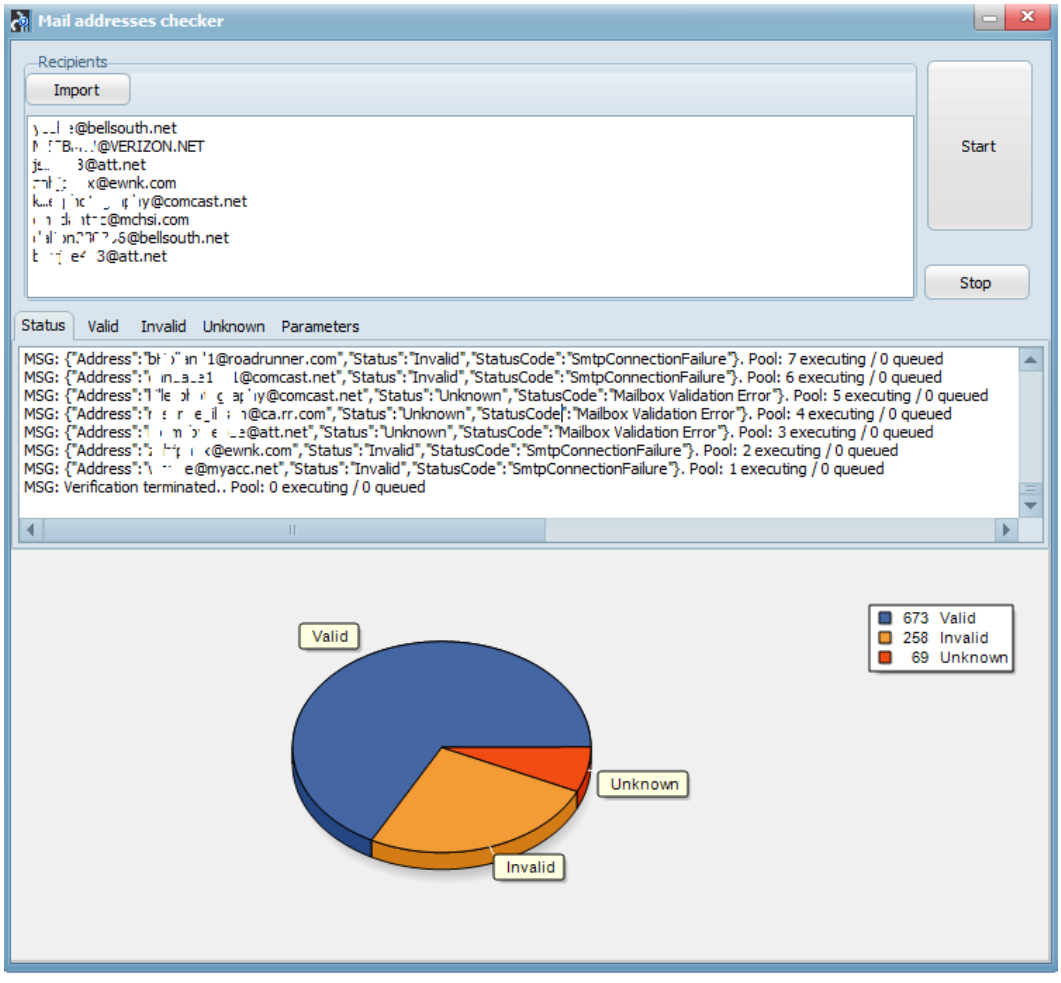
Swift Email Verifier API Client for Windows

Swift Email Verifier API client for Windows is a highly optimized and high speed/multithreaded Windows desktop application that allow users to verify bulk email addresses easily using an API key. The program can verify email addresses at speed up to 500 simultaneous threads. However, you may be able to run more threads up to the limit of your system hardware.

You do not need port 25 (SMTP port) to be open in your network in order to use the application. All you need is a good and stable internet connection. Mailing lists can be uploaded both in plain text formats and CSV formats. To take care of network failures which may result to unknown email results, the program includes a feature to automatically recheck unknown emails up to a number of times specified by the user. This ensures that validation result has minimal unknowns.

Note: This email verifier API client does not use your IP to verify emails. All verifications are done completely in the cloud through our servers. Therefore there is no risk of your IP being blacklisted. In addition, since the program uses our REST based API, you have 100% confidentiality of your email lists since you do not upload the lists to our servers. No requests logs containing your email addresses are kept on our servers.

Program Screenshot:



What is Checked by the Email Validation API:

- ✔ **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
Typo Checking	This status code indicates that a typo error was detected for a known email domain such as : john@hotmaill.com
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

API Key Authentication:

Clients must authenticate to the API by providing their API key. Care must be taken to secure the key from unauthorized access. It is your responsibility to keep your API key secure at all times and ensure that unauthorized users do not have access to it.

If you have placed order for multiple API servers, only one API key is required to authenticate to all of them. The API key can also be used by multiple persons from unlimited devices or computers at the same time without any restrictions.

What is Required to use the Program:

To validate your email addresses using the application, you will need the following:
1. Your Email validation API Key and the list of API servers that was provided to you.
2. The mailing list in the proper and supported format.

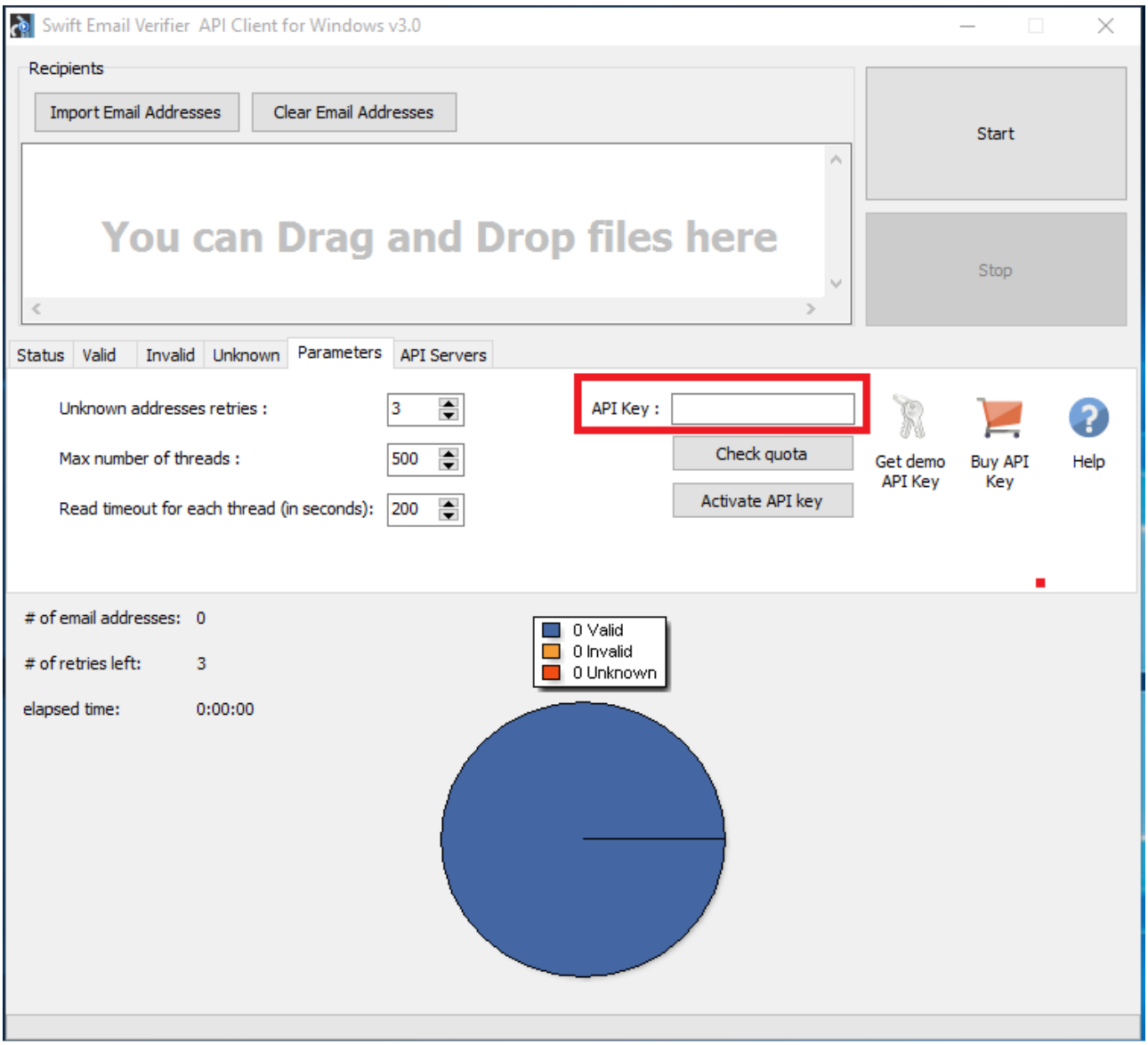
Usage Steps:

Step 1: Download the program on the link below:

http://www.webemailverifier.com/windowsclient.exe

Step 2: Execute the Program: Execute the program by double clicking on it and click on the "Parameters" tab as shown below:

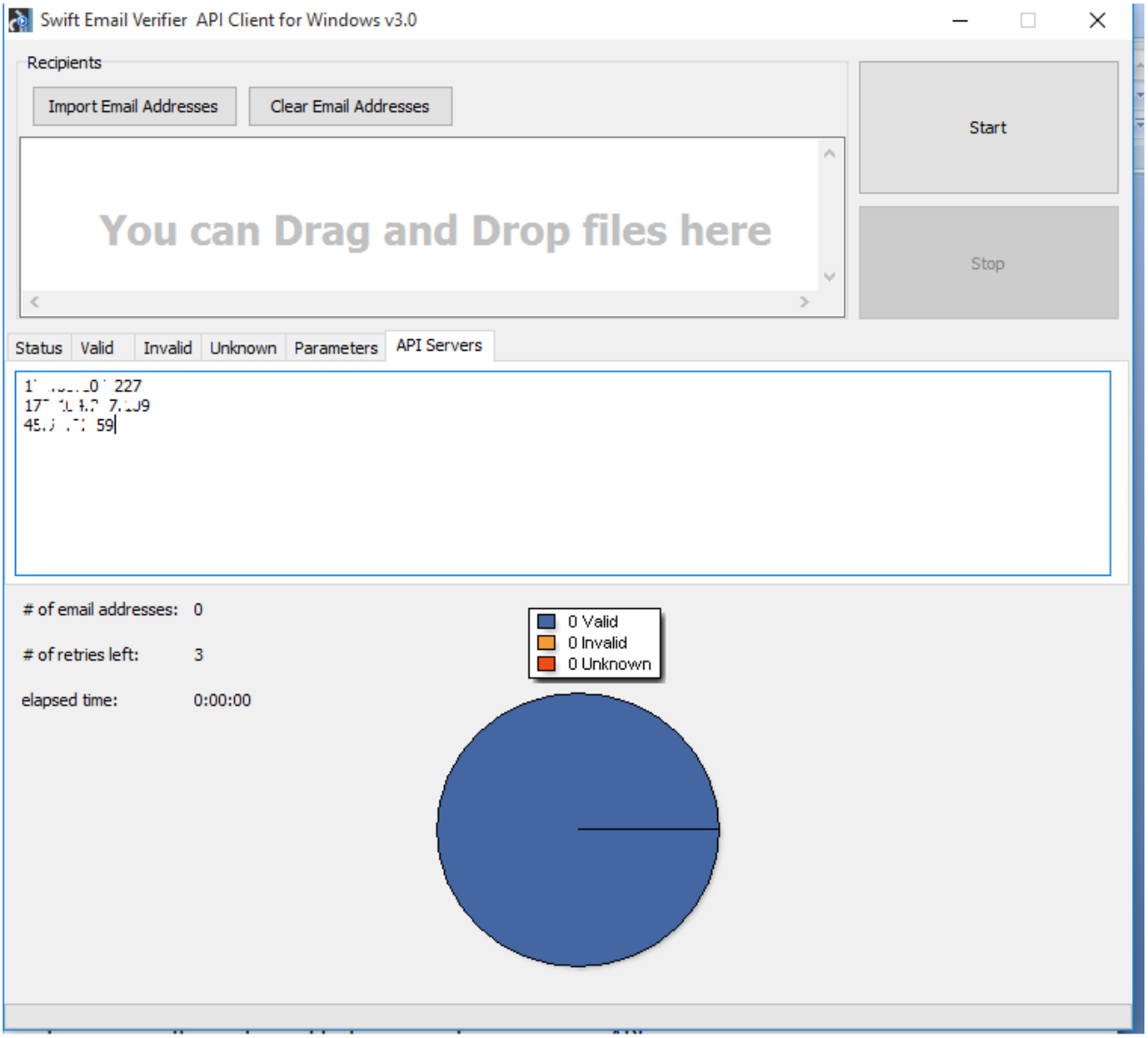
Note: Please make sure you click on the "Activate API Key" button when you run the program for the first time.



Proceed to set the following parameters:

- **API Key:** Please enter the API key you purchased. Then click on the “Store API Key” to save it
- **Activate API Key:** You must click this button to activate and save your API key when you run the program for the first time
- **Unknown addresses retries:** This parameter specifies how many times the unknown email addresses are retried
- **Max number of threads:** Please set this to 500 or more threads for maximum speed and throughput. If you have a very slow network, you may reduce this to 100. If you have a system with powerful hardware such as multiple cores/Multiple CPU, you can run more threads as desired to boost up the number of threads.
- **Read timeout for each thread(in seconds):** Please set this to 200 or more sec

Step 3: Click on the “API Servers” tab and enter the API servers IPs that you received when you placed the order. Make sure you enter the IPs one per line. A sample is shown below:

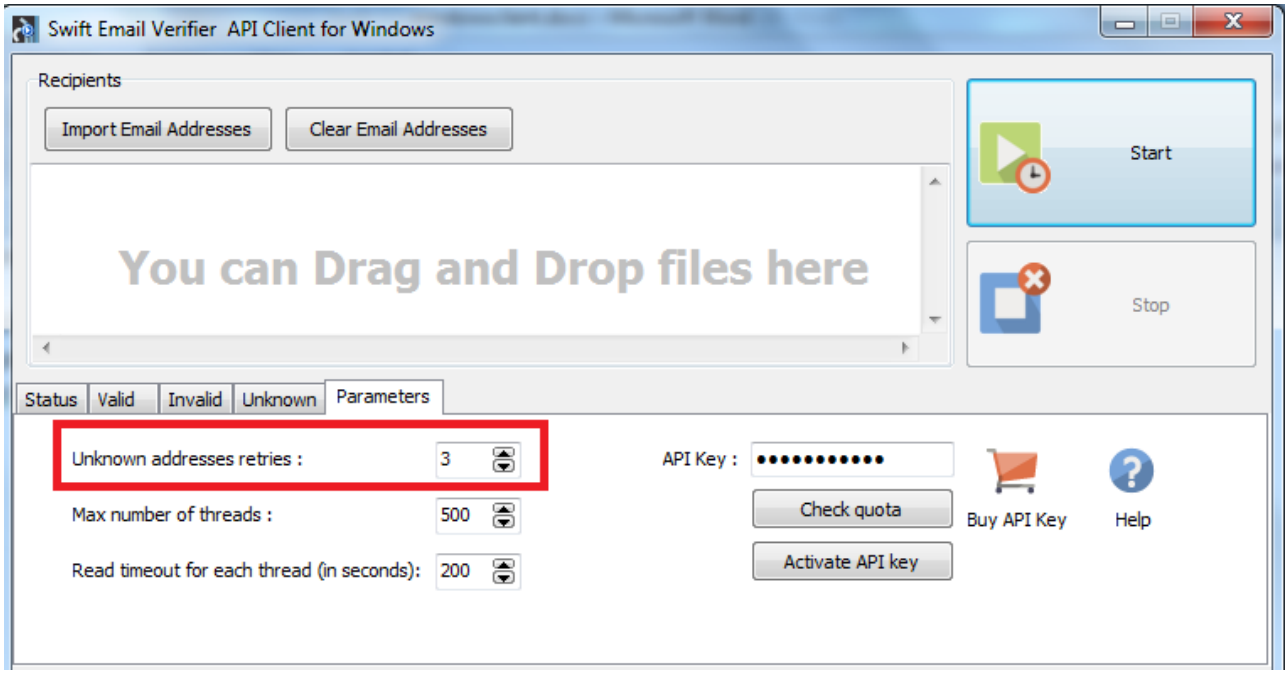


Configuring the number of Automatic Re-Check of Unknown

Due to multiple factors such as network issues, rare server outrage issues or inability to verify an email address where the ISP do not cooperate with the email validation method because it requires an actual message to be sent, unknown results are bound to happen when using our API.

However, since a majority of these network issues causing the unknown results are transient (temporary) it makes sense to retry the emails again. To this end , the program has a feature to automatically re-check or re-validate emails up to a specified number of times in order to improve the success of the validations and minimize unknowns as much as possible.

To configure the number of times you want the application to automatically re-check an email address which previously gave an unknown result, go to the “unknown addresses retries“ parameter and enter a number there. The default value which is 3 is quite OK for most network conditions.


Swift Email Verifier API Client for Windows
Recipients
Import Email Addresses
Clear Email Addresses
You can Drag and Drop files here
Start
Stop
Status
Valid
Invalid
Unknown
Parameters
Unknown addresses retries :
3
Max number of threads :
500
Read timeout for each thread (in seconds):
200
API Key :
Check quota
Activate API key
Buy API Key
Help

Obtaining Email Validation API Key

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.

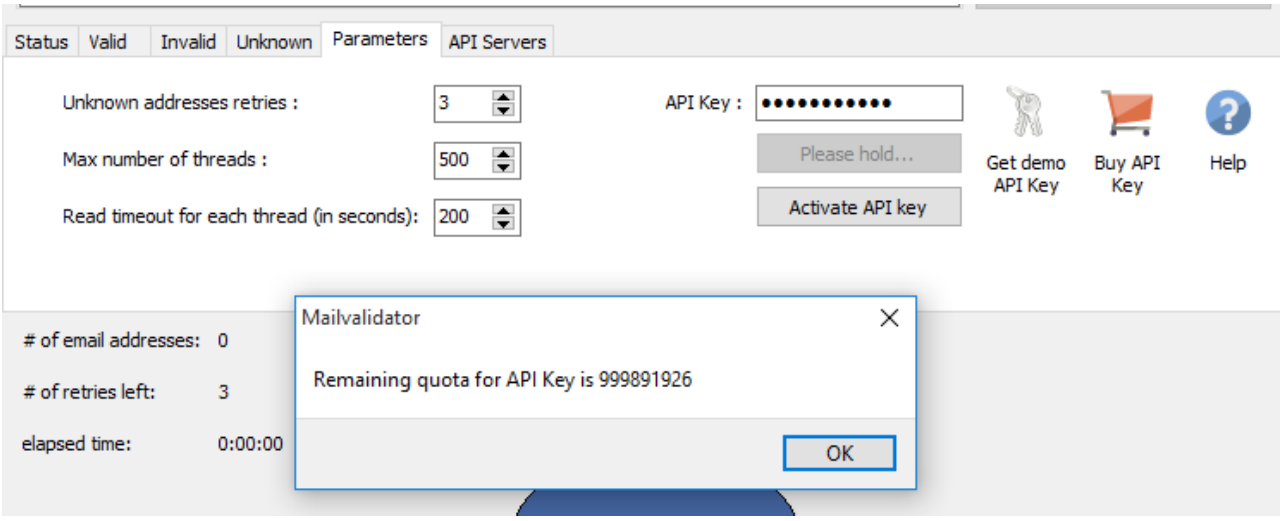
The following payment options are accepted:

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

Step 2: Checking the validity & Remaining Quota of the API Key

If you wish to check the validity of your API key and the remaining quota, simply click on the "Check Quota" button. You should get a popup like the one shown below:

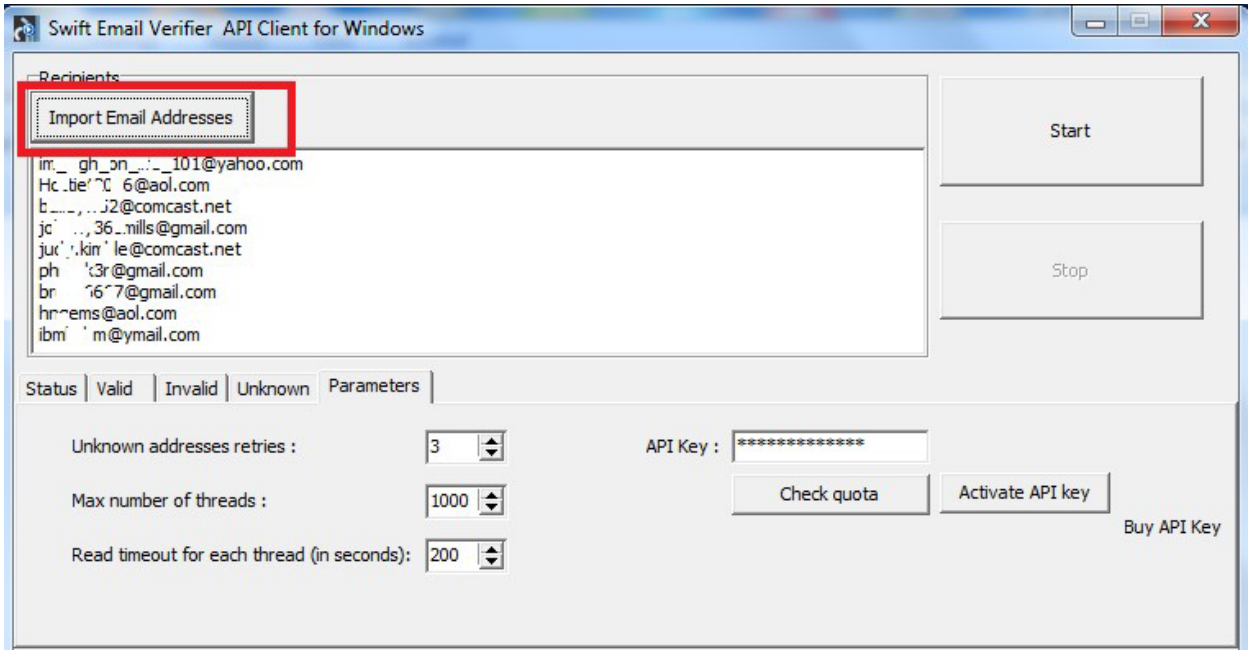
Please note that our API keys now allow you to validate up to 1 million emails per server that you order for per month.



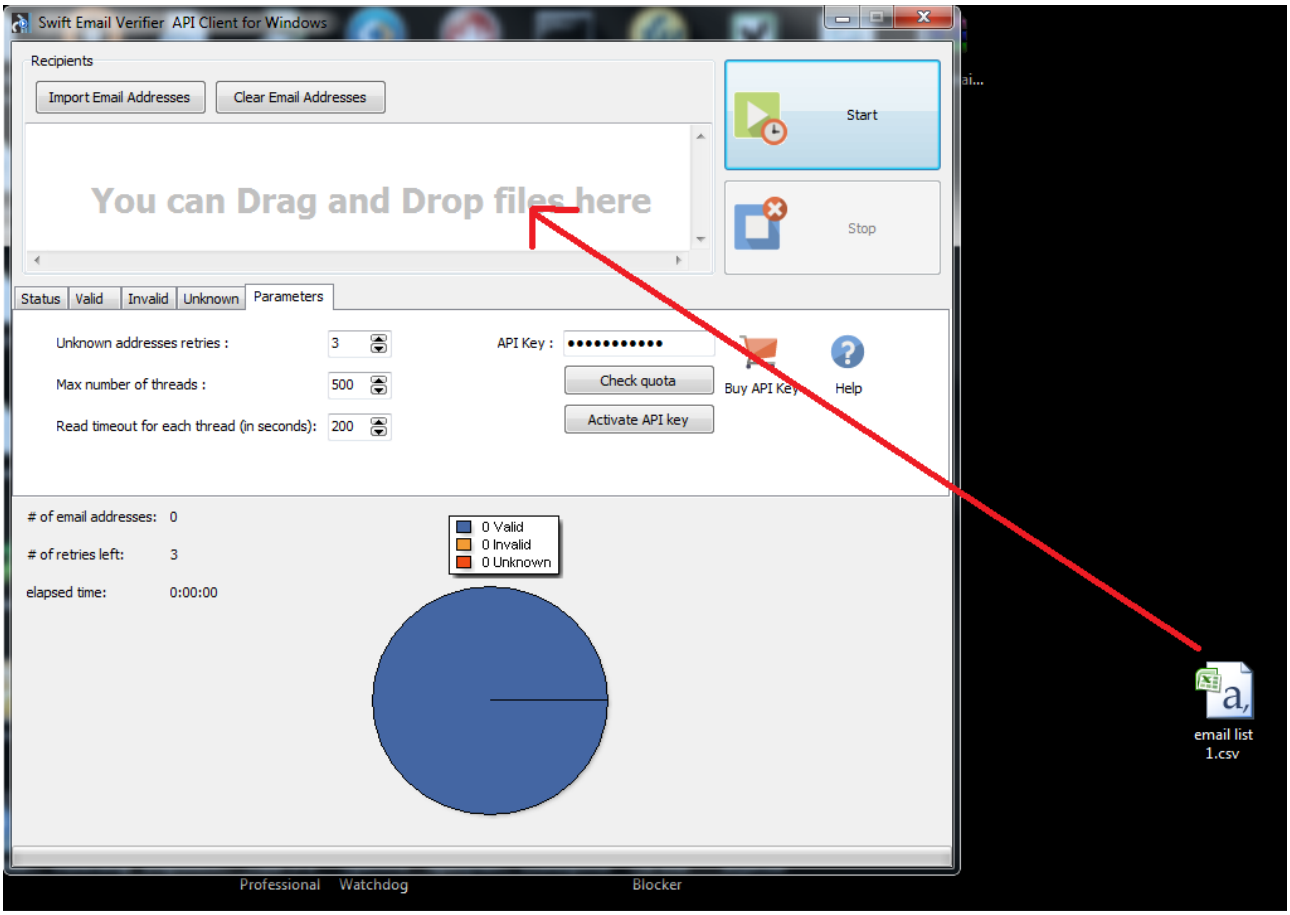
Step 3: Importing your Mailing List:

Once the parameters in the program has been setup, the next step is to import your mailing list. Mailing lists can be imported in plain text file or CSV formats. Mailing lists can also be dragged and dropped into the email address form.
Please note that only 1 single file can be imported or dragged and dropped at a time. If you have multiple mailing lists, you can merge them before importing it.

To import your list, simply click on the "Import" button and browse to the folder or path where your mailing list is located and import it.



To drag and drop your mailing list, simply drag and drop the list into the email address list form as shown below.



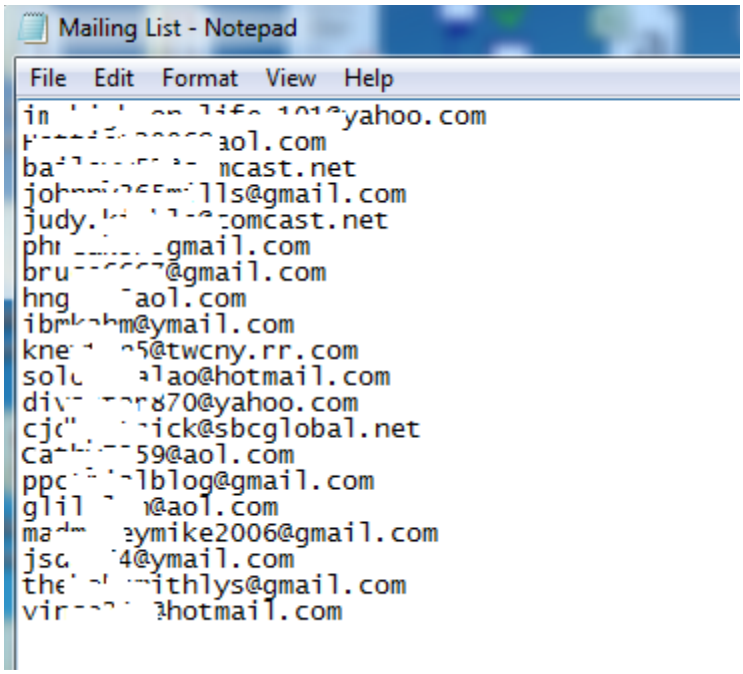
Supported Mailing List Formats:

You can upload csv or txt format files to add mailing list to the program. Swift Email Verifier API client only supports 2 types of mailing list file formats as follows:

- TEXT (.txt)
- CSV (.csv)

The mailing list can be uploaded in either .txt or .csv formats. Custom fields or information such as names, zip codes, addresses or phone numbers are supported and may be present in the mailing lists. If the mailing lists contain extra information, the validation results will also retain the extra information. Note that when you upload your mailing lists into the program, duplicates are automatically removed. This ensures that all email addresses imported into the program is unique.

Samples screenshots for the mailing lists in both TXT and CSV formats are shown below:



Mailing List in .txt format

	A	B
1	i [illegible]n_life_101@yahoo.com	
2	Ho[illegible]6@aol.com	
3	ba[illegible]@comcast.net	
4	joh[illegible]ills@gmail.com	
5	j[illegible]e@comcast.net	
6	p[illegible]3r@gmail.com	
7	b[illegible]7@gmail.com	
8	h[illegible]ns@aol.com	
9	ib[illegible]m@ymail.com	
10	kr[illegible]@twcny.rr.com	
11	sol[illegible]lao@hotmail.com	
12	div[illegible]0@yahoo.com	
13	cjdk[illegible]@sbcglobal.net	
14	Cath[illegible]@aol.com	
15	ppc[illegible]g@gmail.com	
16	gli[illegible]@aol.com	
17	ma[illegible]e2006@gmail.com	
18	js[illegible]1@ymail.com	
19	the[illegible]hlys@gmail.com	
20	vir[illegible]@hotmail.com	
21		

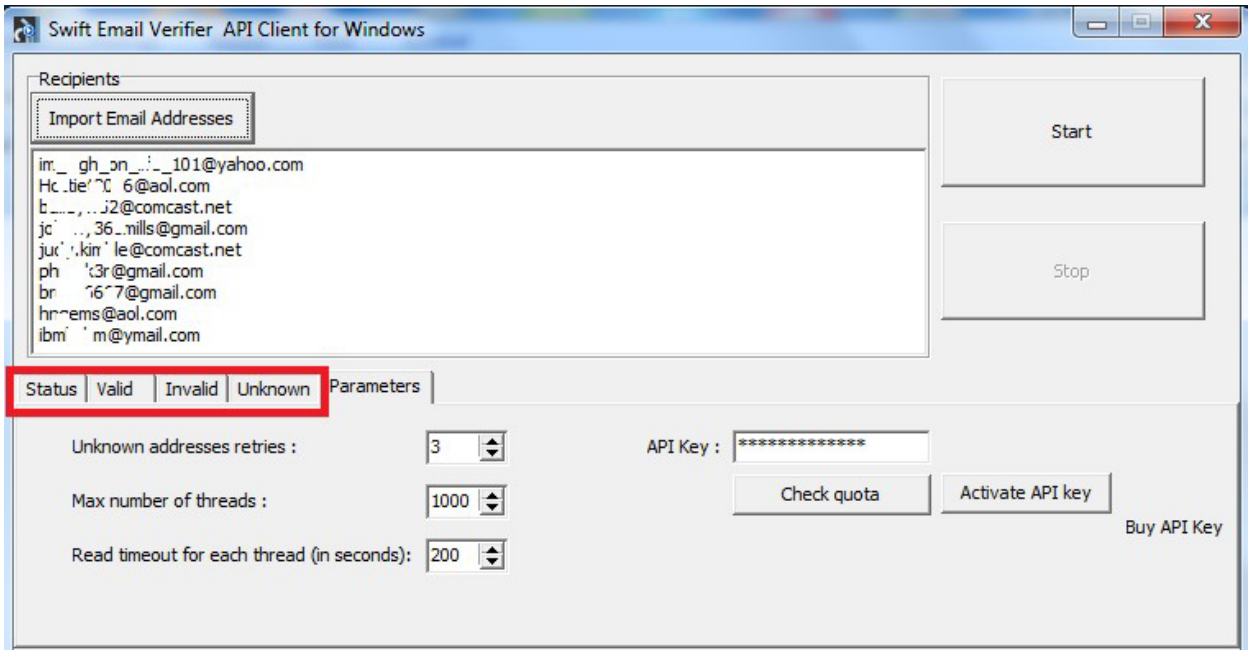
Mailing list in .csv format

Ta[illegible]nes	[illegible]@yahoo.com	2125 Gwene Ln	PORT ALSWORTH	AK	99653
Li[illegible]	[illegible]s@labor.state.ak	1111 W 8th St	Juneau	AK	99801-180
Ke[illegible]Dist	ll[illegible]k12.ak.us	148 N Binkley St	Soldotna	AK	99669-752
J[illegible]E	[illegible]@nycmail.com	12110 Business Blvd - Eagle	EAGLE RIVER	AK	99577
N[illegible]	[illegible]@graphics.com.com	2209AinakaheleSt.	ANCHORAGE	AK	99503
L[illegible]Div	[illegible]@state.ak.us	330 Willoughby Ave	Juneau	AK	99801-172
P[illegible]ons	[illegible]@audax.net	7645 King St # A	Anchorage	AK	99518-305
S[illegible]rmen	[illegible]@sadiecove.com	2001 Seward Hwy	Seward	AK	99664 000
[illegible]ub	[illegible]@hotmail.com	PO Box 101504	ANCHORAGE	AK	99509
U[illegible]ting	[illegible]@hughesair.com	PO Box 770437	EAGLE RIVER	AK	99577
I[illegible]	[illegible]@akrdc.org	null	ANCHORAGE	AK	99501
Is[illegible]s	[illegible]@Island-Services	PO Box 214	Unalaska	AK	99685-021
Y[illegible]or	[illegible]@ykhc.org	4700 Business Park Blvd # E	Anchorage	AK	99503-712
D[illegible]ior	@admin.state.ak.us	2301 Peger Rd	Fairbanks	AK	99709-539
N[illegible]	[illegible]@nnorthwind-inc.cc	235 E 8th Ave # 210	Anchorage	AK	99501-365
A[illegible]	[illegible]@alaskapacificbank.con	2094 Jordan Ave;	Juneau	AK	99801
L[illegible]	[illegible]@kidsarepeople.org	851 Westpoint Dr # 104	Wasilla	AK	99654-718
L[illegible]entary	[illegible]@northstar.k12.ak.u	601 F St	Fairbanks	AK	99701-380
V[illegible]	[illegible]@awt.alaska.net	401 East Northern Lights Bl	ANCHORAGE	AK	99503
[illegible]ra	[illegible]@lithia.com	4700 Gambell St	Anchorage	AK	99503-743
S[illegible]mer	[illegible]@ptialaska.net	2001 Seward Hwy	Seward	AK	99664 000
Matanuska Electric[illegible]nc	[illegible]@matanuska.com	163 E Industrial Way	Palmer	AK	99645-670
D[illegible]	[illegible]@gci.net	1310 W. 32nd Ave	ANCHORAGE	AK	99503

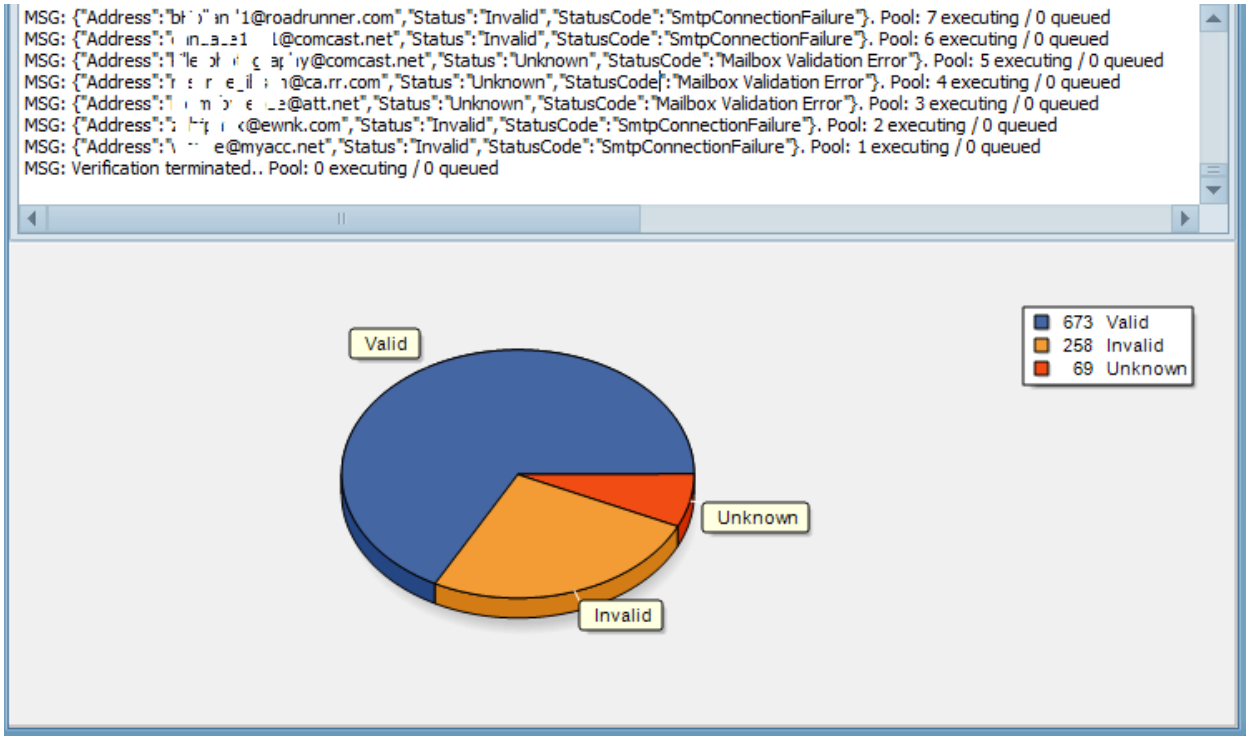
Mailing list in .csv format with extra information

Step 4: Start the verification

Once you have imported your list, you can then begin the verification by clicking on the “Start” button. Once the start button is clicked, the program starts validating the email addresses. You can see the active verifications on the “Status” tab. During the validation, the respective results groups (Valid, Invalid and Unknown) can be seen under the Valid, Invalid and Unknown tabs.



In addition, the real-time results will be displayed in a pie chart which updates in real time as shown below:



Step 5: Retrieve the results CSV files

Upon clicking the “Start” button, 4 CSV files will be generated automatically in the path or folder where the program was executed. The results of the validation will be written to these files. Once the verification completes, you should retrieve these files and review them.

Please note that if you run multiple instances of the application at the same time, all the results from all the instances will be written to the same CSV files.

Understanding 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.

We have compiled a list of all the current known issues which you may encounter while using our email validation system. You can download this document in the link below:

www.webemailverifier.com/issues.pdf

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.

However, please be aware that some emails which return unknown results could be valid. Examples of such emails which are determined unknown by our API and which may be valid are:

- Disposable Email Addresses from email address providers, like Mailinator, 10MinuteMail, GuerrillaMail,etc
- Catch-all email addresses
- Temporarily Unavailable emails (Graylisting) and soft bounces

In order to minimize the number of unknown emails results returned by the program, the JAVA verifier uses an intelligent automatic multiple re-validation of unknown emails up to the number of times specified until a possible valid or invalid result is obtained. By doing this, the number of unknowns is greatly minimized.

Recommended Practices for Dealing with Unknown Results

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

1. Set the "Unknown addresses retries" parameter value to 2 or 3.
2. 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.

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