

RELEASE NOTES IN-APP MESSAGING SDK VERSION 2.7 - Android

These are the main feature releases available in the **In-App Messaging SDK version 2.7 for Android**.

Version 2.7 planned roll-out: September 5th 2017

New functionalities

[Structured content enablement \(Beta\)](#)

[Tablet split-screen supportability](#)

[Secure form branding enhancements](#)

[View-only mode](#)

[Photo sharing permissions callback](#)

[List of certified and supported devices extended](#)

New properties

[Structured content](#)

[Secure Form](#)

New callbacks

[Photo sharing permissions callback](#)

[CSAT launched callback](#)

[CSAT skipped callback](#)

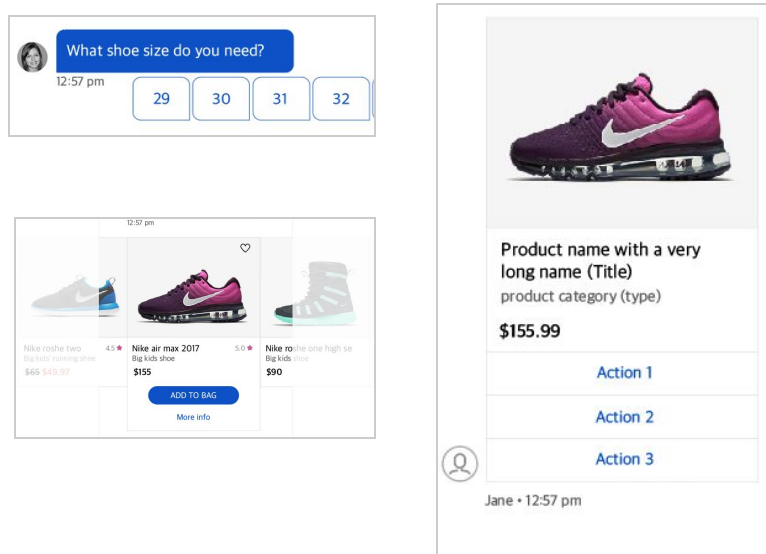
New strings

[Structured content strings](#)

[Accessibility strings](#)

New functionalities

Structured content enablement (Beta)



**This version of the SDK delivers structured content enablement only; the feature will be made fully productive in October.*

Description

Structured message templates and elements, such as cards, images and deep linking buttons, turn a simple app interaction into a conversational user experience. They support a huge variety of messaging interactions and enable:

- Clearer communication with bots, so commands are more easily understood.
- The ability to trigger actions, such as deep-linking navigation, confirmations and transactions, directly from a conversation
- Improved sales through product promotion and simplification of the purchasing process
- An overall improved and more efficient service - just what consumers expect from messaging

SDK 2.7 structured content capabilities

Structured content capabilities are being gradually rolled out during September-October 2017. Dedicated documentation for structured content will be published as part of the gradual rollout.

In-app messaging SDK v2.7 has a structured content renderer for the following elements:

- Image

RELEASE NOTES IN-APP MESSAGING SDK VERSION 2.7 - Android

- Text
- Button
- Clicks (actions and meta-data)

Full list of elements dictionary will be published during the gradual rollout.

What does enablement mean?

Until rollout is complete, the structured content capability in SDK v2.7 is flagged as a Beta feature. The feature has an enablement toggle in the SDK which is disabled by default.

The toggle may be switched on as part of the SDK release within the host app, however it is highly recommended not to release the SDK in the host app with structured content enabled until end to end flow has been fully tested on the brand's account.

In addition to structured content enablement, SDK v2.7 also has a few branding properties and one callback which can be configured and used.

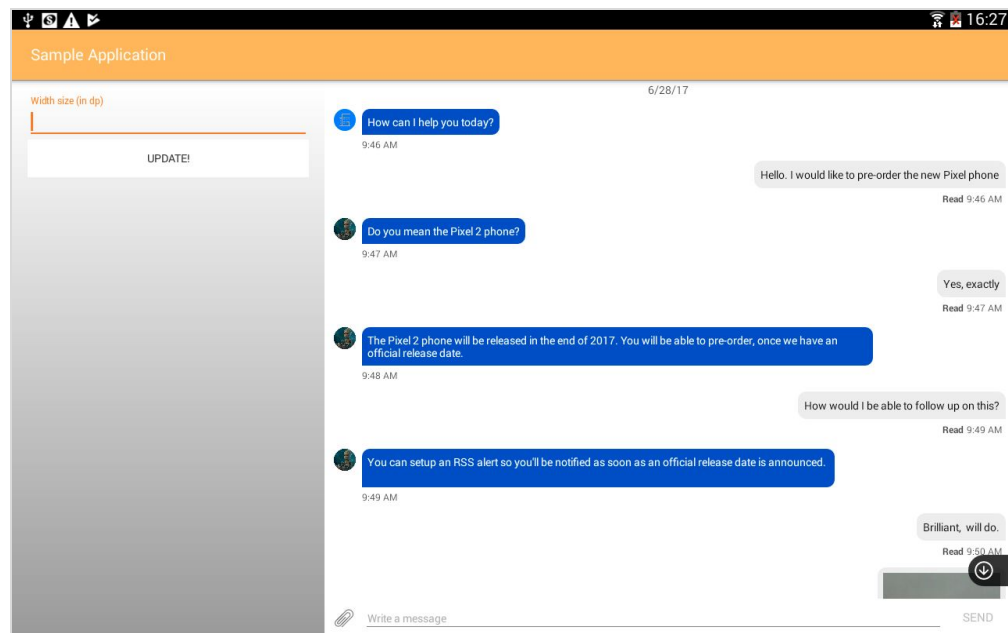
Related properties: [Structured content](#)

Related strings: [Structured content strings](#)

The following additional conditions and configurations are required:*

Backend update	Backend enablement	Backend configuration	SDK enablement	SDK configuration
Yes	Yes	Yes	Yes	Yes

Tablet split-screen supportability



To ensure that consumers using tablets can connect with brands while enjoying the tablet experience, brands can enable tablet applications to host the conversation window within an application page, as a fragment for Android or viewcontroller for iOS.

Until now the SDK has provided support for a full page layout for messaging conversations. SDK 2.7 provides full support for conversations in a split-screen with viewcontroller / fragment modes. Brands can own the wrapper and host the conversation in split-screen.

A full list of supported and certified devices can be found in the [LiveEngage System Requirements document](#).

The following additional conditions and configurations are required*:

Backend update	Backend enablement	Backend configuration	SDK enablement	SDK configuration
N/A	N/A	N/A	N/A	N/A

Secure form branding enhancements

To enable brands to adjust the secure form visuals to accurately reflect their brand experience, the following configurations are now available:

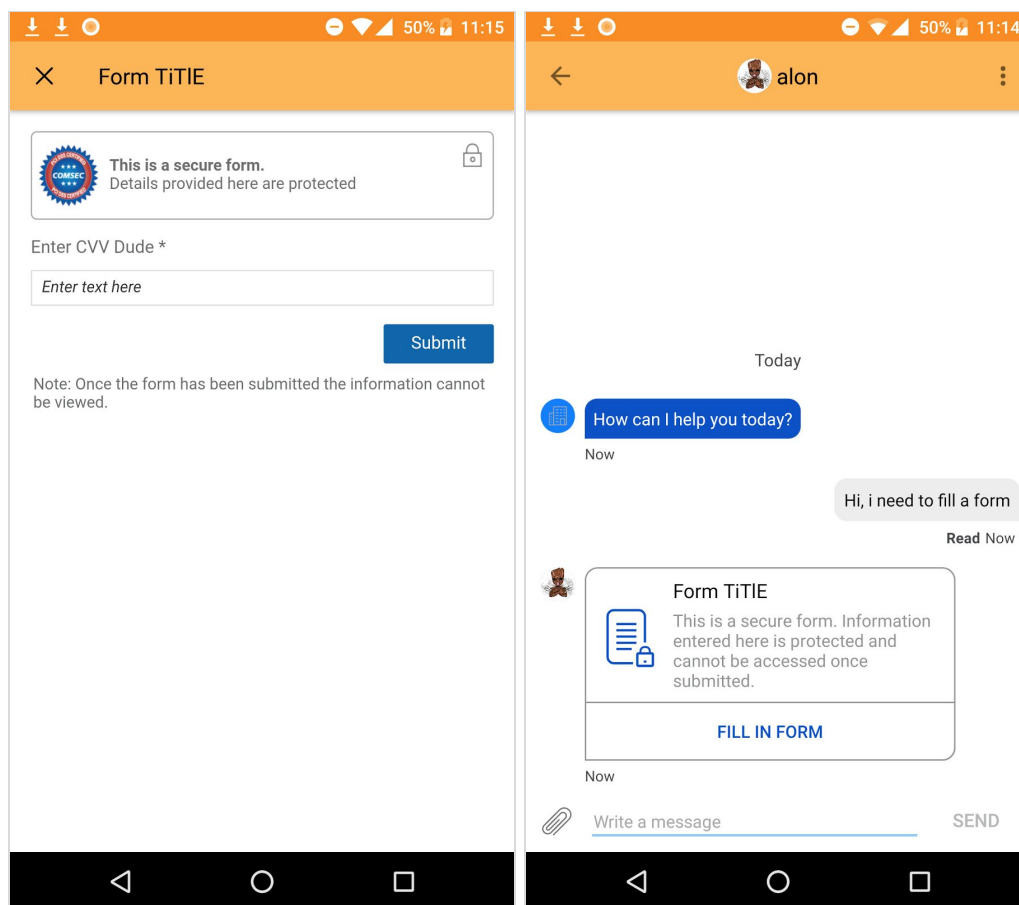
- Secure form fonts
- Bubble loader indicator color

The secure form is essentially a web page running in a web view, within the messaging conversation. As such, the web page may run predefined fonts which can be set by the SDK remotely.

By default, the font is set to Arial. However brands can choose from any of the fonts on the following secure form supported fonts list:

Aria, Arial, Arial Black, Bookman Old Style, Comic Sans MS, Courier New, Garamond, Georgia, Helvetica, HelveticaNeue, HelveticaNeue-Light, Impact, Lato, Lucida Console, Lucida Sans Unicode, MS Sans Serif, MS Serif, Palatino Linotype, Tahoma, Times New Roman, Trebuchet MS, Verdana.

RELEASE NOTES IN-APP MESSAGING SDK VERSION 2.7 - Android



Related properties: [Secure form](#)

The following additional conditions and configurations are required*:

- 1) Secure forms should be enabled on LiveEngage
- 2) For font settings and bubble loading indicator :

Backend update	Backend enablement	Backend configuration	SDK enablement	SDK configuration
N/A	N/A	N/A	N/A	Yes

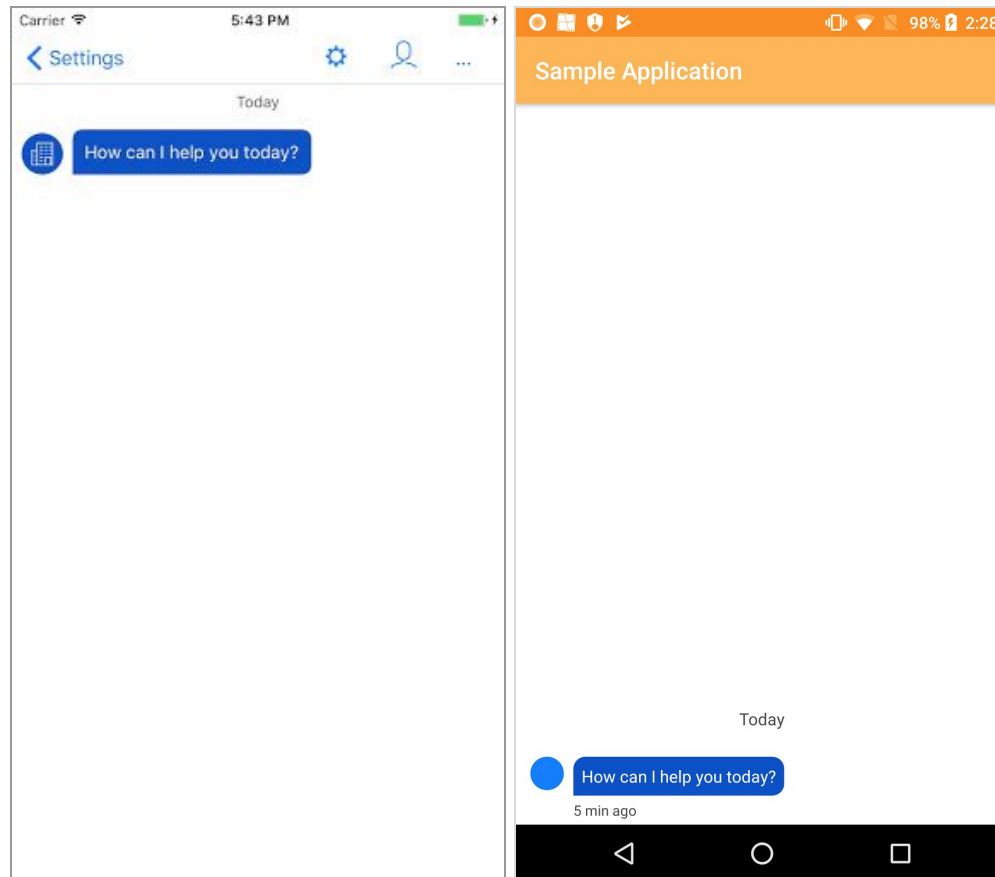
View-only mode

The SDK now offers a new RunTime mode in addition to the edit mode, known as view-only mode. View-only mode means consumers can see the full conversation, but the keyboard and text input area are not displayed. In this mode, new messages can arrive, but the consumer will not be able to respond.

RELEASE NOTES IN-APP MESSAGING SDK VERSION 2.7 - Android

This mode gives brands greater control over how consumers are able to use messaging within the brand's app.

Future SDKs will support additional modes.



The following additional conditions and configurations are required*:

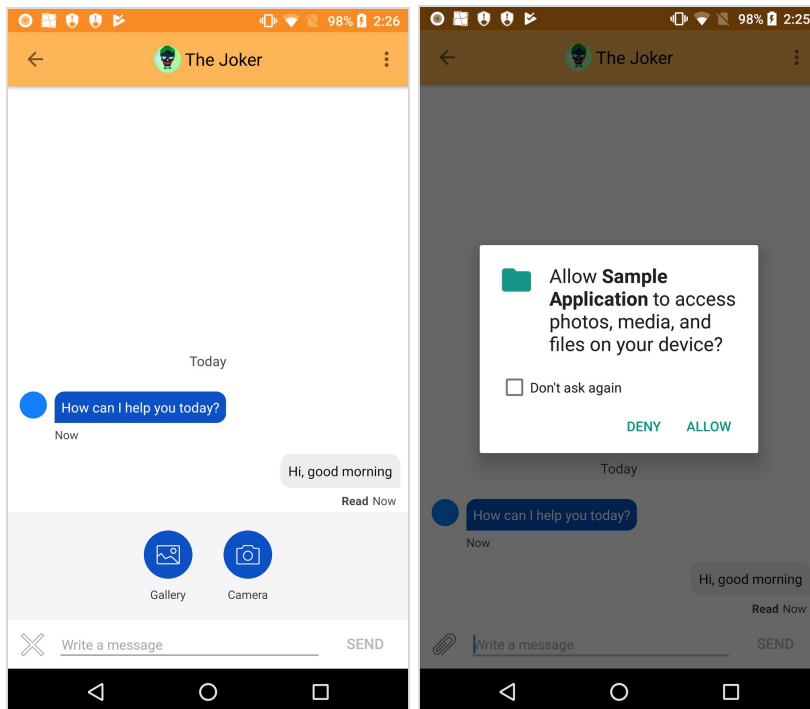
Backend update	Backend enablement	Backend configuration	SDK enablement	SDK configuration
N/A	N/A	N/A	N/A	Yes

RELEASE NOTES IN-APP MESSAGING SDK VERSION 2.7 - Android

Photo sharing permissions callback

When a consumer shares photos during a conversation, a banner appears asking them to grant permission for the app to have access to their camera and/ or photo library.

If the consumer refuses permission, the SDK sends a callback to the host app. Brands are then able to run a customized and branded banner with a second request for the consumer to grant the appropriate photo sharing permissions.



The following additional conditions and configurations are required*:

Backend update	Backend enablement	Backend configuration	SDK enablement	SDK configuration
N/A	N/A	N/A	N/A	Yes

List of certified and supported devices extended

The following devices are now also supported and/or certified to host our in-app messaging SDK:

Mobile

	Operating system			
Device	v5.X (Lollipop)	v6.X (Marshmallow)	v7.X (Nougat)	v8.X (Oreo)
Nexus 6P	N/A	N/A	Certified	Certified

A full list of supported and certified devices can be found in the [LiveEngage System Requirements document](#).

* Key for items as follows:

Backend update: This feature requires an update to the backend.

Backend enablement: This feature requires items to be toggled on in the backend.

Backend configuration: This feature requires configuration in the backend.

SDK enablement: This feature requires items to be toggled on in the SDK.

SDK configuration: This features requires items to be configured in the SDK.

New properties

Structured content

The following properties for structured content can now be configured:

Name	Description	Default
<bool name="enable_structured_content">	Enable/Disable structured content feature	False (structured content disabled)
<color name="structured_content_bubble_outline_color">	Color code for the structured content bubble outline color.	#EDED (light gray)

RELEASE NOTES IN-APP MESSAGING SDK VERSION 2.7 - Android

<code><dimen name="structured_content_b order_width"></code>	Integer in dp for the bubble stroke width of the structured content bubble.	1dp
<code><integer name="structured_content_m ap_zoom"></code>	Integer that defines the zoom level of the structured content map view.	18
<code><bool name="structured_content_li nk_as_callback"></code>	Enable/Disable sending the Structured Content link as a callback instead of a deep link intent (true - use callback, false - deep link intent)	False

Secure Form

The following properties for PCI secure form can now be configured:

Name	Description	Default
<code><bool name="pci_form_hide_logo">f alse</bool></code>	Enable/Disable logo in PCI secure form	False (logo is shown)
<code><string name="pci_form_font_name" ></string></code>	Font to be used in PCI secure form	Default device font is used

New callbacks

Photo sharing permissions callback

```
optional func LPMessagingSDKUserDeniedPermission(_ permissionType: LPPermissionTypes)
```

CSAT launched callback

```
optional func LPMessagingSDKConversationCSATDidLoad(_ conversationID: String?)
```

CSAT skipped callback

```
optional func LPMessagingSDKConversationCSATSkipped(_ conversationID: String?)
```

New strings

Structured content strings

Name	Description	Default
lp_structured_content_display_failed	Message displayed in the conversation if there is an error parsing the structured content message	Content failed to display
lp_new_message	Message displayed on the scroll down indicator when a structured content message is received	New message

Accessibility strings

Name	Description	Default
lp_accessibility_sc_map	Accessibility string for the map element in a structured content message	Map
lp_accessibility_sc_image	Accessibility string for the image element in a structured content message	Image
lp_accessibility_sc_button	Accessibility string for the button element in a structured content message	Button
lp_accessibility_sc_text	Accessibility string for the text element in a structured content message	Text
lp_accessibility_sc_destination	Accessibility string for the map pin on a structured content map element	Destination

RELEASE NOTES IN-APP MESSAGING SDK VERSION 2.7 - Android

This document, materials or presentation, whether offered online or presented in hard copy ("LivePerson Informational Tools") is for informational purposes only. LIVEPERSON, INC. PROVIDES THESE LIVEPERSON INFORMATIONAL TOOLS "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

The LivePerson Informational Tools contain LivePerson proprietary and confidential materials. No part of the LivePerson Informational Tools may be modified, altered, reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of LivePerson, Inc., except as otherwise permitted by law. Prior to publication, reasonable effort was made to validate this information. The LivePerson Information Tools may include technical inaccuracies or typographical errors. Actual savings or results achieved may be different from those outlined in the LivePerson Informational Tools. The recipient shall not alter or remove any part of this statement.

Trademarks or service marks of LivePerson may not be used in any manner without LivePerson's express written consent. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies. LivePerson shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses resulting from the use or the inability to use the LivePerson Information Tools, including any information contained herein.

© 2017 LivePerson, Inc. All rights reserved.