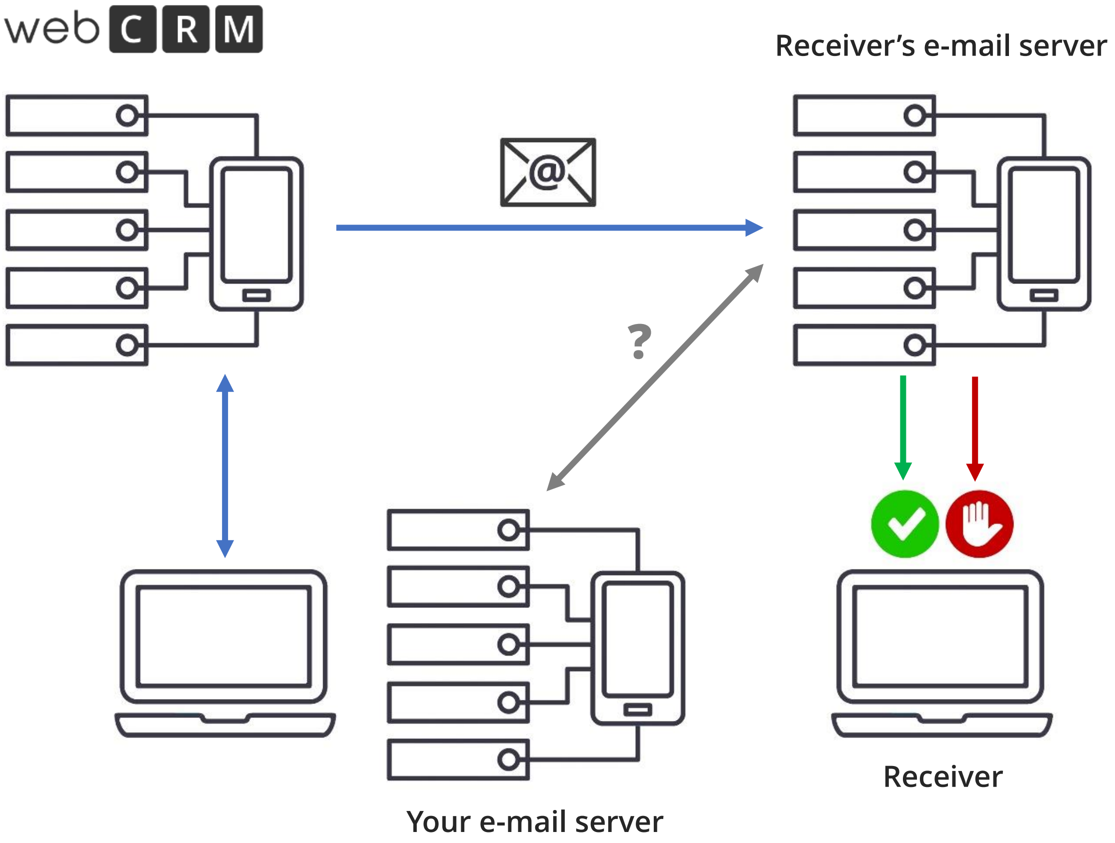
E-mails and Anti-spam

Standard authentication AUTH method

As the spammers become increasing aggressive more and more legit emails get banned as spam.

When you send e-mails from your webCRM system, we use the webCRM servers to send e-mails with your own e-mail address inserted as the sender of the e-mail. Many anti-spam engines mark such e-mails as a potential spam risk because the server sending the e-mail is not the server normally used for sending your e-mails.

1. You send an e-mail from your webCRM system
2. The e-mail arrives at the receivers e-mail server
3. The receiver's e-mail server asks your e-mail server if webCRM may send e-mails on your behalf
4. If this is not the case, then the e-mail may be considered as spam



In your own interest webCRM enforce a policy to reduce the risk of your e-mails being considered as spam.

It is important that your own e-mail server will permit webCRM servers to send e-mails on your behalf. To do this you need to define a so-called SPF record. This normally requires that you have your own e-mail domain. If your e-mail is for example an @hotmail e-mail address you should not send e-mails from webCRM.

To publish that you permit sending your e-mails from the webCRM e-mail domain you need to have your Internet Service Provide create or modify the SPF record to include records from: **spf.webcrm.com**.

Please refer to page 4 for technical details.

As an alternative to SPF records you may be able to permit your own e-mail server to relay the e-mail messages sent from webCRM.

If your security policies will permit relay then the webCRM servers can send the e-mails to your own e-mail server, and then your own e-mail server will send the emails on to the final receivers. It is recommended that you still create a SPF record for your own email server.

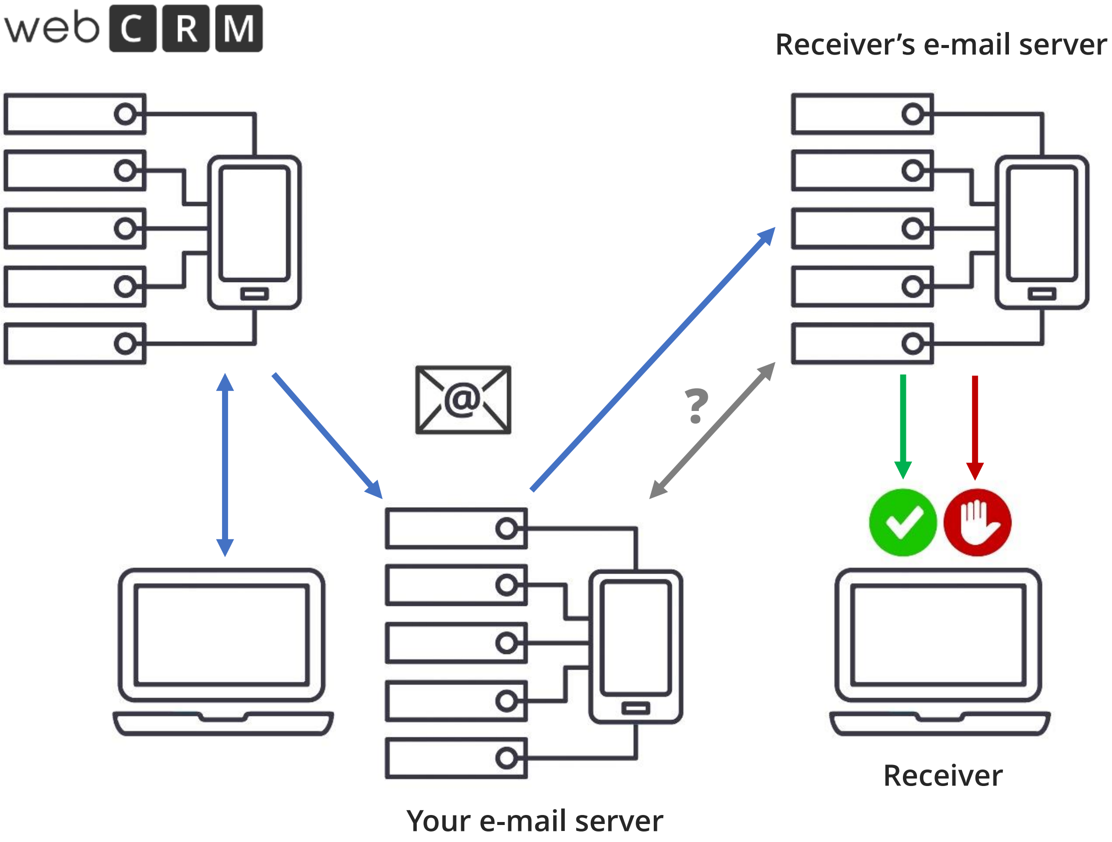
To enable this, please provide us with the following information:

- E-mail domain or IP address to relay by
- The port to relay by
- If you want to apply encryption (TLS)

To apply the standard authentication AUTH method, please also supply us with an account name (username) and password for your SMTP server.

Alternative method

As an alternative to the AUTH method you can instead have an IT professional capable of configuring/enabling the relay in your firewall / e-mail server. We cannot assist you directly with this task. You must enable/permit webCRM to SMTP relay from the IP: 89.188.84.106.



SPF records – a technical note

Sender Policy Framework (SPF) is an email validation system designed to prevent e-mail spam by detecting e-mail spoofing, a common vulnerability, by verifying sender IP addresses. SPF allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific SPF record (or TXT record) in the Domain Name System (DNS). Mail exchangers use the DNS to check that mail from a given domain is being sent by a host sanctioned by that domain's administrators.

Sender Policy Framework is defined in IETF publication RFC 4408.

To publish that you permit sending your e-mails from the webCRM e-mail domain you need to have your Internet Service Provide create or modify the SPF record to include records from:

spf.webcrm.com

SPF record formats do vary and you should consult your IT staff or Internet Service Provider for the exact format to use.

Example text for SPF record permitting webCRM SMTP server as well as your own e-mail server:

"v=spf1 ip4: 111.222.333.444 a mx include:spf.yourdomain.com include:spf.webcrm.com ?all"

"v=spf1 include:spf.webcrm.com ip4:111.222.333.444 -all"

Where 111.222.333.444 is the IP for your own smtp server and your domain is “yourdomain.com”.

What else can you do ?

Even if you have a correct SPF record your emails may still be considered as spam depending on the content of the email.

General Guidelines To Avoid Emails To Be Mistaken For Spam

If you run a mailing list, or email newsletter that sends out numerous similar or identical messages, you may risk being accused of sending spam. If you are accused of spamming, your ISP may cancel your account, you may lose the hosting of your website.

If possible, limit each email shot to 1000 emails.

If your emails are being sent to people who did not sign up to receive them, or to people who may have signed up and forgotten, you may begin receiving spam complaints. If these complaints make it to your Internet Service Provider, some of the consequences mentioned above may result. If unwilling receivers of your email report it to an internet blacklist, you may have your site may blacklisted by thousands of other internet servers.

If you add people to your list without their consent, you will often be labelled as a spammer. Spam doesn't necessarily have to be for bogus products and services. Your legitimate email newsletter may be considered spam simply because it was unsolicited.

If your emails are all identical, with no personalized information whatsoever, these may be considered spam as well. Since spam is mass-emailed to tens of thousands of individuals, its content is usually completely general. If your correspondence contains no personalized or unique information, or appears to be "canned" it may be mistaken for spam.

If you send emails to people on your mailing list that contain topics or information that are irrelevant to the original description of your mailing list, you may be considered a spammer. People who signed up for your list did so in order to receive pertinent information, if you wish to send them email on unrelated topics, you should ask their permission first. Also, if you send correspondence to people at a more frequent rate than you had specified when they signed up, this may be considered spamming as well.

What not to do:

- **E-mail text with more than 76 characters per line.**
  E-mails with text lines exceeding 76 characters in one line are likely to be considered as spam.
- **Do not purchase email lists or so-called opt-in lists** from companies claiming to have "thousands of legitimate email addresses". Most of these companies do not bother to check whether the addresses on their lists are valid and hardly ever ask for consent from their recipients. You will end up sending your mail to unwilling recipients and will be accused of spamming.
- **Do not send unsolicited e-mails with an "opt-out" option** and expect this to legitimize your e-mail. Users should not have to go through the trouble of opting out of a mailing list that they did not sign up for in the first place. Many internet users will also ignore the "opt-out" instructions because spammers use these to validate the e-mail addresses in their lists.
- **Do not request a receipt of delivery for your mailing list.** Many users consider this an invasion of privacy, and spammers also use this ploy for email verification.
- **Do not use any spamming or harvesting software.** This includes automated email programs, e-mail address guessing and verification programs, webpage spiders, Usenet harvesters, or any other unsolicited e-mail software. The use of these devices is universally attributed to spammers.
- **Do not send numerous identical messages.** If you are sending out multiple e-mails, attempt to personalize the subject and body of the messages so they are not completely general. Messages that appear "canned" are often considered spam.

What you should do:

- **Always DOUBLE VERIFY every e-mail address in your list.** This means that upon receiving an e-mail address from an online form, or by any other means, you should send a brief confirmation e-mail stating that their email address was submitted, and asking them to confirm their registration in your mailing list.
- K**eep track of where you receive every e-mail address on your list.** This way, if there is ever a dispute or complaint, you can provide your members with a complete history of their subscription. When you keep track of where each e-mail address came from, you can identify where the "dirty" source was, and cease to use it.
- **Keep your mailing list up to date.** Make requested contact changes promptly, and do requested removals immediately.
- **Personalize the subject and body of your e-mails.** Although this may take more time, it adds a level of credibility and professionalism that will set you apart from spammers.
- **State your terms clearly and stick to them.** If you are going to send out an e-mail every week, make sure that your recipients are aware of this, and do not send out any more than that. If you are going to be sending e-mail about one specific topic, stick to this topic and do not send out unrelated material without prior permission.