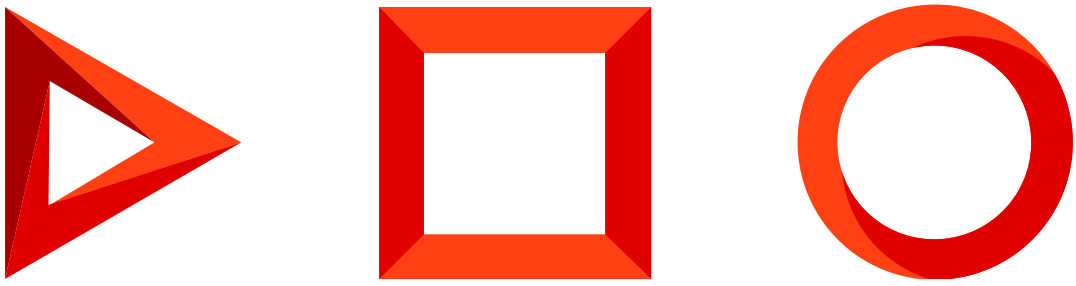
Creatio Academy

Elastic Email

Настроить верификацию для провайдера Elastic Email

Версия 8.0



Эта документация предоставляется с ограничениями на использование и защищена законами об интеллектуальной собственности. За исключением случаев, прямо разрешенных в вашем лицензионном соглашении или разрешенных законом, вы не можете использовать, копировать, воспроизводить, переводить, транслировать, изменять, лицензировать, передавать, распространять, демонстрировать, выполнять, публиковать или отображать любую часть в любой форме или посредством любые значения. Обратный инжиниринг, дизассемблирование или декомпиляция этой документации, если это не требуется по закону для взаимодействия, запрещены.

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления и не может гарантировать отсутствие ошибок. Если вы обнаружите какие-либо ошибки, сообщите нам о них в письменной форме.

Содержание

Настроить верификацию для провайдера Elastic Email

ПРОДУКТЫ: MARKETING

Если вы планируете отправлять рассылки в Creatio с помощью провайдера Elastic Email, то верифицируйте ваш email-адрес и корпоративный домен.

В этом случае получатели, которые используют MS Outlook, Hotmail, Gmail и большинство других современных почтовых сервисов, увидят в строке отправителя, что сообщение прислано с сервера вашего почтового провайдера от вашего имени. В строке отправителя может отобразиться такой текст: “Terrasoft <info@terrasoft.ua> via elasticemail.com”.

Чтобы верифицировать ваши email-адреса и домен, выполните следующие шаги:

1. Добавьте ваш корпоративный домен на страницу настройки email-рассылок. Подробнее >>>
2. Получите SPF- и DKIM-записи. Подробнее >>>
3. Укажите SPF- и DKIM-записи в DNS-зоне вашего домена. Подробнее >>>

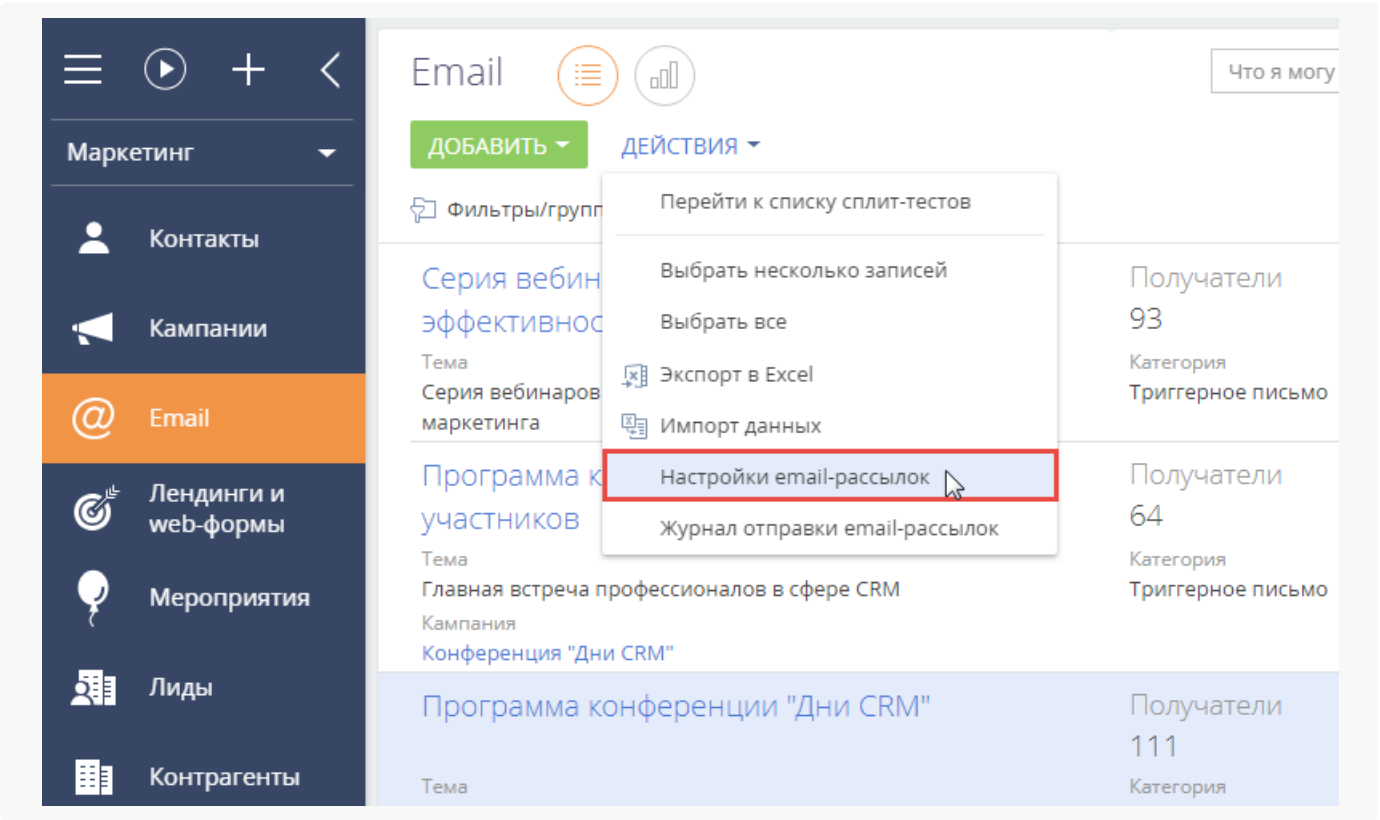
Важно. Если ваш домен не верифицирован, то Elastic Email ограничивает количество отправленных писем до 50 в день.

Добавить корпоративный домен на страницу настройки email-рассылок

До начала отправки массовых рассылок выполните настройки:

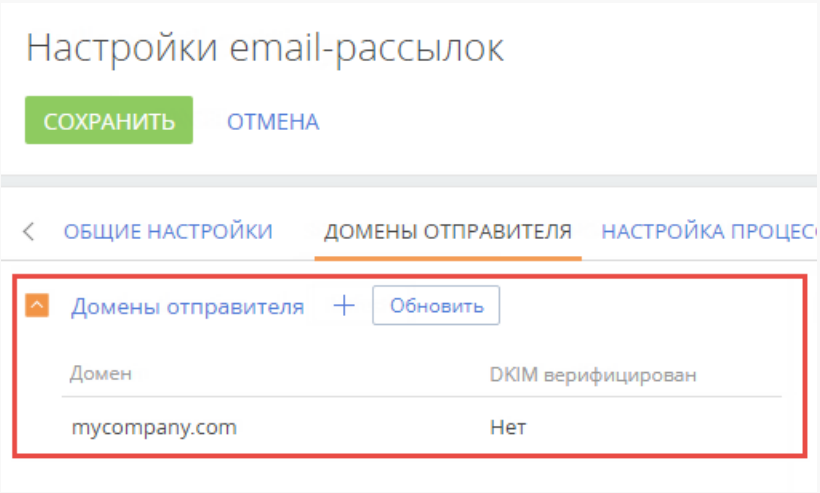
1. В разделе [*Email*] в меню [*Действия*] выберите [*Настройки email-рассылок*] (Рис. 1).

Рис. 1 — Переход на страницу настройки email-рассылок



2. На странице [*Настройки email-рассылок*] на вкладке [*Домены отправителя*] укажите домен вашего email-адреса, с которого будут отправляться рассылки, например “mycompany.com” (Рис. 2).

Рис. 2 — Вкладка [*Домены отправителя*]



Получить SPF- и DKIM-записи

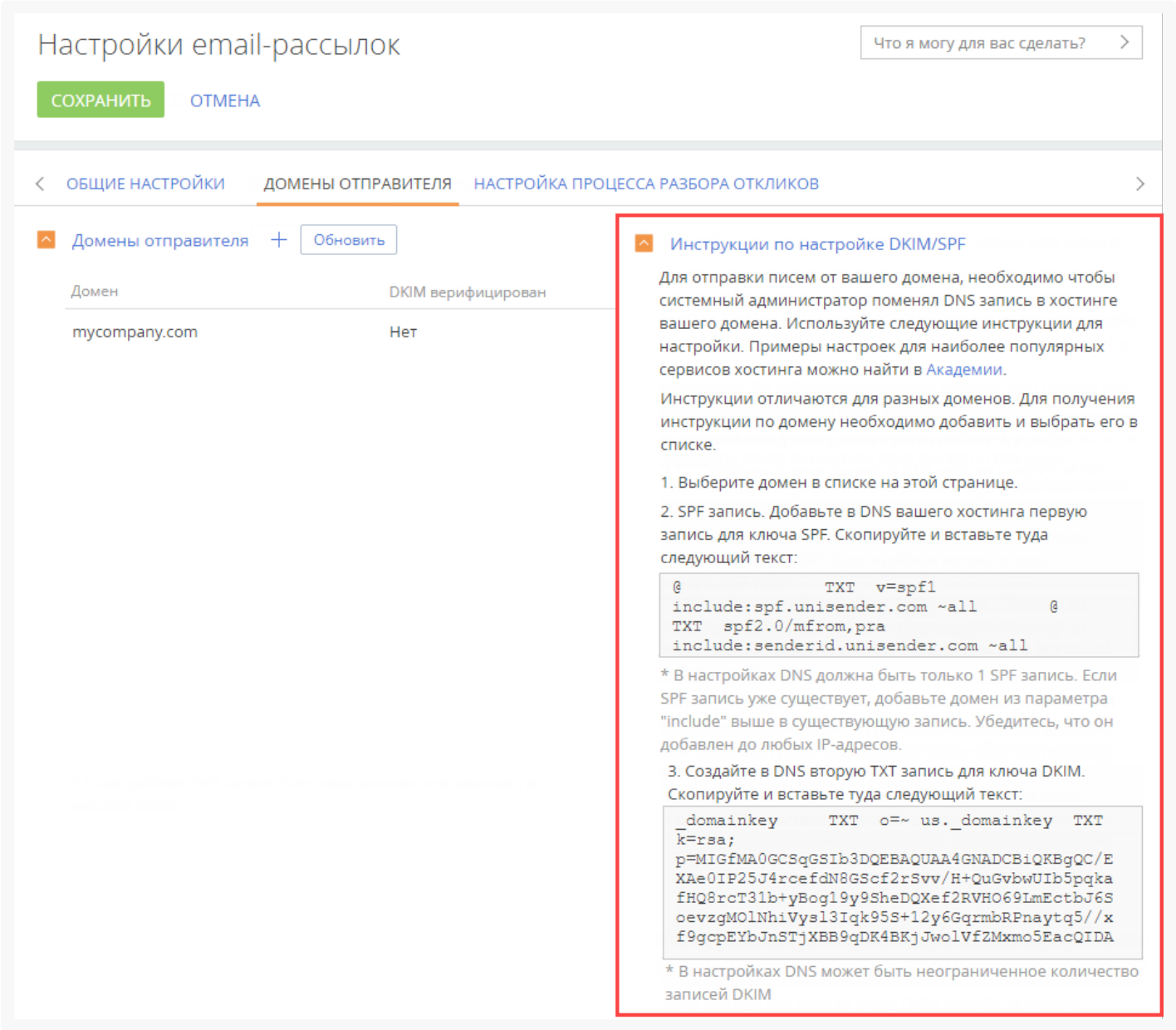
SPF- и DKIM-записи генерируются автоматически в разделе [*Email*] после добавления домена на страницу настройки email-рассылок.

Для получения этих записей в разделе [*Email*] в меню [*Действия*] выберите [*Настройки email-рассылок*].

SPF- и DKIM-записи будут автоматически сгенерированы в поле [*Инструкции по настройке DKIM/SPF*] на

вкладке [*Домены отправителя*] (Рис. 3).

Рис. 3 — Ключи DKIM/SPF для указанного домена



SPF- и DKIM-записи провайдера Elastic Email одинаковы для всех доменов.

Выполнить настройки в DNS-зоне домена

Чтобы обеспечить высокий уровень репутации домена и доставляемости писем, необходимо добавить записи SPF, DKIM, Tracking Domain и политику DMARC в DNS-зону настроек почтового домена.

Для настройки:

1. Укажите SPF- и DKIM-записи в DNS-зоне вашего домена:
2. Если в DNS-зоне вашего домена еще нет SPF-записи, то ее необходимо скопировать из поля [*Инструкции по настройке DKIM/SPF*] на странице **Настройки email-рассылок**. Запись будет

выглядеть следующим образом:

Имя	Тип	Значение
@	TXT	v=spf1 a mx include:_spf.elasticemail.com ~all

3. Если у вас уже есть TXT-запись с SPF информацией, то в конец этой записи, перед ее последним оператором (как правило, это **?all**, **~all**, или **-all**) необходимо добавить следующую строку:

Название	Тип	Значение
@	TXT	include:_spf.elasticemail.com

На заметку. В зависимости от DNS-редактора в поле “Host / Name” DNS-зоны может понадобиться указать символ "@", имя домена, или не указывать ничего. Обратитесь к вашему хостинг-провайдеру для получения информации о том, как правильно ввести это значение.

4. Укажите DKIM-запись в DNS-зоне вашего домена. Для провайдера Elastic Email эта запись имеет такой вид:

Название	Тип	Значение
api._domainkey	TXT	k=rsa;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbmGbQMzYeMvxwtNQoXN0waGYaciuKx8mtMh5czguT4EZlJXuCt6V+l56mmt3t68FEX5JJ0q4ijG71BGoFRkl87uJi7LrQt1ZZmZCvrEII0YO4mp8sDLXC8g1aUAoi8TJgxq2MJqCaMyj5kAm3Fdy2tzftPCV/lbdiJqmBnWKjtwIDAQAB

На заметку. В некоторых настройках DNS в поле “Host/Name” может потребоваться ввести “api._domainkey.yourdomain.com”, заменив значение своим актуальным доменом.

5. Настройте Tracking Domain в DNS-зоне вашего домена.
Чтобы отследить переход по ссылке в полученном письме, Elastic Email переписывает адрес ссылки в шаблоне письма. Поэтому при переходе получателя по ссылке из письма в браузере сначала отобразится адрес с доменом "api.elasticemail.com" и только затем будет выполнена переадресация на указанную при отправке письма ссылку. Чтобы в первой ссылке для отслеживания был указан ваш домен, необходимо создать CNAME-запись в настройках DNS-домена:

Название	Тип	Значение
tracking	CNAME	api.elasticemail.com

6. Укажите SPF- и DKIM-записи в DNS-зоне вашего домена.
Проверка DMARC добавляется только после того, как были добавлены записи SPF и DKIM, и сообщает

серверу-получателю, что делать с письмами, отправленными с домена, который не был верифицирован. Чтобы активировать DMARC, добавьте в записи DNS домена правило в виде записи TXT:

Название	Тип	Значение
_dmarc	TXT	v=DMARC1;p=none;

Тег **v** указывает версию протокола, а **p** — способ обработки писем, которые не прошли проверку.

Больше информации о протоколе в доступно в статье о DMARC в Википедии.Подробная информация о настройке записей SPF, DKIM, Tracking Domain и DMARC доступна в инструкции на сайте провайдера Elastic Email.