Requirements for Managed and SaaS Hosting Clients to use Blackboard's Email Relays

Article Number

000054017

Cause

1. This behavior is caused by a missing SPF record, which authorizes Blackboard as a sender.
2. It is also necessary for the receiving MTA to support TLS version 1.1 or 1.2. The relays purposefully do not support older ciphers, for example TLS 1.0 and SSL 3. If the receiving MTA does not support TLS 1.1 or 1.2 the emails will not be sent at all.

Description

Blackboard Managed and SaaS hosting sites are configured by default to use standard Blackboard-provided mail relays to handle email communications being sent through the System. To ensure that all messages are timely delivered and not flagged as spam or blocked, certain requirements and policies apply.

Information

General Information

There are three main sites to review

http://tools.ietf.org/html/rfc7208#section-4	The official standard documentation
http://www.openspf.org	Driving force behind SPF standards
http://www.openspf.org/FAQ	FAQ from Open SPF

FAQ:

What is an SPF Record?

"Sender Policy Framework (SPF) is a industry-standard technology to defeat forged e-mail. SPF is not directly about stopping spam – junk email. It is about giving domain owners a way to say which mail sources are legitimate for their domain and which ones aren't. However, as the legitimate mail industry is currently at or near 100% adoption, email from Domains without appropriate SPF records is seen as suspicious and is highly likely to be rejected or delayed.

- http://www.openspf.org/FAQ/What_is_SPF

How does SPF Work?

"SPF works by domains publishing "reverse MX" records to tell the world what machines send mail from the domain. When receiving a message from a domain, the recipient can check those records to make sure mail is coming from where it should be coming from."

- http://www.openspf.org/FAQ/How_does_it_work

I Already have the IP's Whitelisted, why do I need an SPF record?

Whitelisting tells servers under your control to ignore spam checks and to just deliver the email. This is a good measure to take if a specific server or service is having issues and can be isolated. However, even though the Blackboard relays have been whitelisted, delivery is still not guarnteed. ISP's are used to relay millions of messages a day. A lot of that email is spam, and they have taken measures to control it.

For example, ISP's will throttle emails based on the reputation of the service sending the emails. One way to build this trust is to simply send email for a extended period of time and to ramp up slowly. However, end users marking the emails as spam (as students may do with notifications), will degrade the trust. When the reputation with an ISP is lowered, the emails may then be filtered into a low priority queue which sends emails in smaller batches over a longer period of time, leading to delayed email. When the reputation becomes poor, the emails may be blocked altogether. With valid SPF records, the emails are trusted, and will not be subject to the throttling rules implemented by the ISP.

The above information is not very well documented across the internet, but a few sites that mention it include :
https://sendgrid.com/blog/what-is-email-throttling/
http://kb.mailchimp.com/delivery/deliverability-research/how-throttling-improves-deliverability
http://www.activecampaign.com/help/mail-sending-throttling-settings-explained/ (Information on how to throttle email)

How do I view my current SPF record?

Popular Internet search engines will find a number of sites that will do this for you by simply entering a URL in a search box. However, this can also be done from command line:

To view current SPF record in Windows:

1. Open the Command Line Terminal (cmd.exe)
2. Type: `nslookup -type=txt mydomain.com`
3. Review the line starting with "v=spf

Example:

```
C:\>nslookup -type=txt blackboard.com 2>&1 | findstr "spf1"
        "v=spf1 include:_netblocks.blackboard.com include:mh.blackboard.com include:spf.bla
```

To view current SPF record in Linux:

1. Open the command prompt
2. type `dig txt +short mydomain.com`
3. Review the line starting with "v=spf

Example:

```
$ dig txt +short blackboard.com | grep 'spf1'
"v=spf1 include:_netblocks.blackboard.com include:mh.blackboard.com include:spf.blackboardc
```

What is the Maximum Size or an Email

At the time of writing: the total size of an individual message including all attachments (taking into account the about 25% inflation of size caused by Base64 encoding), SMTP headers, MIME part separators and other things must not exceed exactly 52,428,800 bytes. Emails exceeding this will be rejected by the Blackboard relays and will not be sent. The application also batches emails such that the total size of an email's SMTP headers will not exceed 32,768 bytes.

These figures are set uniformly and cannot be varied. In practice emails larger than about 25 megabytes may not be deliverable anyway. Blackboard cannot control the behaviour of receiving MTAs and MTAs are permitted by Internet standards to impose a limit on the size of inbound messages to their preference.

KB Product

Learn SaaS

Last Modified Date

Sun Jan 05 09:40:04 GMT 2025

Release

9.1;8.0;9.0

Release (General)

9.1;8.0;9.0

Resolution Workaround

SPF Requirements

The steps to add an SPF record are dependent on where the DNS entry is registered. For specific steps, please consult your DNS service's support or help documentation. The entry that needs to be added is 'include:mh.blackboard.com'. (This also applies if you are SaaS-Hosted, there is not a distinct SPF record for SaaS.) If this were the only thing in the SPF record, the record would look like:

```
"v=spf1 include:mh.blackboard.com ~all"
```

But: It is expected that there will be additional entries for all verified senders, including IP's for the institution's internal relays, domains, or third part vendors. For example, if your institution uses Barracuda, then an appropriate SPF record may look like:

```
"v=spf1 mx/24 a:barracuda.monument.edu include:mh.blackboard.com ~all"
```

Whitelisting

Additionally, Whitelisting will prevent email traffic from being flagged on an institution's network. While the SPF record should be sufficient, it is recommended that the following IP ranges be whitelisted:

```
69.196.242.0/24
192.230.230.0/24
69.196.241.0/24
37.216.222.128/28
69.196.238.0/28
```

Note: The above list was updated on August 12, 2022. Please review and make any changes as s

Additional SaaS Requirements:

In March of 2017 new IP addresses were implemented for SaaS that are used for outbound communication. The goal of having multiple IP addresses is to help reduce the likelihood of an outage. Clients will need to whitelist the following IP addresses, in addition to those that are already whitelisted.

These addresses are not currently implemented into the general mh.blackboard.com SPF record, so they need to be added in addition to mh.blackboard.com the SPF or whitelist. This is only applicable to clients in the United States. There is no impact on non-US clients.

Production

```
54.85.76.43
34.197.133.25
23.22.228.238
34.198.69.238
```

Client Test and Staging

```
54.85.61.20
34.194.81.60
34.198.106.176
34.198.69.122
```

Production, Test, and Staging in the Kermit Fleet

```
54.197.63.203
54.82.255.166
52.206.75.63
52.204.31.221
35.168.199.206
34.231.156.186
```

To determine your fleet, please contact Blackboard Client Support

---

Summary

This article outlines the requirements for Managed Hosting Clients to use Blackboard Email Relays. Please review the list of IPs for recent changes.

Symptoms

This article applies to all email deliverability issues while using Blackboard's mail relays such as

- Mail is blocked
- Marked as spam
- Delivered late
- Has a sender address of donotreply@blackboard.com.

Title

Requirements for Managed and SaaS Hosting Clients to use Blackboard's Email Relays