Email Deliverability in cPanel

(*cPanel >> Home >> Email >> Email Deliverability*)

Overview

Use this interface to identify problems with your mail-related DNS records for one or more of your domains. The system uses these records to verify that other servers can trust it as a sender.

> **Note:**
> - Both DKIM and SPF authentication **require** that you use a DNS server for the domain name. For more information about your DNS servers, contact your hosting provider.
> - The system modifies DKIM and SPF records if it is authoritative for a domain's DNS records.

Email Deliverability table

This table displays your cPanel account's domains and allows you to address any existing problems with your mail-related DNS records.

- Use the navigation controls at the top of the table to search for a domain or navigate through the pages of results.
- Click the gear icon (⚙▾) to select the number of entries you want to display per page or refresh the table results.

Column	Description
Domain	Click *Domain* to sort the list alphabetically by domain name. Click an individual domain to view its public-facing website. **Note:** The *Main Domain* label (Main Domain) identifies the domain that your hosting provider used to create this account.
Email Deliverability Status	Whether a problem exists with the domain's mail-related DNS records.

In This Document

Related Documentation

- Spam Filters
- Mailing Lists
- Global Email Filters
- Forwarders
- Email Filters

For Hosting Providers

- How to Configure the Apache SpamAssassin Report_Safe Option
- Email
- How to Keep your Email Out of the Spam Folder
- How to Prevent Email Abuse
- How to Prevent Spam with Mail Limiting Features

Actions	For each domain, you can perform the following actions: • *Repair* — This feature allows the system to repair a domain's invalid records. A window appears in the interface that allows you to review and confirm the system's recommendations for any invalid records. You can copy or customize a suggested record before you approve the system's repairs. The system will recheck any repaired records. This process can take up to five minutes, depending on the server. **Note:** • This option is unavailable if the system does not control the domain's DNS records. • You **cannot** simultaneously update two or more domains whose records exist on the same zone. However, if two or more domain's records exist on separate zones, you can simultaneously update them. • Reloading the interface does **not** interrupt the repair process. • *Manage* — The *Manage the Domain* interface will appear. This interface allows you manually resolve issues with your domain's mail-related DNS records.

Manage the Domain

The *Manage the Domain* interface allows you to manually configure a domain's mail-related DNS records. Use this interface to resolve any outstanding issues with a domain's records.

The top of this interface displays the following information:

- *Domain* — The domain name.
- *Mail HELO* — The domain's HELO configuration.

> **Note:**
> This information appears if the HELO configuration and domain do **not** match.

DKIM

This section allows you to manage a domain's Domain Keys Identified Mail (DKIM) record. DKIM verifies the sender and the integrity of a message. In addition, it allows an email system to prove that spammers did not alter an incoming message while in transit. DKIM also verifies that the messages your domains receive come from the specified domain.

If any problems exist with the current record, this section displays the properly-configured DKIM record values in the *Suggested "DKIM" (TXT) Record* section. It also allows you to perform the following actions:

- *Generate Local DKIM Key* — Generate a DKIM record, if one does not exist.
- *Copy* — Copy the *Name* and *Value* records that the system provides in the *Suggested "DKIM" (TXT) Record* section. If you do not possess the authority to edit your record, you can provide this information to the person responsible for the listed nameservers to fix it.

> **Note:**
> The *View* option allows you to modify the record displayed in the *Value* field:
>
> - *Full* — The record displays in its entirety. This option is for providers who automatically split their records.

- *Split* — The record, divided into 255-character parts. This option is for providers who do not automatically split their records.

- *View* — Modify the *Value* field's displayed record:
  - *Full* — The record displays in its entirety. This option is for providers who automatically split their records.
  - *Split* — The record, divided into 255-character parts. This option is for providers who do not automatically split their records.
- *Download the Private Key* — Retrieve the suggested private key. The system directs you to the *Download the Private DKIM Key* interface.

> **Important:**
> Exposing your private DKIM key is a **security risk**. If others obtain your private DKIM key, they could sign emails and impersonate you as a sender. Make **certain** that you only provide your private DKIM key to a trusted user.

> **Note:**
> If your hosting provider installs the DSO PHP handler **without** ModRuid2 or MPM ITK, and you enable DKIM, emails that you send will display `nobody` as the sender. The system will **not** display any information in the `Return-Path`, `Reply-To`, or `From` fields in the email header.
>
> To add these fields to the email headers, contact your hosting provider and request that they add the missing fields via the following PHP script:
>
> ```
> <?php
> $to      = 'nobody@example.com';
> $subject = 'the subject';
> $message = 'hello';
> $headers = 'From: webmaster@example.com' . "\r\n" .
>     'Return-Path: webmaster@example.com' . "\r\n" .
>     'Reply-To: webmaster@example.com' . "\r\n" .
> mail($to, $subject, $message, $headers);
> ?>
> ```
>
> > **Warning:**
> > cPanel, L.L.C. does **not** recommend this configuration.

SPF

This section allows you to manage a domain's Sender Policy Framework (SPF) record. SPF verifies that the messages your domains send originated from a listed server. In addition, it provides a list of servers approved to send mail from your domains.

If any problems exist with the current record, a correct SPF record configuration will appear in the *Suggested "SPF" (TXT) Record* section. This section also allows you to perform the following actions:

- *Copy* — Copy the *Name* and *Value* records that the system provides in the *Suggested "SPF" (TXT) Record* section. If you do not possess the authority to edit your record, you can provide this information to the person responsible for the listed nameservers to fix it.
- *View* — Modify the *Value* field's displayed record:
  - *Full* — The record displays in its entirety. This option is for providers who automatically split their records.
  - *Split* — The record is divided into 255-character parts. This option is for providers who do not automatically split their records.
- *Customize* — Modify the the suggested SPF record. This directs you to the *Customize an SPF Record* interface.

Customize an SPF Record

Use this interface to customize the system's recommended SPF record for a domain. The interface displays the domain's current SPF name and value in the *Current "SPF" (TXT) Record* section, if one exists, and the system's recommendations in the *Suggested "SPF" (TXT) Record* section.

You can configure the following settings:

Domain Settings

This section allows you to define the hosts or MX servers allowed to send mail from your domain.

Setting	Description
Additional Hosts	Additional hosts that the system allows to send mail from your domains. The system automatically includes the primary mail exchanger and other servers for which you created an MX record. • Click *Add A New "Host (+a)" Item* to add a new host to the domain's SPF record.
Additional MX Servers	The MX entries allowed to send mail from your domains. • Click *Add A New "+mx" Item* to add a new MX entry to the domain's SPF record.

IP Address Settings

This section allows you to add additional IP Address blocks to the domain's SPF record. The system automatically includes your server's main IPv4 or IPv6 addresses in these lists.

> **Note:**
> You can use CIDR notation (for example, `10.0.0.0/8` for IPv4, or `2001:db8:1a34:56cf::/64` for IPv6).

Additional Settings

This section allows you to modify additional SPF record settings.

Setting	Description
Include List (INCLUDE)	Additional domains to include in your SPF settings. Use this setting, for example, when you send email through another service, such as Mailchimp ®. • Click *Add A New "+include" Item* to add a new domain approved to send mail from your domain.
Exclude All Other Hosts ("-all" Entry)	Exclude any hosts that the other SPF mechanisms do **not** allow. **Note:** • If you enable this setting, the SPF feature causes hosts that you do **not** define to fail. • By default, the system recommends the ~a authorization.

Preview of the Updated Record

This section displays what the updated SPF record will look like, based on its current modifications. Click *Install a Customized SPF Record* to install the new record.

> **Note:**
> If you do **not** possess the authority to update this record, the system **disables** the *Install a Customized SPF Record* option. Use the *Copy* option to copy the record to your computer's clipboard. Email this information to the person responsible for the nameservers and request that they update the SPF record on the authoritative nameserver.

Reverse DNS (PTR)

This section allows you to view and verify a domain's current pointer record (PTR). A PTR record is a DNS record that resolves an IP address to a domain or host name. The system uses this record to perform a reverse DNS (rDNS) lookup to retrieve the associated domain or host name. A PTR record requires an associated A record.

The interface provides information when a problem exists with this record. It also provides instructions for how to fix your PTR record.

> **Note:**

- You **must** have the authority to update a domain's PTR record. If you do not, contact the owner of the IP address. For example, the IP address's data center or your service provider.
- If smarthosting exists on the server, it will **not** display this section.