

SAP Intelligent Notification 365, email API & service

On-boarding process for SAP S/4 HANA marketing cloud / SAP Hybris Marketing customers

SAP Mobile Services

TABLE OF CONTENTS

INTRODUCTION	3
HIGH LEVEL ARCHITECTURE & WORKFLOW DESCRIPTION	3
CHECK-LIST FOR ON-BOARDING	5
Reference Documents	5
Information requested in provisioning form:.....	5
Sender IP Addresses.....	5
Sub-Domain	5
“sender” and “reply to” addresses	5
Information provided as part of provisioning	5
Credentials	5
<i>Important note on DKIM and SPF usage.....</i>	<i>6</i>
ON-BOARDING PROCESS WORKFLOW FOR HYBRIS CUSTOMERS	6

INTRODUCTION

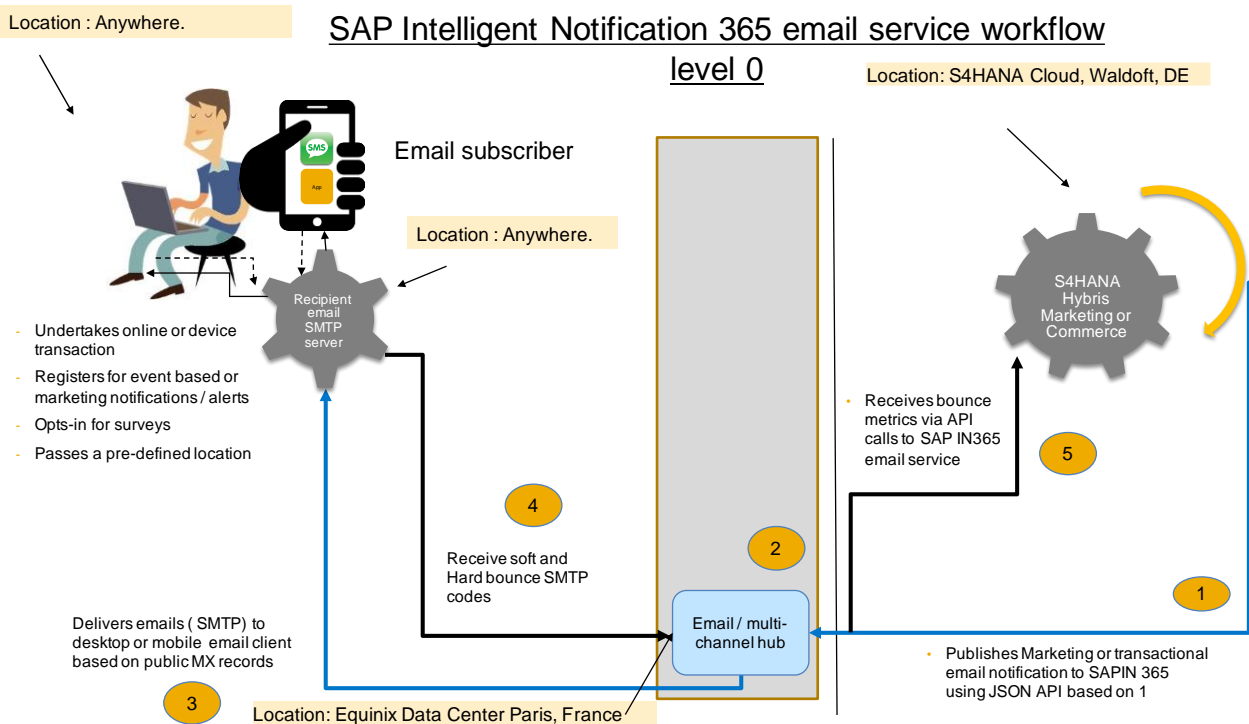
Through SAP Mobile Services it is now possible for SAP S/4 HANA marketing cloud & Hybris Marketing customers to have an integrated email channel

1. SAP Hybris Marketing comes pre-integrated with SAP Intelligent Notification 365, email service (an SAP Mobile Service offering) as a communication channel.
2. The email service is delivered using a new JSON email API interface
3. Both transactional and marketing emails are supported using the same email service.
4. SAP Intelligent Notification 365, email service also delivers ability to secure email notification campaigns using custom domains and DKIM and SPF based deliverability/ reputation management
5. Available for SAP S/4 HANA Marketing Cloud 1603 or younger and SAP Hybris Marketing 1602 or younger.

This on-boarding document describes the high level architecture and functionalities and provides a step by step overview through-out the on-boarding process.

HIGH LEVEL ARCHITECTURE & WORKFLOW DESCRIPTION

The figure below explains how the general flow works:



1. A customer creates campaigns in S4HANA marketing that results in the SAP Intelligent Notification 365 email hub receiving a JSON request via HTTPS API. This request is delivered using the email plug-in built into Hybris Marketing. The request has the following key parameters:
 - Sender address (such as info@marketing.customer.com)
 - Sender name (if needed) ; so it will look like name info@marketing.customer.com
 - Reply_to address (the address where email replies will be delivered)
 - Message body (either as plain text or HTML)

- Recipient email address (1 or more) . Typically, Hybris only sends 1 email address per notification.
- Encoding (none or UTF-8)

These requests are sent to a SAP Mobile Service provided end point (URL/ credentials) that are also set up in Hybris marketing tenant for the customer along with valid sender and valid Reply_To addresses. The recipient email addresses (“subscriber list”) is managed by Hybris marketing and SAP MS only receives it as part of the notification request.

- No encryption is currently undertaken at this stage .
- SAP MS email hub will receive the email notification and create a Notification ID; that is a unique reference ID for every email request.
- Every notification ID is mapped to an ESP job ID for tracking purposes.
- The email address or email content shared in the notification is not stored or handled during processing.

SAP Intelligent Notification 365 maps a customer credential to one or more OpenText / Easylink account credentials depending on sender domains/ sub-domains.

Every Hybris request is mapped to a notification ID that are used to store email metadata information in IQ vent store with associated email events. These are again mapped to easylink Job ID's when the workflow closes.

During the processing; SAP tracks the following event types. These events are necessary from troubleshooting perspective.

- SAP Mobile Services received (from Hybris) timestamp
 - SAP Mobile Services sent (to ESP) timestamp
 - ESP received timestamp and
 - ESP sent timestamp
2. SAP Mobile Services converts the Hybris request to an SOAP/ XML request and sends out the notification to an SAP end-point provided by OpenText / Easylink. SAP IN 365 tracks the processing using notification ID/ Job ID mapping.
 3. OpenText/ Easylink processes each notification job and sends then out as SMTP posts using their mail transfer agent (MTA)
 4. Upon receipt, the recipient mail servers shall provide soft or hard bounce information informing the Easylink MTA on the status of the Job.
 5. Back-end email infrastructure captures these bounce statuses and delivers the bounce report as a CSV dump . SAP Intelligent Notification 365 captures this info as bounce event in IQ event store as well as maintain a bounce statistic service that maintains bounce info with notification ID for 7 days . Hybris Marketing pulls this bounce statistic using scheduled callback services. Bounce data is delivered as Job ID, notification ID, SMTP error status
 - Any email address associated with a notification ID is purged 7 days from receipt.
 - Bounce reports comes after the email is sent out. At that point no email message is maintained. Only email metadata is available from that point onwards.
 - SAP MS only keeps (in cache and not in a store) email between the statuses CAAS RECEIVED and ESP RECEIVED. It's for a very small duration during which we re-try. The only reason failure happen at this step is because ESP is down or network is down.
 - Once SAP MS has a status as ESP received; the email notification is out of SAP MS systems and the only thing maintained is an SAP Intelligent Notification 365 Notification ID / Easylink Job ID mapping.

CHECK-LIST FOR ON-BOARDING

Reference Documents

Before getting started, here is a checklist of reference documents (Please click on links to review them).

- [SAP Intelligent Notification 365 email service – provisioning form](#)
- [SAP Intelligent Notification 365 Multi-Channel API spécification \(with support for email as a channel\)](#)
- [SAP Intelligent Notification 365 email service – Using DKIM and SPF to improve deliverability](#)
- [SAP Intelligent Notification 365 email service – FAQ document](#)

Information requested in provisioning form:

Sender IP Addresses

Only whitelisted IP addresses can send email notification traffic for SAP Mobile Service to process. Please work with your IT teams to obtain dedicated public IP address for the application through which email notifications shall be delivered.

Sub-Domain

It is highly recommended to create a sub-domain in order to manage outgoing email campaign traffic instead of using top-level domain

- For e.g., if notifications are driven from a newsletter; a sub-domain such as newsletter.customer.com would be worth consideration.
- Please talk to your IT representative to provision this.

“sender” and “reply to” addresses

Default “sender” and “reply-to” addresses are used when this information is not passed as part of the notification request. This is important for marketing emails.

- The sender address has to be associated with the sub-domain (for e.g. info@newsletter.customer.com).
- A “reply to” address is not mandatory – we provide you that flexibility. Many senders can have a common “reply to” address or each sender can have a unique “reply to” address. The reply to address can be any valid address that you may want to recipient to respond to.

For transactional emails, the “sender” and “reply to” may be passed as part of the notification request itself.

Information provided as part of provisioning

Credentials

- Credentials (notification URL, username, and pwd); typically as below:
 - VPN Customer URL :
 - https://multichannel-pi.sapmobileservices.com/email/caas_email23115/notifications
 - Non-VPN Customer URL:
 - https://multichannel-pp.sapmobileservices.com/email/caas_email23115/notifications
 - UserID : caas_email23115
 - Password : x5unSucL
 - Sender : name@subdom.customer.com (default sender name)
 - Reply To : contact@customer.com

- DKIM, SPF and MX records (if needed for “reply” tracking) that need to be inserted into the TXT records of the customer sub-domain.

Important note on DKIM and SPF usage

DKIM and SPF need to be inserted into the TXT records of your sub-domain for deliverability management. Please set the expectation around this with your DNS administration teams.

For a detailed understanding on DKIM and SPF based deliverability, please refer to the document titled [“SAP Intelligent Notification 365 email service – Using DKIM and SPF to improve deliverability”](#)

ON-BOARDING PROCESS WORKFLOW FOR HYBRIS CUSTOMERS

Broadly, the on-boarding steps can be categorized into 3 processes as follows:

1. Manage Hybris tenant set-up
2. Manage email service set-up
3. Manage campaign administration and set-up

The high level exit criteria for the on-boarding processes is as listed below:

Process	Exit Criteria
Manage Hybris tenant set up	Static Public IP addresses Marketing Sub-domains
Manage email notification service set up	Custom domain mapping(s) DKIM & SPF mapping confirmation Email end point and credentials Reply to tracking White-listed IP ranges
Manage campaign and user set up	Customer / brand landing pages Campaign user set ups Campaign attributes Campaign KPI's

Each of the above processes have detailed sub-processes & tasks that are needed to be completed. There are additional nuances based on environment and infrastructure. These are as detailed in the table below:

Process	Task	Customer	Hybris Marketing	SAP Mobile Services
Manage Hybris Tenant set up	Provision Hybris Marketing tenant for customer	Yes	Yes	N/A

Manage email notification service set up	Define sub-domains for email notifications. For e.g., if notifications are driven from a newsletter, a sub-domain such as newsletter.customer.com would be worth consideration. The notifications can then be sent via a sender address info@newsletter.customer.com (details of sender of reply to set up in a different step)	Yes	N/A	N/A
	Associate a static public IP address with the Hybris cloud tenant. This public IP address is needed for SAP/yMKT to whitelist the email notification source. Only whitelisted IP addresses can send email notification traffic for yMKT/SAP to process.	Yes	N/A	N/A
	Set up custom sub-domains for email processing. Also set up sender (from) and reply to addresses associated with the sub-domain. This is based on the input received from customer.	N/A	N/A	Yes
	Provide deliverability and reputation management TXT records (DKIM/SPF) in DNS. Please refer to document titled “SAP Intelligent Notification 365 email service – Using DKIM and SPF to improve deliverability”	N/A	N/A	Yes
	Provide MX record (in case customer would like the <i>reply to</i> to be tracked)	N/A	N/A	Yes
	Set up deliverability and reputation management TXT records (DKIM / SPF) & MX record in DNS.	Yes	N/A	N/A

	Please refer to document titled <u>“SAP Intelligent Notification 365 email service – Using DKIM and SPF to improve deliverability”</u>			
	Validate custom domain set up and confirm to customer along with email notification end-point and credentials.	N/A	N/A	Yes
	Set up email notification end-point and credentials in yMKT tenant	Yes	N/A	N/A
	Whitelist yMKT tenant static/public IP address	N/A	N/A	Yes
	Test connectivity / traffic	Yes	Yes	Yes
Manage campaign & user set ups	Create email maketing campaign	Yes	N/A	N/A
	Associate <i>from</i> and <i>reply to</i> user address to campaign	Yes	N/A	N/A
	Validate sub-domain and / or registered addresses (<i>from</i> and <i>reply to</i>). yMKT uses domain check API from SAP MS behind the scene	N/A	Yes	N/A
	Check campaign metrics	Yes	N/A	N/A
	Check deliverability metrics (soft / hard bounces) on Hybris Marketing	Yes	N/A	N/A



© 2016 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.