DNS-O-Matic API - Documentation

DNS-O-Matic gives dynamic IP address users a simple way to distribute their IP changes to multiple services with a single update. The DNS-O-Matic API enables that service for client developers.

The API should be used by all client developers (software or hardware) who need to distribute IP address updates to dynamic DNS services.

- Version **0.9** (*When the API reaches version 1.0, all future changes will be backwards compatible.*)
- Questions or feedback? dnsomatic [at] opendns [dot] com [mailto:dnsomatic %20%5Bat%5D%20opendns%20%5Bdot%5D%20com]

Those familiar with the DynDNS DNS Update API [http://www.dyndns.com/developers/specs/] will find the DNS-O-Matic API similar.

Quick Overview

1. Client software initializes or detects a change in the client IP adddress.
2. Client software sends an update request to DNS-O-Matic.
3. DNS-O-Matic acknowledges update.
4. DNS-O-Matic propagates update across all user subscribed services.

Detecting Changes

A client must know its current public IP address and trigger updates when necessary. Clients can determine the current public IP via the operating system's network stack or via web detection, useful for private IPs (RFC 1918 space).

DNS-O-Matic operates a web service for detecting the user's public IP, available to clients that work with DNS-O-Matic. (TO BE LINKED)

An HTTP request to http://myip.dnsomatic.com/ [http://myip.dnsomatic.com/] will return the public IP of the client. Example:

```
HTTP/1.1 200 OK
Content-Type: text/plain
Server: DNS-O-Matic - MyIP0.3
Connection: close
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 105
1.2.3.4
```

For clients using OpenDNS, a DNS request for myip.opendns.com will always return the public IP of the client. Example: <cli> $dig myip.opendns.com +short 1.2.3.4 </cli>

Sending the update

When a change in IP address is found or a user alters any of their settings, the client should perform an update. All updates are sent using a well-formed HTTP request. DNS-O-Matic will pass back a return code for the client to parse. The API is a REST-based system.

HTTP Request

When sending an update to updates.dnsomatic.com be sure to always do a DNS query to resolve the IP for this host. Implementors MUST NOT hard code the IP for updates.dnsomatic.com as they may change from time to time.

Update requests may be sent using HTTPS (preferred) on port 443 or HTTP on port 80 to updates.dnsomatic.com.

```
Hostname:       updates.dnsomatic.com
HTTPS port:     443
HTTP port:      80
```

All clients must send a well-formed user-agent including company name, model number, and software build revision. An example would be:

```
SoftwareDev - Fast Update Client - 2.0
```

Failure to use a well-formed and consistent user-agent string MAY result in failed update requests.

Sample updates

URL Authentication: For web browsers or utilities (fetch, curl, lwp-request) which parse authentification section in URL.

https://username:password@updates.dnsomatic.com
/nic/update?hostname=yourhostname&myip=ipaddress&wildcard=NOCHG&mx=NOCHG&
backmx=NOCHG   [https://username:password@updates.dnsomatic.com
/nic/update?hostname=yourhostname&myip=ipaddress&wildcard=NOCHG&mx=NOCHG&
backmx=NOCHG]

Users need to enter a DNS-O-Matic username and password. DNS-O-Matic usernames are 3-25 characters. DNS-O-Matic passwords are 6-20 characters. All ASCII letters and numbers accepted. Dots, dashes, and underscores allowed, but not at the beginning or end of the string.

Users will also enter a list of hostnames (FQDNs) to be updated.

Note on service passwords: Many dynamic DNS services have an update password, separate from the account password. When a user sets up a service to be updated by

DNS-O-Matic, they will be asked to provide their update password (if available), and encouraged strongly not to provide their service password unless no other alternative exists.

Regardless, all DNS-O-Matic registration and configuration happens under SSL, and the service information provided will be encrypted with their DNS-O-Matic password.

HTTP Request: Sample request only. Follow your request by sending empty line.

Base64-encoded authorization should be represented by Base 64 encoded username:password string.

We recommend using the GET HTTP method, however either GET or POST may be used.

```
GET /nic/update?hostname=yourhostname&myip=ipaddress&wildcard=NOCHG&mx=NOCHG&backmx=NOCHG HTTP/1.0
Host: updates.dnsomatic.com
Authorization: Basic base-64-authorization
User-Agent: Company - Device - Version Number
```

Update Parameters

This copy is subject to minor change based on feedback!

hostname

Hostname you wish to update. To update **all** services registered with DNS-O-Matic to the new IP address, hostname may be omitted or set to all.dnsomatic.com (useful if required by client). This field is also used for services that use different names for the unique identifier of the target being updated (ex. freedns.afraid.org, TZO). DNS-O-Matic will format the update string appropriately for each supported service at distribution.

myip

IP address to set for the update. If not specified, the best IP address the server can determine will be used (some proxy configurations pass the IP in a header, and that is detected by the server).

wildcard

Parameter enables or disables wildcards for this host. ON enables wildcard. NOCHG value will keep current wildcard settings. Any other value will disable wildcard for hosts in update. *What does wildcard do & mean in this context?*

mx

Specifies a Mail eXchanger for use with the hostname being modified. The specified MX must resolve to an IP address, or it will be ignored. Specifying an MX of NOCHG will cause the existing MX setting to be preserved in whatever state it was previously updated.

backmx

Requests the MX in the previous parameter to be set up as a backup MX by listing the host itself as an MX with a lower preference value. YES activates preferred MX record pointed to hostname itself, NOCHG keeps the previous value, any other value is considered as NO and deactivates the corresponding DNS record.

Other Parameters

DNS-O-Matic will accept and distribute these parameters for compatibility with services which support the DynDNS Update API. However, DNS-O-Matic does not use/need them.

offline Sets the hostname to offline mode. YES activates feature and turns on offline redirect for hostname (if set). NOCHG could be used to keep current state.

system previously used to identify update type

url reserved for future use

Unknown parameters may be ignored or may lead to a return code of abuse. *We have not yet determined if they will be distributed to other services.*

Return Codes

The DNS-O-Matic response does not necessarily reflect the service's response, just the DNS-O-Matic response. DNS-O-Matic distributes the update to the selected services in a separate process.

All responses from the services are logged to the user's account. If the service response is an error which cannot be addressed by DNS-O-Matic, then the user will be notified via email and on the DNS-O-Matic website of the error, with suggestions about how to resolve the error.

DNS-O-Matic returns one error code per line for each service updated, in this form

SUCCESS

```
"good <ip> <hostname> <service>"
```

ERROR

```
"‹code› <ip> <hostname> [<service>]"
```

Success

good means the update was scheduled successfully.

No Change

nochg indicates success, with no change. DNS-O-Matic will not re-distribute successive nochg updates. This is to avoid abuse as well as save bandwidth and server infrastructure for both DNS-O-Matic and the supported services.

Errors

badauth The DNS-O-Matic username or password specified are incorrect. No updates will be distributed to services until this is resolved.

notfqdn The hostname specified is not a fully-qualified domain name. If no hostnames included, notfqdn will be returned once.

nohost The hostname passed could not be matched to any services configured. The service field will be blank in the return code.

numhost You may update up to 20 hosts. numhost is returned if you try to update more than 20 or update a round-robin.

abuse The hostname is blocked for update abuse.

badagent The user-agent is blocked.

good 127.0.0.1 This answer indicates good update only when 127.0.0.1 address is requested by update. In all other cases it warns user that request was ignored because of agent that does not follow specifications.

dnserr DNS error encountered. Stop updating for 30 minutes, and optionally ask the user to contact DNS-O-Matic.

911 There is a problem or scheduled maintenance on DNS-O-Matic. Stop updating for 30 minutes, and optionally ask the user to contact DNS-O-Matic.

api.txt · Last modified: 2007/11/27 03:15 (external edit)

DNS-O-Matic is a free service from OpenDNS | Contact Us