SPF Settings

Sender Policy Framework (**SPF**) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators.[1] The list of authorized sending hosts for a domain is published in the Domain Name System (DNS) records for that domain in the form of a specially formatted TXT record. Email spam and phishing often use forged "from" addresses, so publishing and checking SPF records can be considered anti-spam techniques. (See original source).

Set SPF Settings

- Set **SPF Enabled** field to **YES** or **NO** in order to enable or disable SPF.

> Disabling SPF will also automatically disable DKIM if enabled.

- Set the **Logging Level** field to a logging level of your choice. By default, it's set to **Level 1**.
  - **Level 1** logs no debugging messages, just basic policy results and errors generated through the policy server.
  - **Level 2** adds a log message if no client address (IP address from which the connection was made), Mail From address, or HELO/EHLO name is received by the policy server, and logs SPF results for each Mail From and HELO check.
  - **Level 3** generates a log message each time the policy server starts and each time it exits, as well as logging a copy of the exact header returned to Postfix to be prepended into the message. Each time the policy server starts. Level 3 also logs the configuration information used by the policy server.
  - **Level 4** logs the complete data set received by Postfix via the policy interface and when the end of the entry is read.
  - **Level 5** is used to debug config file processing and, for this purpose, can only be set in code and not via the config file. It also provides additional internal status details generally of interest only to developers.
  - **Level 0** server logs errors only.
  - **Disabled** logs nothing, not even error messages. **This setting is NOT recommended**.
- Set the Test Mode to Enabled or Disabled. Setting it to Enabled Hermes SEG will NOT block any e-mail and simply generate logs.
- Set the **HELO Check Rejection Policy** field to a setting of your choice. By default, it's set to **Reject HELO Fail**.

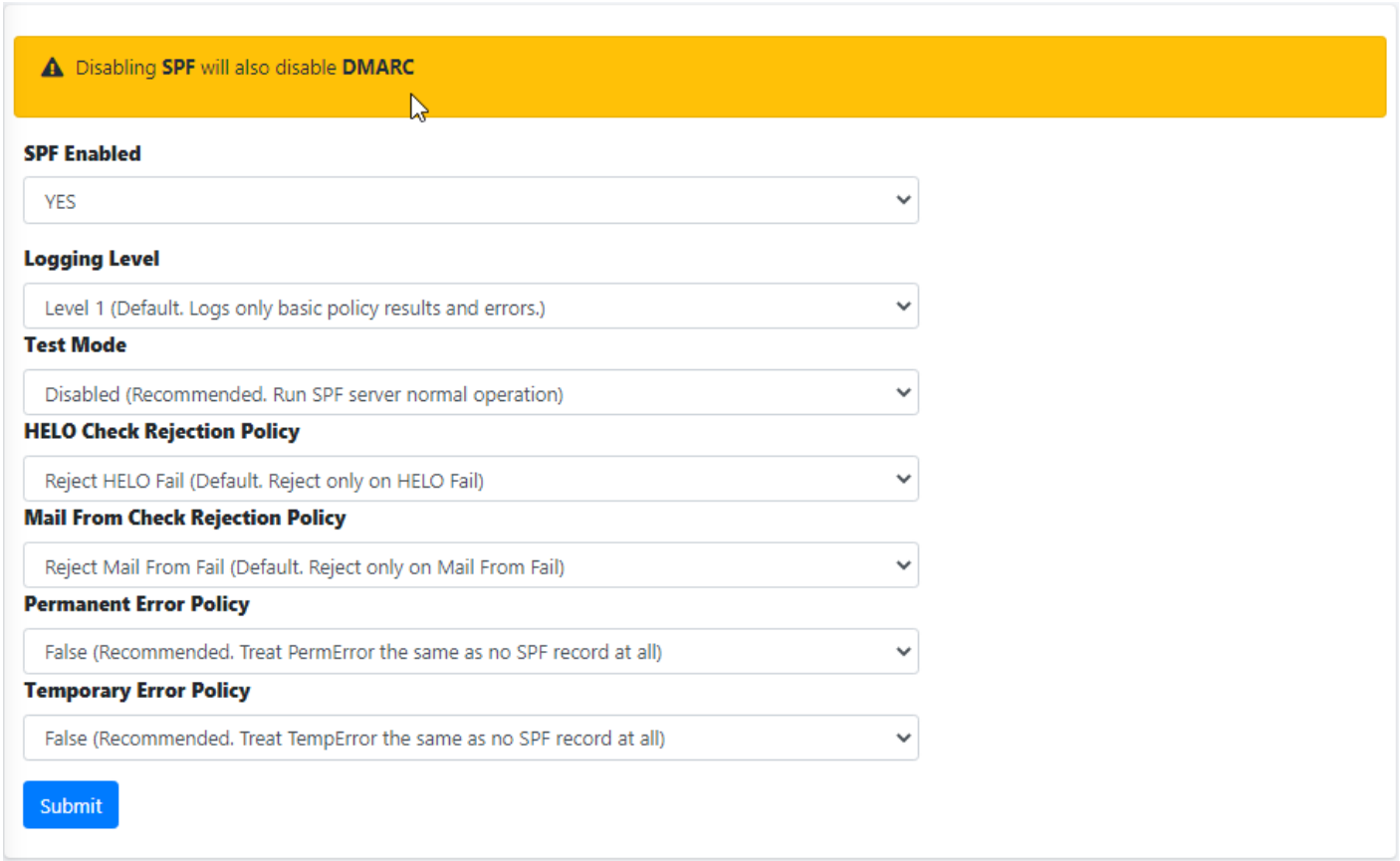
- **Reject HELO Fail** rejects only on HELO Fail. HELO/EHLO is known first in the SMTP dialogue and there is no practical reason to waste resources on Mail From checks if the HELO check will already cause the message to be rejected. This should not cause interoperability problems when used for HELO.
- **Reject All** rejects if the SPF result is **Fail, Softfail, Neutral, PermError**. Unlike the **Mail From Checking Policy**, there are no standard e-mail use cases where a HELO check should not Pass if there is an SPF record for the HELO name (transparent forwarding, for example, is not an issue). HELO/EHLO is known first in the SMTP dialogue and there is no practical reason to waste resources on Mail From checks if the HELO check will already cause the message to be rejected. This is not consistent with the RFC 7208 requirement to treat none and neutral the same, but should not cause interoperability problems when used for HELO.
- **Reject Softfail** rejects on HELO **Softfail** or **Fail**. HELO/EHLO is known first in the SMTP dialogue and there is no practical reason to waste resources on Mail From checks if the HELO check will already cause the message to be rejected. This should not cause interoperability problems when used for HELO.
- **Reject Null** - rejects HELO Fail for Null sender (SPF Classic). This is the approach used by the pre-RFC 4408 reference implementation and many of the pre- RFC specifications. Use of at least this option (SPF_Not_Pass or Fail) are preferred) is highly recommended.
- **Append Only** does NOT reject on HELO but instead appends a header only which the Spam Filter should detect and assign a Spam Score to it.
- **Disable Check** does not check HELO. This is only recommended if you are calling the policy server twice (once for HELO checks and once for Mail From) with two different configuration files. This approach is useful to get both the HELO and Mail From headers prepended to a message. **This setting is NOT recommended and should only be used by VERY experienced users with custom configurations.**

- Set the **Mail From Check Rejection Policy** to a setting of your choice. By default it's set to **Reject Mail from Fail**.
  - **Reject Mail from Fail** rejects on Mail From Fail.
  - **Reject All** rejects if result not Pass/None/Tempfail. This option is not RFC 7208 compliant since the mail with an SPF Neutral result is treated differently than mail with no SPF record and Softfail results are not supposed to cause mail rejection. Global use of this option is not recommended. Use per-domain if needed (per-domain usage described below).
  - **Reject Softfail** rejects on Mail From Softfail or Fail. **Use of this option is NOT recommended**.
  - **Append Only** does NOT reject but instead appends a header only which the Spam Filter should detect and assign a Spam Score to it.
  - **Disable** never checks Mail From/Return Path. This is only recommended if you are calling the policy server twice (once for HELO checks and once for Mail From) with two different configuration files. This approach is useful to get both the HELO and Mail From headers prepended to a message. It could also be used to do HELO checking only (because HELO checking has a lower false positive risk than Mail From checking), but this approach may not be fully RFC 7208 compliant since the Mail

From identity is mandatory if HELO checking does not reach a definitive result. **This setting is NOT recommended and should only be used by VERY experienced users with custom configurations.**

- Set the **Permanent Error Policy** to a setting of your choice. By default it's set to **False**.
  - **False** treats PermError the same as no SPF record at all. This is consistet with the pre-RFC usage (the pre-RFC name for this error was "Unknown").
  - **True** rejects the message if the SPF result (for HELO or Mail From) is PermError. This has a higher short-term false positive risk, but does result in senders getting feedback that they have a problem with their SPF record.
- Set the **Temporary Error Policy** to a setting of your choice. By default it's set to **False**.
  - **False** treats TempError the same as no SPF record at all. This is the default to minimize false positive risk.
  - **True** defers the message if the SPF result (for HELO or Mail From) is TempError. This is the traditional usage and has proven useful in reducing acceptance of unwanted messages. Sometimes spam senders do not retry. Sometimes by the time a message is retried the sending IP has made it onto a DNS RBL and can then be rejected. This is not the default because it is possible for some DNS errors that are classified as "Temporary" per RFC 7208 to be permanent in the sense that they require operator intervention to correct. (**Figure 1**).

Figure 1

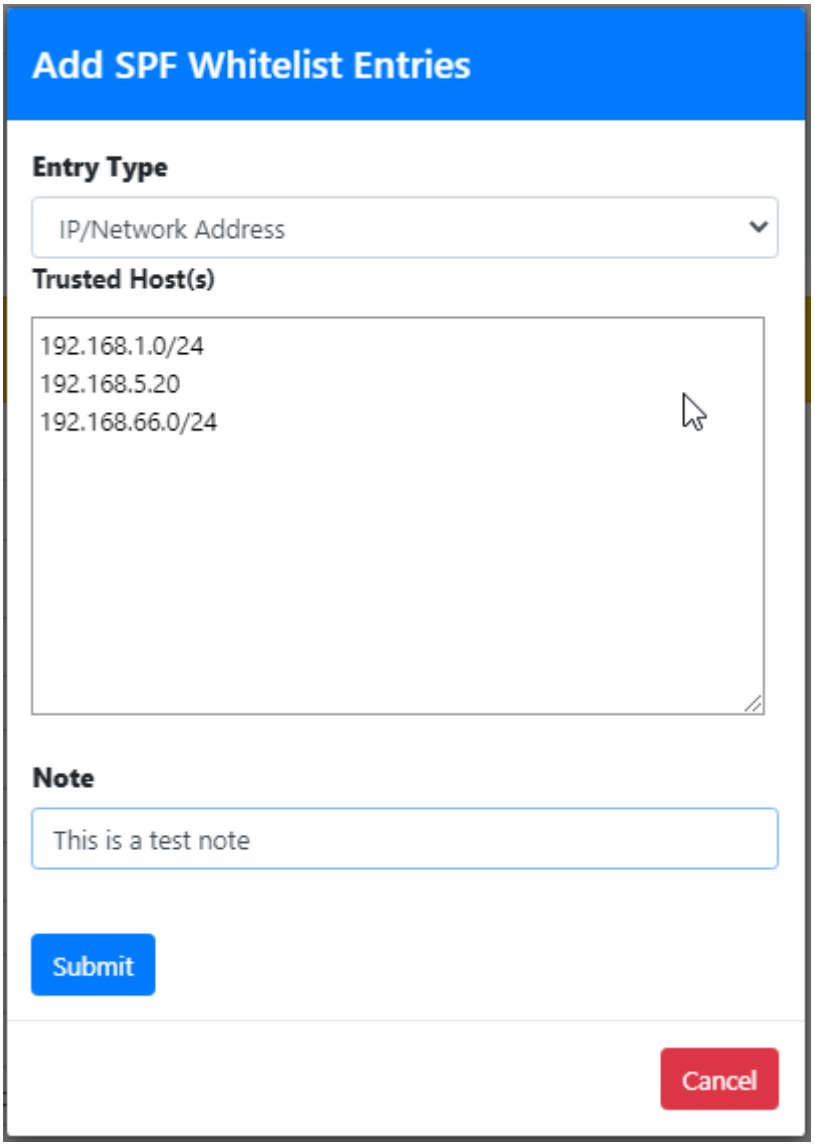


Add SPF Whitelist Entries

Adding entries in the SPF Whitelist will allow Hermes SEG to skip SPF checks for those entries. SPF Whitelist entries can be an IP/Network Address, HELO/EHLO Host Name, Domain Name or PTR Domain.

Click the **Add SPF Whitelist Entries** button and in the resultant menu, select the **Entry Type**, enter the entries the **Trusted Host(s)** field (You can add multiple entries each in its own line), enter an optional note in the **Note** field and click the **Submit** button (**Figure 2).**

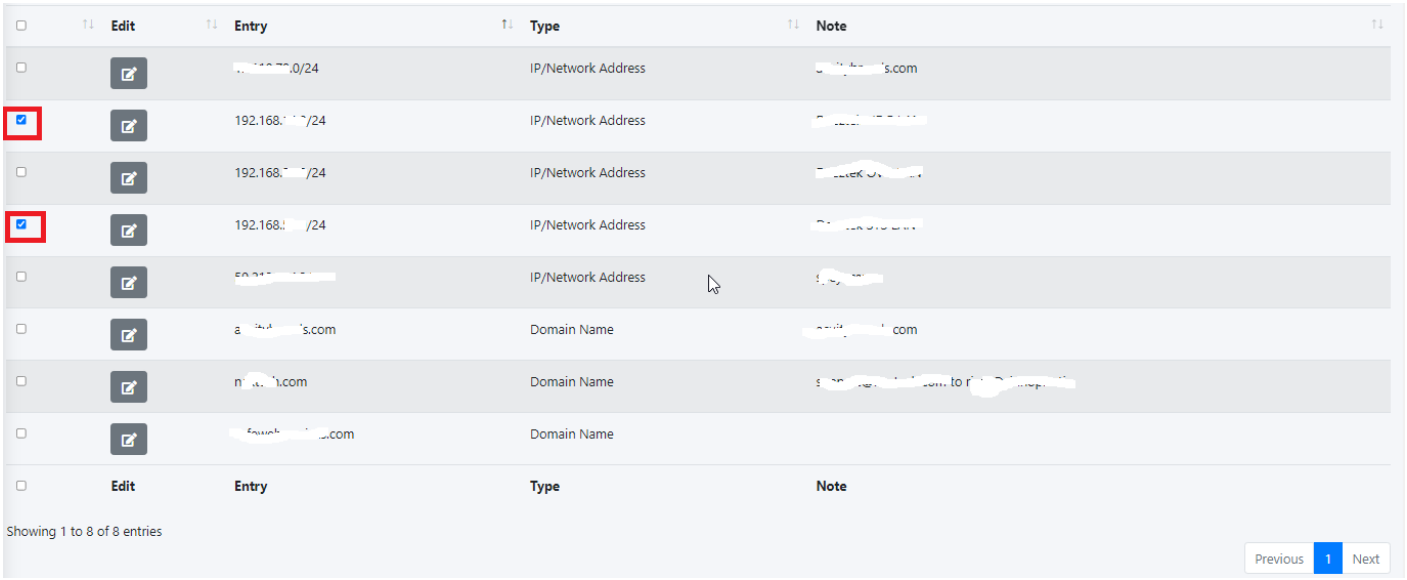
Figure 2



Delete SPF Whitelist Entries

Select the entries you wish to delete by checking their checkboxes and click the **Delete** button on top of the page (**Figure 3**).

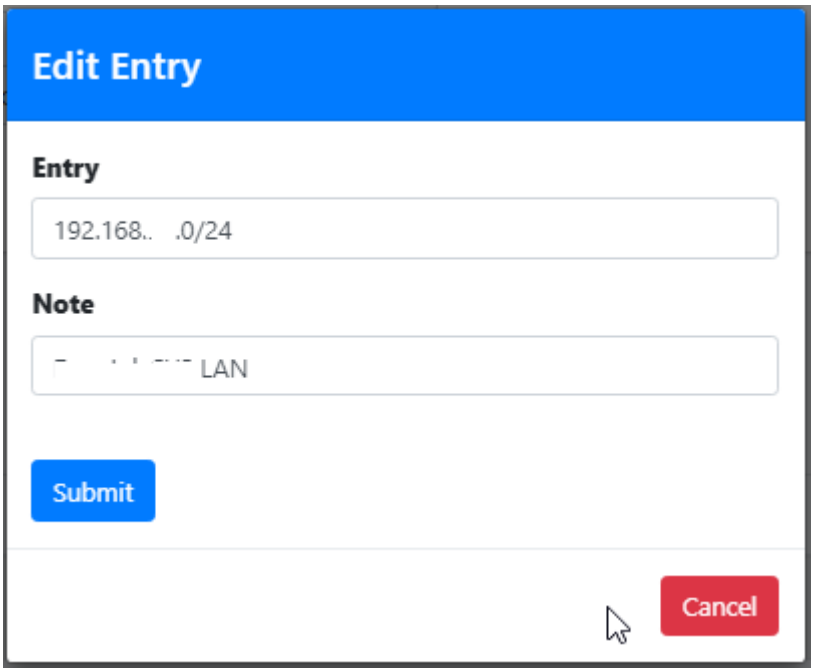
Figure 3



Edit SPF Whitelist Entry

Click the icon next to the entry you wish to edit. In the resultant window, make changes as necessary and click the **Submit** button (**Figure 4**).

Figure 4



Revision #16
Created 2 January 2021 14:14:30 by Dino Edwards
Updated 28 June 2022 19:02:21 by Dino Edwards