Messaging, Malware and Mobile Anti-Abuse Working Group
M³AAWG Sending Domains Best Common Practices

October 2019

The URL to reference this document is: https://www.m3aawg.org/SendingDomsBCP

Abstract

When preparing for bulk or transactional email sending, two items require special attention: outbound IP addresses, and the domain names to be used for these communications. For the latter, ESPs (Email Service Providers) go through this set-up process frequently and have to review the same readiness checklist each time. This process may involve individual client preferences and constraints, both legal and technical.

This document provides the best common practices related to choosing, setting and using a domain name when sending bulk or transactional emails. Senders, receivers and anti-spam organizations participated in writing and assessing these best practices.

The intended audience is primarily senders—both traditional ESPs and other, smaller senders.

Table of Contents

Introduction

M[3]AAWG developed these best common practices for email communication to more readily answer questions faced by ESPs on a regular and frequent basis, but that any sender would also naturally face. Receivers such as filtering systems and mailbox providers have shared their experiences and points of view in a way that ensures this best practice document is not just a self-regulatory guideline for senders, but a cross-functionally developed and vetted consensus.

Senders will naturally wish to use their main domain name to send emails from the brand "Example" will want to use the domain "example.com." Despite being the best choice, it often isn't an option available to brands due to technical and process limitations described later in this document.

Ultimately, selecting a domain to send from consists of choosing between two main options: a) using the main domain name of the brand or subdomains of this zone, or b) deciding upon and procuring a new domain name (related to the brand).

The latter is known as a "cousin domain" because of the potential similarities with the usual, primary domain name of the brand or sending entity, despite having no direct link with it. Cousin domains can be registered at a different registrar than the primary brand domain, be hosted at a different DNS hosting provider, contain different WHOIS information, and so on.

Cousin domains, especially if used for one-off mailings, look like phishing campaigns to users and anti-abuse systems alike, resulting in increased spam complaints and emails being blocked or filtered. **The use of cousin domains is strongly discouraged by M[3]AAWG**, as it exposes the brand to several security issues as well as running the risk of confusing users, employees, and security tools.

Use of the main domain name of a brand or, more realistically, its subdomains is therefore the recommended approach and forms the main recommendation of this industry best common practices document. It is understood that some senders of electronic messaging may not fully implement all of these practices due to the complexity of their network infrastructures, internal or public policy considerations, and the scalability of network platforms. However, these processes do represent the consensus baseline for the industry.

Segmentation Strategy

Receivers request (and may require) that different types of email traffic be separated when possible, distinguishing between, for example, bulk marketing, one-to-one prospection, transactions (welcome, order confirmation, etc.), monthly statements, and the like.

In order to increase visibility, distinguish reputations and aid in troubleshooting, it is also best practice to separate email traffic for different areas of the same company, e.g., per country, per organization department, and so on. These separations all require distinct subdomains, and in certain cases distinct IP addresses, too.

Segmentation decisions should, however, be made in such a way that each segment can create and grow its own reputation, which requires sufficient and relatively consistent traffic volume. Lapses in sending or major fluctuations in traffic volume can impact both forming and sustaining sending reputation. We encourage reading "M³AAWG Sender Best Common Practices"[1] for more information.

Selection of Domain Names

It is strongly recommended that senders assign a separate subdomain of the main domain name for each distinct sending purpose. While the main domain can be used for corporate purposes (communication between employees, or between employees and external one-to-one contacts, for example), several different subdomains can and should be used for other sending purposes.

It should be noted that sending from different subdomains does not mean that the visible **From:** must also use the subdomain, so long as the organizational domains in each match. Different use cases may necessitate having the visible **From:** match the subdomain, but for authentication and abuse prevention purposes, this is not required. Senders should, however, have access to the inbox specified in the visible **From:**.

Using a subdomain of the main domain name makes it easier to identify the sender and is significantly less confusing for recipients and receiving mail systems than using a cousin domain. It also shows that the sender is taking an active role in managing traffic segmentation and quality, as there is a clear link between the brand and the domain names' reputations.

Especially for bulk sending, using distinct subdomains is industry best practice. However, for smaller volumes of email, it is acceptable to use different local parts of the sender address. Use your judgement based on the intended recipients, geographic diversity and abuse prevention needs.

:

Type of email traffic	**Example of subdomain**
Marketing	offers.mybrand.com
Transactional	info.mybrand.com

The subdomain name should be relevant to the type of email traffic sent to avoid confusion for both the recipient and the filtering system (which may include people-based review, so "words matter").

[1] M³AAWG Sender Best Common Practices Version 3.0, updated February 2105, (https://www.m3aawg.org/documents/en/m3aawg-sender-best-common-practices-version-30)

It is recommended to use a consistent organizational domain throughout the email, including domains specified in the **Return-Path** (technically, the RFC5321.From), the visible **From:** (technically, the RFC5322.From) and for the DKIM signature (as described in RFC 6376). It is considered good practice for the **Reply-To** (as described in RFC 5322) to be aligned with the organizational domain as well, but it is not required.

:

Subdomain consistency	
Header field	**Segmented subdomains**
Return-Path	bounce@news.mybrand.com
visible **From:**	<great@news.mybrand.com> "News from MyBrand"
DKIM-Signature **d=**	news.mybrand.com

Each address uses the same subdomain

:

Aligned organizational domains	
Header field	**Subdomain derived from organization domain**
Return-Path	bounce@bounce.mybrand.com
visible **From:**	<service@mybrand.com> "Your MyBrand transaction"
DKIM-Signature **d=**	mybrand.com

Every subdomain is derived from "mybrand.com"

Reputation

Reputation is quickly built from sending activity performed on a subdomain. The reputation attached to any given domain or subdomain name can be used as a major part of the process of email filtering in tandem with other metrics like the email content itself, or the reputation of the sending IP address.

Reputation usually starts as unknown, which makes it similar to bad in that it does not yet have any positive sending history. A domain with history is generally considered better than if it has none; from the history an ISP can deduce the quality of the behavior over time (good or bad), while no history would cause the filter to treat the incoming message with more scrutiny and caution. Proper use of subdomains will help your sending program benefit from the organizational domain's existing reputation.

.

The reputation of a sender generally isn't based on the sending domain alone, but also on the combination of other elements of the email sent. Therefore, switching to a different sending domain (whether from the organizational domain to a subdomain or vice-versa), or switching to different sending IPs, or introducing changes in the headers, can require a ramp-up for the new combination.

Ramp-up

Building domain reputation occurs in two primary phases: the warm-up phase, which brings the sending domain from unknown to noticed, followed by the ramp-up phase, which allows the sender to gradually reach their planned, long-term sending volumes.

Domain reputation warming strategies vary with the mailbox provider, but there are some common rules to consider:

- Stay consistent in the use of domains (content characteristics and sending volumes should not vary abruptly).
- Check SMTP logs to identify and triage in-flight delivery issues.
- Register for data supervision programs if available (Google Postmaster Tools, Netease, Chengxin, e.g.).
- Start low and slow; increase sending volume slowly (consider 6 weeks of warm-up as an average).
- Monitor delivery placements and open rates by mailbox provider.

Setup

The setup of sending domains has already been discussed in "M^{3}AAWG Sender Best Common Practices," but it seems relevant to elaborate on some aspects here.

Authentication

Authentication is an essential component for the delivery of emails, and is quickly becoming required by major mail systems. The process consists of the three main protocols mentioned below. Each protocol relies

on DNS TXT records to store the relevant information to be checked by the receiving email server during the process of authenticating the incoming message and checking for sender alignment.

We encourage reading "M[3]AAWG Trust in Email Begins with Authentication"[2] for more information.

1. SPF (Sender Policy Framework)

To set up SPF, a TXT record must be set in the DNS zone of the **Return-Path** domain (the RFC5321.From). Details on SPF implementation are described in RFC 7208, and in "M[3]AAWG Best Practices for Managing SPF Records."[3]

Example of an SPF record			
Header field	**Address**	**Record Type**	**SPF record**
Return-Path	bounce@news.mybrand.com	TXT	v=spf1 include:_spf.example.com ~all

2. DKIM (DomainKeys Identified Mail)

Described in RFC 6376, DKIM relies on the generation of a cryptographic hash based on parts of the email message (including headers and body), signed using a cryptographic private key. The related public key is made available in the DNS zone of the signing domain. Per RFC 6376 section 3.1, DKIM allows for multiple concurrent keys per signing domains, known as "selectors." DKIM keys are security credentials, and selectors allow different senders to maintain their own private keys to limit the security impact of weak, stolen, or old keys. It is best practice for each sending subdomain to send using a different selector.

The private/public key-pair must be generated with a minimum size of 1024 bits. M[3]AAWG has published a BCP document for DKIM Key Rotation.[4]

Selectors must be chosen appropriately for security needs and contexts.

---

[2] M[3]AAWG Trust in Email Begins with Authentication, updated February 2015, (https://www.m3aawg.org/documents/en/m3aawg-trust-email-begins-authentication)

[3] M[3]AAWG Best Practices for Managing SPF Records, August 2017, (https://www.m3aawg.org/Managing-SPF-Records)

[4] M[3]AAWG DKIM Key Rotation Best Common Practices, updated March 2019 (https://www.m3aawg.org/sites/default/files/m3aawg-dkim-key-rotation-bp-2019-03.pdf)

Example of a DKIM record			
Domain	**Namespace**	**Record Type**	**DKIM record**
news.mybrand.com	newsselec._domain-key.news.mybrand.com	TXT	k=rsa; p=MIGfMA0GCSqG-SIb3DQEBAQUAA4GNADCBiQKBgQCzEOwlT-kZskm6nyMFSR9xPUgqe6X1oE1SeuY8WeXPXWtQ8e2iwQ6xjQqd-GrAq+mngPmcybmlgiRTsX-ALV4SKAzd1V24sjtYV+FSe8/jOnrMapKXE8ZCp11xk6HWpjOqoCjs-DNsjfNyeWdEEil-IVx9Lxc1lRU+hxy-TWV1/YuHs0LQIDAQAB

3. DMARC (Domain-based Message Authentication, Reporting, and Conformance)

DMARC makes use of SPF and DKIM and requires domain alignment with the visible **From:** (RFC5322.From). A TXT record is set in the DNS zone of the visible **From:** domain to publish the domain's policy.

If putting a DMARC policy on the organizational domain is not immediately possible, it is acceptable to put a DMARC record on the subdomain explicitly, so long as it is understood that the goal is for the record to ultimately be on the organizational domain.

Example of a DMARC record			
visible From: address	**Namespace**	**Record Type**	**DMARC policy**
great@news.mybrand.com	_dmarc.mybrand.com	TXT	v=DMARC1; p=reject; rua=mailto:dmarc-rua@mybrand.com

In addition to having a DMARC policy published, the domain of the visible **From:** address must be aligned with a valid DKIM-signing domain **or** the **Return-Path** domain with a valid SPF. More details about DMARC can be found in RFC 7489 or at https://dmarc.org/.

Others

4. MX

Domains used to send emails should have a proper MX record pointing to a functional email server. This includes domains in

- the **Return-Path**:
- the visible **From:**
- the optional **Sender:**
- and of course in the optional **Reply-To:**.

Both abuse@ and postmaster@ address must exist, be read, and never bounce.

5. Alignment

It is said that domains are "relaxed aligned" (per RFC 7489 section-3.1) when the organizational domains of the domains being compared match. This document only deals with relaxed alignment, and all mentions of "alignment" refer to this.

Examples of SPF alignment			
visible From:	**Return-Path**	**DKIM-Signature d=**	**Alignment**
great@news.mybrand.com	bounce@bounce.news.mybrand.com	news.mybrand.com	Relaxed
service@info.mybrand.com	bounce@bounce.mybrand.com	news.mybrand.com	Relaxed
great@news.mybrand.com	bounce@news.mybrand.com	news.mybrand.com	Strict
great@mybrand.com	bounce@brandofmine.com	bounce@brandofmine.com	None

6. Web presence

Users needing to ascertain the innocuity and legitimacy of a sending organization will usually first try to reach the sending domain's website. To allow them to efficiently and quickly identify a sending organization, top domains or subdomains used in the visible **From:** should resolve or forward to a live current web page in relation with the sender.

DNS setup

7. Direct setup

The direct setup consists of setting up records directly in the zone file (or through an interface) in the DNS server. This is the only option when there is no third party (like an ESP) involved in sending emails. A common limitation when trying to update DNS is the inability of outdated registrar systems to publish DKIM records that contain stronger keys or specific characters.

Example of direct setup		
Host	**Type**	**Value**
news.mybrand.com.	TXT	v=spf1 include:spf.example-esp.com ~all
news.mybrand.com.	MX	0 bounce.example-esp.com
t.news.mybrand.com.	A	192.0.2.124
myselec._domainkey. news.mybrand.com.	TXT	k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzEOw lTkZskm6nyMFSR9xPUgqe6X1oE1SeuY8WeXPXWtQ8e2iwQ6xjQqdGrAq+ mngPmcybmlgiRTsXALV4SKAzd1V24sjtYV+FSe8/jOnrMapKXE8ZCp11xk 6HWpjOqoCjsDNsjfNyeWdEEilIVx9Lxc1lRU+hxyTWV1/YuHs0LQIDAQAB
_dmarc.mybrand.com	TXT	v=DMARC1; p=reject; rua=mailto:dmarc-rua@mybrand.com

8. CNAME

One of the preferred options for ESPs, using CNAME records can help overcome some of the limitations involved with direct setup. This approach also allows a third party to update record values transparently for the domain owner. For instance, if the DKIM public key is updated, the ESP can update it without asking for the sender to change anything in the zone file.

Examples of CNAME records		
Host	**Type**	**Value**
news.mybrand.com.	TXT	v=spf1 include:_spf.example-esp.com ~all
news.mybrand.com.	MX	0 bounce.example-esp.com

t.news.mybrand.com.	CNAME	tracking.example-esp.com
myselec._domainkey. news.mybrand.com.	CNAME	myselec.news-mybrand.com.dkim.example-esp.com
_dmarc.news.mybrand.com	CNAME	dmarc.news-mybrand.com.example-esp.com

9. Nameserver (NS) Delegation

NS delegation is another option when using an ESP and consists of delegating a subdomain and all subsequent subdomains to the nameserver control of the ESP sender.

The main benefit for the brand is that the ESP will take care of all of the details of DNS setup once the subdomain is delegated. The main drawback is that the brand doesn't have full visibility over the zone anymore. This is a divestment of control that improves efficiency and guarantees that all the above authentication configuration is properly handled by the ESP, but requires strong trust in the ESP sender.

Example of a nameserver-delegated subdomain address		
Host	**Type**	**Value**
news.mybrand.com.	NS	ns.example-esp.com

Migration

Consistency is key to maintaining healthy domain reputation. Positive domain reputation and consistent behavior are also important when migrating from one system to another (for instance switching to a new ESP), or when changing the sending domain (if the company name has changed, or for some other policy

reason).

When migrating to a different ESP or domain, the items mentioned in this document should be carefully considered. Note that complying with concepts in this document should be judicious decisions made gradually to any sending program. An existing, effective sending program and process may benefit from rethinking strategy according to this document, but metrics of deliverability should always be thoughtfully considered when making any changes to sending configuration.

In order to preserve sending domain reputation, it is recommended to continue using the chosen domain over time. Reputation is built up gradually and consistent sending patterns *over time* are paramount to success.

When a sender decides to switch from one ESP to another, the changeover can be made by modifying the appropriate DNS settings. If both ESPs are to send emails for some time, the DNS settings can be modified to allow the new vendor to send emails, too, notably by adding the required sending IPs in the SPF record, and also by adding the DKIM selector. The MX record, however, should only point to one vendor. Because of this, data such as complaints or asynchronous bounces may not be received by the relevant vendor. Therefore the switch from one ESP to another should use a careful migration plan, and full cutover should only be completed when sending cadence and volume with the new vendor become consistent and sustained at the desired, long-term sending volume.

Conclusion

The sending domain is one of the most important aspects of email sending configuration and can greatly impact both message delivery rates and the perception of the message by the recipient. The most important point to take away from this document is that when choosing a sending domain, a subdomain of the sender's organizational domain should be selected in almost all cases.

Appendix A – Useful tools

M[3]AAWG Documents on Authentication

- "M[3]AAWG Best Practices for Managing SPF Records" (http://www.m3aawg.org/Managing-SPF-Records)
- "M[3]AAWG Trust in Email Begins with Authentication" (https://www.m3aawg.org/documents/en/m3aawg-trust-email-begins-authentication)

Other M[3]AAWG Relevant Best Practices

- **"M[3]AAWG Sender Best Common Practices" https://www.m3aawg.org/documents/en/m3aawg-sender-best-common-practices-version-30**

Relevant RFCs

- RFC 5321: "Simple Mail Transfer Protocol" (https://tools.ietf.org/html/rfc5321)
- RFC 5322: "Internet Message Format" (https://tools.ietf.org/html/rfc5322)
- RFC 6376: "DomainKeys Identified Mail (DKIM) Signatures" (https://tools.ietf.org/html/rfc6376)
- RFC 7208: "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1" (https://tools.ietf.org/html/rfc7208)

- **RFC 7489: "Domain-based Message Authentication, Reporting, and Conformance (DMARC)" (https://tools.ietf.org/html/rfc7489)**

Appendix B – Glossary of standard terms

Bulk/Marketing Messaging – Messages that are sent for the purposes of advertising or building the relationship between the brand/company and the recipient of the message and are not transactional. (Compare with Transactional Messaging.)

ESP (Email Service Provider) – A company that offers services to send email at volume on behalf of its customers; sometimes referred to as a "sender."

Mailbox Provider – A company who provides an email box to an end user. The company may or may not also provide end users with access to the Internet.

Sender – The sender of the email message; may refer to both the ESP who controls the Sending MTA used to send the message and also the brand or company that is responsible for the content of the message.

Transactional Messaging – Messages that are sent for the purpose of confirming a transaction between the sender and the recipient of the email, or for providing individual information about the status of the relationship between a sender and recipient. For example, this could be a bank account alert or a password change notification. (Compare with Bulk/Marketing Messaging.)

As with all documents that we publish, please check the M³AAWG website (www.m3aawg.org) for updates.