Sinch E-Mail 365

Onboarding Guide for SAP Marketing Cloud Customers

Version 1.0 – December 2020

Revision History

Version	Date	Author	Description
1.0	12.03.19	Sinch	Sinch E-Mail 365 onboarding document

Table of Contents

1 Introduction

Sinch E-Mail 365 provides a RESTful JSON API interface that delivers email capabilities. The API interface is easily consumable by any upstream application. Both transactional and marketing emails are supported using the same email service. Sinch E-Mail 365 also delivers ability to secure email notification campaigns using custom domains, DKIM and SPF based deliverability / reputation management.

This document provides a step-by-step overview through the onboarding process for Sinch customers directly integrating with the Sinch E-mail 365 API.

2 Check-list for Onboarding

2.1 Reference Documents

Before getting started, here is a checklist of reference documents (that are part of the on-boarding package):

- Sinch E-Mail 365 – Provisioning form
- Sinch E-Mail 365 – API Specification
- Sinch E-Mail 365 – Deliverability Best Practices Field Guide
- Sinch E-Mail 365 – IP Warmup Template

2.2 Information requested in provisioning form

2.2.1 Sub-Domain

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

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

2.2.2 “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 example: 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.

2.3 Information provided as part of provisioning

2.3.1 Credentials (*notification URL*, *username*, and *password*); typically as below:

URL	https://email-eu1.sapdigitalinterconnect.com/in365-api/caas_email12345/notifications
UserID	For example, caas_abcde23115
Password	For example, x5XXXXcL
Sender	name@subdom.customer.com
Reply To	contact@customer.com

2.3.2 DKIM, SPF and MX records that need to be inserted into the TXT records of the customer sub-domain.

2.4 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 following document: Sinch E-Mail 365 – Deliverability Best Practices Field Guide.

3 Onboarding process workflow

Broadly, the on-boarding steps can be categorized into the following three processes:

3.1 Manage application infrastructure connection

- Define marketing Sub-domains

3.2 Manage email notification service set up

- Custom domain mapping(s)
- DKIM & SPF mapping confirmation
- MX record set up
- Email end point and credentials
- Reply to tracking
- Create plan for IP and Domain warmup

3.3 Manage application event notification for email

- Define email notifications
- Complete IP and Domain warmup
- Develop collection service for notifications

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

	Process	Task	Customer	Sinch
1.	**Manage application**	**Define sub-domains for email notifications**	**Yes**	**N/A**

	infrastructure connection	For example, if notifications are driven from a newsletter, a sub-domain such as newletter.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)		
2.	**Manage email notification service set up**	**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. **Provision email accounts**	**N/A**	**Yes**
		Provide deliverability and reputation management TXT records (DKIM/SPF) Please refer to the "Deliverability and Best Practices Guide" for how this is applied.	**N/A**	**Yes**
		Setup MX record MX record to be provided by the customer domain registrar MX record is mandatory to avoid failing anti-virus checkers against the registered domain/sub domain for this service. MX record is required for the sender domain (it is	**Yes**	**N/A**

		assumed that both the sender and reply-to address are from the sender domain address)		
		Set up deliverability and reputation management TXT records (DKIM, SPF) & MX record in DNS. NOTE DKIM, SPF are mandatory	Yes	N/A
		Dedicated IP's A dedicated IP is recommended for email volumes in excess of 100K / month as forecast at the end of the warm Up period. Anything below this volume will be allocated a Shared IP	Yes	N/A
		Validate custom domain set up and confirm to customer along with email notification end-point and credentials.	N/A	Yes
		Set up email notification end-point and credentials in SAP Marketing tenant	Yes	N/A
		Create IP and Domain warmup plan Please refer to the Sinch provided IP warming template	Yes	N/A
		Test connectivity / traffic	Yes	N/A
3.	Manage application	**Define email notifications based on API specification**	Yes	N/A

	event notification via email	**Develop collection services for delivery metrics (soft, hard bounces, Unsubscribes, Open/ Click throughs, Complaints) – Please refer to API guide.**	**Yes**	**N/A**
		Complete IP and Domain warmup	**Yes**	**N/A**

Table 1 Onboarding process flow

NOTE The update of DNS setting are the responsibility of the Customer and they should seek advise from their DNS Managers (IT or otherwise) to ensure these are amended correctly. DKIM, SPF and MX records updated for the Domain/Sub Domain being set up for Sending.