Authentication

(cPanel >> Home >> Email >> Authentication)

Overview

cPanel's *Authentication* interface allows you to enable or disable Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF). These features provide information about incoming mail. The system uses this information to verify that a trusted sender sent the messages.

Notes:

- Both the DKIM and SPF authentication functions require that you use a DNS server for the domain name. For more information about DNS servers, contact your hosting provider.
- You may see a warning that the system cannot verify the server as an authoritative nameserver for the specified domain name. If either of the following scenarios is true, ignore the warning:
  - You designated the server as the authoritative DNS server for the domain name, but the change did not yet propagate.
  - The server does not view itself as the authoritative DNS server, but outside servers view it as the authoritative DNS server.

DKIM

DKIM verifies the sender and integrity of a message. It allows an email system to prove that spammers did not alter an incoming message while in transit (forgery). DIM also verifies that the messages your domains receive come from the specified domain.

- To enable DKIM, click *Enable*.
- To disable DKIM, click *Disable*.

If your hosting provider installs the DSO PHP handler and you enable DKIM, emails that you send will show `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);
?>
```

SPF

SPF attempts to deny spammers the ability to send email while they forge your domain's name as the sender (spoofing). SPF adds IP addresses to a list of servers that can send mail from your domains. It verifies that messages that your domains send originated from the listed server, which reduces the amount of backscatter that you receive.

- To enable SPF, click *Enable*.
- To disable SPF, click *Disable*.

In This Document

Related Documentation

- Two-Factor Authentication for cPanel
- Authentication

For Hosting Providers

- The failurls File
- Enable DKIM SPF Globally
- Manage External Authentications
- Manage Wheel Group Users
- Two-Factor Authentication for WHM

Advanced settings

You can use the following *Advanced Settings* options to further configure SPF:

> **Notes:**
> - Click *Add* to add domains.
> - Click *Remove* to remove domains.
> - Click *Update* to save your changes.

Setting	Description
Additional Hosts that send mail for your domains (A)	Additional hosts that the system automatically approves to send mail from your domains.
Additional MX servers for your domains (MX)	MX entries that can send mail from your domains.
Additional IP Address blocks for your domains (IPv4 or IPv6)	IP addresses (IPv4 or IPv6) that you approve to send mail from your domains. The system automatically includes your server's main IP addresses in this list. **Note:** You **must** use CIDR notation (for example, `192.168.0.1`, `127.0.0.1/8`, or `2001:db8:1a34:56cf::/64`).
Include List (INCLUDE)	Additional domains to include in your SPF settings. Use this setting, for example, when you send mail with another service.
All Entry (ALL)	Whether SPF causes undefined hosts to fail. - If you enable this setting, the SPF feature causes hosts that you do not define in the above lists to fail. - If you disable this setting, the SPF feature does **not** cause undefined hosts to automatically fail. Instead, the system marks undefined hosts as *Neutral.* When a server receives mail from a neutral host, it functions as though you disabled SPF. After you test the entries in the above lists, we **strongly** recommend that you enable this feature.
Overwrite Existing Entries	Whether to overwrite existing SPF entries. If you enable this setting, the system overwrites existing SPF entries.