

Simple DNS Plus

Version 5.2

Copyright © 1999-2011 JH Software ApS

Table of Contents

Part I Welcome	1
Part II How to...	1
1 Get started	1
2 Host a domain name	2
3 Setup primary / secondary	3
4 Secure your server	4
5 Read the log	9
6 Integrate with other applications	11
7 Use the HTTP API	12
8 Use command line options	15
Part III User Interface	15
1 Main window	16
Views	18
Options dialog	19
General	20
DNS	20
Inbound Requests	20
Outbound Requests.....	20
Resolver	21
Recursion	21
IP Filtering	21
Caching	21
Local Zones	22
Data Files	22
Zone Transfers.....	22
Super Master/Slave.....	23
Secondary Zones.....	24
Suspended Zones.....	25
Automatic SPF.....	25
TSIG Updates	26
Forwarding	27
DNS Forwarding dialog.....	27
Lame Requests.....	27
Non-existing Domains.....	28
NAT IP Alias	29
Miscellaneous	30
HTTP API.....	31
Plug-Ins	32
Plug-In Instance.....	32
Logging	33
Log Details	33
Log Files	34

Syslog Server	34
Active Log View.....	35
Windows Event Log.....	35
Remote Management.....	35
IP Address Blocking dialog	36
2 DNS Records window	37
New Zone Wizard	40
Import Wizard	41
Export Wizard	42
Record Properties	42
Zone Properties	43
Quick Zone Wizard	44
Check Internet Delegations	44
Bulk Update Wizard	45
Default Zone Values	46
IP-to-Name Mappings	46
DNSSEC Sign Zone	47
DNSSEC Key File	47
DNSSEC Key Set	48
3 DNS Look Up window	48
Look Up Types	51
4 DNS Cache Snapshot window	52
Part IV Plug-Ins	53
Part V Definitions	55
1 Authoritative	55
2 Caching	55
3 DNSSEC	55
4 Domains vs. Zones	57
5 Dynamic DNS update	58
6 Forwarding	58
7 Hosts file	60
8 Internationalized domain names (IDNs)	60
9 Recursion	61
10 Reverse DNS	62
11 Root DNS records	64
12 Round Robin	64
13 Suspended Zone	65
14 TSIG	65
15 TTL (Time To Live)	66
16 Zone Transfer	67
Part VI DNS Record types	68
1 A	68

2	A6	69
3	AAAA	69
4	AFSDB	70
5	ATMA	70
6	CNAME	70
7	DHCID	71
8	DNAME	71
9	DNSKEY	71
10	DS	71
11	HINFO	72
12	ISDN	72
13	LOC	72
14	MB, MG, MINFO, MR	73
15	MX	73
16	NAPTR	74
17	NS	74
18	NSAP	75
19	NSEC	75
20	NSEC3	76
21	NSEC3PARAM	76
22	PTR	76
23	RP	77
24	RRSIG	77
25	RT	77
26	SOA	78
27	SPF	79
28	SRV	79
29	TXT	79
30	X25	80
Part VII Event IDs / Error Messages		80
Part VIII Raw log file format		83
Part IX Tools Directory		83
Index		85

1 Welcome

Thanks to the DNS system, we surf the Internet using names, such as www.simplifiedns.com instead of impossible to remember IP addresses.

DNS servers translate these domain names into machine readable IP-addresses needed to locate the requested server (web, mail, FTP, etc.) on the Internet.

With Simple DNS Plus you can host your own domain names, or simply speed up Internet access with local DNS resolving and caching^[55].

Simple DNS Plus also includes a DHCP Server plug-in^[53], a DNS Look Up tool^[48], and many other useful features.

Additional information and support options are available on-line at <http://www.simplifiedns.com/support.aspx>

Select a topic on the left to get started.

2 How to...

2.1 Get started

A "DNS Server" has two core functions "DNS Resolver/Cache" and "Authoritative DNS Server". Simple DNS Plus can be configured to do either one of these functions - or both.

DNS Resolver/Cache

When a DNS server is configured as a DNS Resolver, it provides recursive^[61] domain name resolution to other computers.

This means that it is able to translate Internet domain names into IP addresses and the reverse^[62] (as well as providing other types of data) by sending queries to a number of different DNS servers on the Internet.

Simple DNS Plus caches^[55] the information it learns along the way so that subsequent requests for the same information can be answered more quickly.

With the default Simple DNS Plus configuration, it is ready to work as a DNS resolver/cache.

To take advantage of this, you must configure the computers on the local network (including the one running Simple DNS Plus) to use the now local DNS server instead of DNS servers provided by your ISP.

This is done under the computer's Network TCP/IP properties by assigning the IP address of the computer running Simple DNS Plus as the DNS server.

The exact setup is slightly different for each version of Windows - illustrations are provided at <http://www.simplifiedns.com/kb.aspx?kbid=1128>

Alternatively, local computers (except the one running Simple DNS Plus) can be configured to get this configuration automatically using the DHCP Server plug-in^[53].

Next make sure Simple DNS Plus is running. Then test the configuration by opening a web-page such as www.simplifiedns.com.

To ensure that you are not getting a copy cached by the browser, first empty out the browser cache (delete "Temporary Internet Files") and close all instances of the browser.

And if you are using Windows 2000 or later and have the "DNS Client" service running (the default), type "IPCONFIG /flushdns" at a command prompt to ensure that no DNS data is cached by this

service.

If the expected web-site loads into your browser, everything is now working correctly. You should also be seeing some activity in Simple DNS Plus (Performance Graph^[18], the Active Log^[18], and/or the request counter on the status bar^[18]).

If you are new to DNS it might be helpful to examine the log files^[9] to get an idea how DNS requests are processed.

If you run Simple DNS Plus for a while, you should begin to notice an improvement in the time it takes to access web-pages - especially when you return to one you have visited previously. This is caching^[55] - your computers no longer must access an external DNS server every time you reopen a web-page.

Authoritative DNS Server

The other core function of a DNS server is hosting domain names - a.k.a. authoritative^[55] DNS server.

For more on this see How to host a domain name^[2].

2.2 Host a domain name

With Simple DNS Plus you can host DNS for your own domain names (and/or for others).

NOTE: This requires that you have a static Internet IP address. You cannot reliably host DNS on a dynamic IP address (such as a dialup connection).

First a domain name must be registered on the Internet.

You can use the "WHOIS" look up^[48] function in Simple DNS Plus to determine if a domain name is available.

There is an ever growing number of companies (registrars) and resellers offering domain name registration for ".com", ".net", and ".org" domain names.

For a list of registrars providing generic domain names (".com", ".net", ".org", etc.) see <http://www.icann.org/en/registrars/accredited-list.html>

For information on registering country specific names (such as ".uk") see <http://www.iana.org/domains/root/db/index.html>

When registering a domain name (or modifying a registration), you have to specify which DNS servers will be responsible for the domain name (also referred to as "host records" - or NS-records^[74]).

Here you need to specify your own DNS server(s) by name - such as "ns1.example.com".

If you are already hosting other domain names you can use the existing "ns..." name for your server(s). Otherwise you may have to first create these "host records" ("ns1.example.com" = IP address).

With some registrars you can do this as part of the domain name registration, others have a separate process for this.

When in doubt, contact your registrar for details.

NOTE: The registrar may do a DNS lookup to see if you have the DNS server name listed correctly on your DNS server. So before you use a new DNS servers name ("ns#.example.com") for the first time in a domain name registration, make sure to first setup an NS-record^[74] and associated A-record^[68] for this in Simple DNS Plus.

It may take several days for a new domain name and changes to become fully active on the Internet (most are typically active within a few hours).

This delay is caused by the process of updating the top level DNS servers (the Internet DNS servers responsible for ".com" and other top level domains) with the new information for your domain name.

You can configure your domain name in Simple DNS Plus even before you have registered it and use it yourself, but other people on the Internet won't be able to access it before it is registered and active.

Next you need to configure the domain in Simple DNS Plus.

From the main window^[16], click the "Records" button.

You should now be in the DNS Records window^[37]. This is where you work with your domain names and records.

The easiest way to configure a new domain name is through the Quick Zone Wizard^[44] which is activated with the "Quick" button.

Simply enter the domain name, and the IP addresses of your web, mail, and FTP servers (all optional) and click the OK button.

Now your domain name is ready to go!

NOTE: A "zone" basically represents a domain name and any sub-names under it - see zone definition^[57] for details.

Depending on your own requirements and the requirements of your registrar, you may also need to setup a secondary DNS server^[3].

2.3 Setup primary / secondary

You have probably come across the terms "primary DNS server" and "secondary DNS server".

Actually a DNS server (the computer/software) is not specifically "primary" or "secondary".

A DNS server can be primary for one zone^[57] (domain) and secondary for another.

The DNS specifications (RFCs) require that each domain name is served by at least 2 DNS servers for redundancy.

This may seem a little silly - especially if you run your DNS, web, and mail servers all on the same machine - if this machine goes down, it doesn't really matter that the backup DNS server still works.

But many registrars (companies that register domain names) still require at least 2 DNS servers.

This requirement has been somewhat relaxed lately, and depending which registrar you use, you may only need to specify one DNS server.

NOTE: If your registrar lets you use only one DNS server, some DNS testing tools may still flag this as an error.

NOTE: Registrars requiring 2 DNS servers sometimes refer to these as "primary" and "secondary".

This has absolutely nothing to do with the actual primary/secondary functionality, and it doesn't matter in which order you enter your DNS servers for the domain name. This is just a list of servers, and there could be 1, 2, or any number of DNS servers listed for a domain name.

By definition, a primary DNS server holds the "master copy" of the data for a zone^[57], and secondary servers have copies of this data which they synchronize from the primary through zone transfers^[67] at intervals or when prompted by the primary.

Only one DNS server should be configured as primary for a zone^[57], but you can have any number of secondary servers for redundancy.

Both primary and secondary servers for a zone^[57] serve exactly the same data to clients.

Because of this you could easily "simulate" a secondary server on a single computer with 2 IP addresses.

Simply configure the zone^[57] (as primary), and the server will function as both the primary (on one IP address) and secondary (on the other IP address).

The recommended practice is to configure the primary and secondary DNS servers on separate

machines, on separate Internet connections, and in separate geographic locations (for the purpose of redundancy).

Many do this by making a "swap" deal with someone else: "be secondary for me, and I'll be secondary for you" (check out www.ns2exchange.com).

Or you can use a secondary DNS service such as www.ns2service.net - you will still have full control over your domains as you run the primary DNS server.

Many new "broadband" Internet connections (such as cable modems and DSL) only come with one IP address, so this setup is often used not so much because of redundancy, but because the registrar requires two DNS servers (with separate IP addresses).

When using separated primary and secondary DNS servers, zone transfers^[67] are used to synchronize the zone data from the primary DNS server to the secondary server(s).

With other DNS server software, a zone must initially be created on both the primary and secondary servers (creating individual DNS records and any subsequent changes to a zone need only be done on the primary server).

However, Simple DNS Plus has a unique option to automatically create and remove zones on secondary servers whenever you do this on the primary.

We call this a "Super Master/Slave" pair and is configured through the Options dialog / DNS / Local Zones / Super Master/Slave section^[23].

Both servers must be running Simple DNS Plus (no other DNS servers we know of currently support this).

The secondary server must be listed as a "slave" on the primary server, and the primary server must be listed as a "master" on the secondary.

One Simple DNS Plus server can be master and/or slave for any number of other Simple DNS Plus servers.

To create the zone^[57] on the primary server, you can use the Quick Zone Wizard^[44].

If you are not using the Super Master/Slave setup, or if either of your DNS servers are not Simple DNS Plus, you will also need to create the zone^[57] on the secondary server.

Use the New Zone^[40] function, select the "Secondary Zone" option, and specify the zone name and the IP address of the primary DNS server.

Once a zone is configured on both primary and secondary servers, zone transfers^[67] should automatically occur when needed.

To verify, use the Look Up^[48] function against the secondary server, or check the records on the secondary server through the DNS Records window^[37] on that server.

You can later change the primary/secondary status using the Zone Properties dialog^[43].

The Zone Properties dialog^[43] "zone transfers" tab can be used to secure^[4] the zone, so only authorized secondary servers are allowed to request zone transfer^[67].

2.4 Secure your server

As with all types of Internet servers, DNS servers are also targeted by hackers.

The implications can be quite serious, but the good news is that you can protect yourself better by running Simple DNS Plus compared to trusting your ISP's DNS servers.

There are several security issues with DNS, but Simple DNS Plus addresses them all:

DNS spoofing (a.k.a. "cache poisoning")

DNS spoofing is the act of injecting false data into the cache^[55] of a DNS server causing it to serve this false data to its clients.

This is done by tricking a DNS server into accepting a false DNS response and caching the false DNS

records in this.

Hackers may try to do this simply to prevent someone from accessing the Internet (making a DNS server appear to malfunction), but intentions can be more malicious and the effects more serious. For example, by injecting false MX-records^[73], a hacker could re-route e-mails intended for a company's client or vendor to himself. If the hacker also forwards the e-mails to the correct destination, this might go undetected for as long as the hacker cares. Or with an injected A-record^[68] (for example, www.bank.com = IP 1.2.3.4) and a cloned web-site for www.bank.com, a hacker could get your pin code, password, credit card number etc. (a good reason to check that such web-sites use a valid SSL certificate).

Simple DNS Plus has several automatic features to prevent DNS spoofing:

1) It only caches DNS responses matching DNS requests that it itself sent (same request ID, query name, and query type) and which it has not yet received a response to.

2) It automatically filters out any DNS records in received DNS responses for which the sending DNS server is not authoritative^[55].
This protects against simple DNS spoofing where the false DNS records are included in otherwise normal DNS responses.

3) It uses random request IDs.
This makes it hard to guess the next request ID and use that for impersonating other DNS servers.

4) It queues duplicate requests (same query name and query type) so that each request is not processed before the previous request has been fully resolved.
Besides from making the software more efficient, this also prevents so-called birthday attacks. In such an attack, the hacker tries to guess an outbound request ID (for impersonating another DNS server) by sending many identical recursive requests very quickly. However with Simple DNS Plus, that strategy won't improve the hackers chances (increase the risk), because when the second and following requests are de-queued and processed, these will be served from the cache and won't cause any outbound requests to resolve.

Additionally we recommend that you:

1) Use random port numbers for outbound requests (enabled by default). See Options dialog / DNS / Outbound Requests^[20] section.
This makes it harder for hackers to impersonate other DNS servers because they need to correctly guess from which port a request (sent to somewhere else) came from. This is also essential to protect against Dan Kaminsky's DNS bug.

2) Limit DNS recursion to your own IP range(s). See Options dialog / DNS / Resolver / Recursion^[21] section.
This makes it much harder for anyone on the outside to provoke Simple DNS Plus into doing a recursive DNS lookup at a predictable time (the first step in DNS spoofing).

3) Enable "To protect against cache poisoning (spoofing), only accept responses from other DNS servers which - Come from the IP address that the corresponding request was sent to" in the Options dialog / DNS / Resolver / Recursion^[21] section (enabled by default).
This makes it much harder for hackers to impersonate another DNS servers because they also need to spoof that server's IP address.

4) Enable "To protect against cache poisoning (spoofing), only accept responses from other DNS servers which - Echo the request's question section" in the Options dialog / DNS / Resolver / Recursion^[21] section (enabled by default).
This prevents a variant of the so-called birthday attack where the hacker sends queries for different sub-names and responds without the question section in order to increase his chances.

DNS bounce / amplification attacks

When you send a DNS request to a DNS server, the server will generally send back a response to the IP address that the request network packet appears to come from. So by forging (*) the sender IP address (IP spoofing) of a DNS request, a hacker can make a DNS server send a response packet to a third party (the victim).

The victim will see the sender IP address as that of the intermediary DNS server, while the hacker remains hidden and very difficult to trace.

This is called a bounce attack.

If the DNS request is constructed in a way that results in a larger response packet (as compared to the request packet), this is called an amplification attack (the hacker achieved a bigger "payload" than if he had sent the packet directly to the victim).

Doing this at a fast rate through many different DNS servers targeting the same IP address, the hacker might overload the victim's DNS server and/or Internet connection (a DDoS attack).

Typically the hacker will send requests either for the DNS root, for some domain name that DNS servers are likely to have cached (such as google.com), or simply for random domain names. In other words "lame requests".

So to avoid becoming a participant in such attacks, we recommend configuring Simple DNS Plus to either refuse (default setting) or not respond to lame requests. See Options / DNS / Lame Requests section.

The "Do not respond" option is obviously more efficient against this attack, but may also make it harder to troubleshoot other issues in general (why is the DNS server not responding...).

With the "Refuse" option, it will still send a response but it won't be amplified (response not larger than request) making your server much less interesting as an intermediary for this attack.

If you notice an ongoing attack of this type with a specific domain name / record type, you can also block it using the Ignore DNS Request plug-in,

An attack of this type was rampant in early 2009, where the hacker would send DNS requests to thousands of DNS servers, asking them for NS-records for the DNS root. Many DNS servers would send large responses with a list of all the Internet root servers, flooding the victim.

To deal with this specific attack, we added the "Ignore all DNS requests for <root> (no response, no logging)" option - see Options / DNS / Miscellaneous section.

(*) Forging the sender IP address of a network packet (IP spoofing) is only possible from Internet connections that are not properly protected by the ISP. ISPs should block all outgoing traffic not originating from their own IP address ranges. Most major ISPs do this, but unfortunately not all.

DNS cache snooping

DNS cache snooping is when someone queries a DNS server in order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby deduce if the DNS server's owner (or its users) have recently visited a specific site.

This may reveal information about the DNS server's owner, such as what vendor, bank, service provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period.

This method could even be used to gather statistical information - for example at what time does the DNS server's owner typically access his net bank etc. The cached DNS record's remaining TTL value can provide very accurate data for this.

To prevent DNS cache snooping in Simple DNS Plus, simply restrict recursion (see above) to your own IP addresses.

Only IP addresses allowed recursion will get responses with data from the cache.

DNS rebinding attacks

This type of attack is not directed at DNS servers directly but rather at web-browsers and other client software.

Simple DNS Plus can however provide a very effective defence against this.

A web-browser will generally allow any script, Java object, Flash object, etc. to communicate over HTTP / TCP with the server that served the current web-page for as long as that web-page is open in the browser. This is controlled by the host name specified in the web-page URL.

A DNS rebinding attack is done by having the DNS record for the host name time out very quickly (low TTL and other tricks) and then serve a new IP address for the host name in response to the next DNS request ("rebinding").

The new IP address would be the private/local IP address of an intranet server or device at your location. Now with a bit of scripting, the attacker can in effect use your browser as a gateway to your entire intranet - completely bypassing your firewall.

The same type of attack may also be possible with other Internet applications that rely on host names for security.

Browser companies are taking steps to prevent this in new browser versions, but it is much more efficient and secure to stop this type of attack at the DNS level by filtering out any private/local IP addresses in DNS responses from outside DNS servers.

This is configured in the Simple DNS Plus Options dialog / DNS / Resolver / IP Filtering [\[21\]](#) section.

DNS recursion / Open DNS server

Internet users (other than your own users) may try to take advantage of your DNS server.

For example, if someone feels that their ISP's DNS server is too slow - they might just use another one - like your's.

This actually happens more frequently than most people would think.

Many ISPs and companies "offer" this service free of charge without even realizing it. This of course consumes additional bandwidth and CPU cycles.

If you do not host any domain names, you could prevent this simply by blocking incoming DNS requests on your firewall, or configure Simple DNS Plus to only listen for DNS requests on a private IP address. See Options dialog / DNS / Inbound Requests [\[20\]](#) section.

However, if you are hosting one or more domain names (primary or secondary), you must allow other DNS servers access to your DNS servers.

The difference between Internet users and other DNS servers is recursion [\[61\]](#).

Client applications (users) need the DNS server to perform recursion (fully resolve domain names into IP addresses), whereas other DNS servers perform the recursion themselves.

By specifying only the IP addresses of your own users in the Options dialog / DNS / Resolver / Recursion [\[21\]](#) section, you can effectively block outside users, and at the same time allow other DNS servers to requests data for domain names that your are hosting.

If you are not restricting recursion, then you are running an "Open DNS Server" (not a good thing). Restricting recursion also make your server less vulnerable to DNS spoofing - see above.

DNS port scanning

A hacker may use a utility program to search for potential DNS server targets. This software sends dummy DNS requests to a range of IP addresses simply to register which IP addresses return a response. Any IP address that responds will then be probed further for possible vulnerabilities.

Simple DNS Plus has a special "stealth DNS" option which makes it invisible to such scanners, by not responding to a DNS request unless it is for data in local zones or originates from an IP address that is offered recursion.

See Options dialog / DNS / Lame Requests [\[27\]](#) section.

Zone transfers

Zone transfers [\[67\]](#) are intended for use by secondary DNS servers to synchronize with their primary server.

But you can also request a zone transfer [\[67\]](#) using a number of different tools (including the Look Up [\[48\]](#) function in Simple DNS Plus), which will list all the records contained in a zone [\[57\]](#).

This is great for troubleshooting, but you may not want to expose all the data in your zones [\[57\]](#) to strangers.

Hackers could use this to find out what other servers you are running - and with this information launch other types of attacks.

Zone transfers [\[67\]](#) also require considerably more bandwidth and CPU cycles compared to regular DNS requests.

You can specify which TSIG keys [\[65\]](#) and/or IP addresses are allowed to request zone transfers [\[67\]](#) for each zone [\[57\]](#) in the Zone Properties dialog [\[43\]](#) under the "Zone Transfers" tab, and in the Options dialog / DNS / Local Zones Zone transfers [\[22\]](#) section.

Denial of service (DoS)

This is a very simple (yet effective) type of attack - typically done via "drone computers" / "bot networks".

By sending your server(s) an extreme amount of requests which basically use up all your bandwidth and/or processing power, a hacker can effectively prevent valid users and customers from accessing your services.

Simple DNS Plus has an IP Address Blocking [\[36\]](#) function, which can automatically detect such attacks (specifically directed against the DNS server), and ignore subsequent traffic from the hacker's IP address.

The traffic will still use some of your bandwidth, but Simple DNS Plus won't send replies (which would increase the problem) and won't use up the processing power of the machine it is running on.

Another variant of "DoS" is establishing a lot of TCP connections using up all the resources of the target system.

Simple DNS Plus has an option to limit the maximum number of simultaneous inbound TCP connections (Options dialog / DNS / Inbound Requests [\[20\]](#) section).

The hacker will still be able to use up all these TCP connections and prevent anyone else from making TCP connections to Simple DNS Plus, but at least he won't exhaust system resources and crash Simple DNS Plus and other programs.

DoS attacks are difficult to prevent completely, but if the hacker doesn't succeed in bringing down your systems, he will probably move on to another victim.

BIND version requests

Since many Internet DNS servers are running BIND (a Unix/Linux based DNS server), hackers may initiate an attack by sending a special request for the BIND software version number.

They can then compare the response with a list of known vulnerabilities for that particular BIND version and launch the actual attack.

Simple DNS Plus can be configured to respond to these BIND version requests with a text string of

your choice (for example: "Sorry - no BIND here!") by enabling the "Respond to BIND version requests" option in the Options dialog / DNS / Miscellaneous^[30] section. A warning is always logged (Active Log View^[18] and log files) for BIND version requests. You can test this using the "BIND version" lookup type in the DNS Look Up tool^[48] included with Simple DNS Plus.

DNS forwarding

When you enable forwarding^[58], you basically inherit any security issues of the DNS servers you are forwarding to.

So make sure those DNS servers are also configured securely - or don't forward to them.

Many new users think they need to configure Simple DNS Plus to forward DNS requests to their ISP's DNS servers in order to resolve DNS.

This is a misconception - Simple DNS Plus is perfectly capable of resolving DNS all by itself.

Forwarding to your ISP just adds another step to the process, which makes it take more time resolve, and has the potential of being less secure.

Dynamic DNS updates / IP spoofing

If your Simple DNS Plus server is accessible from the Internet, and you enable standard (un-signed) dynamic updates^[58] for a zone (in the zone properties^[43] dialog) make sure to specify that only local IP addresses are allowed to send update requests, and that your router or firewall filters out any spoofed IP packets coming from the Internet claiming to be from those IP addresses.

Most routers by default filter out any inbound IP packets claiming to be from the standard private IP address ranges (192.168.x.x / 172.16.x.x / 10.x.x.x).

If this is not filtered by the router, a hacker may be able impersonate a trusted local computer by spoofing the origin IP address of the DNS packets, potentially giving him access to change your DNS records.

If you want to receive dynamic updates^[58] across the Internet, make sure to use TSIG^[65] signed updates only - see Options dialog / DNS / Local Zones / TSIG Updates section^[26].

2.5 Read the log

You can open the "full text log files" created by Simple DNS Plus with notepad, or watch the most recent log entries using the Active Log View^[18].

Log lines starting with "->" are details for a previous line.

Writing log files to disk can be activated in the Options dialog / Logging / Log files^[34] section.

In addition to the logs, some events can be recorded to the Windows Event Log, which in turn can be used to send notification via network messages, e-mail, etc. See Options dialog / Logging / Windows Event Log section^[35].

***** Error/Warning:... messages**

For details and explanations see Event IDs / Error Messages^[80].

-> Header:... messages

-> Header: Format Error

Means that the DNS request was not formatted correctly.

This could be caused by network problems, a malfunctioning DNS server, or another network program incorrectly using the DNS port (53).

-> Header: Server Failure

Usually means that a DNS server did not respond or that no NS-record^[74] (or associated A-record^[68]) exists for a domain name.

Often follows the "**** Warning: Lame delegation..." message (see Event IDs / Error Messages^[80]). This could also be caused by network connectivity problems.

-> Header: Non-Existent Domain

Means that the domain name specified in the request does not exist.

If this happens for all outside domain names that you try to resolve, make sure you don't have a <root> zone in the DNS Records window^[37].

-> Header: Not implemented

Means that the DNS server does not support this type of query.

-> Header: Refused

The queried DNS server refuses to respond to this query - usually due to local security^[4] settings. This most often happens in connection with zone transfers^[67] - make sure the primary DNS server allows the secondary servers to zone transfer the zone (see Zone Properties dialog^[43]).

-> Header: Name exists when it should not

This header is returned in a response to a dynamic update^[58] request.

The update could not be completed because the prerequisites specified by the update request were not met.

-> Header: RR Set exists when it should not

This header is returned in a response to a dynamic update^[58] request.

The update could not be completed because the prerequisites specified by the update request were not met.

-> Header: RR Set that should exist does not

This header is returned in a response to a dynamic update^[58] request.

The update could not be completed because the prerequisites specified by the update request were not met.

-> Header: Server not authoritative for zone

This header is returned in a response to a dynamic update^[58] request.

The update could not be completed because the server responding is not configured with the zone specified in the update request.

-> Header: Name not contained in zone

This header is returned in a response to a dynamic update^[58] request.

The update could not be completed because the update name is not contained within the zone specified in the update request.

-> Header: TSIG Signature Failure

This header is returned in a response to a TSIG^[65] signed dynamic update^[58] or zone transfer^[67] request.

The operation was not allowed because the TSIG signature in the update request was invalid.

-> Header: Key not recognized

This header is returned in a response to a TSIG^[65] signed dynamic update^[58] or zone transfer^[67] request.

The operation was not allowed because the server responding is not configured with the TSIG key or signature algorithm used in the update request for the update name.

-> Header: Signature out of time window

This header is returned in a response to a TSIG signed dynamic update or zone transfer request.

The operation was not allowed because the time stamp in the TSIG signature did not match the server's time (not within the requested "fudge" interval).

2.6 Integrate with other applications

Updating zone and record data

DNS record data is stored in standard "zone files" (ASCII based text files), located in the directory specified in the Options dialog / DNS / Local Zones / Data files section.

To examine the file layout, you can open the files generated by Simple DNS Plus with notepad (see [RFC1035](#) for exact specifications).

Typically each zone has its own zone file named "<zone-name>.dns" (ie: "example.com.dns").

The same directory contains the zone database file "_zones.sdzdb" which controls which zones are loaded by Simple DNS Plus and hold various status information about the zones.

The zone database can be examined using the "ZoneDBViewer.exe" application found in the Tools directory.

If programming with .NET, you can also read the zone database using the "SDNSFileLib.dll" library also found in the Tools directory.

The same directory also contains the "_zonegroups.xml" configuration file which lists zone groups (from the DNS Records window zone folder list).

There are several options for making Simple DNS Plus load new or updated zone files "on the fly":

Command line

You can tell Simple DNS Plus to reload one or all zone files by using one of the command line options.

HTTP API

Simple DNS Plus can be prompted to perform a number of actions through HTTP - either directly from a browser, or any other program that can communicate through HTTP.

See How to use HTTP API.

API for .NET and COM

The "Simple DNS Plus API for .NET and COM" is a code library which greatly simplifies and streamlines interacting with and updating data in Simple DNS Plus. It makes it possible to deal with DNS data as simple objects and eliminates the need to work with and understand the intricacies of DNS master files (a.k.a. zone files).

This can be done from any .NET or COM based application or dynamic web-site including ASP.NET, classic ASP, PHP, VB.NET, C#, Delpi, VBScript, JScript, etc.

It can be used on a separate computer (controlling Simple DNS Plus remotely), and is therefore available as a separate download.

See <http://www.simpledns.com/addons.aspx>

Updating options/settings

The various settings from the Simple DNS Plus Options dialog are stored in a "sdnsplus.config.xml" file in the application data directory.

On Windows Vista and Windows Server 2008, this location is typically:

C:\ProgramData\JH Software\Simple DNS Plus

On earlier Windows versions:

C:\Documents and Settings\All Users\Application Data\JH Software\Simple DNS Plus

If you update the "sdnsplus.config.xml" file outside of Simple DNS Plus, you can reload it using command line options `-O`.

You can also retrieve and update this file through the HTTP API `"getconfig" / "updateconfig"` commands.

Settings from other modules / dialogs are also stored in XML files in the same directory.

Extending Simple DNS Plus through plug-ins

Simple DNS Plus has an open plug-in architecture. For details see KB1281.

Locating the Simple DNS Plus directory

Simple DNS Plus installer records the installation path in the registry "Path" value under HKEY_LOCAL_MACHINE\SOFTWARE\JH Software\Simple DNS Plus

2.7 Use the HTTP API

Simple DNS Plus can be prompted to perform different actions through HTTP - either directly from a browser, or any other program that can communicate through HTTP.

This functionality is not intended as a direct user interface, but rather a way to communicate with Simple DNS Plus from other applications over the network (for example, ASP pages running on IIS, PHP pages on Apache, etc.).

By default, Simple DNS Plus listens for HTTP requests on IP address 127.0.0.1 port 8053. With this default configuration, you can open a web-page that lists the available commands in your browser using <http://127.0.0.1:8053>

Port 8053 is used to avoid conflicts with any web server software using the standard port 80 on the same machine.

Please note that only the same computer can connect to IP 127.0.0.1, so if you need to access this from another computer, you will need to configure Simple DNS Plus to listen on a different IP address. You can change these setting in the Options dialog / HTTP API section `31`.

Simple DNS Plus accepts both HTTP "GET" and "POST" requests - use whichever is more convenient for your situation.

When using "GET", all fields and values must be part of the URL.

When using "POST", all fields and values must be in the HTTP request message body.




The response will either be a document (text, XML, or HTML depending on the parameters of the request) containing the result, an error 404 for unrecognized commands, or error 406 for requests that could no be performed.

The request document/path name must be one of the commands described below.

For example, to list the contents of the zone file for example.com, you could use the following (with GET):

`http://127.0.0.1:8053/getzone?zone=example.com`

Commands:

- **status**
Returns server status and request counters.
Optionally include the field "format" with the value "text" (the default), "html", or "xml".
- **clearcache**
Clears the DNS cache.
Same as selecting "Clear Cache" from the main window  / File menu.
- **reloadall**
Reloads all zone data from disk.
- **zonelist**
Returns a list of all zones on the server.
Optionally specify a numeric zone group ID in the field "zonegroup" to limit the list to a single zone group.
Optionally specify the list format in the field "format" (either "xml" or "text").
- **getzone**
Returns the text of a zone's zone file.
Specify the zone name in the field "zone".
- **loadzone**
Reloads an existing zone from disk.
Specify the zone name in the field "zone".
NOTE: You don't need to reload zones updated with other HTTP API commands. However this command can be used if the zone file on disk has been updated from another process.
- **removezone**
Removes an existing zone from the server.
Specify the zone name in the field "zone".
- **updatehost**
Updates, creates, or deletes an A-record or AAAA-record (host address).
A parent zone must already exist for the host name.
Specify the host name in the field "host".
Specify an IP address (IPv4 or IPv6) in the field "data" (if no data is specified, the record is deleted).
Optionally specify a comment for the host record in the field "comment".
- **updatezone**
Updates or creates a new zone on the server.
Specify the zone name in the field "zone".
Specify the zone data in the field "data" (formatted as a standard zone file).
For secondary zones, specify the primary server IP address in the field "masterip".
Optionally specify a numeric ID in the field "zonegroup" matching a group ID in the "_zonegroups.xml" file.
Make sure to increment the SOA-record  serial number when using this command.
- **addrecord, updaterecord, removerecord**
Adds, updates, or removes a DNS record.
Specify the zone name in the field "zone".
Specify the record name in the field "name" using zone file format (@ = zone name, etc.)
Specify the record type in the field "type" (for example: 'A' or 'MX')
Specify the record data in the field "data" using zone file format (optional for removerecord)
Optionally specify the record TTL  in the field "ttl" in seconds.
Optionally specify a comment for the record in the field "comment".

- **getconfig**
Returns the Simple DNS Plus configuration (Options dialog settings) in XML format.
Note: The format of the configuration XML is not documented and is subject to change from version to version.
- **updateconfig**
Updates the Simple DNS Plus configuration (Options dialog settings).
Specify the configuration XML in the field "data".
To update individual settings, first use the "getconfig" command to retrieve the current configuration XML, update this, and then submit it back to the server using this command.
Note: The format of the configuration XML is not documented and is subject to change from version to version.
- **zonegrouplist**
Returns a list of zone groups on the server (from the DNS Records window^[37]).
Optionally specify the list format in the field "format" (either "xml" or "text").
- **addzonegroup**
Adds a new zone group and returns the numeric ID of the new zone group.
Specify the name of the new zone group in the field "name".
- **renamezonegroup**
Renames an existing zone group.
Specify the numeric ID of the zone group to rename in the field "id".
Specify the new zone group name in the field "name".
- **removezonegroup**
Removes a zone group and all zones in it.
Specify the numeric ID of the zone group to remove in the field "id".
- **aliaszonelist**
Returns a list of DNS zones sharing the same zone file as the specified zone.
Specify the name of the zone to list aliases for in field "zone".
Optionally specify the list format in the field "format" (either "xml" or "text").
- **addaliaszone**
Creates a new primary zone which shares its zone file with another primary zone.
Specify the name of the new zone in the field "zone".
Specify the name of the existing zone in the field "aliasfor".
Optionally specify the numeric zone group ID for the new zone in the field "zonegroup".
- **suspendzone, resumezone**
Suspends or resumes a zones.
Specify the name of the zone to suspend/resume in the field "zone".
- **zonestatus**
Returns the current status of a zone (XML format).
Specify the name of the zone in the field "zone".
- **pluginstate**
Returns state information about a running plug-in instance (result of SaveState method).
The format and content of the returned data depends on the plug-in. Not all plug-ins return state data.
Either specify the plug-in instance display name in the field "name" or the instance ID (a GUID) in the field "id".

- **getpluginconfig**
Returns configuration data for a plug-in instance.
The format and content of the returned data depends on the plug-in.
Either specify the plug-in instance display name in the field "name" or the instance ID (a GUID) in the field "id".
- **updatepluginconfig**
Updates a plug-in instance configuration.
The expected format and content of the configuration data depends on the plug-in.
Either specify the plug-in instance display name in the field "name" or the instance ID (a GUID) in the field "id".
Specify the configuration data in the field "data".

2.8 Use command line options

When Simple DNS Plus is running, you can use the following command line (DOS prompt) options:
(Make sure you run these from the directory where Simple DNS Plus is installed)

```
SDNSPLUS -z z:<zone-name> [f:<file-name>] [p:<primary-ip>] [g:<group-id>]
```

Loads, re-loads, and/or updates the status of a specific zone^[57].

The f:file-name parameter is only required if this is a new zone.

The p:primary-ip parameter is only required if this is a secondary zone.

The g:group-id is optional and refers to the numerical zone group ID.

```
SDNSPLUS -r
```

Reloads all zones.

```
SDNSPLUS -r <zone-name> <file-name>
```

Deprecated. For backwards compatibility only. Use -z option instead.

```
SDNSPLUS -u <zone-name>
```

Unloads / removes a zone^[57].

```
SDNSPLUS -c
```

Removes all records from the cache.

Same as selecting "Clear Cache" from the main window^[16] / File menu.

```
SDNSPLUS -o
```

Reloads options file (sdnsplus.config.xml)

```
SDNSPLUS -x
```

Shutdown Simple DNS Plus.

```
SDNSPLUS -m <password>
```

Enables remote management and sets the remote management password (see Options / Remote Management section^[35]).



This can be used to gain remote access to Simple DNS Plus - for example on a Server Core machine - see KB1278.

3 User Interface

The Simple DNS Plus user interface consists of 4 primary modules:

Main window^[16]





DNS Records window^[37]

DNS Look Up window 
DNS Cache Snapshot window 

Each of these 4 modules run as separate processes which can function independently of the others, and each appear separately in the Windows task bar.




Each module has a number of functions and dialogs which are described in the following sections.

3.1 Main window





The main window consists of a Menu , a Toolbar , a Status Bar , and different optional Views .












Menu

• File Menu

- **Pause / Start server**
Used to pause and re-start serving DNS requests.
- **Edit DNS Records**
Opens the DNS Records  window.
- **Reload DNS Records**
Immediately reloads all DNS records.
Use if manual changes have been made to any of the zone files.
- **Clear DNS Cache**
Unloads all cached  records.
Use if you suspect that invalid cached data is causing problem.
Can also be useful, for example, if you want to see how a domain name is resolved from the root up.
- **Connect to Remote...**
Starts a new instance of the Simple DNS Plus user interface for an instance running on a remote computer.
NOTE: Remote Management must be enabled in the Options dialog / Remote Management section  on the remote Simple DNS Plus instance.
- **Shutdown Simple DNS Plus**
Shuts down the Simple DNS Plus service and user interface.

• View Menu





- **Toolbar**
Toggles the Toolbar  on / off.
- **Status Bar**
Toggles the Status Bar  on / off.
- **Pause Active Log**
Pauses the log display in the Active Log View .
- **Performance Graph**
Shows the Performance Graph View .

- **Active Log**
Shows the Active Log View .
- **[Plug-In Views]**
Different plug-ins  such as the DHCP Server plug-in have their own View .
- **Tools Menu**
 - **DNS Look Up...**
Opens the DNS Look Up  tool window.
 - **DNS Cache Snapshot...**
Opens the Cache Snapshot Viewer  window.
 - **Active Log Snapshot...**
Use this function if the Active Log View  is scrolling to fast or you need to copy text from the log.
 - **IP Address Blocking...**
Opens the IP Address Blocking  dialog.
 - **Options**
Opens the Options  dialog.
- **Window Menu**
 - **New Horizontal / Vertical Tab Group**
Splits the display into two tab groups. Only available when other Views  are grouped with the selected View.
 - **Tile Horizontally / Vertically**
Quickly organize the currently open Views .
 - **Reset Window Layout**
Move all open Views  into a single tab group.
- **Help Menu**
 - **Contents & Index**
Opens this help file
 - **Online Support**
Opens the JH Software support web page in your default browser.
 - **Check for Updates**
Checks if you are running the most recent version of Simple DNS Plus.
 - **Activate Product**
Select this function when you have purchased a Simple DNS Plus license (at <http://www.simpledns.com/purchase.aspx>) to enter your license key. This will remove the evaluation time restriction.
 - **Support File**
Generates a file containing various information about your system and the state of Simple DNS Plus which can be helpful for trouble shooting by JH Software support staff.

- **About Simple DNS Plus**

Displays the Simple DNS Plus version number and license status.

Toolbar


- **Options button**
Opens the Options  dialog.
- **Records button**
Opens the DNS Records  dialog.
- **Look Up button**
Opens the DNS Look Up  tool.
- **Cache button**
Opens the Cache Snapshot Viewer .
- **Help button**
Opens this help file.

Status Bar

The Status Bar consists of three sections:

- **Status**
Show current server status - and if running, the total up-time.
- **Requests**
Total number of DNS requests received.
- **Cache**
Number of DNS records currently in the cache.

3.1.1 Views

The center of the Main window  can host different "views".
Use the View menu to open new Views.

You can have multiple views open at the same time.
Initially all open views will be in the same "tab group", and you can switch between views by clicking on the tabs.

To make two or more views visible at the same time, you can open additional tab groups either using the Windows menu, or by mouse-dragging a tab towards the center of the view and releasing it on the "docking diamond" when the desired position is indicated.
When multiple tab groups are visible, you can resize them with the mouse by dragging the splitter bars between the tab groups.

Performance Graph View

Shows a graph of the number of requests received per second during the last minute.

Active Log View

Shows current log activity.

See [How to read the log](#) ^[9].

The level of detail and number of lines displayed can be customized through the Options dialog / Logging / Log Details section ^[33].

If the log windows is scrolling too fast, you can pause it using the "Pause Active Log" function from the View menu, or from the right-click menu, or press F9.

If you need to copy text from the log, use the "Active Log Snapshot" function from the Tools menu, or from the right-click menu, or press CTRL+F9.

You can also clear the window using the "Clear" function from the right-click menu.

Please note that the Active Log uses considerable CPU time due to the volume of data that must be converted into clear text. On a busy server we recommend closing this View when not needed.

Plug-in Views

Some plug-ins also have "views", for example, the DHCP Server plug-in ^[53].

A separate view will be available for each such plug-in instance configured in the Options dialog / Plug-Ins ^[32] section.




3.1.2 Options dialog

The Options dialog has the following sections:


- General ^[20]
- DNS
 - Inbound Requests ^[20]
 - Outbound Requests ^[20]
 - Resolver
 - Recursion ^[21]
 - IP Filtering ^[21]
 - Caching ^[21]
 - Local Zones
 - Data Files ^[22]
 - Zone Transfers ^[22]
 - Super Master/Slave ^[23]
 - Secondary Zones ^[24]
 - Suspended Zones ^[25]
 - Automatic SPF ^[25]
 - TSIG Updates ^[26]
 - Forwarding ^[27]
 - Lame Requests ^[27]
 - Non-existing Domains ^[28]
 - NAT IP Alias ^[29]
 - Miscellaneous ^[30]
- HTTP API ^[31]
- Plug-Ins ^[32]
- Logging
 - Log Details ^[33]
 - Log Files ^[34]
 - Syslog Server ^[34]
 - Active Log View ^[35]
 - Windows Event Log ^[35]
- Remote Management ^[35]

3.1.2.1 General

- **Domain name of this DNS server**

Used as the default primary DNS server name when creating new zones  (for the SOA-record  and NS-record .

This is typically something like "ns1.example.com" - with "example.com" being your main domain name.

This name is also displayed in the title bar of the main window , and as a "Tool Tip" for the tray bar icon for easy reference.

- **Show icon in the Windows taskbar notification area**

When checked, Simple DNS Plus will be represented by a small icon in the tray bar (typically in the lower right hand corner of the screen, the area next to clock).

3.1.2.2 DNS

3.1.2.2.1 Inbound Requests

- **Inbound DNS Requests**

- **Listen for DNS requests on**

Specify the port number and select local IP addresses on which the DNS service will be available.

NOTE: Other DNS servers and client computers expect to find your DNS server on port 53. You should only use a different port number in special situations, for example, if you are mapping port 53 on a NAT router or proxy to a different port number on this computer.

- **Maximum inbound TCP connections**

A hacker may try to open a lot of TCP connections to exhaust server resources.

Use this option to limit the total number of simultaneous inbound TCP connections Simple DNS Plus will accept. When this number of connections has been reached additional connection attempts are logged and then rejected.

3.1.2.2.2 Outbound Requests

- **Outbound DNS Requests**

- **Send outbound DNS and zone transfer requests via**


Specify which IP versions (IPv4/IPv6) and from which local IP addresses outbound requests should be sent.

It can be useful to select a specific local IP address for secondary DNS servers with multiple IP addresses (multi-homed) if the primary DNS server only allows zone transfers from a specific IP address.

When both IPv4 and IPv6 are enabled, you can also enable "Prefer IPv6 servers" to have the server attempt to resolve DNS over IPv6 whenever possible.

- **Send outbound DNS requests from port number**

Specify if Simple DNS Plus should use a new random port number for each outbound request, or send all outbound requests from the same port number.

Using random port numbers helps protect against DNS spoofing attacks. For details see How to secure your server / DNS spoofing .

Using a fixed port number is not recommended unless the DNS server is not offering recursion or it is forwarding to another secure DNS server for all domains.

3.1.2.2.3 Resolver

3.1.2.2.3.1 Recursion

- **Perform DNS recursion (resolve non-local domain names)**

Specify which IP addresses should be offered recursion^[61].

You can list multiple IP addresses, IP address ranges, and/or IP address subnets.

For DNS servers accessible from the Internet, it is highly recommend that you limit recursion to IP addresses on the local area network as this prevents DNS cache snooping and helps protect against cache poisoning (spoofing) - see How to secure your server^[4].

- **Maximum recursive DNS requests to resolve in parallel**

Specifies the maximum number of recursive^[61] requests to resolve at the same time.

- **To protect against cache poisoning (spoofing), only accept responses from other DNS servers which**

- **Come from the IP address that the corresponding request was sent to**

Enabling this option helps protect against DNS spoofing attacks. See How to secure your server / DNS spoofing^[4].

This is only an option because some multi-homed DNS servers may not respond from the same IP address as the DNS request was sent to, making it is impossible to resolve domains hosted by such a DNS server with this option enabled. This is however pretty rare and we generally recommend enabling this option.

- **Echo the request's question section**

Enabling this option helps protect against DNS spoofing attacks. See How to secure your server / DNS spoofing^[4].

This is only an option because older DNS servers/forwarders/devices may not include the question in the response as this was not originally an RFC requirement. This is however pretty rare and we generally recommend enabling this option.

3.1.2.2.3.2 IP Filtering

- **Remove host records (A/AAAA) containing the following IP addresses from responses received from other DNS servers**

When this option is enabled, hosts records with the IP addresses listed will be removed from responses.

- **Trusted DNS servers - host records will NOT be removed from responses from DNS servers with these IP addresses**

IP addresses of trusted DNS servers.

Background:

This function is primarily intended to prevent DNS rebinding attacks^[7] - it can however also be used to filter out undesirable IP addresses in general.

3.1.2.2.3.3 Caching

- **Cache DNS records received in responses from other DNS servers**

Use this option the enable/disable caching^[55]

- **Maximum cache time**

By default, records are removed from the cache based on the TTL received from the original DNS server.

These settings specify the maximum amount of time DNS records are cached.

- **Maximum DNS records cached**

You can use this option to limit the amount of memory Simple DNS Plus will use for caching.

- **Override low TTL values / Minimum cache time / TTL**

WARNING: This option should NOT be enabled by most users.

Enabling this will likely cause problems with many domain names that rely on frequent DNS updates either because they use dynamic IP addresses or some type of DNS based load balancing or failover system.

"cnn.com" is one example of a larger web site, which depends on low TTL values to enable quick changes to their web site (they currently use DNS TTL values of 5 minutes).

Many smaller web-sites also depend on low TTL values because they run on dynamic IP addresses and therefore require frequent DNS updates (when their IP address changes).

There are however special situations such as Internet connections with high latency (satellite connections for example) where it may make sense to trade DNS accuracy for faster DNS lookups.

- **Store cached DNS records on disk between shutdown/startup**

If this option is checked, all cached records are written to disk when Simple DNS Plus is closed (including when the computer is shut down correctly).

When Simple DNS Plus is later restarted, it will reload the cache recalculating the DNS records' TTLs ^[66] based on the time the program was closed.

See also Caching ^[55], TTL ^[66]

3.1.2.2.4 Local Zones

3.1.2.2.4.1 Data Files

- **Location of DNS data files (zone files)**

Specify the directory where data files are stored.

The default is the "ZoneFiles" directory under the Simple DNS Plus data directory:

Windows Vista/2008 and later: C:\ProgramData\JH Software\Simple DNS Plus

Earlier Windows versions: C:\Documents and Settings\All Users\Application Data\JH Software\Simple DNS Plus

- **Defer loading individual zones until first request (load on demand)**

In setups with many zones this can greatly improve the server startup time.

Inactive zones will never be loaded, which may also improve memory usage.

- **When loading zones from disk, limit DNS record TTL (Time To Live) values**

Replace lower/higher DNS record TTL ^[66] values when loading DNS zones.

Can be used when you want to enforce a min/max TTL value - for example when using zone files that someone else has supplied.

3.1.2.2.4.2 Zone Transfers

- **Accept TSIG authenticated zone transfer requests signed with one of the following keys for any zone on this server (from any IP address)**

Secondary DNS servers signing ^[65] zone transfer requests with one of these keys may zone transfer ^[67] any zone on this server.

Zone transfer permissions can also be specified for each individual zone in the Zone Properties ^[43] dialog. However the zone transfer requests signed with the keys listed here are always accepted no matter what the settings are in the individual zones.

- **Accept un-signed zone transfer requests for any zone on this server**

The IP addresses listed here are allowed to request zone transfers^[67] for any zone hosted on this server.

Zone transfer permissions can also be specified for each individual zone in the Zone Properties^[43] dialog. However the IP addresses listed here can always zone transfer no matter what the settings are in the individual zones.

- **Send only one DNS record per message (older BIND secondary servers)**

This option should only be enabled if one or more of the zones on the server has an old BIND server as secondary which doesn't understand zone transfer messages with multiple DNS records.

Note: Enabling this does not prevent newer secondary DNS servers from zone transferring. It will just be less efficient.

3.1.2.2.4.3 Super Master/Slave

The Super Master/Slave feature is used to automatically create and remove zones on secondary (slave) servers.

When you create a new primary zone on the master server, all slave servers (the "Super Slaves" list on the master server) will be notified that there is now a new zone available. When a slave server receives such a notification, it first checks its master list (those listed in "Super Masters") to validate the master, then requests update information and creates the zone (as secondary).

A similar process happens when you delete a zone from the master server.

A Simple DNS Plus server can act as both master (primary zones) and slave (secondary zones) at the same time, and can have multiple masters and slaves.

- **Super Slaves**

- **The following DNS servers are secondary for all primary zones on this server**

List of slave server IP addresses.

- **Accept un-signed zone transfer requests from above IP addresses**

Unless this option is checked, slave servers must TSIG sign^[65] zone transfer requests including zone list synchronization requests.

The acceptable TSIG keys for such signed requests are specified on the in the Zone Transfers section^[22].

- **Super Masters**

- **This server is secondary for all primary zones on the following DNS servers**

List of master server IP addresses.

A TSIG key for signing zone transfer and zone list synchronization requests can optionally be specified for each master server.

- **Bulk refresh / verify zone lists every**

Simple DNS Plus retrieves a list of zones and their current serial numbers from the DNS servers in the Super Masters list (above) at this interval.

It uses this list to synchronize both individual zones and the zone list.

If you have a lot of zones (thousands) you may want to enforce long "Refresh" values on secondary zones (see Secondary Zones section^[24]) in order to reduce synchronization traffic between the DNS servers.

Even with long "Refresh" values, secondary servers will still get zone updates almost immediately as they happen on the primary server because the primary server will send it a NOTIFY message (make sure to enable "Send NOTIFY..." in the Miscellaneous section^[30] on the master).

If you set this (Bulk refresh / verify zone lists every) to a slightly shorter value than the enforced "Refresh" value, the effect is that all secondary zones will be refreshed in a single operation at this interval, and never get around to refreshing individually. This is obviously much more efficient.

NOTE: This functionality (super master/slave) is unique to Simple DNS Plus, and is not currently supported by other DNS server implementations, so both master and slave must be running Simple DNS Plus.

NOTE: In earlier versions of Simple DNS Plus, this feature was called "Master/Slave" (without "Super").

This function has been improved in recent versions of Simple DNS Plus, but the main reason for adding "Super" was that new users often thought that "Master/Slave" was just different terminology for "Primary/Secondary" and therefore didn't realize the full potential of this function. "Super Master/Slave" is fully compatible with "Master/Slave" in earlier versions.

See also Zone Transfer [\[67\]](#), TSIG Signature [\[65\]](#)

3.1.2.2.4.4 Secondary Zones

- **Maximum refresh / IXFR requests to send per second**

On servers with many secondary zones, this settings prevents flooding primary DNS servers with refresh / IXFR (incremental zone transfer [\[67\]](#)) requests.

- **Maximum parallel zone transfers (From different primary servers)**

Limits the number of simultaneous TCP zone transfer connections made to primary servers.
NOTE: Simple DNS Plus will never establish more than one TCP zone transfer connection to any one primary DNS server at a time (based on IP address). Therefore this setting has no effect if all secondary zones come from the same primary server.

- **Retry transferring expired zones every**

This value controls how often the server will attempt to retrieve zone data for expired secondary zones from their primary DNS server (zone transfer). Expired zones include new (never zone transferred) secondary zones.

- **Use incremental zone transfers (IXFR)**

Incremental zone transfers are generally more efficient than full zone transfers.
However it may be necessary or more efficient to disable this setting if your primary DNS server does not support IXFR.

- **Only accept NOTIFY requests from IP address of primary DNS server**

Whenever a zone [\[57\]](#) is updated, the primary DNS server will send a NOTIFY request to secondary DNS servers for the zone to let them know about the update (assuming this is enabled on the primary DNS server - see Miscellaneous section [\[30\]](#)).

The secondary DNS servers will then refresh the zone and request a new copy of the data by zone transfer [\[67\]](#) if necessary.

With this option enabled, such NOTIFY requests will only be accepted if they originate from the IP address that is configured as the primary DNS server IP address for the zone. This prevents stray or malicious requests from triggering the zone refresh process.

NOTE: If the primary DNS server is multi-homed (more than one IP address), NOTIFY requests could originate from a different IP address.

In Simple DNS Plus, the IP address that outbound requests (including NOTIFY requests) are sent from is configured in the Options dialog / DNS / Outbound requests [\[20\]](#) section.

- **Enforce minimum values for secondary zone SOA records**

Can be used to limit the number of refresh and zone transfer requests.
Recommended if you don't control the primary DNS server for the secondary zones you host.

3.1.2.2.4.5 Suspended Zones

- **When receiving DNS requests for names or sub-names of suspended zones**

Select one of the following options to specify how Simple DNS Plus should respond when it receives a DNS request for a name in a suspended zone [\[65\]](#):

- **Respond with a "Refused" error message (default)**

Using this option, you specifically inform the client (or other DNS server) that you will not provide any data for the requested name.

- **Respond as if the zone was not configured on this server**

The server will respond as if the zone wasn't on this server.

If the IP address sending the DNS request is not offered recursion (see Recursion section [\[21\]](#)), the request will be treated as lame, and responded to (or not) according to the settings in the Lame Requests section [\[27\]](#).

- **Respond with synthesized DNS records**

Using this option, you can redirect anyone requesting suspended names for example to a "this web-site is temporarily suspended" web-page.

3.1.2.2.4.6 Automatic SPF

- **Synthesize TXT-records from SPF-records for local domains**

This options allows you to publish SPF-records [\[79\]](#) for your domains without maintaining identical TXT-records [\[79\]](#) (for older e-mail servers).

If the server receives a DNS request for TXT-records for a name, and no TXT-record exists but an SPF-record does exist, it will respond with a synthesized TXT-record containing the same data as the SPF-record.

- **Synthesize missing SPF records (TXT and SPF) for local domains**

Using this option you can provide SPF records for all domain names on your server without having to setup and maintain SPF-records separately for every single domain name.

If you need to provide unique SPF-records for certain domain names, you can still setup individual SPF-records for those names. This function only kicks in when there are no SPF-records defined for a domain name already.

Consider enabling this option with the value to "v=spf1 -all" (meaning "these domains never send e-mail").

This forces you to have specific SPF-records for all domain names that send e-mails.

But it very effectively prevents spamming/phishing from all other domain names on your server - including common sub-names such as www.example.com which most users forget to setup SPF records for.

A good alternative to this is "v=spf1 mx -all" (meaning "these domains only send e-mail from the mail server listed in their MX-record").

This way any domain name that has an MX-record [\[73\]](#) is covered automatically.

And sub-names such as www.example.com which typically do not have MX-records are still excluded.

IMPORTANT: In addition to checking the domain name part of the sender's e-mail address, some e-mail servers also perform SPF checks on the SMTP session HELO/EHLO greeting host name. Therefore always make sure that your e-mail server is configured to use a correct host name (like "mail.example.com") in the HELO/EHLO greeting, and that an A- and/or AAAA-record exists for this

host name in DNS.

And when using this option, make sure that the SPF-record data is also valid for the HELO/EHLO host name used by your e-mail server, or define a specific SPF-record for the HELO/EHLO name in the zone where this belongs (this will override the automatic SPF record).

Note that the default automatic SPF record data "v=spf1 mx -all" will fail such a test if no MX-record exists for your HELO/EHLO name.

For example, if your domain name is "example.com" and your mail server is named "mail.example.com" (and uses this in HELO/EHLO greetings), you would probably only have an MX-record for "example.com" - not for "mail.example.com", and therefore "v=spf1 mx -all" fails to validate "mail.example.com".

Instead you could use "v=spf1 ip4:1.2.3.4 -all" (where 1.2.3.4 is the IP address of your mail server), which would work for both types of tests.

IMPORTANT: These synthesized records are provided in responses to standard DNS lookups for SPF- and TXT-records only - they are NOT provided in zone transfers to secondary DNS servers. Therefore you must configure this option the same way on any secondary DNS servers for your domain names.

NOTE: This function is automatically disabled for requests for any domain name containing the underscore (`_`) character to avoid collision problems with special purpose names such as "_domainkey".

Background:

SPF is a spam and phishing fighting method which uses DNS records to define which hosts are permitted so send e-mails for a domain.

Early implementation of SPF used DNS TXT-records to store these permissions. However a new dedicated SPF-record type was recently added to the DNS protocol specifically for this purpose.

When SPF enabled e-mail servers receive an inbound e-mail (via SMTP) they will lookup the DNS SPF-record (SPF or TXT type) for the domain name of the senders e-mail address in order to verify that sending e-mail server's IP address is permitted to send e-mail for that domain name.

For details more on SPF, please see <http://www.openspf.org>

3.1.2.2.4.7 TSIG Updates

Simple DNS Plus accepts dynamic update requests signed with TSIG keys in this list.

You should configure a unique TSIG key for each client making dynamic updates.

You can specify which domain names (in local zones) that the client may update for each key.

TSIG signed dynamic updates can be used directly with several "DynDNS" client programs - see <http://www.simplesdns.com/kb.aspx?kbid=1195>

Alternatively you can use the DynDNS Service plug-in - see

<http://www.simplesdns.com/kb.aspx?kbid=1260>


This plug-in also supports several HTTP based update methods and is specifically targeted towards "DynDNS" scenarios (computers with dynamic IP addresses on the Internet). However it only supports updates for host records (A-records).


TSIG signed dynamic updates (this section of the Options dialog) allows more advanced updates (any record type, multiple records in a single update, deletions, etc.) and greater flexibility in which records each client/key may update - but only through the DNS protocol (not HTTP).

3.1.2.2.5 Forwarding

- **DNS Forwarding**

List of domain names and the DNS server IP addresses that requests for these names (and their sub-names) are forwarded to.

Clicking the Add or the Edit buttons opens the DNS Forwarding dialog .

See also: Forwarding .

3.1.2.2.5.1 DNS Forwarding dialog

- **Forward DNS requests for**

Specify which domain names to forward DNS requests for.



Forwarding for only a specific domain name (and sub-names) is also known as "conditional forwarding".

- **To DNS servers**

Specify the IP addresses of the DNS servers to forward these DNS requests to.

- **Enable Extended Forwarding**

Also forward non-recursive DNS requests and DNS requests originating from IP addresses that are not offered recursion.


(Standard DNS forwarding only forwards recursive  DNS requests from IP addresses offered recursion )

- **Enable Shadow Forwarding**

Also forward DNS requests for the name or sub-name of a local DNS zone when no matching DNS records exist in that zone.

(Standard DNS forwarding only forwards request which are not for the name or sub-name of a local DNS zone)

In the "Authoritative Answer (AA) flag" dropdown, specify if the AA-flag in the response should be set, cleared, or copied from the response from the forward server.

See also: Forwarding .

3.1.2.2.6 Lame Requests

- **When receiving lame DNS requests**

Select one of the following options to specify how/if Simple DNS Plus should respond to lame DNS requests:

- **Respond with a "Refused" error message (default)**

Using this option, you inform the server/client sending the request that you will not perform any recursion for them or provide any data for the requested domain name.

- **Do not respond (stealth DNS)**

Using this option, simple port scanning will not reveal that you are running a DNS server. This may make you a less interesting target for hackers.

- **Respond with a referral to Internet root DNS servers**

This option is available only because some DNS test tools, including some used by major domain name registrars, expect to see a root referral in response to requests for dummy/random domain names.

Unless needed for such tests, we do not recommend using this option because it might

be abused for DNS amplification attacks^[6].

- **Respond with synthesized DNS records**

Using this option, you can redirect the client to a sign up page, or to a page informing the client that he is using a wrong DNS server.

Background:

A "Lame DNS Requests" is a DNS request sent to a DNS server which is not configured with the requested domain name (local zones^[5] or otherwise) and not configured to perform recursion^[6] for the IP address sending the DNS request.

3.1.2.2.7 Non-existing Domains

- **Redirect requests for non-existing domain names**

- **Requests for A-records (IPv4)**

Enter the IP address to redirect to.

- **Requests for AAAA-records (IPv6)**

Enter the IP address to redirect to.

- **Additional TXT-record explaining synthesized response**

Enter a short text explaining why the client is being redirected.

This will be visible when someone uses diagnostics tools such as NSLOOKUP, DIG, and other DNS lookup tools.

- **Exceptions...**

Click this button to specify the following exceptions:

- **Only redirect domain names starting with 'www'**

Limit redirection to typical web-site domain names.

- **Do not redirect domain names that belong to local zones (authoritative)**

Limit redirection to domain names other than your own.

- **Do not redirect domain names that begin with an IPv4 address (reverse and RBL/DNSBL record names)**

When checked, domain names where the first 4 name segments resemble an IPv4 address will not be redirected.

WARNING: If your e-mail server or spam filter programs are using one or more RBL/DNSBL lists, redirecting non-existing domain names representing RBL/DNSBL records could cause e-mails from valid senders to be rejected. We therefore recommend enabling this exception (default).

- **Do not redirect these domain names and their sub-names**

Limit redirection to domain names other than these.

- **Do not redirect queries from the following IP addresses**

Limit redirection to queries from other IP addresses than these.

Background:

Typically when you enter a non-existing domain name in a web-browser, you either get an error page,

or you are redirected to some search web-site controlled by the web-browser company or possibly your ISP.

This of course happens all the time because of misspellings and bad links on web-sites.

Now you can take advantage of those failed requests (from any client configured to use your DNS server) by redirecting them to your web-server instead of giving this traffic to the browser companies.

This option redirects all recursive DNS requests for non-existing domain names to a server IP address which you control.

This gives you a unique opportunity to present your own custom search page, a domain sale offer, a marketing message, an intranet site, or anything else you can think of.

IMPORTANT: This function redirects ALL DNS requests for non-existing domain names (it is not possible for the DNS server to tell if a DNS request comes from a browser or another type of application), so you may need to use the exception options to limit this.

For example you may want to setup an exception for the IP address of your e-mail server so it won't try to deliver (otherwise failed) e-mails to your web-server's IP address.

NOTE: Only requests which are for domain names confirmed not to exist (NXDOMAIN) will be redirected - not any other error type conditions.

3.1.2.2.8 NAT IP Alias

- **Enable NAT IP alias conversion for DNS requests from LAN**

In DNS responses to DNS requests from LAN clients only, this function changes host records which are pointing to a public IP address of the NAT router to point to the corresponding private IP address of a local server.

This way, for example, HTTP requests from LAN clients for local web-sites will go directly to the local web-server instead of via the NAT router.

- **NAT router IP address mappings (aliases)**

Enter external / internal IP address pairs.

- **LAN IP addresses (internal/private side of the NAT router)**

Enter the private/internal IP addresses/subnets of your local area network.

- **This computer is on the LAN side of the NAT router**

Check if this computer is located on the LAN.

Background:

If you wish to run a web-server behind a NAT router, then you must point the DNS records for your web-site domain names to the public IP address of the NAT router, and on the NAT router map port 80 (for HTTP) to the private IP address of the local web-server computer.

This works fine for all external visitors from the Internet.

However, this setup often creates problems when you want to access your own web-site from the private side of the NAT router (from within the LAN).

Without this function, when your web-browser makes a DNS request for the web-site domain name, it gets your public IP address and then tries to make a HTTP connection to that IP address via the NAT router.

This requires the NAT router to route packets from the LAN side to the public IP address and back into the LAN - which many NAT routers cannot handle correctly. Often you get the router login page instead or nothing at all.

Even if this does work, you are putting unnecessary load on the router.

Please note:

This function is for use with network setups with one or more external/public IP addresses on a NAT router mapped to internal server(s) on private IP addresses.

This only works with one-to-one IP address mappings - each external/public IP address can only be mapped to a single internal/private IP address.

If you need to have different ports on one external IP address mapped to different internal IP addresses, then you should run two DNS servers instead - one for external use and one for internal use.

A "NAT Router" can be a physical device such as those from Cisco, Linksys, DLink, NetGear, etc., or a computer running "Internet Connection Sharing" or similar.

3.1.2.2.9 Miscellaneous

- **Enable Round Robin (rotate DNS records in responses)**

When this option is enabled and multiple records of the same type are defined for the same name, Simple DNS Plus automatically rotates these records in responses (See Round Robin [\[64\]](#)).

- **Synthesize empty reverse zones for standard private IP address ranges**

This prevents leakage of reverse DNS requests for private IP addresses.
For details see draft-ietf-dnsop-default-local-zones

- **Send NOTIFY requests to secondary servers when a primary zone is updated**

Enables faster synchronization of zone changes to secondary DNS servers.
Not supported by older DNS server software.

- **Keep the root server list (a.k.a. "hints file") updated automatically**

With this option enabled, Simple DNS Plus will automatically check for root server [\[64\]](#) updates.
You may want to disable this if you are using an alternate root or if your server is only used on for intranet purposes.

- **Enable EDNS0. EDNS0 payload size**

The original DNS specifications limits DNS request and response packets over UDP to 512 bytes (payload).

As DNS servers need to send more data (for example, as the larger IPv6 addresses are added to TLD DNS servers etc.) this limitation causes truncation and DNS servers have to switch to the much less efficient TCP protocol.

However most networks and Internet connections today support much larger UDP packets.

With this option enabled, Simple DNS Plus will indicate to other DNS servers that it is able to send and receive larger packets over UDP, and it sends larger response packets over UDP to other DNS servers that have indicated that they support it.

A value of 1280 is a good starting point for most setups, as this payload size fits within the standard ethernet packet size.

In many cases values of 4096 and higher will also be fine depending on network, routers, etc.

- **Test EDNS0 at startup to ensure that this is supported by local firewalls**

Older Cisco PIX firewalls and other firewall products are known to drop DNS packets with EDNS0. If you experience this problem please contact your firewall vendor to get a firmware update.

When this option is enabled, Simple DNS Plus will send some test EDNS0 packets at startup. If it determines that EDNS0 is not supported, it will log a warning (and Windows Event if enabled), and will then continue without EDNS0.

- **Respond to BIND version requests**

Since many Internet DNS servers are running some version BIND (mainly Unix/Linux DNS server), hackers often initiate an attack by sending a special request for the BIND software version number.

They can then compare the response with a list of known vulnerabilities for that particular version of the BIND software and launch the actual attack.

With this option enabled, Simple DNS Plus will respond to such BIND version requests with a text of your choice.

When this option is not enabled, Simple DNS Plus will respond to BIND versions requests with a "not implemented" error message.

A warning is always logged for BIND version requests.

- **Limit client caching time (adjust TTLs in responses to recursive requests)**

Recent Windows versions have a "DNS Client" service (enabled by default) which caches DNS records locally. Other operating systems have similar features.

This option can be used to limit the time that client computers/devices cache the DNS records provided by Simple DNS Plus by setting a maximum TTL (time to live) value for DNS records in responses to these clients.

This is independent of the length of time that Simple DNS Plus might itself cache (see Options dialog / DNS / Resolver / Caching section [\[21\]](#)) the same DNS records and only takes effect for clients requesting recursion (not other DNS servers) and only for clients with IP addresses in the "Perform recursion for" list (see Options dialog / DNS / Resolver Recursion section [\[21\]](#)).

Limiting client caching time is useful when you want to be able to enforce quick updates - for example when using black/white-lists that are frequently updated, or plug-ins that might take effect at different times.

NOTE: Microsoft Internet Explorer also caches DNS records (independent of the "DNS Client" service) for 30 minutes no matter what TTL is used. So updates may take up to 30 minutes no matter what unless the user restarts I.E. Other browsers also cache DNS records but typically for a shorter time.

- **Ignore all DNS requests for <root> (no response, no logging)**

This option was implemented to deal with a specific DNS amplification attack [\[6\]](#) which was rampant in early 2009.

The attacker would send requests for the DNS root from a spoofed IP address of the victim, so that DNS servers would respond with a relatively large DNS packet listing all the root DNS servers and thereby flood the victim.

Other features are available to deal with such attacks including the Lame Requests [\[27\]](#) settings and the Ignore DNS Request plug-in [\[53\]](#), but this feature filters out these specific packets at an earlier point in the process reducing CPU usage and preventing logging.

3.1.2.3 HTTP API

- **Enable HTTP API interface**

Check/uncheck to enable/disable this functionality.

- **On IP address**

Select the local IP address(es) that Simple DNS Plus should listen for HTTP requests on.

- **TCP port**

Specify the TCP port number that Simple DNS Plus should listen for HTTP requests on.

- **Password**

If specified, all HTTP requests are authenticated with user "admin" and this password.

- **Accept HTTP connections from**

List the IP addresses which are allowed to make HTTP requests.

See also How to use the HTTP API [\[12\]](#).

3.1.2.4 Plug-Ins

- **Available Plug-In components**

List of the Simple DNS Plus plug-in components currently available on this computer.

This reflects the plug-in .dll files in the "plugins" sub-directory of the directory where Simple DNS Plus is installed.

Additional plug-in components can be downloaded from <http://www.simplesdns.com/kb.aspx?kbid=1271>

To create an instance of a plug-in component, select it in the list and click the "Create Instance..." button. This will open the plug-in instance dialog [\[32\]](#).

For more information about a plug-in component, select it in the list and click the "Info..." button.

- **Plug-In instances**

List of plug-in instances.

To configure a plug-in instance, select it in the list and click the "Properties" button. This will open the plug-in instance dialog [\[32\]](#).

To remove a plug-in instance, select it in the list and click the "Remove" button.

Plug-in instances are queried in the order listed. To change the order, select a plug-in instance in the list and click the "Up" or "Down" buttons.

- **Query plug-ins before local zones (plug-in data overrides local zones)**

Specify in which order to query plug-ins / local zones.

See also: [Plug-Ins Overview](#) [\[53\]](#)

3.1.2.4.1 Plug-In Instance

The Plug-In Instance dialog has 1, 2, or 3 tabs depending on the plug-in type:

- **General tab**

This tab is available for all plug-ins.

- **Plug-in instance display Name**

This name is used to uniquely identify the plug-in instance.

For plug-in types that have a [View](#) [\[18\]](#), this name will also appear in the main window [\[16\]](#) [View](#) menu and on the view tab.

- **Listed IP Addresses**

Only available for plug-ins that in some way lists IP addresses (for plug-in developers: implements `IListsIPAddress`).

- **Perform DNS recursion for IP addresses listed by this plug-in**

When enabled, Simple DNS Plus will resolve DNS requests received from IP addresses listed by this plug-in - even if they are not listed in the Options dialog / DNS / Recursion section.

- **Whitelist IP addresses listed by this plug-in from all DNSBLs**

When enabled, Simple DNS Plus will respond to any DNS request for A-records for names starting with a reversed IP address, that is listed by this plug-in, with a "name does not exist" error code.

When a client computer (who's IP address is listed by this plug-in) sends an e-mail to a local e-mail server which is using this same Simple DNS Plus server, and this e-mail server looks up the sender's IP address (the client computer) in some DNSBL list, this option ensures that the result is always "not black listed".

This can be useful because dynamic IP address ranges are often black listed as e-mail

senders.

- **Threading**

- **Max. parallel threads**

- Only available for plug-ins that implement multi-threading (for plug-in developers: `GetPluginTypeInfo.MultiThreaded` returns `True`).

Specify how many threads may access the plug-in at the same time.

- **Max. threads in queue**

- The maximum number of threads (DNS requests) that may be queued to wait for other threads to finish processing in the plug-in.

- **Plug-In Settings tab**

- This tab is available for plug-ins that have unique settings (for plug-in developers: `GetOptionsUI` returns an `OptionsUI` object).

- The content of this tab defines the behaviour of the plug-in and is different for each type of plug-in.

- **DNS Requests tab**

- This tab is available for all plug-ins that in some way process DNS requests (for plug-in developers: plug-ins not based directly on `IPlugInBase`).

- Specify when the plug-in should process a DNS request - either "Always", "Never", or "Only when...". With the default selection (Always), all DNS requests are processed by the plug-in.

- If the plug-in does a lot of work for each request (such as database lookups) it is recommended to limit this to specific domains, IP ranges, record types, etc. in order to optimize performance.

- With the later option (Only when...) you can construct a set of rules based on a combination of various properties of the DNS request etc.

See also: [Plug-Ins Overview](#)⁵³

3.1.2.5 Logging

3.1.2.5.1 Log Details

- **Log individual requests, responses, and other events**

- Select this option to log DNS requests and other events.

- **Include DNS record details**

- When checked, DNS request activity will be logged at the record level.

- **Include EDNS0 details (UDP payload size)**

- When checked, the EDNS0 details of DNS requests and responses will be logged.

- **Include outbound DNS requests**

- When checked, outbound DNS requests (to resolve DNS) and associated responses are logged.

- **Include requests from blocked IP addresses**

- When checked, DNS requests from blocked IP addresses³⁶ will be logged.

- **Only log Errors and Warnings**

- Select this options to only log events for potential problems.

- **Log internationalized domain names (IDNs) in native characters**

- When checked, all IDNs⁶⁰ will be logged in native characters (log files are UTF8 encoded).

See also: [How to read the log](#)

3.1.2.5.2 Log Files

- **Write full text log files to disk**

When enabled, Simple DNS Plus will write all DNS queries and responses to a log file.

- **Begin new log file**

Select how often a new log file should be created.

- **Recycle log files**

To conserve disk space select how often the log files should be recycled (overwritten with new data).

Log files can grow very big very fast. Recycling them is a good way to conserve hard disk space.

- **Write raw data of incoming DNS requests to disk**

If enabled, Simple DNS Plus will create additional "raw" log files of all incoming DNS requests.

This can be used to create domain / usage statistics and other purposes.

The Tools directory contains a command line tool to extract and filter raw log data and also a .NET programming library for accessing the raw log data.

See [Raw log file format](#)

- **Location of log files**

Specify the directory where log files are written.

Just like with other log files, system performance can be enhanced by writing log files to different physical disk drive (other than where the operating system is installed).

NOTE: Do not use a network drive location for this - because the Simple DNS Plus service runs under the SYSTEM account and therefore does not have access to network shares.

3.1.2.5.3 Syslog Server

- **Send log data to Syslog server**

When this option is enabled, Simple DNS Plus will send log data to a syslog server using the standard syslog protocol (RFC3164).

This can be useful for centralizing logging and/or taking advantage of various alerting and highlighting features of syslog server software.

Many different syslog server software packages are available for various operating systems. An example for Windows is the "Kiwi Syslog Daemon" from Kiwi Enterprises.

- **IP address**

The IP address of the syslog server.

- **UDP port**

The UDP port number of the syslog server.

The default value and standard UDP port number for syslog servers is 514.

- **Send test data**

Click this button to send a test log message to the syslog server at the IP address and UDP port above.

3.1.2.5.4 Active Log View

- **Lines in Active Log View**

The maximum number of log lines displayed in the Active Log View.

When this number of lines is reached, older entries are removed to make room for new ones.

In general we recommend the default value of 100.

Higher values can impact performance, but may be helpful when troubleshooting.

- **Buffer Active Log View**

When this option is enabled, Simple DNS Plus will continuously generate and buffer log data for the Active Log View.

This way the latest log entries will always be immediately available when you open the Active Log View.

This option can be very helpful for occasional troubleshooting, but generally it should be disabled to achieve the best performance.

See also: [How to read the log](#) and [Views](#)

3.1.2.5.5 Windows Event Log

- **Record selected events to the Windows Event Log**

With this option enabled, the events checked in the list are written to the Windows Event log (see Windows Control Panel / Administrative Tools / Event Viewer).

You can use the Windows Event Log to run scripts/programs, send e-mail notifications, or perform other actions whenever a specific event occurs.

To configure this:

- In Windows XP/2003 use the "eventtriggers" command line tool.
- In Windows Vista/2008 use the Windows Task Scheduler.

For details on the different events, see [Event IDs / Error Messages](#).

3.1.2.6 Remote Management

- **Enable Remote Management**

Check this to allow remote management of this server.

- **On IP address**

Select the local IP address that remote management clients connect to.

- **TCP port**

Specify the TCP port number that remote management clients connect to.

Note that the client connection dialog defaults to port 9053 when no port number is specified.

- **Password**

Specify a password to authenticate remote management client.

Background

You can manage the Simple DNS Plus service from a remote computer over your LAN or the Internet using the normal Simple DNS Plus user interface. This is faster and uses much less bandwidth compared to accessing a remote server via Remote Desktop, VNC, or similar.

Traffic between the server and the remote GUI is highly optimized and secure. Authentication uses

SHA-1 challenge/response to prevent password sniffing, all data transferred is encrypted, and larger data chunks (such as zone files) are compressed.

To remote manage Simple DNS Plus, install Simple DNS Plus on the client computer (optionally without the core service), and use the "Remote Management" shortcut in the Windows Start menu - or run "sdnsgui.exe -remote [remote-computer] [password]" / "editrecs.exe -remote [remote-computer] [password]".

3.1.3 IP Address Blocking dialog

Someone sending an extreme number of DNS requests in rapid succession may be a hacker trying to crash the server or prevent others from using the service.

You can use the functions in this dialog to automatically or manually block such hackers or IP addresses which for any reason run amok sending you DNS requests.

Please note that this feature does not block network traffic other than DNS requests - to block any other type traffic use a firewall.

If you enable automatic blocking, make sure to add any local computers and servers that you know may send a lot of DNS requests on the "Trusted IP Addresses" first.

Especially e-mail servers may send a lot of DNS requests to check the validity of incoming e-mails.

The "IP Address Blocking" dialog has 3 tabs:

- **Auto Blocking**

- **Automatically block IP addresses which send too many DNS requests too quickly (DOS attack)**

- Use to enable/disable automatic blocking

- **Max. DNS requests per second**

- When an IP address sends more than this number of DNS requests in one second, it will be automatically be blocked (an entry will be added to list on the "Blocked IP Addresses" tab) and further requests from this IP address are ignored.

- A typical workstation computer should not send more than 10-25 requests in one second, but we recommend you set this value to at least 30 so that no legitimate clients get blocked.

- **Block**

- Specify for how long automatic blocks should last (when/if the automatically added IP blocking should expire).

- **Blocked IP Addresses**

- List of IP addresses currently blocked. You can add, edit, and remove entries.

- When you add or edit an entry you can specify the IP address (single, range, or subnet) to block, for how long, and comments.

- To quickly remove multiple items from the list, you can hold down the Shift or Ctrl keys while selecting items and then click the "Remove" button.

- **Trusted IP Addresses**

- List of IP addresses are trusted and will not be blocked automatically. You can add, edit, and remove entries.

- When you add or edit an entry you can specify the IP address (single, range, or subnet) to trust, for how long, and comments.

- To quickly remove multiple items from the list, you can hold down the Shift or Ctrl keys while selecting items and then click the "Remove" button.

See also How to secure your server [\[4\]](#)

3.2 DNS Records window

The DNS Records window lists local zones [\[57\]](#) and DNS records in an explorer style window.

The zone list (left) shows all zones [\[57\]](#) currently defined, primary zones with a "P" icon, and secondary zones with an "S" icon.

Suspended zones [\[65\]](#) are indicated with a red "paused" symbol (two vertical lines) on the icon and a red name.

The record list (right) shows DNS records in the selected zone.

The optional zone folder list (above or to the left of the zone list) can be used to filter the zone list by zone type or zone group.

To edit the properties of an existing zone (left list) or record (right list), simply double click the item (see Zone Properties [\[43\]](#) and Record Properties [\[42\]](#) dialogs).

You can also right-click on a zone, on a record, or in an empty area of either list to quickly access related functions.

To quickly jump to a zone in the list, first click on any zone to ensure that the zone list has focus, then type the first few letters of the zone name. You can do the same in the records pane.

When you have a reverse zone [\[62\]](#) selected in the zone list, a reverse zone information panel will be available at the bottom of the DNS record list pane.

To easily edit reverse DNS records, click the "Edit IP-to-Name Mappings" button on this panel to open the Reverse zone IP-to-Name Mappings dialog [\[46\]](#).





The following functions are available in the DNS Records window menu:

- **File menu**


- **New** (also available from the tool bar)
 - **New Zone**
Opens the New Zone Wizard [\[40\]](#).
 - **New Record [different record types]** (only visible when a primary zone is selected)
Open the Record Properties dialog [\[42\]](#) to create a new DNS record in the currently selected zone.
 - **New Zone Group**
Creates a new zone group in the zone folder pane.
- **Zone** (also available by right clicking a zone name in the zone list)
 - **Suspend / Resume**
Suspends a zone, or resumes as suspended zone [\[65\]](#).
 - **Save** (also available from the tool bar)
Saves any changes made to the currently selected zone to disk.





- **Reload from Primary**
Forces the currently selected secondary zone to be zone transferred [\[67\]](#) from the primary DNS server.
- **Make Copy**
Make a copy of the currently selected zone.
- **Move to Group** (only available when the zone folders list is visible - see View menu below)
Moves the currently selected zone to a different zone group.
NOTE: You can also move a zone to a different group simply by dragging it with the mouse.
- **Delete** (also available from the tool bar)
Delete the currently selected zone.
- **DNSSEC Sign** (only available when primary zone is selected)
Opens the DNSSEC Sign Zone dialog [\[47\]](#).
- **Properties** (also available from the tool bar)
View/edit the properties of the currently selected zone or record.
- **Zone Group** (only available when the zone folders list is visible - see View menu below)
 - **Rename**
Renames the currently selected zone group.
 - **Delete**
Delete the currently selected zone group and all the zones in it.
- **Import**
Opens the Import Wizard [\[41\]](#).
- **Export**
Opens the Export Wizard [\[42\]](#).
- **Connect to Remote**
Opens a new instance of the DNS Records module connecting to an instance of Simple DNS Plus running on a remote computer.
NOTE: Remote Management must be enabled in the Options dialog / Remote Management section [\[35\]](#) on the remote Simple DNS Plus instance.
- **Exit**
Closes the DNS Records window.
- **Edit menu**
 - **Cut**
Copies the currently selected DNS records to the clipboard and removes them from the currently selected zone.
 - **Copy**
Copies the currently selected DNS records to the clipboard.
 - **Paste**
Pastes previously copied DNS records from the clipboard to the currently selected zone.

- **Paste As**
Pastes previously copied DNS records from the clipboard to the currently selected zone using a different record name.
- **Delete**
Removes the currently selected zone or DNS records - depending on which list (zone or record) has focus.
- **Select All**
Selects all DNS records in the currently selected zone.
- **Invert Selection**
Inverts the current selection of DNS records.
- **Properties**
Opens the Zone Properties dialog^[43] or the Record Properties dialog^[42] for the currently selected item depending which list (zone or record) has focus.
- **Set TTL**
Updates the TTL^[66] value of the currently selected DNS records.
- **View menu**
 - **Zone Folders**
Select where the zone folders list should be displayed in relation to the zone list pane.
 - **Sort Records By**
Select which column and in which order the DNS record list should be sorted.
NOTE: You can also sort the DNS records by clicking on the DNS record list column headers.
 - **IDN native characters**
Enables/disables display of native characters for IDNs^[60].
 - **Toolbar**
Display / hide the toolbar.
 - **Status Bar**
Display / hide the status bar at the bottom of the window.
 - **Auto refresh record list**
Enables/disables automatic refreshing of the record list when the the currently selected zone is updated by another process (zone file changed). For example when an updated copy of a secondary zone is fetched from the primary server, or when records in the zone are dynamically updated by a remote client, or when some external process updates the zone file.
 - **Refresh**
Reloads the currently selected zone (in case it was updated by another process).
- **Tools menu**
 - **Find Zone**
Quickly locate a zone in the zone list.
NOTE: This function only searches zones currently in the zone list. To search all zones makes sure to select "All zones" in the zone folders list (if displayed).

- **Find Next Zone**
Repeats the last "Find Zone" starting at the current selection in the zone list.
- **Quick Zone Wizard** (also available from the tool bar)
Opens the Quick Zone Wizard .
- **Bulk Update Wizard** (also available from the tool bar)
Opens the Bulk Update Wizard .
- **Check Internet Delegations**
Opens the Check Internet Delegations  wizard.
- **Count Zones**
Displays the total number of zones, primary zones, primary forward zones, primary reverse zones, secondary zones, and number of zones in the currently selected zone group (if any).
- **Default Zone Values**
Opens the Default Zone Values dialog .
- **Help menu**
 - **Contents & Index** (also available from the tool bar)
Display this help file.
 - **Online support**
Open the online support page in your browser.

3.2.1 New Zone Wizard

The New Zone dialog is used to create a new zone  of one of the following types:

- **Primary Zone**
Creates a "master copy" in which you create records for your domain name.
- **Forward Zone**
Creates a new primary forward zone.
You will be prompted to enter the zone name.
See also the Quick Zone Wizard  for even faster creation of primary forward zones.
NOTE: You can create a private root zone  by entering a single dot as the zone name - but only do this if your server is for an intranet and is not going to resolve any Internet domain names.
- **Reverse Zone**
Creates a primary reverse zone .
- **IPv4 (32 bit IP addresses)**
Creates a new primary reverse zone for IPv4 addresses.
You will be prompted to enter the first IP address, subnet mask and the zone name.
Enter the first IP address of your range of IP addresses and select the subnet mask according to the number of IP addresses you have.
If you have an IP address range of more than 256 IP addresses (class-C network), you should create a separate reverse zone for each class-C in that range. Reverse zones for larger subnets (/8 and /16) should only be use for delegations.
The zone name defaults to the standard in-addr.arpa  name. For subnets other than 255.255.255.0 (full class-C), you can change the zone name - or use the "Look Up" button to

automatically detect the reverse delegation name used by your IP provider.
After creating the zone, you can use the Reverse zone IP-to-Name Mappings dialog [\[46\]](#) to edit the individual reverse records (reverse zones for 256 IP addresses or fewer).

- **IPv6 (128 bit IP addresses)**

Creates a new primary reverse zone for IPv6 addresses.

You will be prompted to enter the first IP address and select a subnet mask bit size.

Enter the first IP address of your range of IP addresses and select the subnet mask bit size according to the number of IP addresses you have.

- **Alias Zone**

Creates a new primary zone which shares its records and settings with another zone.

Both zones will use the same file, so any changes made to one zone will immediately be reflected in the other.

You will be prompted to enter the new zone name and select the alias for zone (the zone to share the file with).

To later see which zones are sharing the same zone file, see the "Zone File" tab in the Zone Properties dialog [\[43\]](#).

- **Secondary Zone**

Creates a copy of a zone already configured on another primary DNS server for redundancy and load balancing. Records are created on the primary DNS server and automatically copied to this server through zone transfers [\[67\]](#).

You will be prompted to enter the zone name, the IP address of the primary DNS server, and optionally a TSIG key [\[65\]](#) for signing zone transfer requests.

3.2.2 Import Wizard

The Import Wizard makes it easy to migrate data from another DNS server implementation and/or import zone data from various sources.

You can import zones [\[57\]](#) in four different ways:

- **Import a single zone from another DNS server (zone transfer)**

Uses a standard zone transfer [\[67\]](#) to import the zone.

Security settings on the original server might prevent zone transfers. If this is the case, either adjust the security settings, or use one of the following options instead.

- **Import a single zone from a zone file**

Import any standard DNS zone file ([RFC1035](#)).

The zone file can be located on the same computer or in any network shared directory which you have access to.

- **Import a set of zone files listed in a DNS server boot/configuration file**

Import all or some of the zones from another DNS server.

The import wizard can read 3 different types of boot/configuration file formats:

- **Standard boot file**

This file format is used by earlier versions of Simple DNS Plus, BIND (Unix/Linux DNS server) prior to v. 8.0, and several other DNS servers.

This is a simple text file which has one line for each zone, listing authority (primary or secondary), zone name, primary IP address (secondary zones only), and the zone's file name.

- **Simple DNS Plus v. 5.x zone database files (`_zones.sdzdb`)**

Proprietary file format used by Simple DNS Plus v. 5.x.

- **BIND v. 8.0 or later configuration files (named.conf)**

Proprietary file format used by BIND (Unix/Linux DNS server) v. 8.0 and later. This is a text file format structured similar to C programming source code.

IMPORTANT - the boot/configuration file and the zone files must be located in the same directory. You may have to copy the files to a different location if they are arranged differently.

- **Import a list of domains names**

Creates a new zone for each domain name listed in file using the data from an existing zone (either copying it or sharing its zone file).

The file that you import from must be a simple plain text file containing a list of domain names. Each line in the file must contain a single domain name and nothing else. You can create such a file for example with Notepad, or with a spreadsheet program such as Excel using the "Save as" function to save in .txt format.

3.2.3 Export Wizard

The Export Wizard lets you export data from Simple DNS Plus in four different ways.

For all export options, you can select to export all zones or only the zones in specific zone groups, and whether or not to include suspended zones.

- **Zone List**

Generates a list (.csv file) of local zones^[57], including zone type and group.

The generated file can be imported into any software that reads ".csv" files, such as Microsoft Excel.

- **Standard boot file**

Simple DNS Plus uses an optimized proprietary database format for storing its list of DNS zones.

This function exports the zone list to a standard boot file (simple text based format) which most DNS servers can either use directly or import from.

- **Boot file for secondary DNS server**

Generates a standard boot file listing primary zones from this server as secondary zones. The generated file can be imported or used directly on a secondary DNS server. Some secondary DNS service providers offer a function to import such a file directly saving a lot of typing.

NOTE: If you are setting up another Simple DNS Plus server as secondary to this one, we recommend you use the Super Master/Slave^[23] feature to synchronize the two servers. This is much easier and will also automatically synchronize any later zone additions and deletions.

- **IP addresses to "hosts" or ".csv" file**

Scans local zones for A-records and generates a sorted list of IP address/host name pairs. This can be used to track which IP addresses are in use. The generated "hosts" file could also be used directly for simple name resolution.

3.2.4 Record Properties

The Record Properties dialog is used to specify a DNS record's name, data, TTL^[66], and comments.

The record name must be the same as or end with the name of the zone^[57] it belongs to (automatically enforced), and can only be entered when creating a new record.

To specify a wildcard record, enter an asterisk (*) followed by a period (.) and the rest of the name.

The asterisk can only be used as the first character, and only when immediately followed by a period.

The record data depends on the record type - see the individual record types^[68] for more information.

The "Record TTL^[66] (Time To Live)" field specifies how long other DNS server and clients are allowed to cache^[55] this record.

The "Record comments" field can be used to keep any additional information about the record such as what the record does, or a client account number.

For records created or updated via dynamic updates or HTTP, Simple DNS Plus will automatically enter a comment about how and when the record was created.

NOTE: This field is not transferred to secondary DNS servers through zone transfers [67].

For A-Records [68] and AAAA-records [69] there is a special "Update Reverse Zone" option.

This will create or update a PTR-record [76] in a reverse zone [62] to enable reverse lookups on the IP address.

For SPF-records [79] there is a special "Synchronize TXT-record" option.

This will create or update a TXT-record [79] with the same name and data as the SPF-record.

3.2.5 Zone Properties

- **General**

- **Role of this DNS server for this zone**

- Specify primary or secondary.

- If primary, specify the default TTL [66] for new DNS records in the zone.

- If secondary, specify the IP address of the primary DNS server to zone transfer [67] the zone from, and optionally the TSIG [65] key to sign zone transfer [67] requests with.

- **Zone Group** (only visible if zone folders are enabled from the View menu)

- Which zone group/folder the zone belongs to.

- **SOA Record**

- The SOA record [78].

- **Zone Transfers** (see How to secure your server [4])

- Specify which IP addresses are allowed to obtain this zone through zone transfers [67] (typically secondary DNS servers).

- Click the "Add IP addresses of zone's NS-records" button to automatically resolve and add IP addresses of zone level NS-records [74].

- **Notify**

- Specify which secondary DNS servers to notify when the zone has been updated on the primary server.

- **Dynamic Updates**

- Specify which IP addresses to accept standard (un-signed) dynamic update requests from for this zone (typically computers on the local network).

- IMPORTANT: Standard dynamic updates should only be used in a secure environment such as a private network.

- For updates sent over the Internet we recommend using TSIG signed [65] dynamic updates. You can configure this in the Options dialog / DNS / Local Zones / TSIG Updates section [26].

- **DNSSEC**

- Specify the default DNSSEC [55] key file for this zone.

- This file name will automatically be suggested when using the DNSSEC Sign Zone [47] function.

- Use the "Browse..." button to load an existing DNSSEC key file.

- Use the "Create new..." button to create a new DNSSEC key file.

- And use the "Edit..." button to edit an existing DNSSEC key file.

- **Zone File**

Displays the name of the zone file used to store this zone and a list of other zones using the same zone file.

- **Comments**

This is an open text area that can contain and comments or additional information about the zone that you need.

For example, for client account number or information about when the domain expires etc.

For new zones, Simple DNS Plus will automatically enter a comment about how and when the zone was created.

NOTE: This information is not automatically transferred to secondary servers through zone transfers [67].

3.2.6 Quick Zone Wizard

The Quick Zone Wizard automatically creates a new zone [57] with some pre-defined DNS records.

The standard default template contains the following variables / entry fields.

Replace "example.com" in the following with your own domain name:

Domain Name

Enter your domain name "example.com" (without the "www." prefix).

Web server IP (optional)

Enter the IP address of the web server for this domain name.

The wizard creates an A-record [68] for "example.com" with this IP address, and a CNAME-record [70] for "www.example.com" pointing to "example.com".

This allows visitors to access your web-site through both "www.example.com" and just "example.com".

Mail server IP (optional)

Enter the IP address of the e-mail server for this domain.

The wizard creates an MX-record [73] for "example.com" pointing to "mail.example.com", and an A-record [68] for "mail.example.com" with this IP address.

FTP server IP (optional)

Enter the IP address of the FTP server for this domain.

The wizard creates an A-record [68] for "ftp.example.com" with this IP address.

The wizard also automatically creates an NS-record [74] for the primary DNS server (this server), and a SOA-record [78] and NS-records [74] for secondary DNS servers as defined in the Default Zone Values dialog [46].

Clicking the "Use as Default" button will save the current values with the template and these values will automatically appear the next time you use the same Quick Zone Wizard template.

The Quick Zone Wizard is template based and supports multiple templates through a drop-down menu on the "Quick" button.

It is possible to modify the default template as well as adding your own templates. For details see <http://www.simplifiedns.com/quickzonetemplates.htm>

3.2.7 Check Internet Delegations

This feature lets you automatically test if the NS- [74] and SOA-records [78] in your local zone data match the actual current delegations on the Internet (the DNS server names listed in the domain name registrations).

This can be very useful both to check for errors and to make sure that you still own the domain names that you think you do.

It could also be used for example by ISPs to see if any customers have abandoned them (changed their DNS to another provider).

- **Test zones in all zone groups / Only test zones the zone group**
Specify which zone group(s) to check zones from.
- **Test primary zones**
Check this if primary zones should be tested.
- **Test secondary zones**
Check this if secondary zones should be tested.
- **Test suspended zones**
Check this if suspended zones should be tested.
- **Also test that each zone contains NS-records pointing to**
 - **The name of this server (<server name>)**
Compare zone's NS-record values to the local server's name.
 - **The default secondary servers (see Default Zone Values dialog)**
Compare zone's NS-record values to default secondary servers from Default Zone Values dialog [\[46\]](#).

3.2.8 Bulk Update Wizard

Use this wizard to quickly update many zones in a single operation.

For all update options, you can select to update all zones or only the zones in specific zone groups.

- **Find and replace IP address**
Replaces an IP address in host records (A-records [\[68\]](#) for IPv4 addresses / AAAA-records [\[69\]](#) for IPv6 addresses)
Use this option, for example, when changing the IP address of a server hosting web-sites or other services for several different domain names.
You must enter the old IP address and the new IP address of the server.
- **Find and replace host name**
Use this option to replace a host name in the data part of CNAME [\[70\]](#), MX [\[73\]](#), NS [\[74\]](#), PTR [\[76\]](#), RT [\[77\]](#), SOA [\[78\]](#), and SRV [\[79\]](#) records.
You must enter the old host name and the new host name, and select which record types to update.
- **Update DNS record TTL (Time To Live) values**
Use this option to update DNS record TTL [\[66\]](#) values.
You must enter the new TTL value and select which record types to update.
- **Update zone e-mail servers (MX-records)**
Use this option to replace zone level MX-records [\[73\]](#) (MX-records for sub-names will not be updated).
You can enter up to 5 different e-mail server host names and their preference values.
- **Update DNS servers (NS-[\[74\]](#) and SOA-records [\[78\]](#))**
Use this option, for example, when you add or change a DNS server hosting all of your domain names.
You must enter the primary DNS server name and up to 4 secondary DNS server names.

- **Update SOA-record data field values**

Use this option to update individual SOA-record [\[78\]](#) data fields.

You can select which data fields to update and which to leave at their current value.

- **Promote secondary zones to primary zones**

Use this option, for example, if your primary DNS server is permanently down/gone and you wish this secondary DNS server to become the new primary DNS server.

You must select what to do about secondary zones which have already expired (create empty primary zone, leave as secondary, or delete).

- **Update primary DNS server IP address for secondary zones**

Use this option on your secondary DNS servers when the IP address of your primary DNS server has changed in order to quickly update all your secondary zones.

You must specify the current primary DNS server IP address and the new primary DNS server IP address.

3.2.9 Default Zone Values

Use this dialog to specify default values for all new zones.

Most of these values correspond directly to values in the Zone Properties dialog [\[43\]](#).

- **SOA-record**

Specify the default values for new zone SOA-records [\[78\]](#).

- **Secondary DNS servers**

Specify the default secondary DNS servers for new zones.

An NS-record [\[74\]](#) for each of these will automatically be created in new zones.

- **Zone Transfers**

Specify the IP addresses that will be allowed to zone transfer (un-signed [\[65\]](#)) new zones by default. This should typically be the same as the secondary DNS servers.

Use the "Add IP addresses of secondary DNS servers" button to automatically resolve the secondary DNS servers (previous tab) and add their IP addresses to this list.

- **Notify**

Specify which secondary DNS servers to notify when the zone has been updated on the primary server.

- **Default TTL**

Specify the initial default TTL value for new zones.

3.2.10 IP-to-Name Mappings

Use this dialog to edit an existing reverse zone [\[62\]](#) without having to deal with "in-addr.arpa", reversing IP addresses etc.

To edit a record (IP to domain name), simply enter the corresponding domain name next to an IP address.

The fastest way to populate all the records is the "Auto Fill" function.

Enter a domain name, and all the records will be filled with something like "1-2-3-4.example.com", based on the IP addresses.

The "Auto Scan" function automatically populates the reverse records by scanning all forward zones for A-records [\[68\]](#) with IP addresses belonging to this reverse zone.

To create a new reverse zone, use the New Zone [\[40\]](#) function.

3.2.11 DNSSEC Sign Zone

- **DNSSEC sign the zone**

Check this option to DNSSEC [\[55\]](#) sign the zone.

- **Key file location** (only available when connected to remote server)

Specify if the key file is located on the remote server or on the local computer.

- **Key file**

The full path to the DNSSEC key file (containing keys used to sign the zone).

- **Browse** (only available for local files)

Click this button to browse the local file system for the key file.

- **Create new...**

Click this button to create a new key file - using the DNSSEC Key File dialog [\[47\]](#).

- **Edit...**

Click this button to edit an existing key file - using the DNSSEC Key File dialog [\[47\]](#).

- **Use above as the default DNSSEC key file for this zone**

When checked, the same key file will automatically be suggested the next time you sign the zone.

- **Generate and display a list of DS-records for inclusion in parent zone based on zone's DNSKEY-records with the Secure Entry Point (SEP) flag set**

Check this option to generate DS-records.

3.2.12 DNSSEC Key File

This dialog is used to create/maintain a DNSSEC [\[55\]](#) key file.

- **Key sets**

A list of DNSSEC key sets.

A zone which is signed using this key file will be signed with each of the key sets listed here.

Click the Add/Edit buttons to create/maintain individual key sets in the DNSSEC Key Set dialog [\[48\]](#).

- **Encrypt private keys for key sets**

Specify which private keys should be encrypted - None, All, or KSK only.

Specify a password by clicking the Password button.

You will be prompted for the password when signing a zone and one of the encrypted private keys are needed.

Note: Only encrypting KSK key sets makes it possible to re-sign a zone without the password as long as none of the key sets are changed/added/removed. For example, an assistant could re-sign the zone as needed when records were changed etc, but it would require a manager who knows the password to add/remove/update any key sets.

- **NSEC3**

When checked, NSEC3-records will be used instead of NSEC-records. See DNSSEC [\[55\]](#) for details.

- **Salt length**

Length of random salt value used in calculation of NSEC3 record-names.

- **Iterations**

The number of times NSEC3 record-names are hashed.

Note that while using multiple iteration increases security, it also puts additional load on the DNS server serving the zone because it has to calculate this for every single DNS request for non-existing records.

3.2.13 DNSSEC Key Set

This dialog is used to create/maintain a DNSSEC [55](#) key set.

- **Key set ID**

A unique identifier for this key set.

Only used to identify each key set for management purposes. Not part of actual keys/signatures.

Can be any value you want.

- **Key set type**

For details on the 3 key set types, see DNSSEC definition [55](#)

- **Algorithm**

Specify the algorithm to use for calculating signatures.

- **Key size (bits)**

Specify the key strength

- **Public key (DNS zone file format)**

The public key in DNS zone file format - only available when editing existing key set.

- **Signatures expire**

When signatures created with this key set will expire.

The RFCs recommend 13 months for KSKs, and 1 month for ZSKs.

- **DNSKEY only / Do not sign any record sets (key pre-publish / phase-out)**

Check this if you don't want any record sets signed by this key set (but still include the DNSKEY record).

This is typically used in "key pre-publish" scenarios.

3.3 DNS Look Up window

Use this tool to perform lookups against the local and/or other DNS servers.

See Look Up Types [51](#) for details.

The DNS Look Up window consists of a Menu [48](#), a Toolbar [49](#), Domain name entry field [49](#), Result display area [50](#), an Options pane [50](#), and a Status Bar [50](#).

Menu

- **File menu**

- **Look Up**

Choose one of the sub-items to do a specific look up type [51](#).

- **Stop Query**

Cancel to current DNS look up.

- **Exit**

Closes the DNS Look Up window.

- **Edit menu**
 - **Copy selection**
Copy the current selection in the result display area^[50] to the Windows clipboard.
 - **Copy full response**
Copy everything in the result display area^[50] to the Windows clipboard.
- **View menu**
 - **DNS/WHOIS Options**
Shows/hides the Options pane^[50].
 - **IDN Native Characters**
Enables/disables display of native characters for IDNs^[60].
 - **Toolbar**
Shows/hides the toolbar^[49].
 - **Status bar**
Shows/hides the status bar^[50].
- **Help menu**
 - **Contents & Index**
Opens this help file
 - **On-line support**
Opens the support web-page in your Internet browser.

Toolbar

- **Look Up button**
Choose one of the sub-items to do a specific look up type^[51].
- **Stop button**
Cancel to current DNS look up.
- **Copy button**
Copy text from the result display area^[50] to the Windows clipboard.
- **Options button**
Shows/hides the Options pane^[50].
- **Help button**
Opens this help file

Domain name entry field

Enter the domain name or IP address to look up.

Result area

Shows the result of the look up.

Options pane

The Options pane is only visible (to the right of the result area) when enabled in the View menu or the Options button on the Tool Bar.

• **DNS Options**

- **DNS Server**

Specify the host name or IP address of the DNS server to do the look up against.

- **Port number**

The DNS server port number to do the look up against (usually 53).

- **Use TCP connection (virtual circuit)**

Most DNS requests, except for zone transfers, are sent over UDP. However in some situations it can be beneficial to test if a DNS server also responds via TCP (which it should). This is also known as VC or "virtual circuit" in the classic NSLOOKUP command line tool.

- **Request recursion (RD flag)**

When checked (default), the DNS server will be asked to resolve the query if it doesn't have the answer in cache.

Not all DNS servers accept requests for recursion (also an option in the Simple DNS Plus).

- **Include EDNS0 options**

When checked, the following EDNS0 (extended DNS) will be included in the DNS request.

- **UDP payload size (bytes)**

Specify the maximum response packet size for UDP requests.

This can be useful for testing certain requests which return large response messages.

For example, IPv6 records were recently added for the Internet .com and .net top level names, making the full referral message for these domains larger than the standard 512 DNS message size.

- **DNSSEC OK (DO flag)**

Ask the DNS server to return DNSSEC signed data if available.

- **Checking Disabled (CD flag)**

Ask the DNS server not to check DNSSEC signatures.

• **WHOIS Options**

- **WHOIS server**

Specify the host name or IP address of the WHOIS server to do the look up against.

If "Auto" is selected, the tool will automatically try to determine the server name / IP addresses.

- **Port number**

The WHOIS server port number to do the look up against (usually 43).

Status Bar

Shows the current status of the look up process.

3.3.1 Look Up Types

Forward DNS lookup

To do a forward (normal) DNS lookup, first enter the domain name that you want to look up, and then select one of the record types in the first section of the lookup menu or in the "Other record type" sub-menu.

Reverse DNS lookup

To do a reverse lookup (IP address to domain name), simply enter the IP address as the domain name, and do a PTR-record look up. The IP address will automatically be converted to a reverse DNS domain name.

"Any DNS record" lookup

This type of lookup will return DNS records of any type for the requested domain name.

This is NOT necessarily the same as "all" records for the domain name.

If the DNS server that you sent the request to happens to have some records cached for the domain name, it will simply return those.

The records that the DNS server has cached may be the result of a previous lookup for a specific record type and/or different record type for the domain name may have different TTL values, and therefore the DNS server cache may not contain all available records type for a domain name.

The only way to ensure that an "any DNS record" lookup returns all the records for a domain name is to query one of the authoritative DNS servers for the domain directly.

NOTE: Some DNS servers are configured to refuse DNS requests for "ANY" record type.

Zone Transfer lookup

This will list all the records in a zone.

Zone transfers are typically used by secondary DNS servers to synchronize a DNS zone with the primary DNS server.

NOTE: Most DNS servers are (and should be) configured to only allow TSIG signed zone transfers (not possible in Look Up Window) and/or zone transfer requests from specific IP addresses - typically secondary DNS servers.

BIND Version lookup

This can be used to send a special DNS request asking for the software version of a BIND DNS server (a Unix/Linux DNS server).

Default BIND DNS server configurations will return the version number of the BIND software.

However for security reasons, many DNS servers (BIND and others) are configured not to respond to such requests, or to respond with some message indicating that they won't tell you their version number.

Simple DNS Plus can also be configured to respond to BIND version requests - see Options dialog / DNS / Miscellaneous section.

WHOIS lookup

The WHOIS look up function provides detailed information (such as name, address and phone) about the owners of a domain name or IP address.

This is done through special WHOIS servers maintained by the organizations responsible for the top level domains ("TLDs") around the world.

Simple DNS Plus comes with a recent list of these servers and will automatically select the best match when the "Auto WHOIS Server" option in the Tool menu is selected (default). You can add new WHOIS servers to the list by manually editing the "whois.dat" file found in the Simple DNS Plus directory.

If you do a WHOIS lookup for a top level domain not listed in the "whois.dat" file, the lookup tool will try to use the server name "whois.nic." + the last segment of the domain name entered, as this is the most common WHOIS server name.

3.4 DNS Cache Snapshot window

The DNS Cache Snapshot window displays the currently cached [\[55\]](#) records in an explorer style window.

Domain names displayed in the left list are organized in the DNS tree structure from the root up - or backwards compared to a full domain name.

To locate "www.example.com" in the tree, first open "<root>", then "com", then "example" and finally "www".

The right list shows any DNS records for the selected domain name.

The following functions are available in the DNS Cache Snapshot window menu:

- **File menu**
 - **Find**
Quickly locate a domain name in the list.
 - **Exit**
Closes the DNS Cache Snapshot window.
- **View menu**
 - **IDN Native Characters**
Enables/disables display of native characters for IDNs [\[60\]](#).
 - **Negative (Non-existing records)**
Enables/disables display of negative DNS records.
 - **Status Bar**
Shows/hides the status bar.
- **Help menu**
 - **Content & Index**
Opens this help file

- **On-line help**
Opens the support web-page in your Internet browser.

4 Plug-Ins

Simple DNS Plus has a plug-in system for providing additional/optional functionality. This allows us and 3rd parties to develop new features without cluttering the base product, and allowing users to select which of these features they want - or don't want.

The standard Simple DNS Plus installation comes with the following plug-ins:

- **DHCP Server**
A basic DHCP server which provides IPv4 addresses and settings to local computers and devices. The DHCP data is also used to serve DNS requests (forward and reverse) making it very simple to locate any local DHCP client by name on a local network.
For details see KB1216.
- **Domain Blacklist**
Redirects DNS requests for domain names on a blacklist. Can be used to block banner ads, malicious web-sites, porn web-sites, etc. Doing this at a central DNS server makes it easy to enforce company/family policy for your entire network. You can direct browser requests for listed entries either to a dummy IP address, or to an IP address of your own web-server where you serve up some type of "not allowed" message.
For details see KB1253.
- **DynDNS Service**
Makes it easy to run your own "DynDNS" service (just like dyndns.com, no-ip.com, tzo.com, etc.). Besides from running a public DynDNS service, there are many possible uses for this. For example making it easy to connect with company road warriors, branch offices, etc.
A DynDNS service makes it possible to connect, using a static host name, to any kind of service including web-server, mail-server, remote desktop, VPN, etc. running on a computer with a dynamic Internet IP address.
For details see KB1267.
- **Fixed Host Name**
Serves a fixed host name - either to all DNS requests as a CNAME (70) (alias), or to DNS requests for MX (73), NS (74), and/or PTR-records (76).
For details see KB1263.
- **Fixed IP Address**
Serves a fixed IP address (IPv4 and/or IPv6) to all DNS requests for host records (A (68) / AAAA (69)). This can be used as a simple way to host DNS records.
For details see KB1261.
- **Hosts File**
Serves host (A (68) / AAAA (69)) and reverse (PTR (76)) DNS records from a standard hosts file (60).
For details see KB1210.
- **HTTP Redirector**
Redirects HTTP requests for specified host names (and optionally all sub-names). Redirection can be done either "cloaked" in a frame page (redirect URL not visible in browser) or through a standard 302/301 status response.
The redirect-to URL can be either relative (requested path/query appended) or an exact URL with optional substitutions for host name, path and/or query string.
This can be used for example to redirect to a web-server running on a dynamic IP address

(redirecting to a host name updated by a dynamic DNS service) and/or to redirect to a web-server on a non-standard port number (like "http://www.example.com:8000"). These types of redirection services are often offered by domain name registrars and resellers.
For details see KB1258.

- **Ignore DNS Request**

Instructs Simple DNS Plus to ignore (not answer) all DNS requests processed by the plug-in. This can be used to ignore requests from specific IP addresses, for specific domain names, record types, etc.

As an example, you could configure it to ignore DNS requests from IP addresses listed by a blacklist plug-in.

For details see KB1280.

- **MS SQL Server**

Queries a Microsoft SQL Server for host records and optionally reverse records.

For details see KB1211.

- **MS SQL Server Plus**

Queries a Microsoft SQL Server for one or more DNS records of any type.

(Requires an "Unlimited zones" license)

For details see KB1249.

- **Regular Expressions**

Use Regular Expressions to pair host domain names to IP addresses. More powerful and flexible than simple wildcard records.

For details see KB1212.

- **Skip**

Used to skip other plug-in instances when processing DNS requests.

This is typically used to apply one or more conditions (in the "DNS Requests" tab) to several other plug-ins at the same time.

For details see KB1262.

- **Weighted Round Robin**

Serves IP addresses (A⁶⁸ / AAAA⁶⁹ records) for a host name round robin⁶⁴ from a weighted list.

IP addresses are rotated so that the first visitor gets one IP address, the next visitor another IP address, etc. However IP addresses with higher weight values are served more often than IP addresses with lower weight values. This makes it possible for example to send more traffic to high capacity servers in a round robin set.

For details see KB1252.

Additional plug-ins are available for download from <http://www.simplesdns.com/kb.aspx?kbid=1271>

Plug-ins are instantiated in the Options dialog / Plug-Ins section³².

Some plug-ins (including the DHCP Server plug-in) have their own View¹⁸ - a dockable sub-window in the main window¹⁶.

The plug-in architecture is open for users and 3rd parties interested in developing their own plug-ins. In short, this is all based on the .NET Framework 2.0 interfaces found in the "sdnsplugin.dll" file supplied with Simple DNS Plus. More information about developing plug-ins is available on-line in KB1281.

5 Definitions

5.1 Authoritative

A DNS server is said to be authoritative for a domain name when it hosts the DNS records for that domain name.

An authoritative DNS server for a domain name is configured with a local DNS zone [57] for the domain name and its sub-names.

Both the primary and the secondary DNS servers for a domain name are considered authoritative.

An authoritative DNS server for a domain name responds with "Authoritative Answers" for the domain - as indicated by the "AA" header flag set in responses.

5.2 Caching

Each time a recursive [61] DNS request is made to Simple DNS Plus, it caches (stores in memory) the different DNS records it comes across while searching for the requested records.

The cached DNS records are then used to locate information faster for following DNS requests.

By default, cached DNS records are stored until they time-out based on their TTL [66].

Most DNS servers will not cache a DNS record for more than one week. This is also the default in Simple DNS Plus, but you can change this through the "Maximum cache time" option.

To view a snapshot [52] of the currently cached records, from the main window [16] click the "Cache" button or press F4.

To empty the cache, from the main window [16] select File menu - > Clear DNS Cache

Or use the "-C" command line option [15].

Or use the "clearcache" HTTP API [12] command.

You can change the various options related to DNS caching in the Options dialog / DNS / Resolver / DNS caching [21] section.

5.3 DNSSEC

Similar to digital signatures for e-mail, DNSSEC authenticates that DNS records originate from an authorized sender (DNS server) using private/public key cryptography.

The main purpose of this is to protect DNS against falsified information (DNS spoofing [4]).

DNSSEC does NOT encrypt or hide anything - all data is still in "clear text". Its only purpose is verification of data authenticity.

Signing a zone

When a zone [57] is DNSSEC signed, a number of DNS records are added to the zone. Indeed DNSSEC signing a zone can make it many times larger.

First a DNSKEY-record [71] is added for each private/public key set used to sign the zone.

DNSKEY-records hold the public keys that clients can use to verify signatures.

Next, an NSEC-record [75] or NSEC3-record [76] is added for each unique record name in the zone (+ a single NSEC3PARAM-record [76] if using NSEC3).

Each NSEC/NSEC3 record lists all the record types that exist for the name that it represents, and points to the next record name in the zone forming a chain between all existing names in the zone. These (signed) NSEC/NSEC3 records are returned in responses to DNSSEC enabled queries (DO

flag set) for non-existing names/types, so that clients can verify the non-existence. Finally, all the DNS records in the zone (including the DNSKEY and NSEC/NSEC3 records) are signed by adding an RRSIG-record for every unique record name and type combination in the zone. RRSIG-records for the records they sign are returned in responses to DNSSEC enabled queries.

Delegation / link of trust

There are no 3rd party certification authorities involved with DNSSEC - you create your own private/public key sets (see DNSSEC Key File dialog). In order to establish a "link of trust" so that other Internet users can verify your keys and signatures, you create a DS-record (delegation signature) containing a cryptographic hash of one of your DNSKEY-records (see KSK below). This DS-record needs to be included and "counter signed" in the parent zone. For example if your domain name is "example.se", the DS-record needs to be added to the ".se" zone. The procedure for "uploading" the DS-record depends on your parent zone / TLD operator, and/or your domain name registrar. The DNSSEC Sign Zone dialog includes an option to create the DS-record.

Key types - KSK, ZSK, Simple

RFC4641 (DNSSEC Operational Practices) defines two key types; "Key Signing Key" (KSK) and "Zone Signing Key" (ZSK).

Typically a zone is signed with both a KSK and a ZSK.

KSKs only sign the public key records (DNSKEY) for a zone, and usually have a long validity period (like 13 months).

KSKs are used as "Secure Entry Points" (SEP), and are referenced in parents zones through a DS-record (see above).

ZSKs sign all the record sets in a zone, and usually have a shorter validity period (like 1 month).

ZSKs are not Secure Entry Points, and are not referenced directly in parent zones.

This arrangement allows a zone operator to change his keys (ZSKs) more frequently without having to update the delegation signature in the parent zone.

Note that when the signatures for either of these keys are about to expire, new keys and signatures must be added, so that in overlapping periods a zone might be signed by 3 or 4 different keys at the same time.

Using KSK/ZSKs also makes it possible to re-sign a zone with the ZSK as needed without access to the KSK private key as long as no keys are changed, allowing the KSK private key to be stored in a more secure manner.

In Simple DNS Plus, DNSSEC keys are stored in a special key file with an option to password encrypt private keys - optionally only for KSKs.

For example, using a key file where only KSKs are password protected, an assistant could re-sign the zone as needed when records were changed etc, but it would require a manager who knows the KSK password to add/remove/update any DNSSEC keys.

Simple DNS Plus also supports a 3rd key type - "Simple".

This is basically a combined KSK and ZSK - a key used as a Secure Entry Point and also to sign all record sets in a zone.

This is just a simpler model which may be easier to use in some scenarios - but of course doesn't provide the benefits of KSK/ZSK separation.

Off-line signing / dynamic DNS data

To protect private keys and because DNSSEC signing is a very CPU intensive operation, DNSSEC was designed for signing to be done off-line.

In other words, DNS-records are pre-signed so that the private keys can be stored off-line and the DNS server doesn't have to calculate signatures for every request. Note that adding/deleting records in a zone not only requires calculating new signatures for new records, but also requires re-creating the NSEC/NSEC3 records and re-calculating their signatures.

This makes it impractical to use DNSSEC with any type of dynamic DNS data.

WARNING: Several options^[19] in Simple DNS Plus provide dynamic and/or synthesized DNS records, which will not automatically be DNSSEC signed. So make sure not to use those options in any way that would result in serving un-signed records under a domain that should be signed.

Current state of DNSSEC

DNSSEC is not yet widely supported by operating systems or client applications, so practical use is limited at this time (April 2009).

However, this may change soon as several countries, including Brazil (.br), Bulgaria (.bg), Czech Republic (.cz), Puerto Rico (.pr) and Sweden (.se), have now DNSSEC signed their TLDs, and the U. S. government recently mandated that all federal agencies (.gov) must implement DNSSEC by the end of 2009.

DNSSEC has been under way for more than a decade, and has been the subject of many changes and much controversy over the years.

A significant obstacle for DNSSEC is that the Internet DNS root is not signed yet. This is stuck in international politics (has been for years), because this is ultimately about who gets to hold the "master key" to the entire Internet.

Until this happens, DNSSEC enabled resolver / client programs need to manually maintain a list of "trust anchors" for domains they want to verify, making it rather cumbersome.

DNSSEC support in Simple DNS Plus

Simple DNS Plus v. 5.2 supports hosting DNSSEC signed zones (responds with additional DNSSEC records when the DO-flag is set in requests) and has GUI functions for managing DNSSEC keys and for signing zones.

However it does not request or validate DNSSEC signatures while resolving other Internet domain names. We expect to be adding this in future versions when DNSSEC is more widely implemented and supported by client applications.

To DNSSEC sign a zone^[57], in the DNS Records window^[37], right-click a primary zone in the zone list and select "DNSSEC sign..." from the pop-up menu. This opens the DNSSEC Sign Zone dialog^[47].

RFCs

DNSSEC is defined in RFC3225, RFC4033, RFC4034, RFC4035, RFC4641, and RFC5155.

5.4 Domains vs. Zones

Domains are broken into zones for which individual DNS servers are responsible.

A "domain" represents the entire set of names / machines that are contained under an organizational domain name.

For example, all domain names ending with ".com" are part of the "com" domain.

A "zone" is a domain less any sub-domains delegated to other DNS servers (see NS-records^[74]).

A DNS server could be responsible (authoritative^[55]) for all records under the "xyz.com" domain, but by defining NS-records^[74] for "abc.xyz.com", this part of the domain is delegated to other DNS servers - and possibly a different company/entity.

A zone contains exactly one SOA-record^[78] describing the general properties of the zone, and any number of other DNS records.

Entire zones can be transferred from a primary DNS server to secondary DNS servers through Zone Transfers^[67].

To create a new zone use the New Zone^[40] function by clicking the "New" button in the DNS Records window^[37].

5.5 Dynamic DNS update

Dynamic DNS updates are used to create and update DNS records directly via the DNS protocol.

Simple DNS Plus supports standard (un-signed) dynamic updates ([RFC2136](#)) and TSIG^[65] signed dynamic updates ([RFC2845](#)).

Standard dynamic updates are configured for each primary zone in the zone properties dialog^[43]. TSIG signed dynamic updates are configured by setting up keys in the Options dialog / DNS / Local Zones / TSIG Updates section^[26].

Standard dynamic updates can be secured by specifying which IP addresses are allowed to send such updates.

This is simple and efficient in a secure environment such as an intranet.

For updates sent over the Internet where the originating IP address may not be known beforehand (dynamic IP) and does not guarantee the identity of the sender (IP spoofing), the dynamic DNS update can be authenticated using a transaction signature (TSIG).

This is a method of cryptographically signing the update data with a key name / value pair (similar to a user name / password pair).

The key name identifies the client to the DNS server, and the key value is a shared secret known only by this client and the DNS server.

Client applications supporting dynamic DNS updates:

- Recent versions of Microsoft Windows (Me, 2000, and later) have a TCP/IP option "Register this connection's addresses in DNS" which uses dynamic DNS update to automatically update DNS records for itself.
Standard dynamic updates are used by default. TSIG authenticated updates are not supported.
- Several Internet dynamic IP address update clients support TSIG authenticated dynamic DNS updates.
For example: "DynSite" from <http://noeld.com/dynsite.asp> or "DirectUpdate" from <http://www.directupdate.net>

See also:

The DynDNS Service plug-in^[53] (see <http://www.simpledns.com/kb.aspx?kbid=1260>) also supports TSIG signed dynamic updates over DNS as well as several HTTP based update methods and is specifically targeted towards "DynDNS" scenarios (computers with dynamic IP addresses on the Internet).

5.6 Forwarding

When Simple DNS Plus receives DNS request for a domain name configured for forwarding (Options dialog / DNS / Forwarding section^[27]), it skips the normal DNS resolution^[61] process and instead forwards the DNS request to the specified DNS servers asking them to do the resolution work for it.

If local data (own zones / cached records) matching the DNS request already exist, the request will not be forwarded, but rather replied to immediately using this local data.

This also means that setting up DNS forwarding for a domain name which is also a local zone has no effect - data will always be served from the local zone and requests are never forwarded (with the exception of "shadow forwarding" - see below).

You can configure Simple DNS Plus to use forwarding for all domain names and/or for specific domains (including their sub-names), and to use extended and shadow forwarding:

Forwarding for all domain names

You can use forwarding for all domain names, for example, if you have multiple local DNS servers and wish to build up a central cache on one or a few DNS servers, thereby limiting the DNS traffic sent over your Internet connection.

In this case you would setup one (or a few) DNS servers (the central servers) to do normal resolution with no forwarding, and setup the remaining DNS servers to forward requests for all domains to these central servers.

IMPORTANT: We have noticed that for no apparent reason many users have configured Simple DNS Plus (and other DNS servers) to forward DNS requests for all domain names to their ISP's DNS servers.

Generally we do NOT recommend doing this.

Simple DNS Plus is fully capable of resolving any Internet domain name without the help of any forward DNS servers.

Very often forwarding to your ISP's DNS servers only make resolution slower, as this adds another lookup step to the resolution process, and often ISP DNS servers are overloaded and slow to respond. By forwarding DNS requests to your ISP's DNS servers, you also inherit any security issues that those DNS servers might have.

For example, if your ISP's DNS servers are spoofed - so is your DNS server.

However in certain situations, for example, if your Internet connection is slow, it may be appropriate to forward DNS requests to your ISP in order to limit traffic on your own connection and take advantage of DNS caching on your ISP's DNS servers.

Domain specific forwarding (a.k.a. "conditional forwarding")

You can use domain specific forwarding, for example, if you wish to be able to resolve both Internet domain names as well as a private domain name hosted on another DNS server.

In this case you would configure forwarding specifically for the private domain name only.

Extended Forwarding

Standard forwarding only forwards recursive DNS requests, and only when the request originates from an IP address which is offered recursion (Options dialog / DNS / Recursion section).

However Simple DNS Plus also has a unique "extended forwarding" option which, when enabled, causes ALL DNS requests for the specified domain and sub-names to be forwarded.

There are several scenarios in which you might want to do this, for example:

- You are hosting part of your DNS data on a separate DNS server, but you only have one public IP address available for hosting DNS.
- You are hosting some or all of your DNS data on a separate specialized DNS server (for example; an RBL list server) which requires a lot of resources (for example; serving data from a database), and you want to offload this by having Simple DNS Plus sit in front of it caching the data, and thereby causing fewer requests to hit the specialized DNS server.
- You are hosting some or all of your DNS data on a separate DNS server which you don't want to expose directly to the Internet (for example; if you have to use some other DNS software with known vulnerabilities). Simple DNS Plus will only forward standard DNS requests, only for the specified domain name, and it automatically filters out most malformed data.

In all 3 scenarios, you can setup Simple DNS Plus on a computer with both a private IP address and a public IP address (or with a public IP address NAT mapped to it), setup the other DNS server on an private IP address only, and configure Simple DNS Plus to use extended forwarding for domains hosted on the other DNS server.

Shadow Forwarding

Standard DNS forwarding only forwards request which are not for the name or sub-name of a local DNS zone.

However Simple DNS Plus also has a unique "shadow forwarding" option which, when enabled, causes DNS requests for the name or sub-name of a local DNS zone to also be forwarded when no matching DNS records exist in that zone.

5.7 Hosts file

Before DNS servers were invented, domain name translation depended entirely on the "hosts file", a text file stored on a server or the PC. The hosts file listed, line by line, Internet domain names and their associated IP addresses. The "master hosts file" was compiled and stored on the machines at the Internet "NIC" and was downloaded on a regular basis by everyone accessing the Internet (not many at the time). Obviously this hosts file quickly grew much too large to be manageable. As the Internet grows, new domain names are added by the minute, and it is impossible for every computer on the Internet to keep downloading this file.

The solution of course was the DNS server system. Unlike the hosts file, DNS servers don't rely on a single large mapping file. Instead DNS servers only contain information about the domain names they are directly responsible for and some limited reference data on how to find other domain names.

Computers can still use the "hosts" file for name to IP-address translation instead of DNS, and this works fine on a small network where there are few changes and a limited number of computers to maintain.

On Windows computers, the "hosts" file is located in the following directories:
Windows XP, 2003, Vista and 2008: "c:\windows\system32\drivers\etc"
Windows NT4 and 2000: "c:\winnt\system32\drivers\etc"
Windows 95, 98 and Me: "c:\windows"

A sample "hosts" file is supplied with Windows named "hosts.sam" located in the same directory.

Please note that the hosts file must be named "hosts" without any extension and it must be located in the above directories for Windows to automatically use it without a DNS server.

One popular use of hosts files today is to block banner ads and other unwanted Internet content. For example, pointing "ad-images.example.com" to 127.0.0.1, would prevent anything including banner ad images from being downloaded from that domain. This may also help to conserve bandwidth and actually make Internet surfing significantly faster. Some web-sites offer hosts file for download with updated lists of ad servers, malicious contents, etc.

With Simple DNS Plus you can easily share one or more hosts file between all computers on your local network using the Hosts File plug-in⁵³ making it easy to maintain this in just one place.

5.8 Internationalized domain names (IDNs)

Technically the DNS protocol is limited to standard ASCII characters (byte values 0-127), which does not include any non-english characters.

However in some recent end-user applications, like FireFox and Microsoft Internet Explorer 7, it is now possible to use domain names containing non-english characters - so called "internationalized domain names" or "IDNs".

This is done by puny-encoding (RFC3492) the IDN behind the scenes so that the domain name sent to the DNS server and web-server is in an encoded form containing only the standard characters allowed in the DNS protocol.

Puny-encoded domain name segments (between dots) always starts with "xn--". Each domain name segment is encoded separately, and only domain names segments which contain international characters are encoded.

You can say that an IDN has two display forms:

- "native character form" containing international characters.
- "puny-encoded form" containing only ASCII characters and where some or all segments start with "xn--".

For example, if you enter the domain name `www.東京.net` (`www.tokyo.net` in Japanese) into FireFox or IE7, the browser will convert this into "`www.xn--1qs71d.net`" (the puny-encoded form) before sending it to the DNS server and web-server.

It is important to note that the server (DNS, web, etc.) will only see the puny-encoded form of the IDN, not the native character form entered by the user.

So if the server software does not have direct support for IDNs, you must use the puny-encoded form of the IDN when configuring the server software, for example, when setting up a web-site in IIS or Apache.

Simple DNS Plus has direct support for IDNs and automatically converts IDNs to the puny-coded form behind the scenes.

You can enter IDNs in either form (native characters / puny-encoded). Both ways will result in the same data and works equally well.

You can choose to display IDNs in either form in the DNS Records^[37], DNS Look Up^[48], DNS Cache Snapshot^[52] windows through the View menu / IDN Native Characters function in each of those windows.

NOTE: On older Windows versions some international characters may not display correctly or at all depending on regional settings and fonts installed.

You can also choose in which form to log IDNs in DNS requests and responses. See Options dialog / Logging / Log Details^[33] section.

5.9 Recursion

DNS requests can either be "recursive" or "non-recursive".

Client applications (such as Internet browsers) request that the DNS server performs recursion for them by setting an RD (Recursion Desired) flag in the request packet. This is a recursive request. Client applications do this both because they do not possess the ability to resolve domain names themselves, and also to take advantage of centralized caching^[55] on the DNS server.

However, when a DNS server sends requests to other DNS servers as part of the recursion process, these requests are typically non-recursive (the RD flag is not set).

The DNS server indicates back to the client if it is willing to perform recursion by setting or not setting an RA (Recursion Available) flag in the DNS response packet.

When a DNS server receives a recursive request from a client that it is willing to perform recursion for, it will go through the process of resolving the requested domain name by first asking the root servers^[64], which respond with a referral to the top level DNS servers, then asking one of those servers, which respond with a referral to the next level DNS servers, etc.

When a DNS server receives a non-recursive request or a request from a client that it is not willing to perform recursion for, it typically responds immediately with whatever local data it has available at the time without doing any additional processing.

Simple DNS Plus can also be configured to respond to such requests with an error, with synthesized records, or not respond at all. This is configured in the Options dialog / DNS / Lame Requests section [\[27\]](#).

A recursive DNS request requires much more processing by the server compared to a non-recursive request.

So it is important to configure Simple DNS Plus to only offer recursion to trusted clients.

You can configure this in the Options dialog / DNS / Resolver / Recursion [\[21\]](#) section.

NOTE: For programs like browsers and e-mail clients to work, they must have access to a DNS server that offers recursion. Therefore local computers (including the server itself) should always be offered recursion.

5.10 Reverse DNS

Reverse DNS is IP address to domain name mapping - the opposite of forward (normal) DNS which maps domain names to IP addresses.

Reverse DNS is maintained in a separate set of data from forward DNS.

For example, forward DNS for "abc.com" pointing to IP address "1.2.3.4", does not necessarily mean that reverse DNS for IP "1.2.3.4" points to "abc.com".

Reverse DNS is mostly used by humans for such things as tracking where a web-site visitor came from, or where an e-mail message originated, etc.

Reverse DNS is typically not as critical in as forward DNS - visitors will still reach your web-site just fine without any reverse DNS for your web-server IP or the visitor's IP.

However there is one important exception: Many e-mail servers on the Internet (including AOL's) are configured to reject incoming e-mails from any IP address which does not have reverse DNS.

So if you run your own e-mail server, reverse DNS must exist for the IP address that outgoing e-mail is sent from.

In most cases it does not matter what the reverse DNS record for your IP address points to as long as it is there. If you host multiple domains on one e-mail server, just setup a single reverse DNS record to point to whichever domain name you consider primary.

(e-mail servers checking for reverse DNS know that it is normal to host many domains on a single IP address and it would be impossible to list all those domains in reverse DNS for the IP).

A special PTR-record [\[76\]](#) type is used to store reverse DNS entries.

In Simple DNS Plus, a zone [\[57\]](#) for reverse DNS records is created using the New Zone [\[40\]](#) function in the DNS Records window [\[37\]](#).

Reverse records can also be created automatically by checking "Update reverse zone" in the Record Properties [\[42\]](#) dialog when editing A-Records [\[68\]](#) or AAAA-records [\[69\]](#).

Reverse DNS is also different from forward DNS in who points (delegates) the zone to your DNS server.

With forward DNS, you delegate the zone to your DNS server by registering that domain name with a registrar.

With reverse DNS, your Internet connection provider (ISP) must delegate the reverse zone to your DNS server.

Without this delegation from your ISP, your reverse zone will not work.

IPv4 specifics

For IPv4, the name of a reverse DNS PTR-record is the IP address with the segments reversed + ".in-addr.arpa".

For example, the reverse DNS entry for IP "1.2.3.4" would be stored as a PTR-record for "4.3.2.1.in-addr.arpa".

If you are assigned the class C network 1.2.3.X, your ISP can delegate DNS authority for the "3.2.1.in-addr.arpa" domain name to your DNS server.

Your DNS servers should in this case have a zone^[57] called "3.2.1.in-addr.arpa" containing PTR-records^[76] for all active IP addresses in the class C network (1.2.3.0 - 1.2.3.255).

Simple DNS Plus provides an easy to use Reverse zone name-to-IP mappings dialog^[46] which makes it easy to maintain reverse IPv4 zones and records (without dealing with "in-addr.arpa", reversing IP addresses etc.). This is accessible from the bottom of the DNS Records window^[37] whenever an IPv4 reverse zone is selected.

It is also possible to delegate "in-addr.arpa" authority for less than one class C network (256 IP addresses).

This can be achieved in different ways, but typically follows the style described in [RFC2317](#).

(Please note: Many ISPs will not do this sub-delegation if you only have one or a few IP addresses. In this case your ISP has probably already setup some default reverse DNS for your IP addresses)

For example, if you are assigned network 1.2.3.24/29 (1.2.3.25 to 1.2.3.30 subnet mask 255.255.255.248), the owner of the class C 1.2.3.X (your ISP) would have these DNS entries on his DNS server:

```
NS[74] 24/29.3.2.1.in-addr.arpa = your-dns-server-name1
NS[74] 24/29.3.2.1.in-addr.arpa = your-dns-server-name2
CNAME[70] 25.3.2.1.in-addr.arpa = 25.24/29.3.2.1.in-addr.arpa
CNAME[70] 26.3.2.1.in-addr.arpa = 26.24/29.3.2.1.in-addr.arpa
CNAME[70] 27.3.2.1.in-addr.arpa = 27.24/29.3.2.1.in-addr.arpa
CNAME[70] 28.3.2.1.in-addr.arpa = 28.24/29.3.2.1.in-addr.arpa
CNAME[70] 29.3.2.1.in-addr.arpa = 29.24/29.3.2.1.in-addr.arpa
CNAME[70] 30.3.2.1.in-addr.arpa = 30.24/29.3.2.1.in-addr.arpa
```

And your DNS server would have a zone^[57] named "24/29.3.2.1.in-addr.arpa" with the following records:

```
NS[74] 24/29.3.2.1.in-addr.arpa = your-dns-server-name1
NS[74] 24/29.3.2.1.in-addr.arpa = your-dns-server-name2
PTR[76] 25.24/29.3.2.1.in-addr.arpa = name1.your-domain-name
PTR[76] 26.24/29.3.2.1.in-addr.arpa = name2.your-domain-name
PTR[76] 27.24/29.3.2.1.in-addr.arpa = name3.your-domain-name
PTR[76] 28.24/29.3.2.1.in-addr.arpa = name4.your-domain-name
PTR[76] 29.24/29.3.2.1.in-addr.arpa = name5.your-domain-name
PTR[76] 30.24/29.3.2.1.in-addr.arpa = name6.your-domain-name
```

A reverse lookup for IP 1.2.3.27 (PTR-record^[76] for "27.3.2.1.in-addr.arpa"), would first return an alias (CNAME-record^[70]) for "27.24/29.3.2.1.in-addr.arpa" from the class C owner's DNS server, which is then translated to "name3.your-domain-name" by your DNS server.

IPv6 specifics

For IPv6, the name of a reverse DNS PTR-record is each hex digit of the IP address in reverse order,

with dots between each digit, and with "ip6.arpa" appended to the end.

For example, the reverse DNS entry for IP "1234:5678:90ab:cdef:1234:5678:90ab:cdef" would be stored as a PTR-record for "f.e.d.c.b.a.0.9.8.7.6.5.4.3.2.1.f.e.d.c.b.a.0.9.8.7.6.5.4.3.2.1.ip6.arpa".

IPv6 reverse zones can be delegated at the hex digit level. So the smallest possible delegation would be for 16 IPv6 addresses, then 256, then 4096, etc.

5.11 Root DNS records

At the top of the domain name hierarchy is the root domain (typically written as a single dot or as <root>). Information about this domain resides on root servers located around the world.

All Internet DNS servers are configured with references to these root servers referred to as the "root file", "hints file" or "cache file".

Below the root domain are the top-level domains (TLDs), which are either country specific or generic. Examples of country specific top-level domains are SG (Singapore) and CA (Canada), while generic top-level domains include the well-known COM (commercial organizations), EDU (educational institutions), GOV (governmental organizations), and NET (network organizations), among others. Below the top-level domains are the second-level domains (whitehouse.gov, microsoft.com, simpledns.com), and then the third-level domains, and so on.

To locate any domain name, a DNS server starts by asking one of the root servers (unless it already has a closer match cached^[55])

The root server will supply a referral (NS-records^[74]) to DNS servers responsible for the next level (.com, .net, etc.).

The DNS server then repeats the request to one of those server, which will supply a referral to DNS servers for the next level (for example; simpledns.com), and so on, until the requested domain name is found.

This process is know as recursion^[61].

This way a DNS server can locate any name in the world, as long as it knows the IP addresses of the root DNS servers.

Simple DNS Plus includes the standard root file (a.k.a. "hints file") "named.root" containing records for the current Internet root DNS servers. This file is automatically loaded at startup.

Simple DNS Plus can automatically check for root file updates to keep it current - see Options dialog / DNS / Miscellaneous section^[30].

5.12 Round Robin

Round Robin is a method of managing server (web, ftp, mail etc.) congestion by distributing connection load across multiple servers containing identical content.

Round robin works on a rotating basis in that one record is handed out, then moves to the back of the list; the next record is handed out, then it moves to the end of the list; and so on, depending on the number of servers being used. This works in a looping fashion.

Let's say a company has one domain name and with identical web pages residing on three separate web servers with three different IP addresses. When one user accesses the home page she will be sent to the first IP address. The second user who accesses the home page will be sent to the next IP address, and the third user will be sent to the third IP address. In each case, once the IP address is given out, it goes to the end of the list. The fourth user, therefore, will be sent to the first IP address and so forth.

Round Robin is enabled in the Options dialog / DNS / Miscellaneous^[30] section.

Round Robin kicks in whenever two or more records with the same name and type exist in your own records or cached data - such as two A-records with identical names (but different IP addresses).

5.13 Suspended Zone

Suspending a zone allows you to temporarily stop serving data for a a zone without deleting the zone.

This can be useful for example if you are hosting the domain name for someone else, and they forgot to pay the bill...

You can suspend / resume zones in the DNS Records window by right-clicking a zone in the left list and selecting Suspend / Resume from the pop-up menu.

A suspended zone is indicated by a "paused" icon and a red zone name.

How Simple DNS Plus responds (or not) to DNS requests for names in a suspended zone depends on the settings in the Options dialog / DNS / Local Zones / Suspended Zones section.

When you suspend or resume a zone on a "super master" server, the zone's suspended status is automatically transferred to all Simple DNS Plus "super slave" servers. For more on "Super Master/Slave" see Options dialog / DNS / Local Zones / Super Master/Slave section. If the secondary server is not Simple DNS Plus or if you are not using the Super Master/Slave feature, you need to remember to suspend/resume the zone on both primary and secondary DNS servers.

5.14 TSIG

Simple DNS Plus supports TSIG signed zone transfers and dynamic updates.

TSIG (is an extension to the DNS protocol where a cryptographic signature is added to DNS packets. This is used to ensure that DNS packets originate from an authorized sender, and that they have not been tampered with along the way.

Both request and response packets are signed by the sender and verified by the receiver.

In order to exchange TSIG signed DNS packets the client and server must both know and use the same TSIG key. A response to a signed request is always signed with the same key as the request.

A TSIG key consists of a key name, a signing algorithm, and a secret:

- **Key name**

Similar to a login user ID.

The key name must be specified in domain name format, but can otherwise be anything you wish. RFC2845 recommends to use a name which identifies both the client and the server, for example, "client.domain1.server.domain2".

However, it does not have to be part of, or related to, any real domain name. It works just as fine, and is probably easier, using just a simple name like "robert".

- **Signing algorithm**

Simple DNS Plus supports HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512.

HMAC-MD5 is the most widely supported algorithm but is considered outdated and less secure than the SHA based algorithms.

If some software (including earlier versions of Simple DNS Plus) supports TSIG signatures but does not allow you to specify an algorithm, this typically means that it only supports HMAC-MD5 (originally the only defined option).

HMAC-MD5 uses a 128 bit signature, HMAC-SHA1 uses a 160 bit signature, and the other

HMAC-SHA algorithms use a signature with a bit length equal to the number in the algorithm name. While algorithms with longer signatures are more secure, they also take up more space in DNS packets, which limits the size of actual DNS data that can fit in a response packet sent over UDP. For incremental zones transfers, this directly affects how often the servers are forced to switch to slower TCP operations for synchronization.

- **Secret**

A base 64 encoded binary value. Similar to a login password.

In the Simple DNS Plus user interface, you can click a "Generate" button to create a random or pass phrase based value.

Using a pass phrase based value makes it easier to copy the key to a client application or another server which has the same function, but it also potentially makes the secret easier to guess.

IMPORTANT: To prevent "replay attacks" TSIG signatures are time stamped and only valid within a short time window (usually +/- 5 minutes). It is therefore critical that both client and server have the correct time. This is best achieved using automatic periodic time synchronization against an Internet time server - which is enabled by default on newer Windows versions, but may require special configuration or software on older Windows versions and other operating systems. Also make sure that the correct time zone is configured on both computers since the TSIG time stamp is based on UTC time (= local time +/- time zone).

TSIG is defined in [RFC2845](#).

5.15 TTL (Time To Live)

All DNS records have a TTL (Time To Live) property, specifying the maximum amount of time other DNS servers and applications may cache the record.

Setting a DNS record's TTL value to zero, means that applications and DNS servers must not cache the record.

When a DNS record is stored in the cache of a DNS server, the record's TTL is continuously reduced as time goes by, and when the TTL finally reaches zero the record is removed from the cache.

When a DNS server passes DNS records from the cache along to applications and other DNS servers, it supplies the current TTL value - not the original. This way the original TTL is guaranteed no matter how many DNS servers the record passes through.

When deciding on the TTL, you need to consider how often the record will be updated.

Because of caching, changes to a DNS record will not reach the entire network until the original TTL has expired - a good reason for setting a short TTL.

However caching helps reduce network traffic. The longer the TTL, the longer the record will live in other DNS server caches around the world, and so fewer requests to the original DNS server are needed - a good reason for setting a long TTL.

Generally, for a record pointing to a server/device with a static IP address and no need for quick updates, a TTL value of one day is a good starting point.

However, if the record is for a host with a dynamic IP address or for server which is part of some kind of failover set, you should be using a TTL value of a few minutes or less.

Most DNS servers will not cache a DNS record for more than one week. This is also the default in Simple DNS Plus, but you can change this through the "Maximum cache time" option - see Options dialog / DNS / Resolver / Caching section^[21].

Use the Record Properties dialog^[42] to modify a record's TTL (select the record in the DNS Records window^[37] and click the "Properties" button).

See also: Caching [55](#)

5.16 Zone Transfer

A primary DNS server has the "master copy" of a zone [57](#), and secondary DNS servers keep copies of the zone [57](#) for redundancy.

When changes are made to zone data on the primary DNS server, these changes must be distributed to the secondary DNS servers for the zone.

This is done through zone transfers.

Most DNS servers automatically notifies secondary servers whenever changes are made through a NOTIFY request, and most DNS servers will request a Zone Transfer whenever such a notification is received.

You can specify if Simple DNS Plus should send these NOTIFY requests to secondary DNS servers in the Options dialog / DNS / Miscellaneous section [30](#).

For this to work correctly, NS-records [74](#) and corresponding A-records [68](#) for each secondary DNS server must exist in the zone [57](#).

Secondary servers also periodically check for changes by querying the primary server for the SOA-record [78](#) of the zone [57](#), and checking the serial number.

In addition to whatever other changes are made to a zone and its records, the serial number of the SOA-record [78](#) must always be incremented.

NOTE: Simple DNS Plus does this for you automatically as long as you do not change the serial number yourself.

The periodic polling by the secondary servers is controlled by the refresh, retry, and expire parameters of the SOA-record [78](#).

The secondary server waits for the "refresh" interval before checking with the primary for a new serial number. If this check cannot be completed, new checks are started every "retry" interval.

If the secondary finds it impossible to perform a serial check within the "expire" interval, it discards the zone.

When the poll shows that the zone has changed (higher serial number), the secondary server will fetch a fresh copy of the zone through a zone transfer request.

A standard (full) zone transfer transfers all the records in the zone from the primary to the secondary server.

Simple DNS Plus also supports an optimized "incremental zone transfer" method which saves bandwidth by only transferring changes made since the last zone transfer, and by using UDP packets instead of TCP.

By default Simple DNS Plus will request incremental zone transfers when getting zone updates. If the primary server does not support this and returns an error, Simple DNS Plus will then revert to doing a full zone transfer.

If you know that your primary DNS server does not support incremental zone transfers, you can prevent Simple DNS Plus from using this with a setting in the Options dialog / DNS / Local Zones / Secondary Zones section [24](#).

Simple DNS Plus does not allow zone transfer requests by default because this could be used by hackers to lists all your servers etc. and thus give them a list of potential targets.

You obviously have to configure your primary DNS server to accept zone transfer requests from your secondary DNS server(s).

This can be done by using TSIG signatures [65](#) or by configuring which IP addresses to accept un-signed zone transfer requests from, either in the Zone Properties dialog [43](#) for each individual zone [57](#), or in the Options dialog / DNS / Local Zones / Zone Transfers section [22](#) for all zones.

Using TSIG signatures is more secure and is recommend over limiting access by IP address, because

IP addresses can be spoofed. Incremental zone transfers over UDP are particularly vulnerable to IP address spoofing.

See also [How to setup primary / secondary](#)

6 DNS Record types

The most commonly used record types are:

A (Host address)
 AAAA (IPv6 host address)
 CNAME (Canonical name for an alias)
 MX (Mail eXchange)
 NS (Name Server)
 PTR (Pointer)
 SOA (Start Of Authority)
 SPF (Sender Policy Framework)
 TXT (Descriptive text)

To setup one of these records, right-click a zone in the left list in the DNS Records window, and select the "New ...-record" from the pop-up menu.

The following are all less commonly used / experimental record types:

A6 (IPv6 prefix/suffix)
 AFSDB (AFS Data Base location)
 ATMA (Asynchronous Transfer Mode address)
 DHCID (DHCP Information)
 DNAME (Non-Terminal DNS Name Redirection)
 HINFO (Host information)
 ISDN (ISDN address)
 LOC (Location information)
 MB, MG, MINFO, MR (mailbox records)
 NAPTR (Naming Authority Pointer)
 NSAP (NSAP address)
 RP (Responsible person)
 RT (Route through)
 SRV (location of service)
 X25 (X.25 PSDN address)

To setup one of these records, right-click a zone in the left list in the DNS Records window, and select "Other new record" from the pop-up menu.

The records types used for DNSSEC are:

DNSKEY (DNSSEC public key)
 DS (Delegation Signer)
 NSEC (Next Secure)
 NSEC3 (Next Secure v. 3)
 NSEC3PARAM (NSEC3 Parameters)
 RRSIG (RRset Signature)

To setup one of these records, use the DNSSEC Sign Zone function.

6.1 A

The A-record is the most basic and the most commonly used DNS record type.

It is used to translate human friendly domain names such as "www.example.com" into IP-addresses such as 23.211.43.53 (machine friendly numbers).

A-records are the DNS server equivalent of the hosts file^[60] - a simple domain name to IP-address mapping.

A-records are not required for all computers, but are needed for any computer that provides shared resources on a network.

To create a new A-record, right-click a zone in the left list of DNS Records window^[37], and select "New A-record" from the pop-up menu.

This record type is defined in [RFC1035](#).

6.2 A6

NOTE: This record type and the RFC describing it has been deprecated to "experimental" status. Most IPv6 enabled applications will only use AAAA-records^[69] to lookup IPv6 host addresses.

An A6-record is used to specify the IPv6 address (or part of the IPv6 address) for a host.

A6-records expands the functionality of AAAA-records by adding support for aggregation and renumbering.

A lookup for an IPv6 address could involve several A6-records which each specify only part of the final address.

This is achieved through the additional prefix-length and prefix name fields.

To create a new A6-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC2874](#).

6.3 AAAA

An AAAA-record is used to specify the IPv6 address for a host (equivalent of the A-record^[68] type for IPv4).

IPv6 is the future replacement for the current IP address system (also known as IPv4).

The current IPv4 addresses are 32 bits long ($x . x . x . x = 4$ bytes), and therefore "only" support a total of 4,294,967,296 addresses - less than the global population.

With this limitation there is an increasing shortage of IPv4 addresses, and to solve the problem, the whole Internet will eventually be migrated to IPv6.

IPv6 addresses are 128 bits long and are written in hexadecimal numbers separated by colons (:) at every four digits (segment).

A series of zero value segments can be shortened as "::", and leading zeros in a segment can be skipped.

For example: 4C2F::1:2:3:4:567:89AB.

To create a new AAAA-record, right-click a zone in the left list in the DNS Records window^[37], and select "New AAAA-record" from the pop-up menu.

This record type is defined in [RFC3596](#).

6.4 AFSDB

An AFSDB-record maps a domain name to an AFS (Andrew File System) database server.

The server name points to an A-record^[68] for the database server, and the sub-type indicates server type:

- 1 = AFS version 3.0 volume location server for the named AFS cell.
- 2 = DCE authenticated server.

To create a new AFSDB-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC1183](#).

6.5 ATMA

An ATMA-record maps a domain name to an ATM address.

The ATM address can be specified in either E.164 format (decimal) or NSAP format (hexadecimal).

To create a new ATMA-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in "ATM Name System Specification Version 1.0" published by the ATM Forum.

6.6 CNAME

CNAME-records are domain name aliases.

Computers on the Internet often performs multiple roles such as web-server, ftp-server, chat-server etc.

To mask this, CNAME-records can be used to give a single computer multiple names (aliases). For example, the computer "computer1.xyz.com" may be both a web-server and an ftp-server, so two CNAME-records are defined:

"www.xyz.com" = "computer1.xyz.com" and "ftp.xyz.com" = "computer1.xyz.com".

Sometimes a single server computer hosts many different domain names (take ISPs), and so CNAME-records may be defined such as "www.abc.com" = "www.xyz.com".

The most common use of the CNAME-record type is to provide access to a web-server using both the standard "www.domain.com" and "domain.com" (with and without the www prefix).

This is usually done by creating an A-record^[68] for the short name (without www), and a CNAME-record for the www name pointing to the short name.

CNAME-records can also be used when a computer or service needs to be renamed, to temporarily allow access through both the old and new name.

A CNAME-record should always point to an A-record^[68] and never to itself or another CNAME-record to avoid circular references.

To create a new CNAME-record, right-click a zone in the left list in the DNS Records window^[37], and select "New CNAME-record" from the pop-up menu.

Please note that you cannot create a CNAME-record for the zone name itself as this will always conflict with the zone's SOA-record^[78].

For more on this see <http://www.simplifiedns.com/kb.aspx?kbid=1176>

This record type is defined in [RFC1035](#).

6.7 DHCID

DHCID-records store Dynamic Host Configuration Protocol (DHCP) Information, and can be created and used by some DHCP servers and clients.

You cannot create DHCID record through the Simple DNS Plus user interface - these records can only be added by DHCP servers/clients themselves through dynamic updates.

This record type is defined in [RFC4701](#).

6.8 DNAME

A DNAME-record is used to map / rename an entire sub-tree of the DNS name space to another domain.

It differs from the CNAME-record^[70] which maps only a single node of the name space.

To create a new DNAME-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC2672](#).

6.9 DNSKEY

A DNSKEY-record holds a public key that resolvers can use to verify DNSSEC^[55] signatures in RRSIG-records^[77].

DNSKEY-records have the following data elements:

- Flags: "Zone Key" (set for all DNSSEC keys) and "Secure Entry Point" (set for KSK and simple keys).
- Protocol: Fixed value of 3 (for backwards compatibility)
- Algorithm: The public key's cryptographic algorithm.
- Public key: Public key data.

To add a DNSKEY-record to a zone, use the DNSSEC Sign Zone^[47] function.

This record type is defined in [RFC4034](#).

6.10 DS

DS-records are used to secure delegations (DNSSEC)^[55].

A DS-record with the name of the sub-delegated zone^[57] is placed in the parent zone along with the delegating NS-records^[74].

This DS-record references a DNSKEY-record^[71] in the sub-delegated zone.

DS-records have the following data elements:

- Key Tag: A short numeric value which can help quickly identify the referenced DNSKEY-record^[71].
- Algorithm: The algorithm of the referenced DNSKEY-record.
- Digest Type: Cryptographic hash algorithm used to create the Digest value.
- Digest: A cryptographic hash value of the referenced DNSKEY-record.

To create a new DS-record, right-click a zone in the left list of DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC4034](#).

6.11 HINFO

A HINFO-record specifies the host / server's type of CPU and operating system.

This information can be used by application protocols such as FTP, which use special procedures when communicating with computers of a known CPU and operating system type.

Standard CPU and operating system types are defined in [RFC1700](#) (Page 206 / 214).

The standard for a Windows PC is "INTEL-386" / "WIN32".

To create a new HINFO-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC1035](#).

6.12 ISDN

The ISDN-record maps a domain name to an ISDN (Integrated Services Digital Network) telephone number.

The ISDN phone numbers / DDI (Direct Dial In) used should follow ITU-T E.163/E.164 international telephone numbering standards.
For example: 12121234567 (1=USA, 212=Manhattan New York area code, 1234567=number)

The ISDN sub-address is an optional hexadecimal number.

To create a new ISDN-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC1183](#).

6.13 LOC

This record type is used to specify geographical location information about hosts, networks, and subnets.

A LOC-record describes a location with the following properties:

- Latitude / Longitude.
- Altitude.
- Size (diameter of the location described).
- Horizontal / Vertical precision of the data.

Because of the binary storage format used, only the first digit of the size and precision properties can be non-zero.

Additional interesting and practical information about LOC-records is available at <http://www.ckdhr.com/dns-loc/>

To create a new LOC-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC1876](#).

6.14 MB, MG, MINFO, MR

IMPORTANT: Most Internet e-mail servers only support MX-records^[73]. Only use MB, MG, MINFO and MR records if you have specific requirements for these.

MB-records (Mailbox)

Maps a mailbox to a host (server).

The host must be a valid A-record already defined (in the same zone or elsewhere).

MG-records (Mail group member)

Used to specify mail group members (one MG-record per member).

Each member mailbox must be identical to a valid mailbox (MB-record).

MINFO-records (Mailbox or mail list information)

Specifies the mailbox of the responsible person and optionally a mailbox for errors for this mailbox or list.

Each mailbox must be the same as a valid mailbox (MB-record) that already exist in the zone.

MR-records (Renamed mailbox)

Specifies a renamed mailbox.

An MR-record can be used as a forwarding entry for a user who has moved to a different mailbox.

To create a new mailbox record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

These record types are defined in [RFC1035](#).

6.15 MX

MX-records are used to specify the e-mail server(s) responsible for a domain name.

Each MX-record points to the name of an e-mail server and holds a preference number for that server.

If a domain name is handled by multiple e-mail servers (for backup/redundancy), a separate MX-record is used for each e-mail server, and the preference numbers then determine in which order (lower numbers first) these servers should be used by other e-mail servers.

If a domain name is handled by a single e-mail server, only one MX-record is needed and the preference number does not matter.

When sending an e-mail to "user@example.com", your e-mail server must first look up any MX-records for "example.com" to see which e-mail servers handles incoming e-mail for "example.com".

This could be "mail.example.com" or someone else's mail server like "mail.isp.com".

After this it looks up the A-record^[68] for that e-mail server name to connect to its IP-address.

IMPORTANT: An MX-record must point to the name of a mail server - not directly to the IP-address. Because of this, it is very important that an A-record^[68] for the referenced mail server name exists (not necessarily on your DNS server, but wherever it belongs), otherwise there may not be any way to connect to that e-mail server.

Do not point an MX-record to a CNAME-record^[70]. Many e-mail servers don't understand this. Add another A-record^[68] instead.

To create a new MX-record, right-click a zone in the left list in the DNS Records window^[37], and select "New MX-record" from the pop-up menu.

This record type is defined in [RFC1035](#).

6.16 NAPTR

NAPTR-records are used to store rules used by DDDS (Dynamic Delegation Discovery System) applications.

One example is "ENUM" which allows an end user to type a telephone number into e.g. a web browser and access a listing of Internet resources (URI) for that number, such as addresses for IP telephony, e-mail or web sites.

For more information on "ENUM", see <http://www.ripe.net/enum> or <http://enum.nic.at>
See also ENUM - Mapping telephone numbers to SIP or e-mail addresses in DNS

The "Order" field is a number (0 to 65535) specifying the order in which multiple NAPTR records must be processed (low to high) by the application.

The "Preference" field is equivalent to the Priority value in the DDDS algorithm. It is a number (0-65535) that specifies the order (low to high) in which NAPTR records with equal Order values should be processed.

The "Flags" field contains flags to control aspects of the rewriting and interpretation of the fields in the record. Flags are single characters from the set A-Z and 0-9. The use of this field is specified by the individual DDDS application.

The "Services" field specifies the service parameters applicable to this delegation path. The individual DDDS application specifies the possible values for this field.

The "Reg. Exp." field contains a substitution expression that is applied to the original string held by the client in order to construct the next domain name to lookup. See the DDDS algorithm specification for the syntax of this field.

The "Replacement" field specifies the next domain name (fully qualified) to query for depending on the potential values found in the flags field. This field is used when the regular expression is empty (a simple replacement operation). The "Reg.Exp." and "Replacement" fields are mutually exclusive (only one can contain a value).

To create a new NAPTR-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC3403](#).

6.17 NS

NS-records identify the DNS servers responsible (authoritative^[55]) for a zone^[57].

A zone^[57] should contain one NS-record for each of its own DNS servers (primary and secondaries). This is mostly used for zone transfer^[67] purposes (notify messages). These NS-records have the same name as the zone in which they are located.

The more important function of the NS-record is delegation. Delegation means that part of a domain is delegated to other DNS servers. For example, all ".com" sub-names (such as "example.com") are delegated from the "com" zone. The "com" zone contains NS-records for all ".com" sub-names (a lot!).

You can delegate sub-names of your own domain name (such as "subname.example.com") to other DNS servers the same way.

To delegate "subname.example.com", create NS-records for "subname.example.com" in the "example.com" zone.

These NS-records must point to the DNS server responsible for "subname.example.com", for example, "ns1.subname.example.com" - or a DNS server somewhere else like "ns1.othername.net".

An NS-record identifies the name of a DNS server - not the IP-address.

Because of this, it is important that an A-record^[68] for the referenced DNS server exists (not necessarily on your DNS server, but wherever it belongs), otherwise there may not be any way to connect with that DNS server.

If an NS-record delegates a sub-name ("subname.example.com") to a DNS server with a name in that sub-name ("ns1.subname.example.com"), an A-record^[68] for that server

("ns1.subname.example.com") must exist in the parent zone ("example.com").

This A-record is called a "glue record", because it doesn't really belong in the parent zone, but is necessary to locate the DNS server for the delegated sub-name.

To create a new NS-record, right-click a zone in the left list in the DNS Records window^[37], and select "New NS-record" from the pop-up menu.

This record type is defined in [RFC1035](#).

6.18 NSAP

An NSAP-record maps a domain name to an NSAP address.

The NSAP address is entered using hexadecimal digits - any NSAP address format is allowed.

To create a new NSAP-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC1706](#).

6.19 NSEC

An NSEC-record links to the next record name in the zone^[57] (in DNSSEC^[55] sorting order) and lists the record types that exist for the record's name.

These records can be used by resolvers to verify the non-existence of a record name and type as part of DNSSEC validation.

NSEC-records have the following data elements:

- Next domain name: The next record name in the zone (DNSSEC sorting order)
- Record types: The DNS record types that exist for the name of this NSEC-record.

To add NSEC-records to a zone, use the DNSSEC Sign Zone^[47] function.

This record type is defined in [RFC4034](#).

6.20 NSEC3

An NSEC3-record links to the next record name in the zone (in hashed name sorting order) and lists the record types that exist for the name covered by the hash value in the first label of the NSEC3-record's own name.

These records can be used by resolvers to verify the non-existence of a record name and type as part of DNSSEC validation.

NSEC3-records have the same functionality as NSEC-records, except NSEC3 uses cryptographically hashed record names to prevent enumeration of the record names in a zone.

NSEC3-records have the following data elements:

- Hash Algorithm: The cryptographic hash algorithm used.
- Flags: "Opt-out" (indicates if delegations are signed or not).
- Iterations: How many times the hash algorithm is applied.
- Salt: Salt value for the hash calculation.
- Next Hashed Owner Name: The name of the next record in the zone (in hashed name sorting order).
- Record Types: The record types that exist for the name covered by the hash value in the first label of the NSEC3-record's own name.

To add NSEC3-records to a zone, use the DNSSEC Sign Zone function.

This record type is defined in [RFC5155](#).

6.21 NSEC3PARAM

An NSEC3PARAM-record is used by authoritative DNS servers to calculate and determine which NSEC3-records to include in responses to DNSSEC requests for non-existing names/types.

NSEC3PARAM-records have the following data elements:

- Hash Algorithm: The cryptographic hash algorithm used.
- Flags: "Opt-out" (indicates if delegations are signed or not).
- Iterations: How many times the hash algorithm is applied.
- Salt: Salt value for the hash calculation.

To add an NSEC3PARAM-record to a zone, use the DNSSEC Sign Zone function.

This record type is defined in [RFC5155](#).

6.22 PTR

PTR-records are primarily used as "reverse records" - to map IP addresses to domain names (reverse of A-records and AAAA-records).

For a reverse IPv4 mapping, the name of the PTR-record is the IP address with the segments reversed and with "in-addr.arpa" appended to the end.

As an example, looking up the domain name for IP address "12.23.34.45" is done with a query for the PTR-record for "45.34.23.12.in-addr.arpa".

For a reverse IPv6 mapping, the name of the PTR-record is each hex digit of the IP address in reverse order, with dots between each digit, and with "ip6.arpa" appended to the end.

As an example, looking up the domain name for IPv6 address "1234:5678:90ab:cdef:1234:5678:90ab:cdef" is done with a query for the PTR-record for "f.e.d.c.b.a.0.9.8.7.6.5.4.3.2.1.f.e.d.c.b.a.0.9.8.7.6.5.4.3.2.1.ip6.arpa".

For more information see the section on Reverse DNS.

To create a PTR-record use one of the following options:

- The Reverse zone IP-to-Name Mappings dialog^[46].
- The "Update Reverse Zone" check box in the Record Properties dialog^[42] for an A-record or AAAA-record.
- Right-click a reverse zone in the DNS Records window^[37], and select "New PTR-record" from the pop-up menu.

This record type is defined in [RFC1035](#).

6.23 RP

An RP-record specifies the mailbox of the person responsible for a host (domain name).

A SOA-record^[78] defines the responsible person for an entire zone^[57], but a zone may contain many individual hosts / domain names for which different people are responsible.

The RP-record type makes it possible to identify the responsible person for individual host names contained within the zone.

Optionally specify the domain name for a TXT-record^[79] with additional information (such as phone and address).

To create a new RP-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC1183](#).

6.24 RRSIG

An RRSIG-record holds a DNSSEC^[55] signature for a record set (one or more DNS records with the same name and type).

Resolvers can verify the signature with a public key stored in a DNSKEY-record^[71].

RRSIG-records have the following data elements:

- Type Covered: DNS record type that this signature covers.
- Algorithm: Cryptographic algorithm used to create the signature.
- Labels: Number of labels in the original RRSIG-record name (used to validate wildcards).
- Original TTL: TTL^[66] value of the covered record set.
- Signature Expiration: When the signature expires.
- Signature Inception: When the signature was created.
- Key Tag: A short numeric value which can help quickly identify the DNSKEY-record^[71] which can be used to validate this signature.
- Signer's Name: Name of the DNSKEY-record^[71] which can be used to validate this signature.
- Signature: Cryptographic signature.

To add RRSIG-records to a zone, use the DNSSEC Sign Zone^[47] function.

This record type is defined in [RFC4034](#).

6.25 RT

An RT-record specifies an intermediate host that provides routing to the host with the name of the RT-record.

A preference value is used to set priority if multiple intermediate routing hosts are specified - lower

values tried first.

For each intermediate host specified, a corresponding host (A) address resource record is needed in the current zone.

To create a new RT-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC1183](#).

6.26 SOA

A zone^[57] contains exactly one SOA-record, which holds the following properties for the zone:

- **Name of primary DNS server**

The host name of the primary DNS server for the zone.

The zone should contain a matching NS-record^[74].

NOTE: For dynamic updates from Windows clients and Active Directory to work correctly, it is important that this contains the correct host name for the primary DNS server for the zone, and also that an A-record exists for this name pointing to the correct IP address.

- **E-mail address of responsible person**

The e-mail address of the person responsible for the zone.

The standard for this is the "hostmaster" alias - such as "hostmaster@example.com".

- **Serial number** (see Zone Transfers^[67])

Used by secondary DNS servers to check if the zone has changed.

If the serial number is higher than what the secondary server has, a zone transfer^[67] will be initiated. This number is automatically increased by Simple DNS Plus when changes are made to the zone or its records (happens when you save the zone).

Unless you have a specific reason for changing this number, it is best to let Simple DNS Plus manage it.

You should never decrease a serial number.

- **Refresh Interval** (see Zone Transfers^[67])

How often secondary DNS servers should check if changes are made to the zone.

- **Retry Interval** (see Zone Transfers^[67])

How often secondary DNS server should retry checking if changes are made - if the first refresh fails.

- **Expire Interval** (see Zone Transfers^[67])

How long the zone will be valid after a refresh.

Secondary servers will discard the zone if no refresh could be made within this interval.

- **Minimum (default) TTL**

Used by other DNS servers to cache^[55] negative responses (such as record does not exist etc.).

A SOA-record is automatically created when you create a new zone^[40].

This record type is defined in [RFC1035](#).

6.27 SPF

An SPF-record specifies the hosts (e-mail servers) which are permitted to send e-mails from a domain name.

This is used to prevent spam and phishing. For details please see <http://www.openspf.org>

Simple DNS Plus also has an option to automatically provide missing SPF records - see Options dialog / DNS / Automatic SPF ^[25] section.

To create a new SPF-record, right-click a zone in the left list in the DNS Records window ^[37], and select "New SPF-record" from the pop-up menu.

This record type is defined in [RFC4408](#).

6.28 SRV

SRV-records are used to specify the location of a service.

They are used in connection with different directory servers such as LDAP (Lightweight Directory Access Protocol), and Windows Active Directory, and more recently with SIP servers (see <http://www.simplesdns.com/kb.aspx?kbid=1218>).

They can also be used for advanced load balancing and to specify specific ports for services, for example, that a web-server is running on port 8080 instead of the usual port 80 (theoretical example - this is not yet supported by any major browsers).

This record type is however NOT supported by most programs in use today, including web-browsers.

The name of a SRV-record is defined as "_service._protocol.domain", for example, "_ftp._tcp.xyz.com".

Most internet services are defined in [RFC1700](#) (page 15), and the protocol is generally TCP or UDP.

The "service location" is specified through a target, priority, weight, and port:

- Target is the domain name of the server (referencing an A-record ^[68] or AAAA-record ^[69]).
- Priority is a preference number used when more servers are providing the same service (lower numbers are tried first).
- Weight is used for advanced load balancing.
- Port is the TCP/UDP port number on the server that provides this service.

To create a new SRV-record, right-click a zone in the left list in the DNS Records window ^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC2782](#).

6.29 TXT

TXT-records are used to hold descriptive text.

They are often used to hold general information about a domain name such as who is hosting it, contact person, phone numbers, etc.

One common use of TXT-records is for SPF (see <http://www.openspf.org>).

This is however gradually being replaced by the new SPF-record ^[79] type.

To create a new TXT-record, right-click a zone in the left list in the DNS Records window ^[37], and select "New TXT-record" from the pop-up menu.

This record type is defined in [RFC1035](#).

6.30 X25

An X25-records maps a domain name to a Public Switched Data Network (PSDN) address number.

Numbers used with this record should follow the X.121 international numbering plan.

To create a new X25-record, right-click a zone in the left list in the DNS Records window^[37], and select "Other new record" from the pop-up menu.

This record type is defined in [RFC1183](#).

7 Event IDs / Error Messages

Simple DNS Plus may write the following event IDs to the Windows Event Log (enabled in the Options dialog / Logging / Windows Event Log section^[35]), and log associated messages in the log files / Active Log View:

Error Events

The following are recorded as "Error events" to the Windows Event Log, and appear in the Simple DNS Plus logs with a ***** Error:** prefix:

Event ID Description

- | | |
|------------|---|
| 101 | <p>Could not start DNS service on <ip-address> [port <port>] (<error message>)
 This usually means that another DNS server or another program is occupying the DNS port (53) on the same computer. Can also occur when using "Internet Connection Sharing". For more information, please see KB1058
 Once you have corrected the problem, use "Start server" from the File menu.</p> |
| 103 | <p>Could not start HTTP API on port <ip-address> port <port-number> (error message)
 This usually means that the HTTP port is occupied by another program or possibly another instance of Simple DNS Plus.
 You may need to change the port number used for HTTP in the Options dialog / HTTP API^[37] section.</p> |
| 105 | <p>Failed to start remote management on <ip-address> port <port> (error message)
 This usually means that the remote management port is occupied by another program or possibly another instance of Simple DNS Plus.
 You may need to change the port number used for HTTP in the Options dialog / Remote Management^[35] section.</p> |
| 203 | <p>Could not save zone <zone-name> to zone file <file-name> - <error message>
 Another program may be accessing the zone file, the hard disk may be full, or something else is preventing Simple DNS Plus write access to the file.</p> |
| 251 | <p>Failed to load plug-in <plug-in instance display name>: <error message>
 A plug-in^[53] could not be loaded.</p> |

- 257 Error calling "<method name>" for plug-in "<plug-in instance display name>": <error message>**
An exception was throw executing a plug-in ⁵³ method.
- 258 Asynchronous operation error in plug-in "<plug-in instance display name>": <error message>**
An exception was throw while a plug-in ⁵³ was executing something in a separate thread.
- 999 Application error: [<error-description>]**
In the unlikely event that you should see this error message, please contact support@simpledns.com for assistance.

Warning Events

The following are recorded as "Warning events" to the Windows Event Log, and appear in the Simple DNS Plus logs with a *** **Warning:** prefix:

Event ID Description

- 140 Open DNS Server. Limiting recursion to trusted IP addresses is recommended (Options dialog / DNS / Resolver / Recursion)**
See the "DNS spoofing" and "Recursion" sections in How to secure your server ⁴.
- 150 EDNS0 test failed. A local firewall appears to be blocking EDNS0**
EDNS0 enabled DNS requests are not getting through and Simple DNS Plus will continue without using EDNS0.
This startup test can be enabled/disabled in the Options dialog / DNS / Miscellaneous ³⁰ section.
- 201 Could not open zone file for <zone-name> from <file-name> - <error message>**
Another program may be accessing the zone file.
- 259 Tread queue error for plug-in "<plug-in instance display name>": <error message>**
A problem related to queuing threads for plug-in processing.
- 302 IP address <ip-address> blocked (more than <n> DNS requests per second)**
See the "Denial of service" section in How to secure your server ⁴.
- 303 Request from <ip-address> for BIND version - possible hack attempt**
See the "BIND version requests" section in How to secure your server ⁴.
- 305 TCP connection request from <ip-address> ignored - Exceeds maximum connections (<n>)**
See the "Denial of service (DOS)" section in How to secure your server ⁴.
- 310 Could not refresh zone <zone-name> from primary IP <ip-address> - Not configured to send outbound requests via <IPv4/IPv6>**
A secondary zone is configured to use a primary server IP address for which the IP version is not enabled in the Options dialog / DNS / Outbound Requests section ²⁰.
- 311 Socket error accepting TCP DNS connection: <error code / message>**
An exception was thrown while some attempted to establish a TCP connection with this server.
- 401 Lame delegation for <zone-name> on this server (<ip-address>)**

A "Lame delegation" is when a DNS server, which is listed in the domain registration for a domain, is not configured with data for that domain.

"Lame delegation" sometimes happen because someone has registered a domain but only has one or no DNS servers, so they simply specify some random DNS servers to act as place-holders, even though none of these servers have a zone defined for the domain in question. Hence the domain is "lame" without a leg to stand on.

If you see this message about your own server ("this server"), you should take steps to correct this immediately.

If the domain-name in question is not yours, do a WHOIS look up^[48] to determine the owner, and contact them to change it immediately (they are causing additional traffic on your Internet connection and additional processing for your DNS server).

If the domain-name is yours - add the zone^[40] to your server immediately.

501 Notify request not sent to <server-name> for <zone-name> - Could not resolve IP address

Changes were made to a primary zone on this server, but the server could not notify (see zone transfers^[67]) a secondary DNS server.

This typically means that no A-record^[68] is available for the DNS server name specified in the NS-record^[74] for the secondary DNS server.

502 [<server-name>] [<ip-address>] did not respond to Notify request for <zone-name>

Changes were made to a primary zone on this server, but the server did not get any response when trying to notify a secondary DNS server.

This typically means that the secondary server is down, or there is some type of network problem.

503 Failed to Zone Transfer <zone-name> [and <n> other zones] from <ip-address> (<error-description>)

This server (secondary) could not complete a zone transfer^[67] from the primary DNS server.

This could be caused by general network problems or security^[4] settings on the primary server.

The server will continuously retry the zone transfer.

601 Forward server <ip-address> does not offer recursion

One of the forward DNS servers specified in the Options dialog^[19] does not offer recursion^[61].

Select a different forward DNS server, or disable forwarding (not needed in most cases).

701 Error opening log file - <error-description>

There was a problem writing a log file to disk. The server has temporarily stopped writing to this log file, and will attempt to open the file again in 5 minutes.

702 Error writing to log file - <error-description>

There was a problem writing a log file to disk. The server has temporarily stopped writing to this log file, and will attempt to open the file again in 5 minutes.

703 Error opening raw log file - <error-description>

There was a problem writing the raw log file to disk. The server has temporarily stopped writing to this log file, and will attempt to open the file again in 5 minutes.

704 Error writing to raw log file - <error-description>

There was a problem writing the raw log file to disk. The server has temporarily stopped writing to this log file, and will attempt to open the file again in 5 minutes.

Information Events

The following are recorded as "Information events" to the Windows Event Log, and appear in the Simple DNS Plus logs without any prefix:

<u>Event ID</u>	<u>Description</u>
1	DNS service started on <ip-address> port <port>
2	Server paused
3	Server shut down

See also: How to read the log [\[9\]](#)

8 Raw log file format

Simple DNS Plus raw log files (.sdraw) contain an entry for each received DNS request as follows:

<u>Bytes</u>	<u>Description</u>
3	Number of seconds since midnight *
2	DNS request packet bytes 3 and 4 (header flags)
2	Query type *
2	Query class *
1	Length of query name less 1
variable	Query domain name (DNS packet format)
1	Length of request source IP address (IPv4=4, IPv6=16)
variable	Request source IP address

* bytes represent integer value in network byte order (most significant byte first / big-endian).

The Tools directory [\[83\]](#) contains a command line tool to extract and filter raw log data and also a .NET programming library for accessing the raw log data.

Raw request logging is enabled in the Options dialog / Logging / Log Files section [\[34\]](#).

9 Tools Directory

Under the directory where Simple DNS Plus is installed, you will find a "Tools" sub-directory with the following tools:

- **FilterRawLog.exe**

Command line application which parses a Simple DNS Plus raw log file (.sdraw), filters and summarizes the data, and writes the result to a text file as comma separated values (csv format).

See the "FilterRawLog-ReadMe.txt" file for details.

Raw log files are enabled in the Options dialog / Logging / Log Files [\[34\]](#) section.

- **SDNSFileLib.dll**

This is a .NET code library which provides programmatic access (read-only) to the Simple DNS Plus zone database files (_zones.sdzdb) and raw log files (.sdraw).

See the "sdnsfilelib.chm" help file for details.

Note: The "sdnsfilelib.chm" help file mentions Simple DNS Plus v. 5.0 but the library also works with v. 5.2. The file formats have not changed between these two versions.

- **ZoneDBViewer.exe**

Simple DNS Plus v. 5.x uses a proprietary database file format for its zone list (_zones.sdzdb).

This tool (GUI application) can be used to view the data in this file.

Index

- * -

* (Wildcard records) 42

- A -

A record type 68
A6 record type 69
AAAA record type 69
Active Log 35
Active Log View 18
AFSDB record type 70
Alias 70
Andrew File System 70
API 11
arpa 62
ATM address 70
ATMA record type 70
Authoritative 55
Automatic SPF Records 25

- B -

BIND version requests 4, 30
Blocking 36
Bulk Update Wizard 45

- C -

Cache Poisoning 4
Cache Snapshot Window 52
Caching 21, 55
Canonical name 70
CNAME record type 70
Command line 11
Command line options 15
Conditional forwarding 58

- D -

Data files 22
Default Zone Values 46

Defer loading 22
Denial of service 4
Descriptive text 79
Directory services 79
DNAME record type 71
DNS Cache 55
DNS Cache Snapshot 52
DNS forwarding 58
DNS Look Up 48
DNS rebinding attack 4, 21
DNS Records 37
DNS Recursion 61
DNS Resolution 61
DNS spoofing 4
DNSKEY record type 71
DNSSEC 47, 48
DoS (denial of service) 4
DOS prompt 15
DS record type 71
Dynamic DNS update 58
Dynamic updates 43

- E -

EDNS0 30
Error messages 9, 80
Event IDs 80
Event log 35
Expire interval 78
Export Wizard 42
Extended forwarding 58

- F -

FilterRawLog.exe 83
Find and replace IP 45
Forwarding 27, 58
From port number 20

- G -

GPS 72

- H -

Header messenger 9
HINFO record type 72

Hints file 30
 Host address 68, 69
 Host information 72
 Hosting DNS 2
 Hosts File 60
 HTTP API 11, 12, 31

- I -

IDN 60
 Import Wizard 41
 in-addr.arpa 62
 Inbound Requests 20
 Incremental zone transfer 24
 Integrate 11
 Internationalize domain names 60
 IP Address Blocking 36
 ip6.arpa 62
 IP-to-Name Mappings 46
 IPv4 host address 68
 IPv6 69
 IPv6 host address 69
 ISDN record type 72
 IXFR 24

- K -

key file 47
 key set 48

- L -

Lame DNS Requests 27
 LDAP 79
 Listen on 20
 LOC record type 72
 Location information 72
 location of service 79
 Log 9
 Log details 33
 Log files 34
 Look Up Types 51
 Look Up Window 48

- M -

Mail exchange 73

Mail server 73
 Mailbox record types 73
 Main window 16
 Master 23
 Maximum cache time 21
 MB record type 73
 MG record type 73
 Migration 41
 MINFO record type 73
 Minimum cache time 21
 Minimum TTL 22, 78
 Miscellaneous 30
 MR record type 73
 MX record type 73

- N -

Name Redirection 71
 Name server record 74
 Naming Authority Pointer 74
 NAPTR record type 74
 NAT IP Alias 29
 NAT router 29
 NAT to LAN 29
 New Zone Wizard 40
 Non-existing domains 28
 Non-recursive 61
 Non-Terminal 71
 NOTIFY requests 30
 NS record type 74
 NSAP record type 75
 NSEC record type 75
 NSEC3 record type 76
 NSEC3PARAM record type 76
 NXDOMAIN redirect 28

- O -

Options dialog 19
 Outbound Requests 20

- P -

Performace Graph 18
 Plug-In instance 32
 Plug-in View 18
 Plug-Ins 32, 53

Port scanners 4
Primary 3
Promote server 45
PSDN 80
PTR 62
PTR record type 76

- Q -

Quick Zone Wizard 44

- R -

Raw log 34
Raw log file format 83
Records 37
Records properties 42
Recursion 4, 21, 61
Recursive 61
Refresh interval 78
Registrar 2
Replace IP 45
Resolution 61
Response filtering 21
Responsible person 77
Retry interval 78
Reverse Look Up 62
Reverse record 76
Reverse Zone 62
Reverse Zone Wizard 46
Root DNS Records 64
Root server list 30
Round robin 20, 64
Route through 77
RP record type 77
RRSIG record type 77
RT record type 77

- S -

SDNSFileLib.dll 83
sdraw 83
Secondary 3, 24
Secondary Zones 24
Security 4
Sender Permitted From 79
Sender Policy Framework 79

Serial number 78
Server name 20
Shadow forwarding 58
Sign zone 47
Slave 23
SOA record 43
SOA record type 78
SPF 25
SPF record type 79
SPF records 79
Spoofing 4
SRV record type 79
Start of authority 78
Stealth DNS 27
Super Master 23
Super Slave 23
Suspended Zone 25, 65
Synchronize 67
Syslog 34

- T -

Taskbar Icon 20
Time To Live 66
Tools directory 83
Traybar Icon 20
TSIG 58
TSIG Dynamic Updates 26
TTL 66
TXT record type 79

- V -

Version requests 4
Views 18

- W -

Warning messages 9, 80
welcome 1
Wildcard records 42
Windows event log 35

- X -

X25 record type 80

- Z -

Zone 40

Zone files 22

Zone Properties 43

Zone Transfers 22, 43, 67

ZoneDBViewer.exe 83

Zones 57