G-Lock Software

Swift Email Verifier

HOW TO VALIDATE EMAILS THROUGH API USING ADVANCED EMAIL VERIFIER

Introduction

Webemailverifier.com has partnered with worldwide leader in email marketing and SEO applications vendor; Glocksoft.com to provide an affordable and powerful email validation web API service to users of Advanced Email Verifier (AEV) software. AEV is an easy to use, powerful, and reliable utility to verify and clean up your mailing list. Starting from version 8.1.0 of AEV, users can now validate emails easily using the integrated API to overcome such issues as port 25 blocks, lack of proper SMTP emulation authentication/integrity properties such as Reverse DNS, Forward Reverse DNS, SPF, Valid HELO identifier, clean IP reputation, Greylisting detection etc.

This guide explains the steps to take to use the integrated API feature in AEV. Please note that this guide will not provide all details on how to install and use AEV. It is expected that you are already familiar with the software and how it works generally such as installation, importing your mailing lists etc. If you do not have a copy of AEV already, we recommend that you visit AEV website and place your order. You can also request for assistance from AEV staff that will be able to help you should you encounter any issues while using the software.

Overview of Email Validation API

Our real-time email validation API allows you to check if an email address really exists and if it can receive messages. For every email address checked, a specific status is presented which tells you if the email address is valid or invalid or whether it is damaging or undesirable for your email marketing including over 21 status codes for investigating the reason of a specific email validation failure.

What is Checked by Email Validation API (In progressive order):

✓ **Email syntax:** This checks the email addresses syntax and ensures that they conforms to IETF standards

✓ **Mail Server Existence Check:** This checks the availability of the email address domain using DNS MX records

✓ **Mail Existence Check:** This checks if the email address really exists and can receive email

✓ **Catch-All Domain Email Check:** This checks if the email domain will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server.

- ✓ **Disposable Email Address Check:** This checks if the email is provided by a known Disposable Email Address (DEA) provider such as Mailinator, 10MinuteMail, GuerrillaMail and about 2000 more.

Email Validation API Statuses and Status Codes

Our email validation API is a web service API and uses status codes to indicate API success or errors. The status codes provide further information regarding the result of the validation and indicate why the validation of an email may have failed.

The API defines the validity of an email address as follows using only 3 statuses and each of these statuses have their corresponding status codes.

Status	Description/Meaning
Valid	Mailbox exists and not handled by Catch-all domains or known to be a DEA
Invalid	Mailbox does not exists
Unknown	Mailbox could not be verified or is determined to be handled by a Catch-all domain, DEA, Greylisted,, SMTP/Mailbox timeouts, Temporary mailbox unavailability. Specific reason for failure is provided in the status codes.

Each of these Statuses is linked to the following status Codes:

Status Codes	Meaning
Mailbox Exists and Active	The email was successfully verified as Valid
Known Disposable Email Domain	This failure means that the email address is provided by a well-known disposable email address provider (DEA) such as mailinator.com
Syntax Error	This failure means that the email is not syntactically correct

Domain Does Not Exist	This means that the email domain has be found to be non-existent
Mailbox Not Found	This failure means that the mailbox for the provided email address does not exist.
DNS Query Error	This failure means that there was a DNS error when querying the MX server
SMTP Connection Blocked	This failure means that the external mail exchanger rejected the local sender address or the incoming connecting IP.
Mailbox Validation Error	This failure means that a timeout or error occurred while verifying the existence of the mailbox for the provided email address.
Mailbox temporary not reachable (Graylisting)	This failure means that the requested mailbox is temporarily unavailable; this is not an indicator that the mailbox actually exists or not but, often, a message sent by external mail exchangers with greylisting enabled.
Mailbox Not Reachable	This failure means that the email address could not be verified because the remote server was not responding
Catchall Email Domain	This failure means that the external mail exchanger under test accepts fake, non existent, email addresses; therefore the provided email address MAY be inexistent too. In most cases, these Catch-all domains are now setup by ISPs and ESPs as Catch-all Spam Trap domains specifically targeted to catch spammers using Dictionary Spam Attacks.
SMTP Connection Error	This failure means that a connection could not be established with the remote SMTP server

InvalidToken	An invalid API key was used. Please check the API key and make sure it is correct
NoMoreQueries	The allocated # of queries or requests for the API key has been exhausted.
InternalError	There was an unexpected error on our server.
InternalDBError	This error indicates that the API request failed due to database connection error from our server
Unable to get response from API:0	This error means that AEV dropped connection by timeout (set by user in the toolbar) when no data received from the API server. It may happen when user set low timeout and high number of Connections like 1000.
Invalid JSON Response	This error indicates that an error was received in the output of the results during the API call.

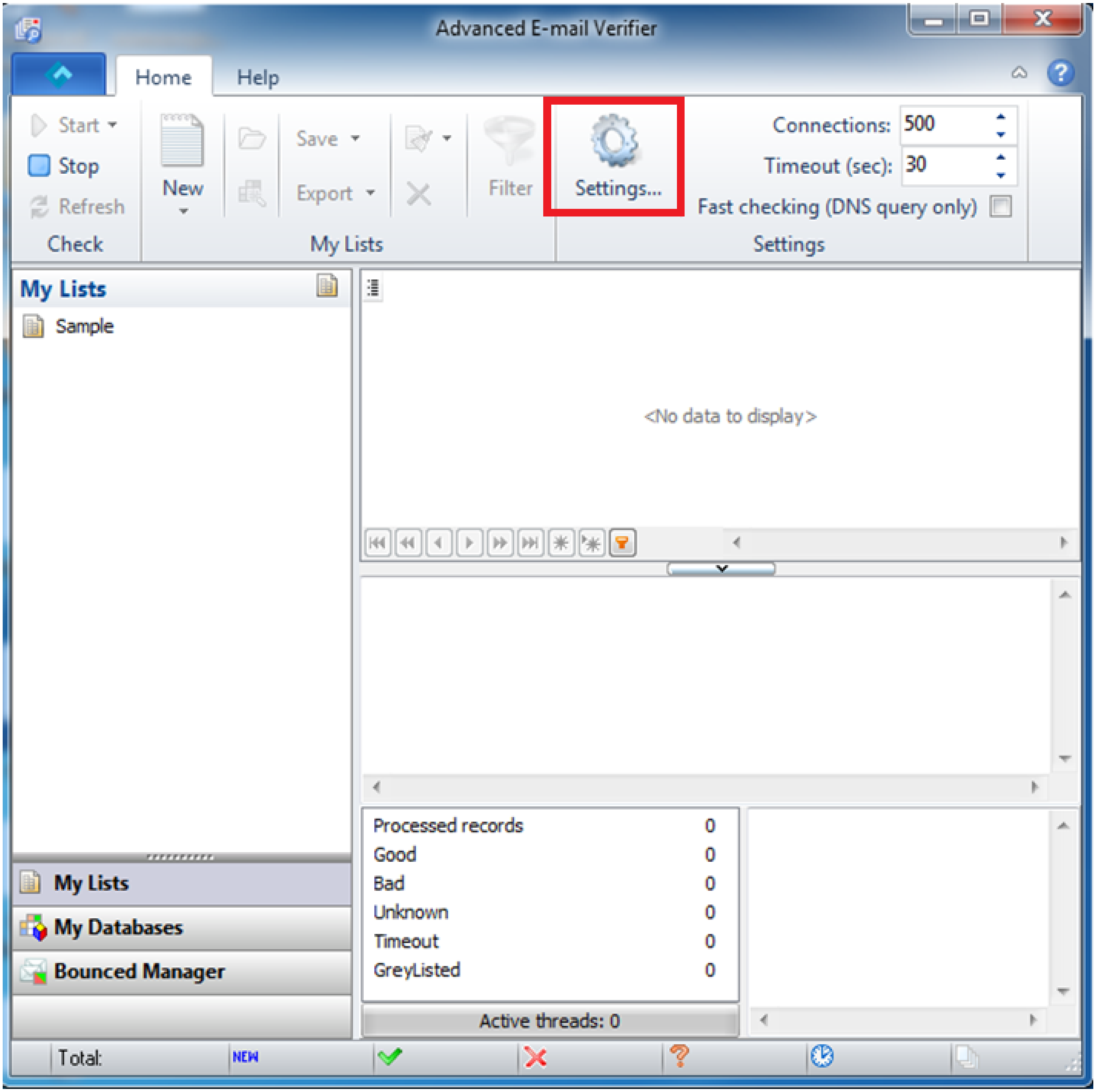
How to configure Email Validation API into AEV

The following steps are required to use the email validation in AEV:

Step1: It is expected that you already have a licensed version of the latest AEV version running on your computer. In addition, make sure you have your emails imported into the AEV software. To learn more, please go to the link below:

http://support.glocksoft.net/kb/articles/43-how-to-load-the-emails-for-verification

Step 2: Navigate to the settings menu of AEV as shown below and click on it.



Connections: 500

Timeout (sec): 30

Fast checking (DNS query only) □

Processed records	0
Good	0
Bad	0
Unknown	0
Timeout	0
GreyListed	0

Active threads: 0

Then click on the “DNS” tab to configure the “DNS servers List”, “Mail From” and “Domain name for HELO” settings.

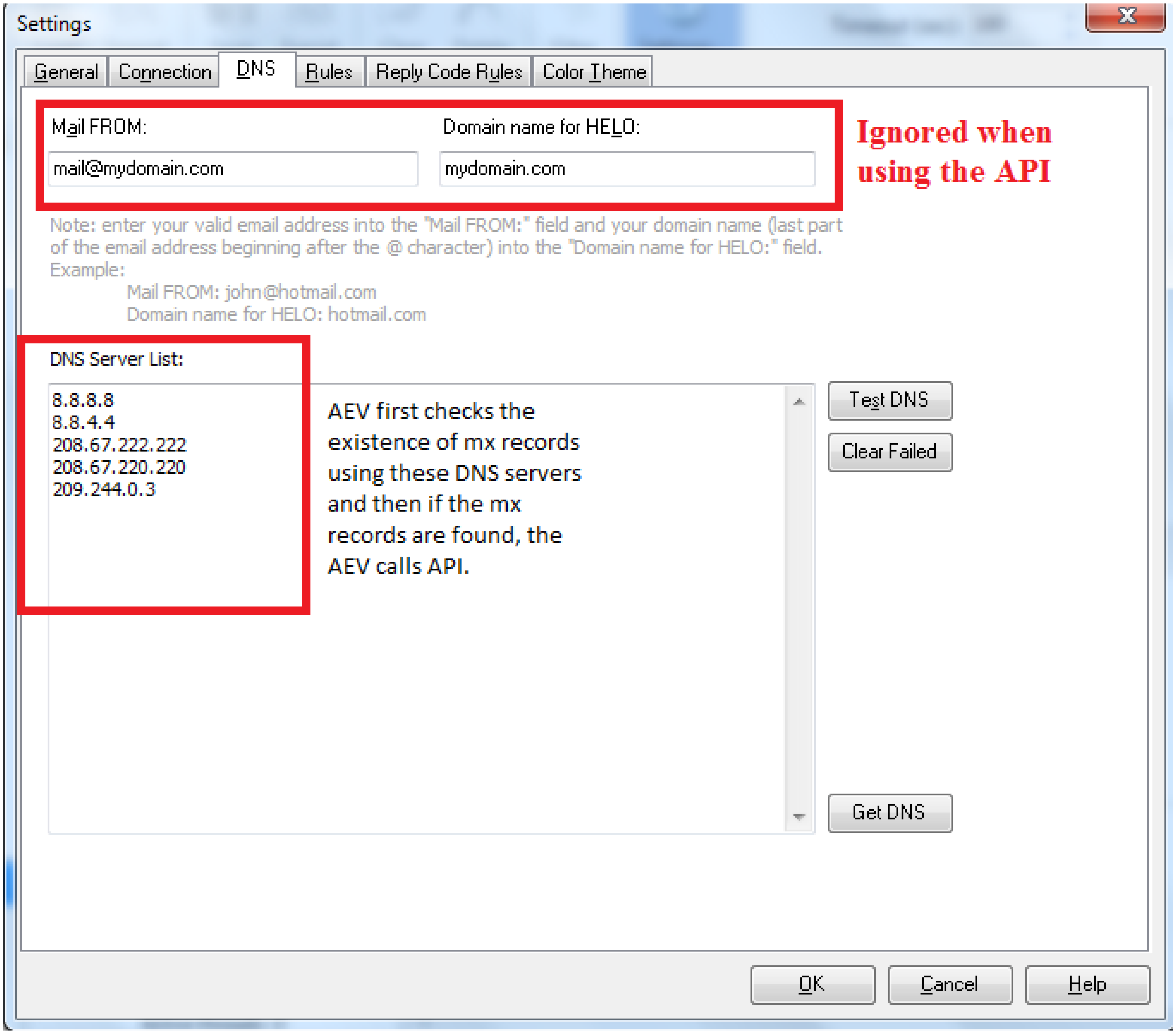
On the DNS settings window, then proceed to fill out the following fields:

- In the “Mail From” field, you may leave this blank or put any email since this is ignored when using the API. Any email address can be filled in here as this is not used by the API. The API already has its own built-in “Mail From” property.

- In the “Domain name for HELO” field, you may leave this blank since this parameter is ignored when using the API. The email validation API already has its own built-in “Domain name for HELO” property which is automatically used when activated in AEV.

- In the “DNS Servers List” form, proceed to add the following open DNS servers as follows:

  - 8.8.8.8
  - 8.8.4.4
  - 208.67.222.222
  - 208.67.220.220
  - 209.244.0.3



Mail FROM: mail@mydomain.com

Domain name for HELO: mydomain.com

Ignored when using the API

Note: enter your valid email address into the "Mail FROM:" field and your domain name (last part of the email address beginning after the @ character) into the "Domain name for HELO:" field.
Example:
Mail FROM: john@hotmail.com
Domain name for HELO: hotmail.com

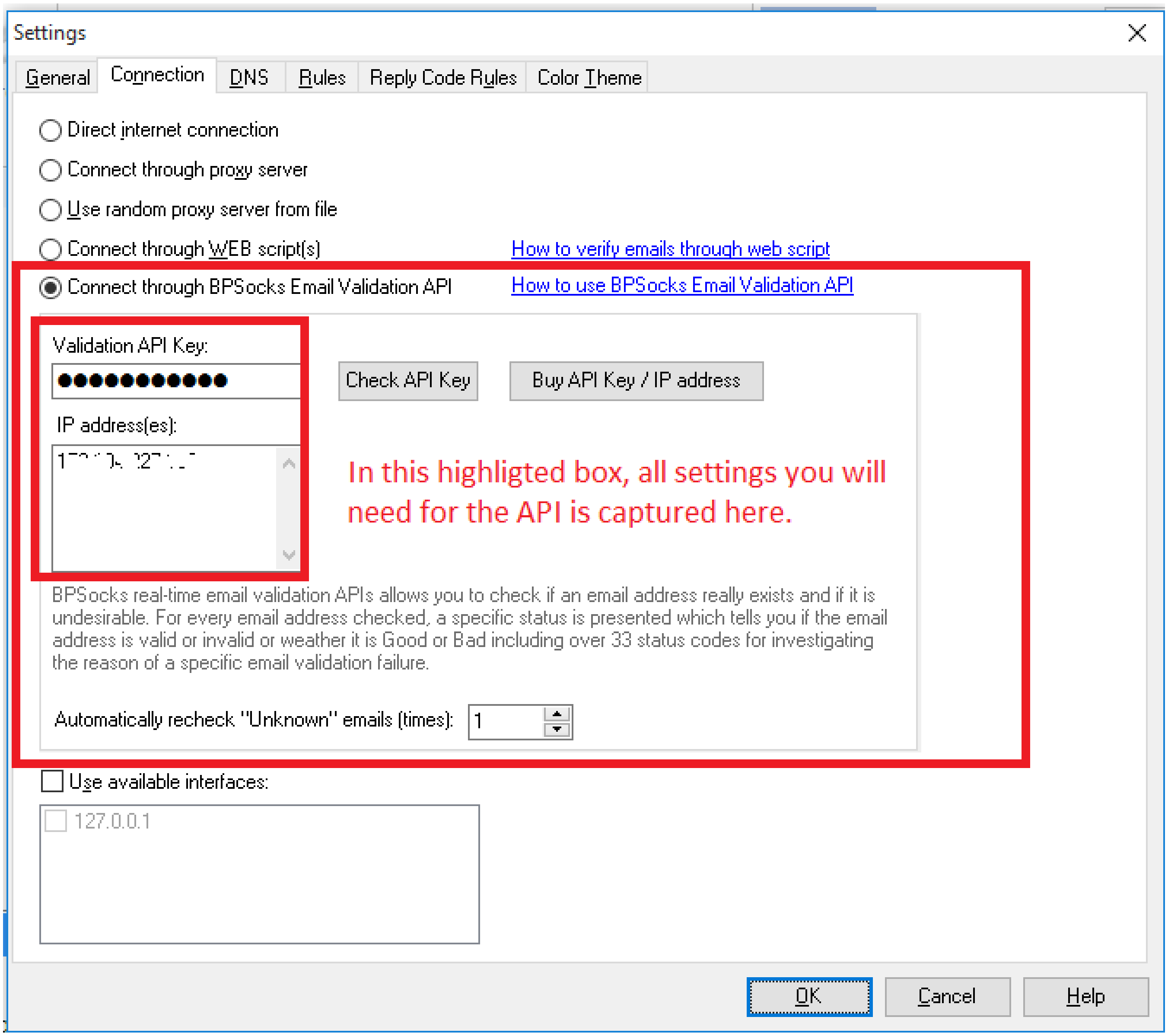
DNS Server List:

8.8.8.8
8.8.4.4
208.67.222.222
208.67.220.220
209.244.0.3

AEV first checks the existence of mx records using these DNS servers and then if the mx records are found, the AEV calls API.

Step 3: Have your API key and API servers IPs ready that you received when you placed the order which is required to allow you authenticate to the API.

To configure AEV to use our validation API, click on the "Connection" tab in the settings window and enter your API key and the API servers IPs (one per line) as shown below:



○ Direct internet connection

○ Connect through proxy server

○ Use random proxy server from file

○ Connect through WEB script(s)

● Connect through BPSocks Email Validation API

Validation API Key: ●●●●●●●●●●●●

IP address(es): [illegible]

In this highligted box, all settings you will need for the API is captured here.

BPSocks real-time email validation APIs allows you to check if an email address really exists and if it is undesirable. For every email address checked, a specific status is presented which tells you if the email address is valid or invalid or weather it is Good or Bad including over 33 status codes for investigating the reason of a specific email validation failure.

Automatically recheck "Unknown" emails (times): 1

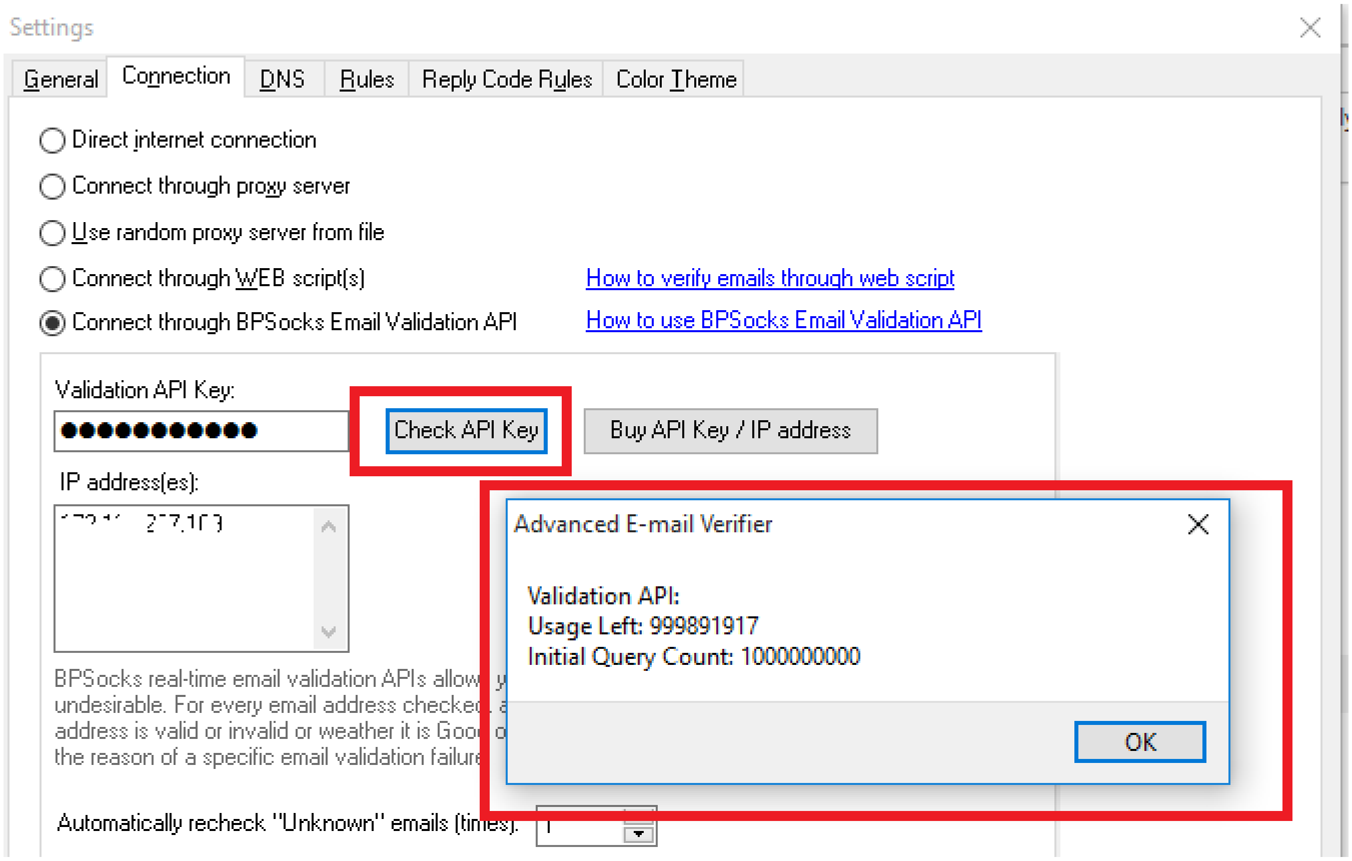
☐ Use available interfaces:

☐ 127.0.0.1

Important: To specify how many times you wish to have the unknown email results automatically re-validated, please enter a number in the "Automatically recheck "unknown" emails (times) field. We recommend you enter 2-3.

Please note that you are allowed to re-check the unknown emails as many times as you want. We do not charge for unknown emails and your credits will not be deducted for any unknown email status.

Step 4: Check for the quota of the API key. You can also check the validity including the current quota or used quota of the key anytime by clicking on the "Check API Key" button as shown below:



○ Direct internet connection
○ Connect through proxy server
○ Use random proxy server from file
○ Connect through WEB script(s) — How to verify emails through web script
● Connect through BPSocks Email Validation API — How to use BPSocks Email Validation API

Validation API Key: ●●●●●●●●●●●

IP address(es): [redacted]

BPSocks real-time email validation APIs allow y
undesirable. For every email address checked a
address is valid or invalid or weather it is Good o
the reason of a specific email validation failure

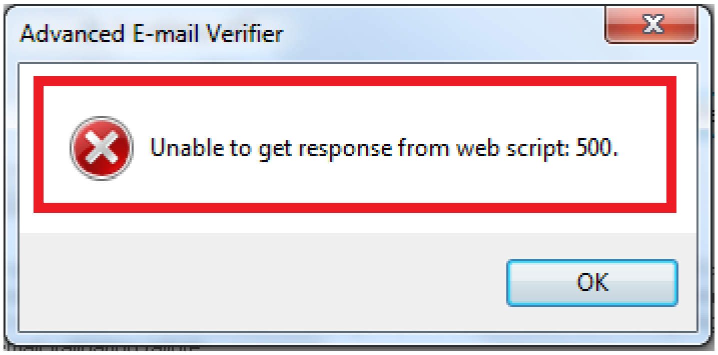
Automatically recheck "Unknown" emails (times): 1

Advanced E-mail Verifier

Validation API:
Usage Left: 999891917
Initial Query Count: 1000000000

The displayed "Usage Left" is the remaining API quota that is left on the API key. Please note that you can always top-up the API key at any time without having to order for a new API. To do this simply place an order and instruct us to top-up your existing API key.

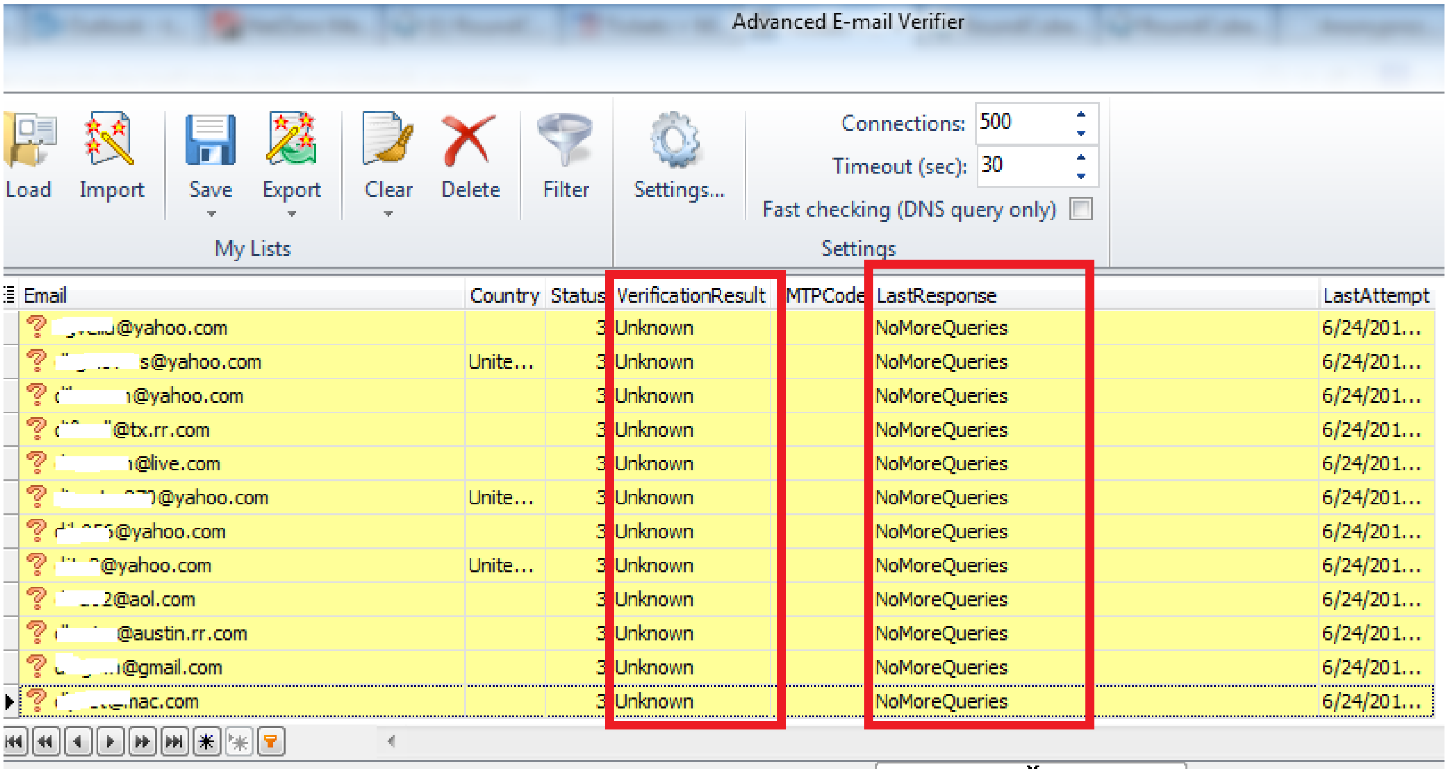
Do note that sometimes the API quota check function may time out occasionally. This is normal and you should simply retry it again by re-clicking on the Check Quota button. When the API key quota check function time out, you will get the message below:



Advanced E-mail Verifier

Unable to get response from web script: 500.

Note: If you have exhausted your API Key quota and you have an active validation job running, the results will return "Unknown" with a status code of "NoMoreQueries". This is illustrated in the sample screenshot below. Please note that there is no feature to alert you when you reach your limit in AEV. Hence, you must check your current quota limit for the API key before you start your validation with AEV. Make sure the number of emails loaded in AEV is less than your current key quota before starting the validation.



Connections: 500
Timeout (sec): 30
Fast checking (DNS query only) □

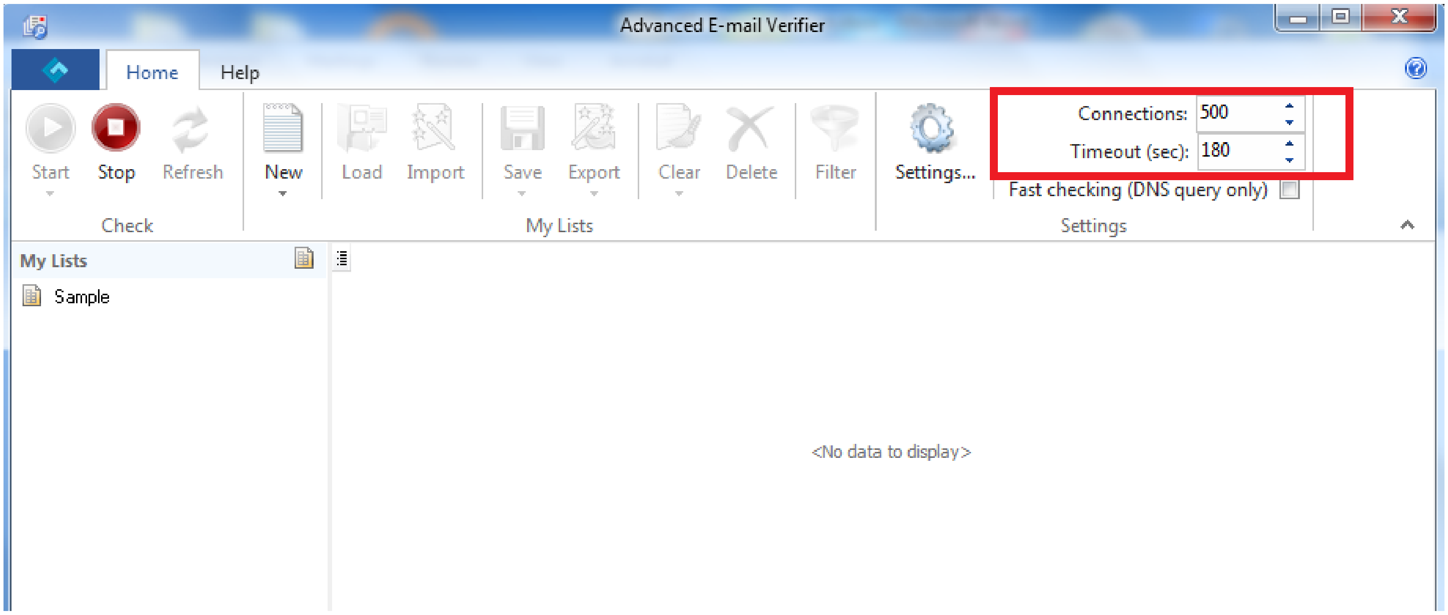
Email	Country	Status	VerificationResult	MTPCode	LastResponse	LastAttempt
[redacted]@yahoo.com		3	Unknown		NoMoreQueries	6/24/201…
[redacted]s@yahoo.com	Unite…	3	Unknown		NoMoreQueries	6/24/201…
[redacted]@yahoo.com		3	Unknown		NoMoreQueries	6/24/201…
[redacted]@tx.rr.com		3	Unknown		NoMoreQueries	6/24/201…
[redacted]@live.com		3	Unknown		NoMoreQueries	6/24/201…
[redacted]@yahoo.com	Unite…	3	Unknown		NoMoreQueries	6/24/201…
[redacted]@yahoo.com		3	Unknown		NoMoreQueries	6/24/201…
[redacted]@yahoo.com	Unite…	3	Unknown		NoMoreQueries	6/24/201…
[redacted]2@aol.com		3	Unknown		NoMoreQueries	6/24/201…
[redacted]@austin.rr.com		3	Unknown		NoMoreQueries	6/24/201…
[redacted]@gmail.com		3	Unknown		NoMoreQueries	6/24/201…
[redacted]nac.com		3	Unknown		NoMoreQueries	6/24/201…

Step 5: Check AEV rules by clicking on the "Rules" tab in order to view your current email validation rules that has been defined in AEV. Please note that AEV comes with a default rule to exclude the validation of emails from certain free email providers such as Yahoo.com, Hotmail.com and Gmail.com. With our API, you will not have any issues validating emails from these free email domains although with Yahoo in particular do sometimes gives false positives because it is not possible to verify Yahoo emails with 100% success rate without actually sending messages to the Yahoo mailbox.

Therefore, if you are not 100% satisfied with the verification performance of our API with respect to a particular email ISP or domain as seen from the results, you are free to exclude such email domains from your email validations via our API. To do this, click on the rules tab and search for the domain(s) and make sure it is checked. You are free to enable other custom rules that suit you.

Note: Please be aware that the rules specified here will take priority over the API. Email addresses will be processed using these rules first before being processed via the API. To enable exclusive processing of all email addresses via the API, please disable these rules.

Step 6: Enter your desired # of connections for multi-threaded validations. Depending on your system hardware and network speed, you may use between 500 to 1000 threads as number of parallel connections in the connections field and set the maximum timeout of 180 sec in the Home menu window. Although AEV supports up to 1000 simultaneous connections, please do not use a very high number of threads if your system cannot support it as doing so would result to many unknowns with the status code "Unable to get response from API". If you have a multi-core or dual CPU system and a fast network, using the 1000 threads will be OK.

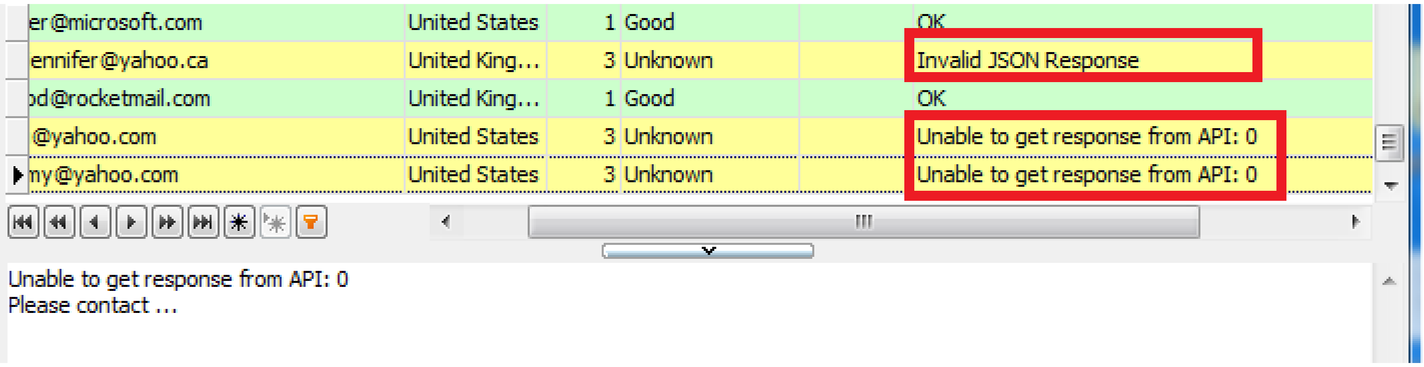


Connections: 500

Timeout (sec): 180

Fast checking (DNS query only) □

<No data to display>



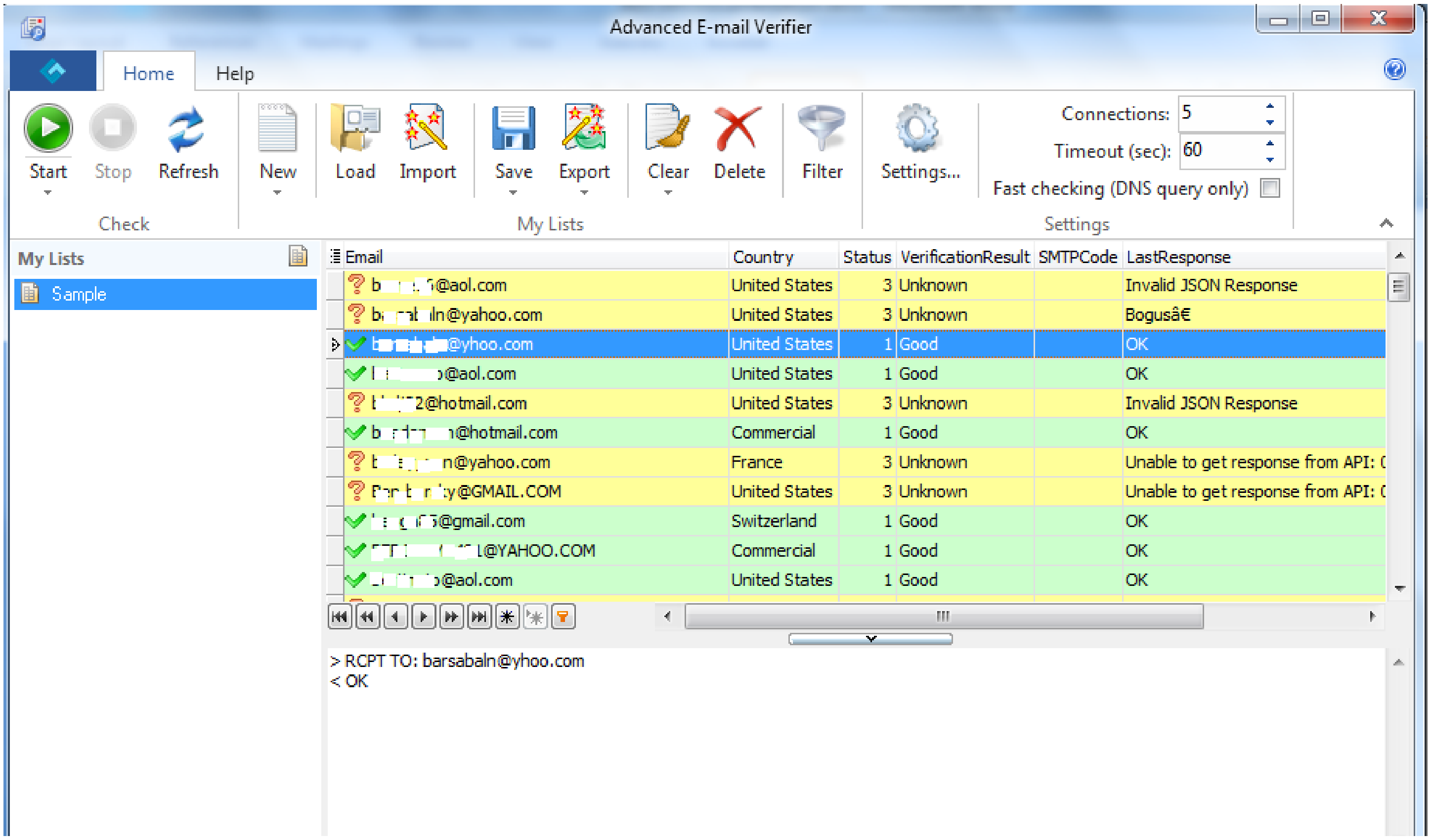
er@microsoft.com	United States	1	Good		OK
ennifer@yahoo.ca	United King...	3	Unknown		Invalid JSON Response
od@rocketmail.com	United King...	1	Good		OK
@yahoo.com	United States	3	Unknown		Unable to get response from API: 0
ny@yahoo.com	United States	3	Unknown		Unable to get response from API: 0

Unable to get response from API: 0
Please contact ...

Please note that if you set the # of connections too high with a low timeout, you will encounter the error: "Unable to get response from API:0"

In addition, to prevent connection timeout errors, it is advisable to add Advanced Email Verifier to the list of allowed programs in your firewall settings if using one in your computer. If you have anti-virus software, please switch it off before verifying the email addresses.

Step 7: To start validating your emails, click on the “Start” green button on the AEV program. After some time, the program will display the verification results of the checks with the corresponding response codes for each email address validated. A sample is shown below:



Connections: 5
Timeout (sec): 60
Fast checking (DNS query only) □

	Email	Country	Status	VerificationResult	SMTPCode	LastResponse
?	b[redacted]@aol.com	United States	3	Unknown		Invalid JSON Response
?	b[redacted]ln@yahoo.com	United States	3	Unknown		Bogusâ€
✓	[redacted]@yhoo.com	United States	1	Good		OK
✓	[redacted]@aol.com	United States	1	Good		OK
?	[redacted]2@hotmail.com	United States	3	Unknown		Invalid JSON Response
✓	b[redacted]n@hotmail.com	Commercial	1	Good		OK
?	[redacted]n@yahoo.com	France	3	Unknown		Unable to get response from API: (
?	[redacted]y@GMAIL.COM	United States	3	Unknown		Unable to get response from API: (
✓	[redacted]5@gmail.com	Switzerland	1	Good		OK
✓	[redacted]L@YAHOO.COM	Commercial	1	Good		OK
✓	[redacted]@aol.com	United States	1	Good		OK

```
> RCPT TO: barsabaln@yhoo.com
< OK
```

When the validation process has finished, you may then proceed to save or export your results as usual. For details, please refer to AEV official documentation.

Configure the Email Validation API Keys and Servers IP(s)for AEV

You can purchase your API keys securely from our website using the link below: https://www.gondorland.com/member/signup.php or you can click on the “Buy Validation API Key” button directly from the program.

The following payment options are accepted:

- Paypal
- Swift Wire Money Transfer
- Perfect Money
- Bitcoin

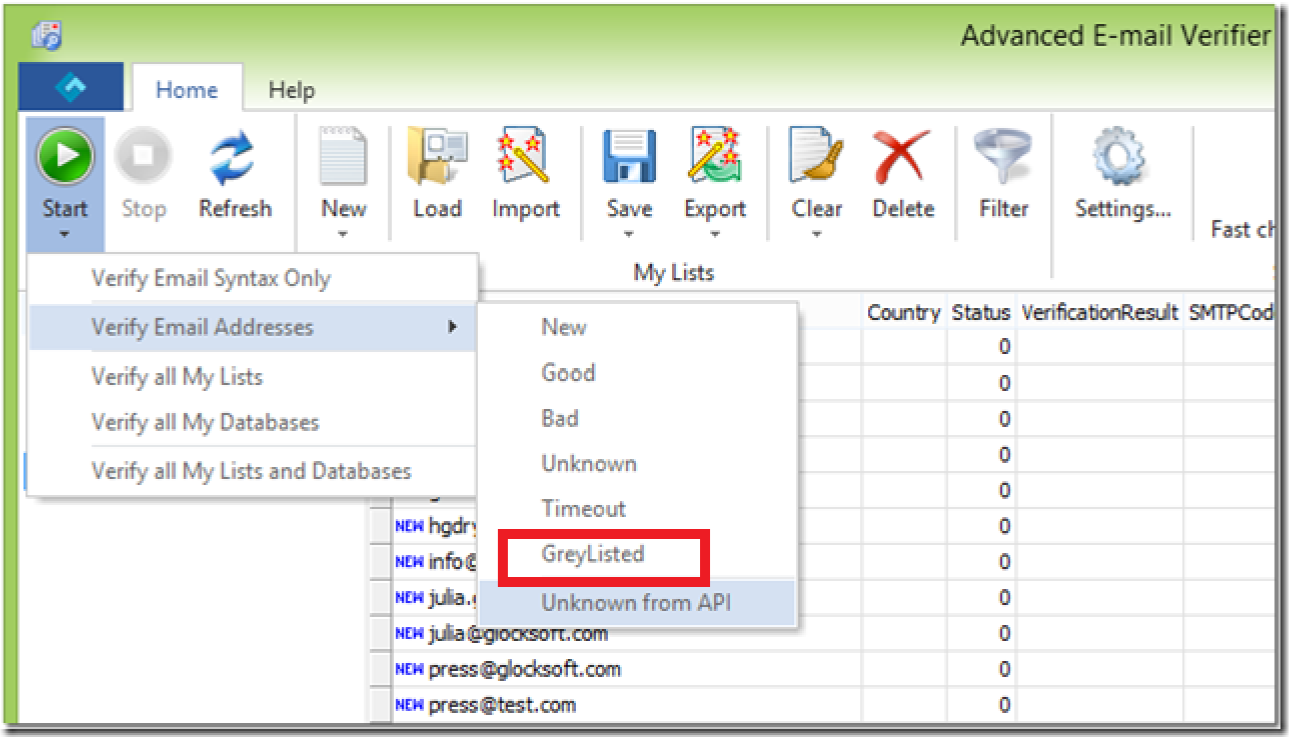
Each API key has a fixed maximum quota of 1 million which can be consumed by each API server you are issued. Please purchase the package that best suits your mailing list size and needs. Please contact us to order for discounted purchases.

Greylisting Detection and Handling

Our email validation API comes with a powerful automatic Greylisting detection and handling otherwise known as email temporary mailbox unavailability which is technology that reduces spam by rejecting initial email delivery attempts. Greylisting works by returning a temporary failure response ("Temporarily Unavailable") to the first attempt to deliver an email, but accepts it on the second attempt. Thus every proper email server will attempt to redeliver a message after a temporary failure response.

While performing validations with the API, any SMTP status code that reports a temporary unavailability of a mailbox will return the “Mailbox temporary not reachable (Graylisting)” verification status which indicates that the mail server has Greyisting enabled. To take care of this, the specific emails that returned this status code (MailboxTemporarilyUnavailable) must be filtered out from the results and re-loaded for re-validation after some time has elapsed.

In AEV, emails with the “Mailbox temporary not reachable (Graylisting)” status code are automatically classified as “Greylisted”. To re-validate greylisted email addresses in AEV, go to Settings menu and then to the General menu. There you will find an option to re-check Greylisted emails in one session. This is illustrated in the screenshot below:



	Country	Status	VerificationResult	SMTPCod
		0		
		0		
		0		
		0		
		0		
NEW hgdr		0		
NEW info@		0		
NEW julia.		0		
NEW julia@glocksoft.com		0		
NEW press@glocksoft.com		0		
NEW press@test.com		0		

CatchAll Email Domains Detection and Handling

Our email validation API has the capability to automatically detect Catch-all emails which is a mailbox on an email domain that will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server. This Catch-All domain test is performed at the “Mailbox Existence” level. First the checker engine checks if the mailbox being verified actually exists on the mail server and if this succeeds, it goes a step further to check if the email domain will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server.

Thus emails that return “Catchall Email Domain" status may be VALID or INVALID. The emails could not be conclusively determined as VALID because the email server under test accepts fake, non-existent, email addresses; therefore the provided email address MAY be inexistent too. In some cases, these Catch-all domains are now setup by ISPs and ESPs as Catch-all Spam Trap domains specifically targeted to catch spammers using Dictionary Spam Attacks.

Therefore, it is impossible to verify conclusively whether the email address is good or not. You won't know definitively until the message bounce. We recommend bounce processing be used to take care of unknown emails. AEV includes an in-built bounce handling module that can be used to process the bounced emails to the unknown results list. Simply download the unknown results mailing list and send your campaign to the list using a bounce-to email address. Thereafter, use the bounce handling module to connect to the bounce-to email address and process the bounced emails which will then be subtracted from the unknown mailing list. You can run the Bounce Handler to process bounced emails during 2-5 days after you send your email campaign because bounced emails may arrive within 2-5 days.

Alternatively, you may use our hybrid email validation program

How to Handle Unknown Results

The Unknown results are those emails which could not be verified due to one reason or the other. These unknown results in most cases results from Greylisting which is technology that reduces spam by rejecting initial email delivery attempts. The Greylisting works by returning a "Temporarily Unavailable" message to the sending mail server the first (and only the first) time a message is received from a given sender. Hence, it makes sense to retry these validations again after some time has elapsed.

Also unknown results can also result from the inability to verify the emails by simulating a message sending to the recipient email server because the recipient email server requires that a REAL message is sent. Thus, it is impossible to verify whether the address is good or not. You won't know definitively until the message bounce because these mail servers won't cooperate or cannot be checked without sending a real message to them.

Thus, we highly recommend that you attempt to re-validate the unknowns again to increase the success rate.

Other reasons why emails could return unknown statuses can be found on the status/status codes table here

Automatic Refund of Credits Used for Unknown Results

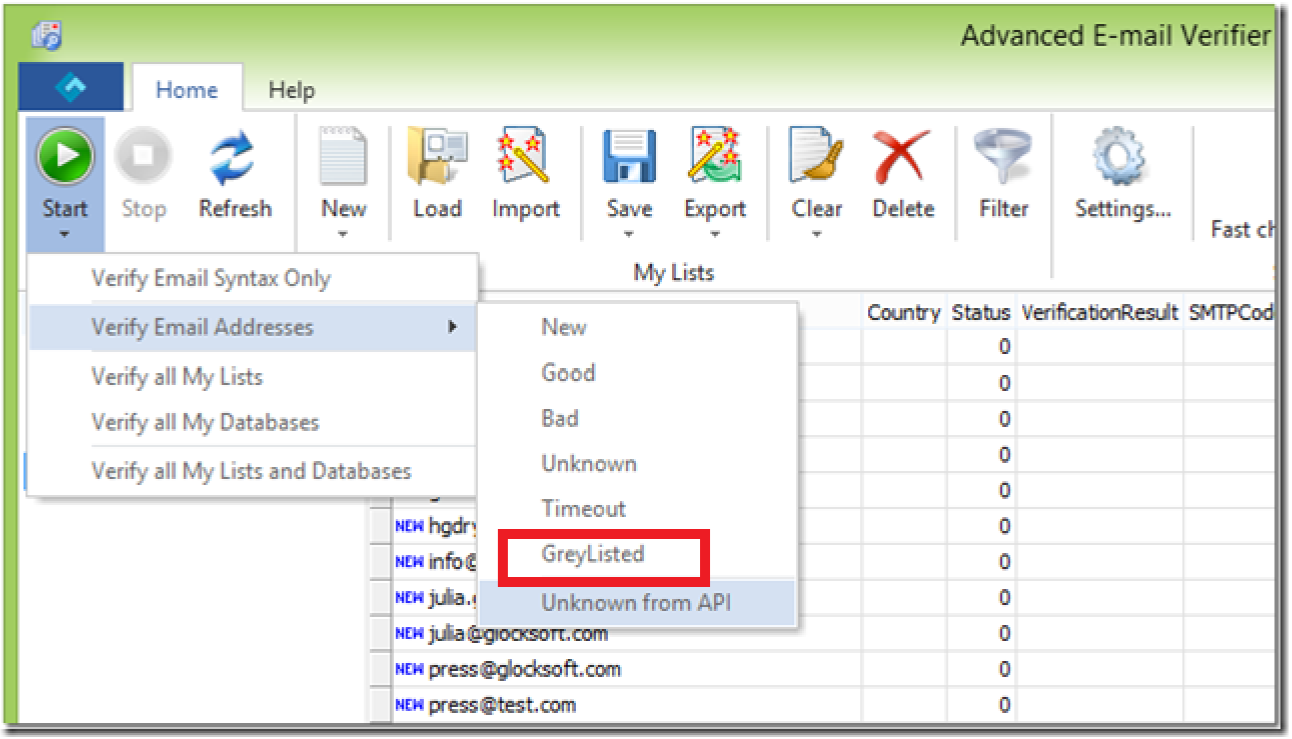
Automatic refund of API key credits used for unknown results has been implemented in the email validation API. All unknown email validation results from our email validation server will no longer count towards your API key quota. This means that we will not charge credits from your API key quota when the result of a validation is unknown. Therefore you do not need to contact us anymore to replace the quota for the unknown results.

Since we no longer charge for unknown results users now have more flexibility on how they choose to handle the unknown results. You can choose to re-validate the unknown emails after several days in case of greylisted emails or non-cooperating email domains.

Automatic Multiple Re-validation of Unknown Results

In order to improve your email validation results and minimize unknowns, AEV have implemented an intelligent and automatic multiple re-validation of email addresses which return the unknown status starting from version 8.2.0. Thus by retrying the validation several times, temporary or transient errors are avoided and the end result is very low unknowns.

In addition, to take care of email which needs to be re-validated at a later time after some time have elapsed such as Greylisted emails, AEV has also implemented a new option to manually re-check unknown emails returned by the API to the program Start button menu. The program re-tries the re-validation the number of times that is indicated in the settings. For example, if you want to re-validate only the Greylisted emails after some time have elapsed, simply click go to the Start button, then go to "Verify Email Addresses" click on "Greylisted. However, if you want to re-validate the whole unknown results, click on the "Unknown from API" button. This is illustrated in the screenshot below:



Note: The resultant unknown results from your email validation job in AEV can be re-checked as many times you like because these will not count towards your API key credits but you may have to wait for some time to elapse like 1-24 hrs. However, the best way and the recommended way to deal with the final resultant unknown emails is to use a bounce handling utility. AEV has a bounce handling feature. For details, please consult AEV manual.

Important Information Regarding Unknown Results

The following recommended practices are strongly recommended to deal with the unknown results reported by the API:

1. Since a majority of the unknown results are caused by temporary issues (Soft Bounces) such as SMTP server timeout or downtime, Greylisting, Mailbox size Exceeds quota, temporary mailbox suspension/deactivation, and temporary blockings due to IP reputation, it is strongly recommend to re-validate the entire unknown list again at a later time. We do not recommend deleting the unknown list immediately after running your verification job. Chances are that previous emails which previously tested as unknown could test valid after re-validating the list.

2. Due to multiple factors beyond our control, it is not technically possible to validate all emails with 100% success rate using the SMTP emulation method which involves connecting to the remote SMTP server and emulating to be a SMTP server without actually sending any messages. This method although works for most email servers cannot work for ALL SMTP servers.

Using Your Cleaned Emails in Third Party Email Delivery Services

Many companies and email marketers are now using third party email delivery services to handle the delivery of their transactional and marketing emails. By using a professional third party email delivery service, a higher inbox placement or delivery rate can be achieved. These third party email delivery services have relationships with various ISPs/ESPs and also provide strict acceptable "Bounce Rate" threshold for those who use their service to avoid being labeled as a server that delivers spam.

Although, the benefits of using a third party email delivery service is obvious, extreme care must be taken in order not to exceed the acceptable or permitted "Bounce Rate" for any email campaign you send through their platforms. Bounce rate is simply the percentage of emails that is returned undelivered when you send out your campaign. Although most third party email services do not explicitly specify their bounce rate limit, as a rule of thumb, anything between 10-15% may be considered high.

The Bounce Rate is expressed as a percentage and is calculated as follows:

$$Bounce\_Rate = \frac{No.\_of\_Bounces}{Total\_No.\_Emails\_Sent} x100$$

Undeliverable emails, email "bouncebacks" or "bounces" are becoming more and more of a challenge for email marketers these days. Hence, all third party email delivery services has a specific allowed or permitted bounce rate for every email campaign you send using their services. If you exceed this rate, your account may be suspended or deactivated. In most cases, these third party email delivery services are required by ISPs/ESP and Spam Advisory Groups such as Spamhaus to enforce the bounce rate thresholds and suspend any account that exceeds these thresholds in order to prevent Spam.

In order to avoid your third party email delivery service account suspension or deactivation, it is important that you review and adopt the following best practices before importing your cleaned emails into your third party email delivery service as follows:

1. After validating your list, save the VALID emails marked by the verifier. Do NOT add the emails marked as Unknown to the valid emails. As a rule, never upload the unknown emails to your third party email delivery service.

2. As we indicated above, never upload the emails marked as unknown by our email validation API to your third party email delivery service provider platform. Doing so may cause a lot of bounces and you may risk your account suspended. If you wish to verify the unknown emails by sending a re-confirmation or re-

verification messages to the unknown emails addresses, you can use our new hybrid or real-time bounce processing API client application for Windows users which allows you to send real messages and process any bounces all in real-time via our special program. The program uses the same validation API key and the price for validating each email remains at the same price.

Frequently Asked Questions on Email Validation API

Question 1: How does your email validation API work. Will my IP address get blacklisted when using the API?

Answer: Your IP will never be blacklisted when using our API. Therefore there is no need to worry about your IP being blacklisted.

Our email validation API is a simple and REST based API which can be used to validate emails effectively using the following order of validation processing:

- **Syntax Check:** This checks the email addresses and ensures that they conforms to IETF standards using a complete syntactical email validation engine
- **Fake Email Pattern Detection:** This checks the email address against a powerful in-built fake email pattern detector algorithm. This fake email pattern detector is capable of detecting thousands of fake email automatically with very high accuracy.
- **Typo Check and Curse Words Check:** This checks the email address against all known common typos for most email domains. The API can also detect certain curse words present in the email address.
- **Mail Server Existence Check:** This checks the availability of the email address domain using DNS MX records
- **Mail Existence Check:** This checks if the email address really exists and can receive email via SMTP connections and sending email emulation techniques.
- **Catch-All Domain Email Check:** This checks if the email domain will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server
- **Disposable Email Address Check:** This checks if the email is provided by a known Disposable Email Address (DEA) provider such as Mailinator, 10MinuteMail, GuerrillaMail and about 2000 more

Question 2: How does your email scrubbing API work?

Answer: AEV email scrubbing API is a real time email cleaning system that allows you to scrub email addresses against our millions of undesirable and bad email database such as bogus/stale email addresses, role accounts, disposable email addresses (DEA), publicly harvested/extracted email addresses and blacklisted emails/email domains.

The following email cleaning processes can be achieved using the scrubbing API:

- **Bad/Bogus Email :** Bad or bogus email addresses can be detected

- **Fake or High Risk Email/Domains Check:** All known publicly harvested addresses can be detected and removed from your list

- **Disposable Email Address Check:** This checks if the email is provided by a known Disposable Email Address (DEA) provider such as Mailinator, 10MinuteMail, GuerrillaMail and about 2000 more. If you run a service in which you would like to reduce the number of anonymous subscribers using disposable email addresses, you can use our API to block such subscribers at point of signup thereby helping you to reduce the number of anonymous subscribers to your service.

- **Role Accounts** such as admin@domain.com, webmaster@domain.com, support@domain.com etc

- **Known Blacklisted/Bogus emails and Email Domains Check:** All records matching our millions of known spammers emails, malicious or bogus emails and emails belonging to known spam domains emails database can be used to scrub your mailing lists and any matches are removed using our scrubbing API.

Question 3: What is the difference between the email validation API and the email scrubbing API?

Answer: Although some similarities exists between the email validation and email scrubbing API, a key difference between them is that whereas the email validation API performs a full email check and check if the email address actually exists on the remote mail server via SMTP connections, the scrubbing API do not perform any actual email existence check. Therefore, emails marked “Good” by the scrubber API may be nonexistent because the actual existence of the email address was not performed.

Ideally if you are an email marketer that that acquires or rents email list from third party list brokers, we strongly recommend the use of the scrubbing API to clean the list in addition to using the email validation API to verify if they emails actually exists. By using both APIs, you can obtain a high quality cleaned email list.

Question 4: What do I need to start using your API in AEV to validate emails?

Answer: First you must obtain the API key which allows you to authenticate to the API service. To obtain your API key, simply click on the purchase links in your AEV connections settings tab which will redirect you to the payment processor website. Once you have obtained your key, you can simply enter your key to activate the API. We offer a very flexible and affordable API pricing system. Our pricing plan is based on **$0.001** per email address validation or scrubbing.

You can also purchase your API keys securely from our website using the link below:
https://www.gondorland.com/member/signup.php

Question 5: What is the recommended number of threads and Timeout to use in AEV when using your API
Answer: We strongly recommend that you use no more than 500 threads unless you have a very powerful system such as multi-core (Quad core or dual/Quad CPU). Also please make sure you set the highest timeout as 120 sec. Doing this will ensure that you get minimal number of unknowns.

Question 6: How is your email validations performed? Does it send out any email?

Answer: Email validations carried out through the API is done using 3 progressive levels automatically as follows:

- **Syntax** : This checks the email addresses and ensures that they conforms to IETF standards using a complete syntactical email validation engine
- **Email Server Existence** : This level checks the availability of the email address domain using DNS MX records
- **Mailbox Existence** : This is a deep level verification which attempts to check if the email address really exists and goes a step further to check if the email domain is a Catch-all domain (a domain that will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server). The Mailbox verification establishes SMTP dialogs with external SMTP servers and this level usually requires longer time depending on multiple network factors.

The API employs DNS and SMTP protocol functionalities to perform email address validations and absolutely avoids sending any email message to external mail servers.

Question 7: Is it possible to verify all emails with your email verifier API service? How does the system handle Unknown emails?

Answer: It is not possible to validate all emails due to multiple factors beyond our control. The Unknown results are those emails which could not be verified due to one reason or the other. These unknown results in most cases results from Greylisting which is technology that reduces spam by rejecting initial email delivery attempts. The Greylisting works by returning a "Temporarily Unavailable" message to the sending mail server the first (and only the first) time a message is received from a given sender. Hence, it makes sense to retry these validations again after some time has elapsed.

In addition, unknown results can also result from the inability to verify the emails by simulating a message sending to the recipient email server because the recipient email server requires that a REAL message is sent. Thus, it is impossible to verify whether the address is good or not. You won't know definitively until the message bounce because these mail servers won't cooperate or cannot be checked without sending a real message to them. To accommodate for this, AEV includes an in-built bounce handling module that can be used to process the bounced emails to the unknown results list. For details, please consult the AEV manual.

Question 8: Can I achieve low bounce rates with the email validation API?

Answer: One of the main reasons why you must validate your emails regularly is to ensure that you avoid high bounce rates when you send your campaign to your lists. When you send emails to invalid emails, the message will bounce. A bounced message is one that has been rejected by the recipient’s email server. If your emails get bounce rates of over 10-15%, your email marketing service provider may likely disable your account until you can determine the cause of the bounces. This is because high bounce rates can get your email marketing service provider IPs blacklisted and will also negatively affect your sender reputation which will result to poor inbox deliverability. There are two types of bounces as follows:

- Hard bounces: These are bounces caused as a results of permanent failure during delivery (typically 5.x.x / Mailbox does not exist at the domain)

  Please see : http://www.basics.net/index.php/2011/07/27/e-mail-smtp-error-codes/

- Soft Bounces: These are bounces caused by temporarily failure such as Mailbox full errors ((beginning with a 4.x.x code as seen in above link)

With our email validation API, you will be able to verify your emails and detect a good number of emails that would have bounced (hard bounces) and these will be marked “Invalid”. Hence, you will be able to stay within the acceptable bounce rate limits typically permitted by email service providers. Emails with soft bounces will be marked “Unknown” and has be to revalidated. However, to identify emails with soft bounces which could turn out to become valid later, it is advisable to re-validate the unknown emails again after some days (1-3 days).

Question 9: Why are some invalid emails sometimes marked as Valid?

Answer: First, it is important to understand that our email validation technology uses the SMTP connection method to check whether a specific email address is valid or not by simulating email sending. However, due to certain multiple factors such as anti email harvesting technology, it is not possible to verify all emails with 100% success rate. This is because some mail servers such as public mail servers like Yahoo, AOL, etc have some measures in place which makes it impossible to accurately determine whether the email is valid or invalid because the mail servers will not cooperate and as a result the email address will be marked as valid when validated.

For example, Yahoo will always mark disabled or discontinued emails as Valid when verified. However, when you try to send to such disabled or discontinued emails, it will return this error message:

Remote server replied: 554 delivery error. Sorry your message to <email_address> cannot be delivered. This account has been disabled or discontinued.

For such mail servers, the only means to conclusively know if the email is valid or not is when the email bounce. Hence, it is recommended to use the bounce handler in AEV to process the bounces for such non cooperating mail servers in order to obtain the invalid emails or use our real-time bounce email processing API client program. For details on how to use the bounce processing feature of AEV, please consult the AEV manual.

Question 10: How secure are my email addresses validated through your API servers?

Answer: We take your mailing lists confidentiality seriously. If using our API for email address validation via AEV, your email addresses are never stored on our servers. All checks are done in real-time. In addition, all API calls or requests are transmitted via Secure Socket Layer (SSL) technology to prevent any potential credential sniffing

Question 11: Why do I have so many unknowns? What can be done to prevent getting many unknown?

Answer: The most common cause of the many unknowns is caused by network congestion or inability for your computer to process all the requested threads within the requested time when a very high number of threads and low timeout set the AEV user. We recommend you use no more than 100 threads and high timeout of about 200-300sec for best results.

Nevertheless, you can re-run the unknown emails again immediately after the current job is done. If any unknowns still come out, then re-run it again until you get very minimal unknowns that could not be verified not because of network factors but because the email server refused the validation for one reason or another. Another way you can automatically re-validate unknowns is to set the "Automatically re-check unknown emails(times)" value in the Connections tab of AEV to a higher number such as 3. Using 3 means that the unknowns will be automatically re-checked 3 times until they give a valid or invalid status.

Question 12: My question is not answered here. How can I get in touch with you?

Answer: Please contact us via our support center or email us at: digitalzone@strongmailvault.com