

Endpoint: spamassassin

Endpoint

[/3.0/spamassassin](#)

Description

This endpoint is internally used by TorneAUTH and controls spam filters for mail addresses created and hosted by Tornevall Networks. **Special API permissions are required.**

Syntax

As this endpoint works mostly with TorneAUTH the key parameter is **email**.

Sending an email to **getUserWhiteList** like below

```
{
  "email": "test@tornevall-domain.com"
}
```

The response - depending on the configured whitelist - will look like this:

```
{
  "getUserWhiteListResponse": [
    "*@*.whitelisted.com",
    "*@marvel.com",
    "tomas.tornevall@second.domain.com"
  ]
}
```

Available syntax

VERB	PARAMETERS	DESCRIPTION	RETURNS
<code>getUserWhiteList</code>	email	Returns user chosen whitelist	
<code>getGlobalWhiteList</code>	-	Returns globally whitelisted domains and mail addresses (that is whitelisted regardless of receiving email address)	<p>The behaviour in this response is based on that some senders is using something like contract@invoice.company.com and employee@company.com depending on what's being sent. To not miss one of them, they always are set up in pairs. If eff.org is whitelisted, the response will contain one *@*.eff.org and one *@eff.org</p> <pre>{ "getGlobalWhiteListResponse": ["*@*.eff.org", "*@*.facebookmail.com", "*@*.jetbrains.com", "*@*.youtube.com", "*@eff.org", "*@facebookmail.com", "*@jetbrains.com", "*@youtube.com"] }</pre>

getGlobalBlackListSender	-	Global blacklist	<p>Example</p> <pre> { "getGlobalBlackListSenderResponse": ["@fritt-val.se", "@nam-mail.com", "@spinxdigitalmedia.com", "@sverigeerbjudanden.com", "@tilbud-nu.net", "*yachtmarket*", "d.green@virgin.net"] } </pre>										
setGlobalWhitelistHost	host	Set hostname /domain name as whitelisted in the global region	true/false/exception										
delGlobalWhitelistHost	host	Removes hostname /domainname in the global whitelist	true/false/exception										
verifyAccount	email password	<p>Verify an email account that it actually has access (used by TorneAUTH to verify that users owns the account before configuring it).</p> <p>To protect user login information we prefer to test the email address rather than the username.</p>	true/false/exception										
setAddressWhitelist	email - Receiver emailmask - Sender	<p>Set up hostnames and senders to be whitelisted for a specific mail address (with or without wildcards).</p> <p><i>Emailmask can be *@*.domain.com, full. email@address.com, etc</i></p>	true/false/exception										
removeAddressWhiteList	email - Receiver emailmask - Sender	Remove hostname or sender that was before whitelisted for a specific mail address	true/false/exception										
getSpamAssassinOptions	email	Get current configuration for a specific email address	<p>Current settings, current defaults, info about which of the preferences that is strict (meaning preferences that is only globally configurable).</p> <table border="1" data-bbox="558 1671 1344 1885"> <thead> <tr> <th>json-object-tag</th> <th>Content description</th> </tr> </thead> <tbody> <tr> <td>preferences</td> <td>By user current configuration</td> </tr> <tr> <td>descriptions</td> <td>Each preference description</td> </tr> <tr> <td>booleans</td> <td>For webforms, tells which setting that can use checkboxes</td> </tr> <tr> <td>strict</td> <td>Data from the API that can not be changed and should be considered static</td> </tr> </tbody> </table> <p>Example</p>	json-object-tag	Content description	preferences	By user current configuration	descriptions	Each preference description	booleans	For webforms, tells which setting that can use checkboxes	strict	Data from the API that can not be changed and should be considered static
json-object-tag	Content description												
preferences	By user current configuration												
descriptions	Each preference description												
booleans	For webforms, tells which setting that can use checkboxes												
strict	Data from the API that can not be changed and should be considered static												

SpamOptions

```
{
  "getSpamAssassinOptionsResponse": {
    "preferences": {
      "bayes_auto_learn": "1",
      "fold_headers": "1",
      "normalize_charset": "1",
      "ok_languages": "sv se en",
      "ok_locales": "sv se en",
      "report_safe": "2",
      "rewrite_header": "Subject [SPAMASSASSIN]",
      "skip_rbl_checks": "0",
      "use_auto_whitelist": "1",
      "use_bayes": "1",
      "use_pyzor": "1",
      "use_razor2": "1",
      "required_hits": "5"
    },
    "descriptions": {
      "bayes_auto_learn": "Whether SpamAssassin should automatically feed high-scoring mails (or low-scoring mails, for non-spam) into its learning systems",
      "fold_headers": "By default, headers added by SpamAssassin will be whitespace folded. In other words, they will be broken up into multiple lines instead of one very long one and each continuation line will have a tabulator prepended to mark it as a continuation of the preceding one.",
      "normalize_charset": "Whether to decode non- UTF-8 and non-ASCII textual parts and recode them to UTF-8 before the text is given over to rules processing",
      "ok_languages": "This option is used to specify which languages are considered okay for incoming mail. SpamAssassin will try to detect the language used in the message text.",
      "ok_locales": "This option is used to specify which locales are considered OK for incoming mail. Mail using the character sets that are allowed by this option will not be marked as possibly being spam in a foreign language.",
      "report_safe": "0=Flagged spam: SpamAssassin will only add X-Spam-header in original message\n1=Flagged spam: SpamAssassin will create a new report with original message inside\n2=Flagged spam: SpamAssassin will attach original message as plain message. This setting may be required for safety reasons on certain broken mail clients that automatically load attachments without any action by the user. This setting may also make it somewhat more difficult to extract or view the original message.",
      "rewrite_header": "Adds a specific string to the mail when spam is detected",
      "skip_rbl_checks": "By default, SpamAssassin will run RBL (blacklist) checks. You need spam? Then you should skip the checks.",
      "use_auto_whitelist": "Whether to use auto-whitelists. Auto-whitelists track the long-term average score for each sender and then shift the score of new messages toward that long-term average.",
      "use_bayes": "Whether to use the naive-Bayesian-style classifier built into SpamAssassin. This is a master on/off switch for all Bayes-related operations",
      "use_pyzor": "Not described",
      "use_razor2": "Not described"
    },
    "booleans": {
      "bayes_auto_learn": "1",
      "fold_headers": "1",
      "normalize_charset": "1",
      "ok_languages": "0",
      "ok_locales": "0",
      "report_safe": "0",
      "rewrite_header": "0",
      "skip_rbl_checks": "1",

```

			<pre> "use_auto_whitelist": "1", "use_bayes": "1", "use_pyzor": "1", "use_razor2": "1" }, "strict": { "bayes_auto_learn": "1", "use_auto_whitelist": "1" } } </pre>
update SpamAssassin Option	email preference value	Updates spamassassin options for a specific email address	true/false/exception