

Table of Contents

Overview

Domains

Manage Zone

[Add a DNS zone record](#)

[Edit a DNS zone record](#)

[Delete a DNS zone record](#)

[Reset zone files](#)

DNSSEC

[DNSSEC Keys table](#)

[Create Key](#)

[Import a DNSSEC key](#)

[Export a DNSSEC key](#)

[Public DNSKEY](#)

[DS Records](#)

[Delete a DNSSEC key](#)

[Domain registrar DS records](#)

Did you find this document helpful?



# Zone Editor

Version: 82 84 86 88 96

Valid for versions 96 through the latest version

Last modified: March 25, 2021

## Overview

The *Zone Editor* feature allows you to create, edit, and delete Domain Name System (DNS) zone records. DNS converts human-readable domain names (for example, [example.com](#)) to computer-readable IP addresses (for example, [192.0.0.1](#)). DNS relies on zone records that exist on your server to map domain names to IP addresses.

## Domains

By default, the *Zone Editor* interface displays a list of your domains and their DNS zone records. To filter the list, enter a name in the text box or select an available record type filter.

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 [Domain Name System Security Extensions \(DNSSEC\)](#) records. When you select this record type, the system directs you to the [DNSSEC](#) interface.
- Manage* — Add or edit additional domain records. When you click *Manage*, the system directs you to the [Manage Zone](#) interface.

To refresh the list of domains, click the gear icon and select *Refresh List*.

## Manage Zone

The *Manage Zone* interface displays the DNS zone records for the selected domain. 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.
- [Reset the zone files](#).

### Important:

To access all available zone record types and records that the system automatically generated, your systems administrator must enable the following features in WHM's [Feature Manager](#) interface (*WHM >> Home >> Packages >> Feature Manager*):

- Zone Editor (A, CNAME)*
- Zone Editor (AAAA, CAA, SRV, TXT)*

## Add a DNS zone record

To add a record, perform the following steps:

1. Click *Manage* for the domain that you want to modify. A new interface will appear.
2. Click *Add Record*. You can also click the arrow icon (▼) next to *Add Record* and select the [desired record type](#) from the menu.

**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's information.
4. Click *Save Record* or *Save All Records*, or click *Cancel*.

## Edit a DNS zone record

To edit a 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.

### 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 option, 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.

## 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).

## 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 (*cPanel >> 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 record, perform the following steps:

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

## Reset zone files

### Important:

- This function erases any modifications that you made to your zone records. The system attempts to save the domain's TXT entries. We recommend that you record any changes that you want to save before you use this feature.
- To reset your DNS zone files, your systems administrator must enable the following features in WHM's [Feature Manager](#) interface (*WHM >> Home >> Packages >> Feature Manager*):
  - *Zone Editor (A, CNAME)*
  - *Zone Editor (AAAA, CAA, SRV, TXT)*

To reset your DNS zone files to the defaults that your hosting provider specifies, perform the following steps:

1. Click *Manage* next to the domain that you want to reset. A new interface will appear.
2. Click *Actions* and select *Reset DNS Zone*.
3. Click *Continue* to reset your zone, or click *Cancel*.

## DNSSEC

The *DNSSEC* interface lets you manage your domain's DNSSEC keys. [DNSSEC](#) can help to protect you from various forms of attack, such as spoofing or a [Man-in-the-Middle](#) attack. A DNS resolver will compare the DNS server's DNSKEY record to the Delegation Signer (DS) record at your domain's registrar. If the records match, then the DNS resolver knows that the record is valid.

DNSSEC uses 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.



### Important:

If you transfer the account to another server, you **must** remove the DS records from the registrar before you transfer the domain. If you do not remove the old DS records from the registrar, the domains may produce DNS resolution issues due to invalid DNSSEC responses.

To transfer an account with DNSSEC-enabled domains, perform the following steps for each domain:


1. Remove the DS records from the registrar.
2. Wait for the changes to propagate. This may take up to 72 hours.
3. Perform the transfer.
4. Manually update the registrar with the new DS records.

## DNSSEC Keys table

### Important:

If you deactivate or delete a DNSSEC key, you **must** remove the DS record at [your domain registrar](#).

The *DNSSEC* interface displays a table that lists the following information:

-  — Click the arrow icon to display the following details about the DNSSEC key:
  - *Algorithm* — The key's [algorithm](#).
  - *Status* — Whether the key is active or inactive.
  - *Activate* or *Deactivate* — Activate or deactivate the key. Deactivating a DNSSEC key will **not** delete it.
  - *Delete* — Delete the key.
  - *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 is a Zone Signing Key (ZSK), Combined Signing Key (CSK), or Key Signing Key (KSK).
- *Algorithm* — The DNSSEC algorithm type that constructs the digest.
- *Created* — The key's creation date.

### Note:

The interface will display a recommendation for when you should rotate a DNSSEC key. For information, read our [How to Rotate a DNSSEC Key](#) documentation.

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

- *View DS Records* — Display the domain's DS records. The [DS Records](#) interface will appear.
- *Export* — Export the domain's DNSSEC key. The [Export](#) interface will appear.

## Create Key

### Important:

When you create a domain's DNSSEC key you **must** also configure a DS record with [your domain registrar](#).

The *Create Key* function lets you create a new DNSSEC key. You can select whether to create a system-generated key or create a customized DNSSEC key:

## Quick DNSSEC key creation

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

1. Click *Create Key*. A confirmation interface will appear.
2. Click *Create*. The *DS Records* interface will appear with the new DNSSEC key's details.

## Custom DNSSEC key creation

If you want to create a customized key with a stronger algorithm, perform the following steps:

1. Click *Create*. A confirmation window will appear.
2. Click *Customize*. The *Generate* interface will appear.
3. Select the desired key setup for the DNSSEC key:

- *Classic* — Creates a ZSK and a KSK.
  - *Simple* — Creates a CSK, which the system will use as both the ZSK and KSK.
4. Select the desired algorithm from the *Algorithm* menu.

**Note:**

The interface disables incompatible algorithms.

5. Select whether to activate the newly-generated key.
6. Click *Create Key*. The *DS Records* interface will appear with the new DNSSEC key's details.

To validate the DNSSEC configuration for a domain, use Verisign's [DNSSEC Analyzer](#) website.

## Import a DNSSEC key

The *Import* interface lets you import an existing DNSSEC key. To import a DNSSEC key for a domain, perform the following steps:

1. Click *Import Key*. The *Import* interface will appear.
2. Select the key type that you want to import:
  - *ZSK* — Zone Signing Key.
  - *KSK* — Key Signing Key.
3. Enter the key information in the *Key* text box.
4. Click *Import*.

## Export a DNSSEC key

The *Export* interface provides the information you need to export a DNSSEC key. 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

The *Public DNSKEY* interface lets you view a public DNSKEY record's details. This interface displays the following information:

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

## DS Records

When you click *View DS Records* for a key, the *DS Records* interface will appear. This interface displays the following DNSSEC key 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 digest.
- *Created* — The key's creation date.
- *Digests* — A list of available digests. The interface displays each digest's algorithm type (*Digest Type*) and algorithm information (*Digest*).

You can use this information to add a DS record to [your domain's registrar](#). To do so, perform the following steps:

1. Determine the *Digest Type* that your registrar uses.
2. Click *Copy* for the appropriate *Digest* record.
3. Go to your registrar's website and add the information that they request for your domain.

## Delete a DNSSEC key

**Important:**

Before you delete the domain's DNSSEC key in cPanel & WHM, you **must** remove or disable the DS with [your domain registrar](#). After editing the DS record, wait at least 24 hours for the changes to propagate. Once the changes propagate, you may delete the DNSSEC key in cPanel & WHM.

To delete a DNSSEC key, perform the following steps:

1. Click *Delete* next to the appropriate record.
2. Click *Continue* to confirm that you want to delete the security record.

# Domain registrar DS records

Any time you create, modify, or remove a domain's DNSSEC key, you **must** update your 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

---

[Addon Domains](#)  
[Domains](#)  
[Dynamic DNS](#)  
[Redirects](#)  
[Site Publisher](#)



© 2021 All Rights Reserved / [Legal Notices](#) / [Privacy Policy](#) / [Transparency Report](#)

cPanel, WebHost Manager and WHM are registered trademarks of cPanel, L.L.C. for providing its computer software that facilitates the management and configuration of internet web servers.