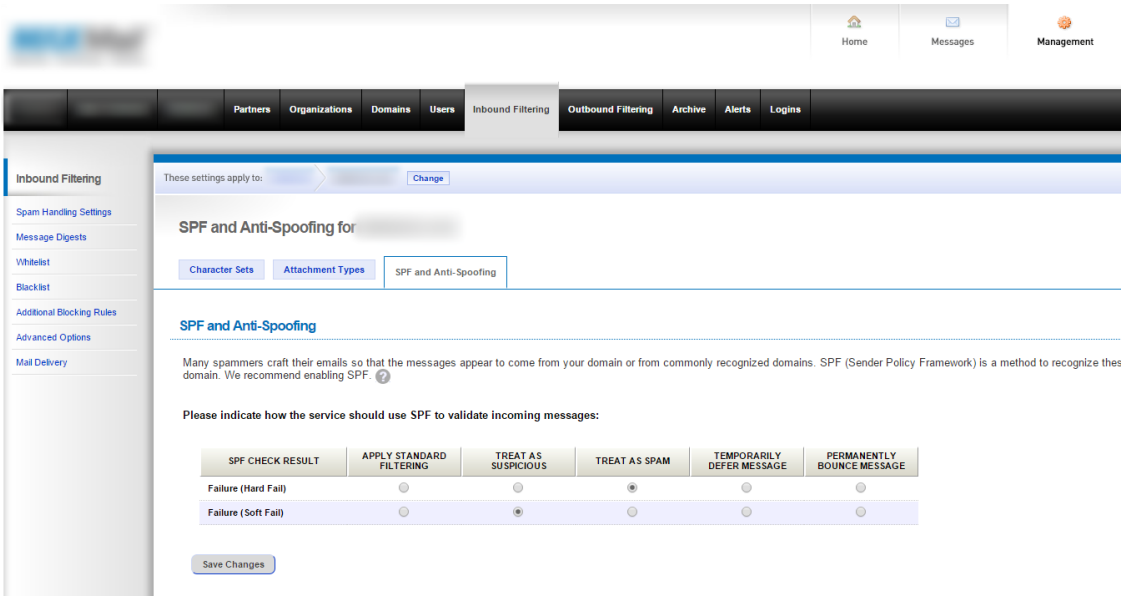
MAX by LOGICnow | Mail

Sender Policy Framework (SPF) and Anti-Spoofing – Overview

MAX Mail Security

With the ongoing threat of phishing attacks conducted by email, advanced control over SPF (Sender Policy Framework) handling is an important part of preventing spoofed messages from unauthorized senders reaching your mail infrastructure. The proper use of SPF provides both a layer of validation of incoming email legitimate third-party senders, and an additional method of detecting fraudulent email, including messages purporting to be from a customer's own domain.

Within MAX Mail, the SPF and anti-spoofing controls are accessible within the Management > Inbound Filtering > Additional Blocking Rules section.



Within MAX Mail, all inbound messages are subject to an SPF check that compares the sending IP address for a message, with the published SPF records (if available) with the DNS record for the domain of the sending address for that message. If the sending domain has no SPF records within its DNS record, the SPF check will have no impact. If the sending domain has SPF records that match the sending IP address of the email, MAX MailProtection will tend to trust that the message is authentic (although the message will still be scanned by all standard anti-spam and anti-virus engines).

LOGICnow
CHOOSE INTELLIGENCE

Administrators can control the handling of an inbound message that fails the SPF check, based on whether the failure is a "hard" or "soft" failure.

Hard fail – When an SPF record is configured in DNS with a "hard fail" ("**-all**" at the end of the record), this means that the administrator for that domain is confident that messages for that domain should only be sent from the IP address(es) specified within the SPF record. Spam detection systems in turn can be more aggressive about blocking emails that fail an SPF check in this manner.

Soft fail – When a soft fail is specified within DNS ("**~all**" at the end of the SPF record), this means that the administrator is less confident (or is being more cautious) compared to a hard failure. This may be used for a limited time for testing. Typically, messages that fail an SPF check with a soft failure will be accepted rather than rejected, but may not be automatically considered spam. Within MAX Mail, administrators can choose whether they should be equally or less aggressive in handling soft SPF failures relative to hard SPF failures.

When an SPF failure is detected, the MAX MailProtection service may take any one of several options for handling that message:

Apply standard filtering – Continue scanning the message with standard anti-spam and anti-virus engines, but do not apply any additional weight or score based on the SPF check. This essentially tells the service to ignore the results of the SPF failure.

Treat as suspicious – Apply an additional low spam score to the message. This, in conjunction with any other scoring applied by other filters within MAX Mail, may classify the message as spam depending on the spam handling aggressiveness configured for the recipient..

SPF CHECK RESULT	APPLY STANDARD FILTERING	TREAT AS SUSPICIOUS	TREAT AS SPAM	TEMPORARILY DEFER MESSAGE	PERMANENTLY BOUNCE MESSAGE
Failure (Hard Fail)	◉	○	○	○	○
Failure (Soft Fail)	◉	○	○	○	○

Treat as spam – Treat the message as spam.

Temporarily defer message – Issue a 400 series temporary failure code at the SMTP connection phase of transmission. This will instruct the sending MTA to retry delivery. If the SPF record changes to allow the sending sever to relay for this domain, or if the message is sent from an IP address matching the SPF record, the message will subsequently be accepted. Otherwise, the deferrals will continue, and the message will eventually bounce (in accordance with the retry schedule of the sending server).

Permanently bounce message – a 500 series permanent failure code will be issued to the sending MTA, indicating that delivery has failed.

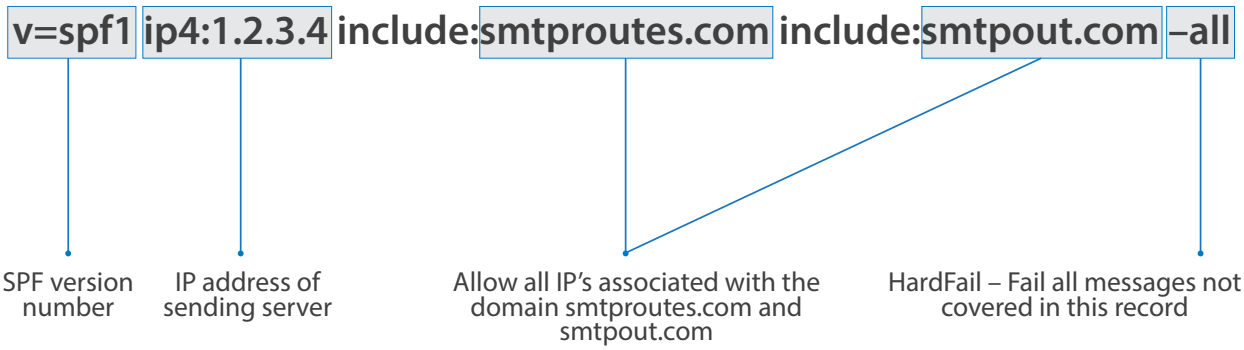
The recommended settings are:

SoftFail – Treat as suspicious

HardFail – Treat as spam

How to create an SPF record

With the rise in phishing attacks, it is increasingly important that companies specify an SPF record in their public DNS, to help prevent spoofed messages from their domain(s). We recommend that our customers create an SPF record for each of their domains; the SPF records are simply text entries within the DNS record. While SPF records will differ depending on the system(s) used to send outbound mail for the domain in question, a typical SPF record is:



This indicates that outbound mail for the domain should only come from the domain's mail server (1.2.3.4) or from MAX Mail (smtpout.com and smtproutes.com are the domains used by the MAX MailProtection outbound filtering service). If any other mail servers (such as an email marketing service) are legitimately used to send outbound mail for the domain, that sender should also be added to the SPF record.

Connect with us!

Please get in touch if you have any questions about any of our services.

UK: +44 0 1313 414899
US: +1 855 801 5461
APAC: +61 8 7123 4068

info@LOGICnow.com

@LOGICnow

LOGICnow
CHOOSE INTELLIGENCE