United States, and All Other Countries Not Covered by (A) Above

An end-user must receive a sign-in prompt on their device in order to use the wif-fi access network. The prompt must meet the requirements described in these Guidelines.

1. The prompt will require end-user to agree to the Privacy Policy and the Terms of Use for the Internet access service by means of either:

   - a button that says “click to accept the privacy policy and terms of use for wi-fi access”, or

   - unchecked check-box that says “I accept the privacy policy and terms of use for wi-fi access”

2. The prompt must include an active link to the Privacy Policy and Terms of Use.

7.1. [

EXHIBIT A

GLOSSARY OF TERMS

The following definitions will apply to this Offer Description and to the Offering. Any other definitions will be as provided in the remainder of this Offer Description. If there is a conflict between the definitions contained in this Offer Description and this Agreement, the definitions in this Offer Description will prevail.

Term	Definition
Agreement	See definition in the introduction to this Offer Description
API	Application Programming Interface
Business Day	The days of operation per week within the relevant region where the Offering shall be provided, excluding local holidays as observed by Cisco.
Captive Portal	See Section 7.1 (Data Privacy)
Advanced Services	See Glossary of Terms from Cisco.com; at www.cisco.com/go/servicedescriptions/
Cisco-Authorized Reseller	means a Cisco authorized reseller
Content	See Glossary of Cisco SaaS Agreement
Customer	The legal entity or individual purchasing the Offering under this Offer Description and associated SaaS Agreement
Customer Site	A physical location owned or operated by Customer, such as a Customer store location (for a retail customer), or Customer hotel or stadium (for a hospitality or sports customer)
Customer Data	Means network data, including but not limited to MAC address, IP address, location information and device type, which Cisco processes in the course of making the Offering available to Customer.
Data Protection Countries	See Section 7.12 (Data Privacy)
Documentation	See Glossary of Cisco SaaS Agreement
Emergency Maintenance	Means an unplanned and/or unscheduled period of time during which Cisco or its suppliers perform maintenance.
CMX Engage	See definition in Introduction Section
Enterprise Connection	See Section 3.7
Guidelines	See Attachment 2 to Section 7 (Data Privacy)
Implementation Period	See Section 4.1
Maintenance Releases	See Glossary of Terms from Cisco.com; at www.cisco.com/go/servicedescriptions/
Native App	See Section 7.1 (Data Privacy)
Offer Description	See definition in the introduction to this Offer Description
Offering	See definition in the introduction to this Offer Description
Order	See definition in the introduction to this Offer Description
Personal Data	Means Customer Data related to a person that is identified or identifiable, as defined in the Directive 95/46/EC of the European Parliament of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data, or any replacement legislation.
Portals	See Section 3.1 of this Offer Description
Privacy Laws	See Section 7.10 (Data Privacy)
Products	See Glossary of Terms from Cisco.com; at www.cisco.com/go/servicedescriptions/
Restrictions	See Section 7.11 (Data Privacy)
Scheduled Down Time	Means an unanticipated period of service outage during a period of Scheduled Maintenance

Scheduled Maintenance	Means a planned, defined and scheduled period of time during which

	Cisco or its suppliers perform routine maintenance on an Offering
Services	See Section 5.1 of this Offer Description
Services Not Covered	See Section 5.2 of this Offer Description
Severity and Escalation Guidelines	See Section 5.2 of this Offer Description
SLA	See Section 6.1 of this Offer Description
Submission Data	See Glossary of Cisco SaaS Agreement
Standard Business Hours	See Glossary of Terms from Cisco.com; at www.cisco.com/go/servicedescriptions/
Sub-processor	Means any sub-contractor that processes Personal Data on behalf of Customer. References to the Agreement will be construed as including this Data Protection Annex
TAC	See Section 5.5 of this Offer Description
Updates	See Section 5.5 of this Offer Description
User	See Glossary of Cisco SaaS Agreement
User Data	See Section 7.1 (Data Privacy)
User Profile	See Section 7.1a (Data Privacy)