DELIVERABILITY SETUP

Table of Contents

Improving Deliverability

Swift Digital recommends a number of procedures to improve email delivery rates, make your account secure and trusted, and maintain your online reputation. These include:

1. Using your own subdomain
2. Using an SSL certificate
3. Setting up DKIM
4. Setting SPF record(s)
5. Using a custom Return-Path

These steps will ensure everything possible is in place to get your mail delivered. Note that none of these are compulsory and can be done before or after your Swift Digital account has been set up with templates and module activation. However, they are highly recommended.

This document contains explanations written with a business audience in mind, as well as technical instructions for systems administrators

SYDNEY
31-33 Trafalgar Street,
Enmore, NSW 2042
Australia

MELBOURNE
Suite 907, 9 Yarra Street,
Melbourne, VIC 3141
Australia

TEL 1300 878 289
FAX +61 2 9557 7392

www.swiftdigital.com.au

Using Your Own Subdomain

Having a particular subdomain (e.g. subdomain.mycompany.com.au) is better for branding, improving subscriber confidence and if, for whatever reason, you decide to move to a different email service later on, you will have control of your subdomain.

Setup

1. Contact your IT team, website administrator or domain manager and ask that they create your desired subdomain. Since the Suite can be used for all sorts of internal and external communications, one suggestion would be to name it comms.mycompany.com.au

2. Once the subdomain has been created, it will need to have its CNAME record updated to point to the Swift Digital Suite server. Please have the CNAME record directed to suite.swiftdigital.com.au.

3. Inform Swift Digital and we will update your account accordingly.

4. A second subdomain (ie. CNAME record) can be separately configured for Suite surveys should you wish to do so. A sensible name for this would be surveys.mycompany.com.au

Using an SLL Certificate

While not directly relevant to email delivery, this section is included as it pertains to using your own subdomain with the Suite, and to building trust in your readers. It is also usually handled by the same IT team who will be assisting you with the other settings in this document so can effectively be configured at the same time.

A valid SSL certificate – commonly represented by a padlock symbol and the https prefix in your browser's address bar – assures your audience that...

1. the web site they are visiting is authorized by you, and
2. that the information it provides has not been tampered with in transit, and
3. that the information you submit to it is encrypted

SSL certificates cost a few hundred dollars and typically expire after a few years. For the first-time buyer, the purchase process can be confusing. Swift Digital recommends GeoTrust (geotrust.com) as a certificate vendor, for no other reason that they have never failed us and we are familiar with their purchase process. We recommend their True BusinessID for single certificates, or True BusinessID Wildcard for multiple certificates on the same domain.

You are responsible for certificate purchase and renewal. Swift Digital will generate the required CSR (see below) and install and test your certificate. This process requires a few hours.

Setup

1. Send the following certificate ownership information to your accountmanager:

Question	Example Answer	Notes
Country	AU	
State	New South Wales	
Locality	Sydney	
Organization	My Company Ltd	Your legal entity, not a trading name.
Organizational Unit	IT	
Common Name	comms.mycompany.com.au	This must be your custom subdomain.
Email Address	john.doe@mycompany.com.au	This is the person who will receive notices to renew the certificate.

2. Swift Digital's Systems Administrator will generate a Certificate Signing Request (CSR) on the Suite server and send it back to you by email.

3. Provide the CSR to your certificate vendor (eg. GeoTrust) during the purchase process. Be sure to note the expiry date in your calendar.

4. Send the resulting text files (containing the certificate for your domain name, as well as any intermediate certificates) to your account manager.

5. Swift Digital's Systems Administrator will schedule and install the certificate after hours and test that your templates work correctly.

Setting up DKIM

Domain Keys Identified Mail (DKIM) is a method of digitally signing an email. When we sign an email on your behalf, recipient email servers will trust that you gave us approval to send the email for you. A valid DKIM signature also prevents an email from being secretly tampered with and modified, which could theoretically happen as your email is in transit.

Although we can send emails without DKIM, the recipient mail server and your recipients may assume that your email is a spoof. This will result in reduced readership and is a poor reflection on your brand.

Each sending domain will require its own DKIM record. This means that if the emails that you send from the Suite always originate from jane@mycompany.com.au and john@mycompany.com.au and mary@someotherdomain.com.au, you will need two DKIM keys – one for mycompany.com.au and one for someotherdomain.com.au. Only emails from the Suite associated with those two domains will be signed.

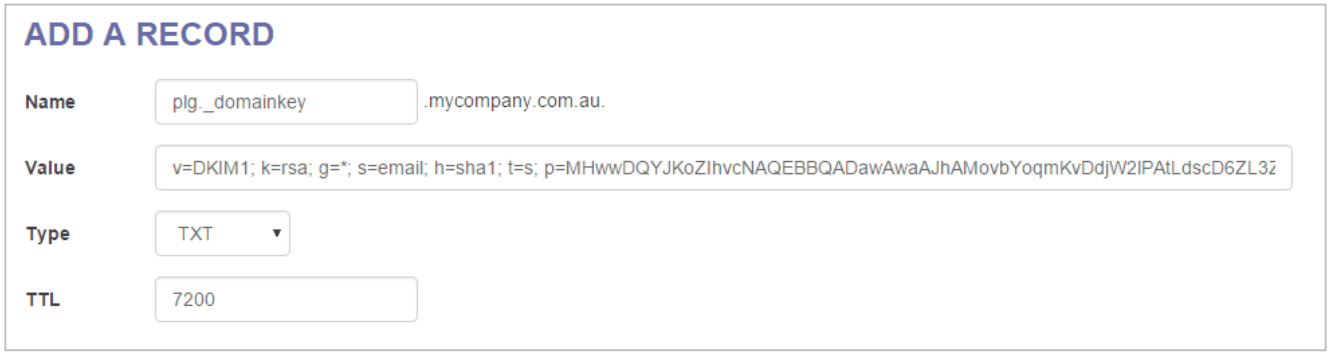
Setup

1. Send an email to your account manager and request that one or more DKIM keys be generated. In the email please include the email domains that you want the DKIM setup for (eg. mycompany.com.au, someotherdomain.com.au, etc.).

2. Support will send back one or more 2,048-bit DKIM keys which you can give to your IT department. If

you require shorter keys (which are less trustworthy), please let us know.

3. Your IT department will need to take the (public) keys and create new TXT records in your DNS (Domain Name System) as shown (example key only):



Note that the TTL is up to you; two hours is reasonable for DKIM keys.

Setting SPF Record (s)

Whereas DKIM validates domain senders and safeguards against tampering, Sender Policy Framework (SPF) only does the former. By using SPF to focus on authorizing a specific IP address, Swift Digital maximizes the benefit from using both mechanisms in tandem.

Your IT administrators can designate which servers are allowed to send mail for your domain by adding TXT records to your Domain Name System (DNS). When receiving your emails broadcast from the Suite, mail servers check your DNS to see whether the mail is sent from an authorized source. Your emails are more likely to be successfully delivered if your domains sanction Swift Digital – or rather its IP address – as a verified sender.

Setup

For the domain name(s) that you will be using to send emails, ask your IT team to add the following TXT record to your DNS

"v=spf1 include:spf.swiftdigital.com.au include:_spf.google.com ~all"

As with DKIM, you will need one such record for all the sending domains that you use with Swift Digital. Just name them _spf1, _spf2, etc. The IP address will be the same for each.

Using a Custom Return–Path

In much the same way that envelopes help to deliver physical mail, every email is delivered from A to B inside a wrapper (a.k.a. "header") which contains information about the email's origin and destination. For example:

From: jane@mycompany.com.au

To: harry@somecompany.com.au

Reply-To: marketing@mycompany.com.au

Return-Path: bounces@mycompany.com.au

The From address is the one that is presented to the To recipient. The Reply-To address is frequently the same as the From address but need not be. And, as you can probably guess from this example, the Return-Path address is used to capture bounces – emails that fail to be delivered.

Some mail servers check header information to verify that the Return-Path of an email is the same as the From address. The Swift Digital Suite (like most email services) uses its own domain for sending emails and receiving and reporting on your bounced emails. This means the From address will be yours but the Return-Path address will be Swift Digital's. Typically this takes the form:

yoursuiteaccountid@bouncer.swiftdigital.com.au or

It is possible to make the Return-Path the same as the From, making the email appear as though it was sent from

your domain and potentially lowering the chance the email will be marked as spam. We still need to track your bounces, though, so a custom Return-Path redirects them to us.

Setup

1. Nominate a dedicated domain (you may already have this set up); this is a domain that is not used for anything else. This could be a subdomain, for example if your domain is example.com you could use emails.example.com as your dedicated domain.

2. After this domain has been created, contact your account manager and let us know you would like to set up a "Custom Return-Path". We will adjust the settings of your account accordingly.

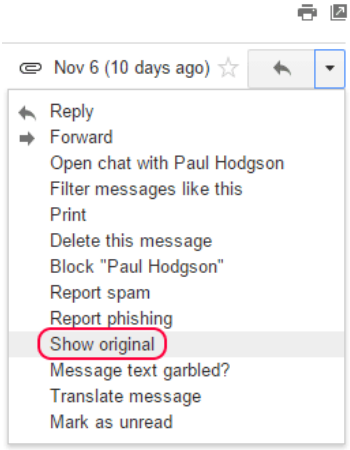
3. Ask your IT department to set the MX of your dedicated domain to point to bouncer.swiftdigital.com.au

4. Notify us once this has been completed.

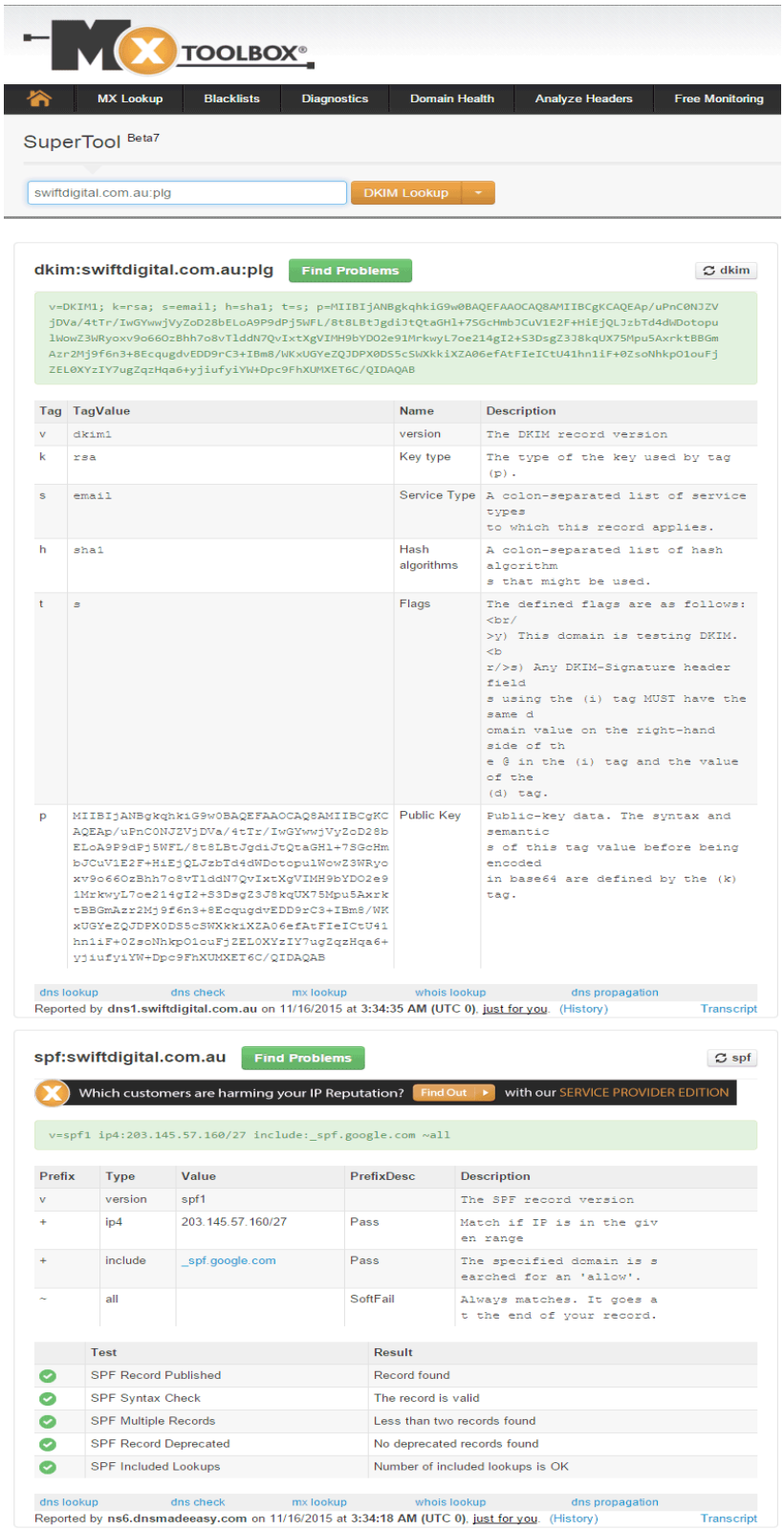
Verification

To confirm that these measures are in place, you can either:

1. Examine the source code of emails sent from the Suite. In Gmail this is via the ***Show original*** option:



2. Use a site such as mxtoolbox.com to query your DNS records. Remember to specify the selector used (plg or suite) if necessary for DKIM lookups:



MX TOOLBOX®

MX Lookup | Blacklists | Diagnostics | Domain Health | Analyze Headers | Free Monitoring

SuperTool Beta7

swiftdigital.com.au:plg — DKIM Lookup

dkim:swiftdigital.com.au:plg Find Problems — dkim

```
v=DKIM1; k=rsa; s=email; h=sha1; t=s; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp/uPnC0NJZV
jDVa/4tTr/IwGYwwjVyZoD28bELoA9P9dPj5WFL/8t8LBtJgdiJtQtaGHl+7SGcHmbJCuV1E2F+HiEjQLJzbTd4dWDotopu
lWowZ3WRyoxv9o66OzBhh7o8vTlddN7QvIxtXgVIMH9bYDO2e91MrkwyL7oe214gI2+S3DsgZ3J8kqUX75Mpu5AxrktBBGm
Azr2Mj9f6n3+8EcqugdvEDD9rC3+IBm8/WKxUGYeZQJDPX0DS5cSWXkkiXZA06efAtFIeICtU41hn1iF+0ZsoNhkpO1ouFj
ZEL0XYzIY7ugZqzHqa6+yjiufyiYW+Dpc9FhXUMXET6C/QIDAQAB
```

Tag	TagValue	Name	Description
v	dkim1	version	The DKIM record version
k	rsa	Key type	The type of the key used by tag (p).
s	email	Service Type	A colon-separated list of service types to which this record applies.
h	sha1	Hash algorithms	A colon-separated list of hash algorithm s that might be used.
t	s	Flags	The defined flags are as follows: <br/ >y) This domain is testing DKIM. s) Any DKIM-Signature header field s using the (i) tag MUST have the same d omain value on the right-hand side of th e @ in the (i) tag and the value of the (d) tag.
p	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp/uPnC0NJZVjDVa/4tTr/IwGYwwjVyZoD28bELoA9P9dPj5WFL/8t8LBtJgdiJtQtaGHl+7SGcHmbJCuV1E2F+HiEjQLJzbTd4dWDotopulWowZ3WRyoxv9o66OzBhh7o8vTlddN7QvIxtXgVIMH9bYDO2e91MrkwyL7oe214gI2+S3DsgZ3J8kqUX75Mpu5AxrktBBGmAzr2Mj9f6n3+8EcqugdvEDD9rC3+IBm8/WKxUGYeZQJDPX0DS5cSWXkkiXZA06efAtFIeICtU41hn1iF+0ZsoNhkpO1ouFjZEL0XYzIY7ugZqzHqa6+yjiufyiYW+Dpc9FhXUMXET6C/QIDAQAB	Public Key	Public-key data. The syntax and semantic s of this tag value before being encoded in base64 are defined by the (k) tag.

dns lookup | dns check | mx lookup | whois lookup | dns propagation

Reported by **dns1.swiftdigital.com.au** on 11/16/2015 at **3:34:35 AM (UTC 0)**, just for you. (History) Transcript

spf:swiftdigital.com.au Find Problems — spf

Which customers are harming your IP Reputation? Find Out with our SERVICE PROVIDER EDITION

```
v=spf1 ip4:203.145.57.160/27 include:_spf.google.com ~all
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	ip4	203.145.57.160/27	Pass	Match if IP is in the giv en range
+	include	_spf.google.com	Pass	The specified domain is s earched for an 'allow'.
~	all		SoftFail	Always matches. It goes a t the end of your record.

	Test	Result
✓	SPF Record Published	Record found
✓	SPF Syntax Check	The record is valid
✓	SPF Multiple Records	Less than two records found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Included Lookups	Number of included lookups is OK

dns lookup | dns check | mx lookup | whois lookup | dns propagation

Reported by **ns6.dnsmadeeasy.com** on 11/16/2015 at **3:34:18 AM (UTC 0)**, just for you. (History) Transcript

SYDNEY
31-33 Trafalgar Street,
Enmore, NSW 2042
Australia

MELBOURNE
Suite 907, 9 Yarra Street,
Melbourne, VIC 3141
Australia

TEL 1300 878 289
FAX +61 2 9557 7392

www.swiftdigital.com.au