



Proper DNS Settings for Email

Help Documentation

Proper DNS Settings for Email

There are several major things to set up on your DNS server for every domain you set up within SmarterMail. How you set these up is dependent upon two things: who hosts your DNS and what DNS software is used. Therefore, you'll need to check with your DNS provider, or check your DNS server documentation, for instructions on how to set up the following records. NOTE: In the items below, simply replace "example.com" with the proper domain name.

Also, please bear in mind that your DNS may need to be set up differently. This is only a guideline that is recommended for most installations.

General DNS Entries

There are several DNS entries that are required in order to run a mail server. These not only make the mail server visible to the world, but also can help ease the use of mail accounts by end users. Below, these are listed as well as their function.

- WebMail URL - In order to use a URL for allowing users to log in to their SmarterMail mailboxes, you'll need to add an A record for their domain. For example, "mail.example.com". This record will need to point to the IP address of the webmail interface for that domain.
- MX Record - This record should point to the A record you created. Again, "mail.example.com". This will allow other email servers to locate the mail server used for the domain.
- Reverse DNS Record - Add a reverse DNS record for any IP addresses assigned on the server to provide extra assurance to other mail servers. Also, it is recommended that the primary IP address of the server also have a reverse DNS record.
- Sender Policy Framework - Some large email providers like Gmail and Yahoo! require specially formatted TXT records to be added to your DNS. This special format is known as SPF (Sender Policy Framework). Information about how these records should be formatted can be found at <http://spf.pobox.com> . Please keep in mind that the owners of the domains may have significant input on what goes into these records.

Optional, But Recommended DNS Entries

Autodiscover

Autodiscover is a way to allow users to quickly and easily set up accounts in email clients, both on desktop and mobile. Autodiscover is just that: a way for user settings to be discovered, automatically, by the email client. These settings include incoming/outgoing mail server info, ports used, etc. However, in order for autodiscover to work, it requires DNS entries.

To set up autodiscover in DNS, you need to add the following:

- A Record - This should be set to "autodiscover.example.com", and point to the IP address of that domain's mail server. (I.e, the IP assigned to the webmail URL.)
- SRV Record - This record returns the available domain and the service being used back to the client. The format for the SRV is "_autodiscover._tcp.example.com". Here's an example of the SRV for SmarterTools:

```
Domain: smartertools.com Service: _Autodiscover Protocol: _tcp Priority: 0
Weight: 0 Port: 443
```

In addition to the DNS settings, above, you will also want to create a host header for your autodiscover URL in IIS that's tied to the SmarterMail web interface for a domain. As an example, SmarterTools has an IIS binding to ports 80 and 443 for "autodiscover.smartertools.com". This is in addition to the bindings created for "mail.smartertools.com" as that URL is what we use for setting up our mail clients and for accessing the web interface.

NOTE: Not all devices and email clients handle autodiscover in the same way. Therefore, just because you set up autodiscover doesn't mean it will work for each user.

DKIM

Most major email providers require an additional layer of security before they'll accept incoming email. Free email providers like Gmail, Yahoo! and Outlook.com are using these "mail signing protocols" as a way to further protect their users from unwanted email and phishing schemes. Therefore, having DKIM set up for your mail domains is a very, VERY good idea.

To set up DKIM, you'll first want to enable it for a domain within SmarterMail. This is handled on the Domain Admin side, so if you're logged in as a system administrator, you'll need to impersonate the Domain Administrator for any domain you set up with DKIM. Alternatively, you can Manage the domain as that automatically logs a system admin into a domain as the Domain Administrator.

Once you're managing the domain, go to the domain's Settings page. On the Email Signing card, click "Enable". A modal window opens up containing both a Text Record Name and a Text Record Value . BOTH of these need to be added as TXT records to the DNS for the domain in order for DKIM to work. You can simply copy/paste the values into whatever interface is used for DNS management. For example:

```
Host Name: 8D48750357DA749._domainKey.example.com Text:
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAK+caX2o1xAtkGdQSNrtNNhvNCpfbdxOVTmm+o10E7
uKWYTqbFuyFEncusd1XGNQSC8Nzifn0qikrgSBG0xHUZJ+6GVcyQw42oRl7Kej1F8YY
bX4uHzLVv1uned21eDpSiSOLca2Q0arBtlyxzPNZ4P8YqujHydRsRwfJvYqvO9ge5eJFbEwCXq0d1bF8F
```

cCkm6gghYzQyaPPCpni8bu99uYwlqf7kJHEG4gH2YKhkYDgzg61+3wmu7gIv6ix3p5rBFmY6tC62d5p9Y8ZOyL1kFGMnvKc1CaxkTCoupBOfl1TOkDMzwht3RGClOk5DX3in6/80DQmwsFNfZkDa3QIDAQAB Time
to Live (TTL): 5 minutes

Once DKIM is set up for a domain in SmarterMail, the domain administrator can modify the Settings and manage how closely the system monitors messages in transit. For more information, see the Settings page of SmarterMail help.