Did you find this document helpful?

👍 👎

DNS Zone Manager

Version: 86 88 92 96

Valid for versions 96 through the latest version

Last modified: *March 12, 2021*

Overview

This feature allows you to edit the records in a domain's DNS (Domain Name System) zone file. DNS converts human-readable domain names (for example, `example.com`) to computer-readable IP addresses (for example, `192.0.0.1`). To perform this function, DNS relies on zone records that exist on your server to map domain names to IP addresses.

> **Important:**
> - We **deprecated** the MyDNS and NSD nameserver software in cPanel & WHM version 78 and plan to remove them in a future release. If you use either of these nameservers, we **strongly** recommend that you migrate to either the PowerDNS or BIND namesevers. For more information, read our cPanel Deprecation Plan documentation.
> - DNS zones that reside on other Write-only DNS servers in a DNS cluster do **not** appear in this interface.

Domains

The *DNS Zone Manager* interface displays all of your server's domains. To filter the list, enter a name in the text box. For each listed domain, you can perform the following actions:

- *A Record* — Create a new A record. When you select this record type, a new window will appear. Enter a valid DNS zone name in the *Name* text box and a valid IPv4 address in the *Address* text box. Click *Add An A Record* to save your changes.
- *CNAME Record* — Create a new CNAME record. When you select this record type, a new window will appear. Enter a valid DNS zone name in the *Name* text box and a FQDN in the *CNAME* text box. Click *Add A CNAME Record* to save your changes.
- *MX Record* — Create a new MX record. When you select this record type, a new window will appear. Enter the record's priority value in the *Priority* text box and a FQDN in the *Destination* text box. Click *Add An MX Record* to save your changes.
- *DNSSEC* — Manage the domain's DNSSEC (Domain Name System Security Extensions) records. When you select this record type, the system directs you to the *View DNSSEC Keys* interface.
- *Manage* — Add or edit additional domain records. When you select this setting, the system directs you to the *Manage DNS Zone Records* interface.

Manage DNS Zone Records

This interface displays a table with a list of the selected domain's DNS zone records. To filter the list, enter a name in the text box or select an available record type filter.

The record table contains the following information for each record:

- *Name* — The record's name.
- *TTL* — The record's Time to Live (TTL).
- *Type* — The record's type.
- *Record* — The record's information.
- *Actions* — The option to edit or delete the record.

You can also use this interface to:

- Add or edit one or more DNS zone records.
- Delete a DNS zone record.
- View the raw DNS zone file.
- Reset the DNS zone.

Add a DNS zone record

To add a DNS zone record, perform the following steps:

1. Click *Manage* next to the domain you want to modify.
2. Click *Add Record*. You can also click the arrow icon (▾) and select the desired record type from the list.

   > **Note:**
   >
   > To add multiple records, click *Add Record* multiple times or select the desired record types from the list. The system adds the new records to the top of the table.

3. Enter the record information.
4. Click *Save Record* or *Save All Records*, or click *Cancel*.

Edit a DNS zone record

To edit a DNS zone record, perform the following steps:

1. Click *Manage* for the domain that you want to modify. A new interface will appear.
2. Click *Edit* next to the record or records that you want to edit.
3. Update the information in the text boxes.

   > **Note:**
   >
   > If you change an existing record's *Type* value, the system preserves the current record's data until you save your changes.

4. Click *Save Record* or *Save All Records* to save your changes, or click *Cancel*.

DNS zone record types

When you add or edit a DNS zone record, you can select from the following record types:

A

IPv4 Address Record — This record maps hostnames to IPv4 addresses. These records allow DNS servers to identify and locate your website and its various services on the internet. Without appropriate A records, your visitors cannot access your website, FTP site, or email accounts. You can set the following values:

- *Name* — A new or existing DNS zone name. When you enter a zone name, the system automatically appends the domain name to the zone record. For example, if you create the `user` zone, the system will add the `example.com.` domain information.
- *Address* — Enter the domain's IP address.

AAAA

IPv6 Address Record — This record is the same as an A record, but maps hostnames to IPv6 addresses.

AFSDB

Andrew File System Data Base Location — This record provides the location of the domain name's Andrew File System (AFS) database server or Distributed Computing Environment (DCE) authentication server. You can set the following values:

- *Subtype* — The type of server the record points to. You can use one of the following values:
  - `1` — An AFS location server.
  - `2` — A DCE authentication server.
- *Hostname* — The domain name of the database server.

CAA

Certificate Authority Authorization Record — This record controls which certificate authorities (CA) can issue SSL certificates for a domain.

> **Note:**
>
> - If no CAA records exist for a domain, **all** CAs can issue certificates for that domain. If conflicting CAA records already exist, remove the existing CAA records or add one for the desired CA.
> - MyDNS does **not** support this record type.
> - The system stores these records in the RFC 3597 format.

You can set the following values:

- *Issuer Critical Flag* — Whether the CA will issue an SSL certificate if the CAA Resource Record contains unknown property tags. For more information about CAA record flags, read the RFC 6844 documentation.

  - *0* — Non-critical. The CA will issue an SSL certificate if the CAA Resource Record contains unknown property tags.
  - *1* — Critical. The CA will **not** issue an SSL certificate if the CAA Resource Record contains unknown property tags.
- *Tag* — The CAA record's property type:
  - *issue* — Authorize a CA to issue a certificate for the domain.
  - *issuewild* — Authorize a CA to issue a wildcard certificate for the domain.
  - *iodef* — Specify a URL to which a CA may report policy violations.
- *Value* — The CA's domain, or the CA's URL if you select the *iodef* setting in the *Tag* section.

CNAME

Canonical Name Record — This record creates an alias for another domain name, which DNS resolves. This is useful, for example, if you point multiple CNAME records to a single A record in order to simplify DNS maintenance. You can set the following values:

- *Name* — A new or existing DNS zone name. When you enter a zone name, the system automatically appends the domain name to the zone record. For example, if you create the `user` zone, the system will add the `example.com.` domain information.
- *Record* — Enter a fully-qualified domain name (FQDN). For example, the `example2.com` domain. You cannot point a CNAME record to an IP address.

DMARC

Domain-based Message Authentication, Reporting, and Conformance — This record indicates the action for a mail server to take when it receives an email from this domain, but that message fails Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) checks.

When you select this setting, the system creates a TXT record with a default DMARC record. The system also displays a form that allows you to define the domain's DMARC *Policy* (*None*, *Quarantine*, or *Reject*), as well as the following optional parameters:

- *Subdomain Policy* — The action the mail server will take when it receives an email from the domain's subdomain. The server only takes this action if the email fails its SPF and DKIM checks.
  - *None* — Do not take any action.
  - *Quarantine* — Send spam email to a different folder on the account.
  - *Reject* — Reject spam email.
- *DKIM Mode* — The DKIM level that the server enforces for the domain. An email must have a valid DKIM signature. The server will check a DKIM signature against the email's `From:` domain entry. You can set the following identifier alignment settings:
  - *Relaxed* — Only the organizational domains must match. For example, an email from the `domain.example.com` subdomain of `example.com` would pass the DKIM check.
  - *Strict* — The domains **must** match exactly. For example, the server will accept email from the `example.com` domain, but it would reject email from the `domain.example.com` subdomain.
- *SPF Mode* — The SPF level that the server will enforce for the domain. The server sending email must pass SPF authorization. The server checks the server sending an email with the SMTP `MAIL FROM` command. The server then checks the `MAIL FROM` domain entry against the email's `From:` domain entry. You can set the following identifier alignment settings:
  - *Relaxed* — Only the organizational domains must match. For example, an email from the `domain.example.com` subdomain of `example.com` would pass the SPF check.
  - *Strict* — The domains **must** match exactly. For example, the server will only accept email if the domain is `example.com`. It would reject an email from the `domain.example.com` domain.
- *Percentage* — The percentage of emails that you want the server to filter.
- *Generate Failure Reports When* — The error reporting policy between the sender and receiver's Mail Transfer Agents.
- *Report Format* — The format that the server uses to report an email's possible spam status.
- *Report Interval* — The amount of time, in seconds, that elapse between each aggregate email report. This parameter's value defaults to `86400`.

  > **Note:**
  >
  > This value does **not** include email failure messages.

- *Send Aggregate Mail Reports To* — A comma-separated list of Uniform Resource Identifiers (URIs) to which to send the aggregate email reports. If your URI includes a comma, you **must** URI-encode the comma. To add a size limit for the report, include an exclamation point, a number, and a file size unit to the end of the URI. For example: `mailto:reports@example.com!50m`. You can specify the following file size units:
    - `k` — Kilobytes.
    - `m` — Megabytes.
    - `g` — Gigabytes.
    - `t` — Terabytes.
- *Send Failure Reports To* — A comma-separated list of URIs to which to send failure email reports.

DNAME

Delegation Name — This record sets an alias for an entire DNS name space. This differs from the CNAME record, which only provides an alias for a single name.

DS

Delegation Signer — This record identifies the DNSSEC signing key of a delegation zone. You can obtain this information from your domain's registrar.

> **Important:**
>
> This record type does **not** update the information with your registrar.

You can set the following values:

- *Key tag* — The key tag of the DNSKEY the DS record refers to, in network byte order.
- *Algorithm* — The algorithm number of the DNSKEY the DS record refers to.
- *Digest Type* — The algorithm used to generate the *Digest* field.
- *Digest* — The digest that the algorithm generates.

For more information, read the View DNSSEC Keys section.

HINFO

Host Information — This record provides information about the host's CPU type and operating system. This allows protocols to choose the best way to communicate with a similar host. You can set the following values:

- *CPU* — The host's CPU type.
- *Operating System* — The host's operating system.

LOC

Location Record — This record specifies a domain name's geographical location. You can set the following values:

- *Latitude* — The location's latitude, in Degrees Minutes Seconds (DMS) format.
- *Longitude* — The location's longitude, in Degrees Minutes Seconds (DMS) format.
- *Altitude* — The location's altitude, in meters.
- *Size* — The diameter of a sphere that encloses the entire location, in meters,
- *Horizontal* — The location's horizontal precision, in meters.
- *Vertical* — The location's vertical precision, in meters.

MX

Mail Exchanger — This record identifies the servers that handle a domain's email. Changes that you make to this record control where the server delivers a domain's email. You can set the following values:

- *Priority* — Identifies the servers that handle a domain's email. This value for each MX record determines the order in which other mail servers will use the domain's mail server. A lower value indicates a higher priority level. A value of `0` indicates the highest priority level.
- *Destination* — The mail server. This must be a fully-qualified domain name (FQDN).

NAPTR

Naming Authority Pointer — This record specifies a regular-expression-based rewriting rule. This creates a domain label to use with lookup services that aren't in domain name syntax. You can set the following values:

- *Order* — A 16-bit unsigned integer that specifies the order that the NAPTR records process. Low numbers process before high numbers.
- *Preference* — A 16-bit unsigned integer. This value sets the order in which two or more records with identical *Order* values process. Low numbers process before high

numbers.

- *Flags* — A flag that controls how NAPTR uses the query output. You can use one of the following flags: `S`, `A`, `U`, or `P`.
- *Service* — A string that specifies the protocol and service available on the rewrite path.
- *Regexp* — A string that contains the regex expression to find the next domain lookup.
- *Replacement* — The next fully-qualified domain name (FQDN) to query. This action depends on the *Flags* field.

NS

Name Server Record — This record delegates a DNS zone to use the specified authoritative name server. This must be a fully-qualified domain name (FQDN).

PTR

PTR Resource Record — This record provides a pointer to a canonical name. Unlike the CNAME record, DNS processing stops and **only** returns the name. This is most commonly used to implement reverse DNS lookups.

RP

Responsible Person — This record provides information about the person responsible for the domain. You can set the following values:

- *Mbox-dname* — The responsible person's email address. Replace the `@` in the email address with a period (`.`) character. This entry **must** end in a period (`.`) if you use a fully-qualified domain name.
- *Txt-dname* — A related hostname or domain name for which TXT records exist. This entry **must** end in a period (`.`).

SOA

Start of Authority Record — This record specifies the authoritative information about a DNS zone. This includes the following information:

- Primary name server.
- The domain administrator's email.
- The domain's serial number.
- Other information related to refreshing the zone.

> **Important:**
> You **cannot** add or delete an SOA record. You can only edit it.

This record contains the following values:

- *Serial* — The version number of the original copy of the zone. Zone transfers will preserve this value.

  > **Note:**
  > You **cannot** edit this value. This value increments by one every time you alter a domain's DNS record.

- *Mname* — The name server that provides the data for a zone.
- *Retry* — The time interval, in seconds, before the zone tries to refresh again after a failure.
- *Refresh* — The time interval, in seconds, before the zone refreshes.
- *Expire* — The time interval, in seconds, that specifies the time before a zone is no longer authoritative.
- *Rname* — The responsible person's email address. Replace the `@` in the email address with a period (`.`) character. This entry **must** end in a period (`.`) if you use a fully-qualified domain name.

SRV

Service Record — This record provides data about available services on specific ports on your server. You can set the following values:

- *Priority* — The service record's priority value. A lower value indicates a higher priority level. A value of `0` indicates the highest priority level.
- *Weight* — This value ranks entries that share the same *Priority* value. For example, a record with a `0` priority level and an `8` weight value will rank lower than a record with a `0` priority level and `4` weight value.
- *Port* — The service's target port number.
- *Target* — The service's target hostname.

TXT

Text Record — This record contains text data for various services to read. For example, TXT records can specify data for SPF, DKIM, or DMARC email authentication. You can use WHM's *Email Deliverability* interface (*WHM >> Home >> Email >> Email Deliverability*) to manage your server's SPF and DKIM records.

> **Important:**
> The *Record* text box will accept invalid data. Make **certain** you enter the correct record information.

Delete a DNS zone record

To delete a DNS zone record, perform the following steps:

1. Click *Manage* for the domain that you want to modify. A new interface will appear.
2. Click *Delete* next to the record that you want to remove.
3. Click *Continue* to delete the record, or click *Cancel*.

Reset DNS zone files

> **Important:**
> When you reset a zone file, the system removes **all** custom zone records. Make certain that you save any records you wish to keep **before** you perform this action.

To reset a domain's DNS zone file, perform the following steps:

1. Click *Manage* for the domain that you want to modify. A new interface will appear.
2. In this interface, click *Actions* above the zone record table.
3. Select *Reset DNS Zone* from the menu. A confirmation window will appear.
4. Click *Continue* to reset the domain's DNS zone file, or click *Cancel*.

View Raw DNS Zone File

To view the DNS zone file in raw format, perform the following steps:

1. Click *Actions* above the zone record table.
2. Select *View Raw DNS Zone File* from the menu. A new interface will appear that displays the DNS zone file in its raw format.
3. To copy the file, click *Copy*, or click *Return to Editor* to exit the *Manage DNS Zone Records* interface.

View DNSSEC Keys

This interface lets you manage a domain's DNSSEC keys. DNSSEC keys use digital signatures to strengthen DNS authentication. These digital signatures use public key cryptography to sign the DNS data. However, these digital signatures do **not** sign the DNS queries and responses.

The interface displays the following information:

- › — This setting will display the following details about a DNSSEC key:
  - *Algorithm* — The DNSSEC key's algorithm.
  - *Status* — Whether the key is active or inactive.
  - *Deactivate* — Deactivate the DNSSEC key. If you click this setting, a confirmation window will appear.
  - *Delete* — Delete the DNSSEC key. If you click this setting, a confirmation window will appear.

    > **Important:**
    > When you deactivate or delete a DNSSEC key, you **must** remove the Domain Server (DS) record at your domain registrar.

  - *Public DNSKEY* — Display the public DNSKEY record. The *Public DNSKEY* interface will appear.
- *Key Tag* — An integer value that identifies the domain's DNSSEC record.
- *Key Type* — Whether the key configuration is Zone Signing Key (ZSK), Combined Signing Key (CSK), or Key Signing Key (KSK).
- *Algorithm* — The algorithm type that constructs the digests.
- *Created* — The key's creation date.

You can also perform the following actions for each DNSSEC key:

- *View DS Records* — Display the domain's DS records. The DNSSEC Key Details interface will appear.

- *Export* — Export the domain's DNSSEC key. The Export DNSSEC Key interface will appear.

Create Key

This feature lets you create a new DNSSEC key. You can select whether to create a system-generated key, or create a customized DNSSEC key.

> **Important:**
> When you create a domain DNSSEC key, you **must** configure a DS record with your domain registrar.

Quick DNSSEC key creation

To quickly create a DNSSEC key, perform the following steps:

1. Click *Create Key*. A confirmation window will appear.
2. Click *Create*. The *DNSSEC Key Details* interface will appear with the keys' details.

Custom DNSSEC key creation

To create a custom DNSSEC key with a stronger algorithm, perform the following steps:

1. Click *Create*. A confirmation window will appear.
2. Click *Customize*. The *Create DNSSEC Keys* interface will appear.
3. In the *Key Setup* section, select the desired DNSSEC key configuration:
    - *Classic* — Create with a ZSK and a KSK keypair.
    - *Simple* — Create with a CSK, which the system will use as both the ZSK and KSK. This setting **disables** the *RSA/SHA-256 (Algorithm 8)* and *RSA/SHA-512 (Algorithm 10)* settings in the *Algorithm* section.
4. In the *Algorithm* section, select the desired algorithm:
    - *RSA/SHA-256 (Algorithm 8)*
    - *RSA/SHA-512 (Alroithm 10)*
    - *ECDSA Curve P-256 with SHA-256 (Algorithm 13)*
    - *ECDSA Curve P-384 with SHA-384 (Algorithm 14)*
5. In the *Status* section, select whether to activate the newly-generated key.
6. Click *Create Key*. An interface will appear with the new key's details.
7. To enable DNSSEC for your domain, you **must** go to your domain registrar. Use the information provided in this interface to fill out their DNSSEC forms. For more information about some popular domain registrars, read the Domain registrar DS records section.

Import Key

This feature lets you import a DNSSEC key. When you select this setting, the system directs you to the *Import DNSSEC Key* interface. In this interface, you can perform the following steps:

1. In the *Key Type* menu, select whether to import a key as a KSK or ZSK key.
2. Enter the DNSSEC key's details in the text box provided in the *Key* section.
3. Click *Import* to import the DNSSEC key. A confirmation interface will appear.

Export

This feature provides the information you need to export a DNSSEC key. When you select this setting, the system directs you to the Export DNSSEC Key interface. This interface displays the following details about a domain's DNSSEC key:

- *Domain* — The domain in the DNS record.
- *Key Tag* — An integer value that identifies the domain's DNSSEC record.
- *Key Type* — Whether the key is ZSK, CSK, or KSK.
- *Key* — The DNSSEC key. Click *Copy* to copy the key to your computer's clipboard.

Public DNSKEY

This feature allows you to view a public DNSKEY record's details. When you select this setting, the system directs you to the *Public DNSKEY* interface. This interface displays the following information:

- *Domain* — The domain in the DNS record.
- *Public DNSKEY* — The public DNSKEY record.

View DS Records

This feature allows you to view a DNSSEC key's details. When you select this setting, the system directs you to the *DNSSEC Key Details* interface. This interface displays the following information:

- *Domain* — The domain in the DNS record.
- *Key Tag* — An integer value that identifies the domain's DNSSEC record.
- *Algorithm* — The algorithm type that constructs the digests.
- *Created* — The key's creation date.
- *Digests* — The alphanumeric strings the algorithm generates.

To add a DS Record to the domain's registrar, perform the following steps:

1. Determine the digest type that your registrar uses.
2. Click *Copy* for the appropriate digest record.
3. Visit your registrar's website and add the information that they request for your domain. For more information about some popular domain registrars, read the Domain registrar DS records section.

Domain registrar DS records

Any time you create, modify, or remove a domain's DNSSEC key, you **must** configure a Delegation Signer (DS) record with your domain registrar. The following are some of the most popular domain registrars. Visit their website to read their DNSSEC management documentation.

- GoDaddy
- Namecheap
- OpenSRS

Additional Documentation

Delete a DNS Zone
Edit DNS Zone
Edit MX Entry
Edit Zone Templates
Email Routing Configuration