



Customer Domain Setup Guide

Updated on: 19/11/2009

Step 1 – Introduction

Step 2 – Technical Details

Step 3 – Route Web & Mail Traffic To Our Servers

Step 4 – Implement SPF / Sender ID Authentication

Step 5 – Implement DomainKey / DKIM Authentication

Step 6 – Check the Domain and Final Thoughts

Step 7 – Environment Appendix



1. Introduction

You are reading this because you or someone else in your organisation wants to use a different domain for our emarketing product CommuniGator.

If you do not already know, CommuniGator is an emarketing application used to basically email about whatever you want, to whomever you want. What it all comes down to though, is making sure that where the email comes "from" is valid and authenticated. CommuniGator will only allow you to send a campaign from a valid and authenticated sender email address. This ensures maximum deliverability potential.

CommuniGator has a few options for your Sender E-Mail Address so you can control what your recipients see as they read your messages. The ability to use your own domain or sub-domain (aka web address), allows you to retain your own branding and still take full advantage of CommuniGator's robust message handling.

This document goes into the technicalities of this and how to set it up. Read on, we warn you though, it only gets more technical from here!

2. Technical Details

The next thing you need to do is decide what domain or sub domain to assign us. Some examples are provided below...

- yourdomain.com
- email.yourdomain.com
- news.yourdomain.co.uk
- marketing.yourdomain.org
- info.yourdomain.com

It really does not matter to us what the domain is, however there are some words you should not use such as "sales". The domain just needs to be setup correctly. There are some options, conditions and considerations for you to think about though. See below...

- **You must be able to create TXT records on the domain for email authentication.** Some DNS providers allow this, some do not. Some allow you to create them, some only allow TXT records if they create them. More information on authentication after this bulleted list.
- **The domain must be solely linked to us, we cannot use a domain that is already in use.** So if the domain is already used to route email or to show a website when visited, it means we cannot use it. Unless of course if you want to break what the domain currently does in favour of using it with CommuniGator.
- **No matter what domain is used, all emails going to the domain are sent to us not you.** This is so we can process any bounces from your mailings. You can set a reply address in CommuniGator to capture genuine replies.
- **It does not matter what is before the @ sign for your sender address.** For example if you assign "yourdomain.com", it means you can send email from anything at the domain, like marketing@yourdomain.com.
- **Web traffic going to the domain will come to us not you.** This is so we can capture tracking activity for actions made on a contact receiving an email. For example a tracked link will use <http://yourdomain.com/<the-rest-of-the-tracked-link>>.
- **It is possible to assign two domains to us, one for the web traffic, and one for the email traffic.**
- **It is possible to assign multiple domains to us.** So you can choose per campaign what URL to use for the sender address and URL links in the sent emails.
- **When it comes to blacklisting sub domains are ignored.** For example sending from "news.yourdomain.com" will result in only "yourdomain.com"

being blacklisted. Domains can be blacklisted if there are sufficient spam complaints from your mailings. If you are a large sender then we recommend you do not assign a sub domain of your main day to day domain to us. Instead use another domain or buy a new one.

A bit more about authentication because it is that important. This list is what is currently known for the authentication types of receiving ISPs, and while we will make a best effort to ensure it is up to date, the data should always be independently verified:

ISP	Authentication type
AOL (aol.com)	SPF/Sender-ID/Goodmail/DKIM
CompuServe (compuserve.com)	SPF/Sender-ID/Goodmail
Netscape (netscape.com)	SPF/Sender-ID/Goodmail
Bellsouth (bellsouth.net)	SPF
Charter (charter.net)	SPF
Comcast (comcast.net)	SPF
Cox (cox.net)	DKIM
Earthlink (earthlink.net, mindspring.com, peoplepc.com)	DK
Google(gmail.com)	SPF/DK/DKIM
Juno/NetZero (juno.com, netzero.net)	SPF/Sender-ID
Microsoft (msn.com, hotmail.com, hotmail.co.uk)	SPF/Sender-ID
RoadRunner (rr.com)	SPF
Verizon (verizon.net)	SPF
Yahoo! (yahoo.com)	DK/Goodmail
SBCGlobal (sbcglobal.net)	DK
British Telecom (btinternet.com)	DK
Rogers Cable (rogers.com)	DK
Rocket Mail (rocketmail.com)	DK

So as you can see its used by the major ISPs out there. Without the authentication, your emails will have a very high chance of bouncing back, or simply being blocked from the start. This email authentication is added via the use of TXT records in DNS. You need to make sure TXT records are supported with your domain provider, if not, it is still possible to use the domain for URL content only. But using it for the sender email address will not be an option.

This list is what is currently known for domain providers who **DO NOT** support TXT records, and while we will make a best effort to ensure it is up to date, the data should always be independently verified:

- 1&1 Interet Ltd.
- Amen
- Cbeyond
- DomainPeople
- Fasthosts.co.uk
- Jumpdomain.com



- Katz Global
- Namesecure.com
- NetBenefit
- Network Solutions
- Online.net
- pakNIC
- XO Communications
- UK2 (no sub domain support)

Once you know your provider supports TXT records and have chosen the domain to assign to us, you basically just need to create the various DNS records to assign and authenticate it to us. The rest of the guide details how to do this with step by step instructions to help you do it correctly.

The last page of this guide has our environment appendix details which you will need for creating all the DNS records. You **MUST** know what environment you are on before you proceed. If you do not know this let us know and we will tell you which it is.

Once this is all done, email your CommuniGator representative the domain you are using, the DomainKey details, and any comments / issues that you may have had and we will take it from there.



3. Route Web & Mail Traffic To Our Servers

In order for our application to use your domain in tracked links we need to have an A record pointing to our web server IP address.

Follow the steps below...

1. Using the environment appendix at the end of this document, set in the external DNS for your domain an A record pointing to the IP specified.

WARNING: If you create a sub-domain **do not change the A record for your main domain.** We do not want to interfere with your main website. We only want to receive handle the website for the sub-domain itself.

2. Using the environment appendix at the end of this document, set in the external DNS for your domain an MX record pointing to the record specified.

WARNING: If you create a sub-domain **do not change the MX record for your main domain.** We do not want to interfere with your main emailing. We only want to receive e-mail for the sub-domain itself.

3. Proceed to the next section.

If you use a third party company or outsource your IT, make sure you pass on the above warnings when getting the sub domain to be assigned to us.



4. Implement SPF / Sender ID Authentication

SPF and Sender ID authentication is a Microsoft technology used to help the fight against spam. By not implementing this you will suffer from worse deliverability and a higher likelihood of blacklisting and sender reputation problems.

If you want to know more about SPF and Sender ID please visit the Microsoft website for it.

<http://www.microsoft.com/mscorp/safety/technologies/senderid/default.aspx>

SPF and Sender ID authentication is essential for the domain to be used for the email sender address. However it is not essential for the domain used in the URLs of the email. Therefore if for any reason you cannot setup TXT records, you can still assign a domain to us for the web traffic only.

Follow the steps below...

1. Using the environment appendix at the end of this document, set in the external DNS for your domain both TXT records specified.

WARNING: If for any reason you already have a TXT record to manage SPF you will need to add our "include:" part into your record. Overwriting any existing record with ours could affect mail authentication for whatever you had the record for in the first place.

2. Proceed to the next section.

5. Implement DomainKey / DKIM Authentication

DomainKey and DKIM authentication is a Yahoo! technology and is also used to help the fight against spam. By not implementing this you will suffer from worse deliverability and a higher likelihood of blacklisting and sender reputation problems.

If you want to know more about DomainKeys please visit the Yahoo website for it.

<http://antispam.yahoo.com/domainkeys>

Like SPF and Sender ID authentication, DomainKeys is essential for the domain to be used for the email sender address. It is not essential for the domain used in the URLs of the email. Therefore if for any reason you cannot setup TXT records, you can still assign a domain to us for the web traffic only.

Setting up DomainKeys is more involved than any other records in this guide, the steps below will follow an example to help you...

1. Visit the Port25 DomainKeys wizard website below...

http://www.port25.com/support/support_dkwz.php

2. Enter your **domain name** in the box provided.

E.G: news.yourdomain.com

3. Enter the **DomainKey Selector**. This is just a reference so can be anything you want.

E.G: key1

4. Select a **Key Size** option. Leaving it at the default 512 is fine.

5. Click "**Create Keys**" and you will now see the results of the DomainKey Wizard. The rest of the steps are provided by Port25 but to reiterate a few of them.

6. You need to add the "**Selector**" and "**Policy**" records into your DNS server for your domain. Note: most DNS systems will append your root domain to the record you are about to add. Therefore when adding these records you may need to only enter the text before your domain.

E.G: Port25 says add "key1._DomainKey.yourdomain.com" but you should add "key1._DomainKey".

7. We need to complete steps 2 and 3 so once you are looking at the wizard results, please save this page (File -> Save As) and send it to us.

8. Proceed to the next section.

6. Check the Domain and Final Thoughts

There are various places to check the domain is setup ok but as they are all external sites we have provided more than required just in case one of them is offline when you try to use it.

NOTE: DNS changes do not always take affect the moment you make them. It can take up to 24 hours for the DNS to propagate around the world. So if you have only recently made changes and tests fail, you should wait and try again later.

1. Check the A record at any of these sites...

<http://www.dnswatch.info/>
<http://www.dnsstuff.com/>

Everything is ok as long as the IP returned matches the A record IP from your given environment details. If for any reason the test fails you will need to re-check your DNS and try again.

E.G: Looking at **thegators.gtml1.com** you will get the following result:

A record found: 212.93.64.206

Domain	Type	TTL	Answer
thegators.gtml1.com.	A	86400	212.93.64.206

2. Check the MX record at any of these sites...

<http://www.dnswatch.info/>
<http://www.mxtoolbox.com/index.aspx>
<http://www.dnsstuff.com/>

Everything is ok as long as the record returned matches the MX record from your given environment details. If for any reason the test fails you will need to re-check your DNS and try again.

E.G: Looking at **thegators.gtml1.com** you will get the following result:

MX record found: 10 mail1.gtml1.com.

Domain	Type	TTL	Answer
thegators.gtml1.com.	MX	86400	10 mail1.gtml1.com

3. To check the SPF record you should do it directly at the Microsoft site below...

<http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/>

Everything is ok as long as the SPF record is found and shows a green tick. If for any reason the test fails you will need to re-check your DNS and try again.

E.G: Looking at **thegators.gtml1.com** you will get the following result:

SPF Record Found

 One or more functional SPF record(s) have been found for the domain **thegators.gtml1.com**

The full text of the domain's SPF record is as follows.

- spf2.0/prd include:gtml1.com -all
- v=spf1 include:gtml1.com -all

Choose the SPF record that you want to edit.

You can also use the following sites to check TXT records...

<http://www.dnswatch.info/>

<http://www.dnsstuff.com/>

4. Methods to check the DomainKey are provided by the Port25 wizard at the time of creating it. If for any reason the test fails you will need to re-check your DNS and try again.
5. The final check that needs to happen we will do. This is to use the Port25 authentication checker email address. Assuming the result passes all checks (we will show you the output) the domain is ready to be used.
6. Email your CommuniGator representative the domain you are using, the DomainKey details, and any comments / issues that you may have had and we will take it from there.



7. Environment Appendix

Here are the environment details which you will need to create the A, MX, and TXT records mentioned in this guide. You MUST know what environment you are on before any DNS records are created.

Our environment details are as follows...

Environment	A Record IP	MX Record	TXT Records
CommuniGator UK	212.93.64.206	mail1.gtml1.com	v=spf1 include:gtml1.com -all
CommuniGator US	212.93.64.209	mail1.gtml3.com	v=spf1 include:gtml3.com -all
Sage EMarketing UK	212.93.64.206	mail1.sgml1.co.uk	v=spf1 include:sgml1.co.uk -all
Sage EMarketing US	212.93.64.209	mail1.sgml1.com	v=spf1 include:sgml1.com -all
Gator EMarketing	212.93.64.206	mail1.geml1.co.uk	v=spf1 include:geml1.co.uk -all
White Label	212.93.64.206	mail1.ceml3.co.uk	v=spf1 include:ceml3.co.uk -all

NOTE: The TXT records column only contains SPF / Sender ID records because the DomainKey records are unique and provided by the Port25 Wizard.