DELIVERABILITY SETUP

Table of Contents

Improving Deliverability........... 1

Using Your Own Subdomain 2

Setup 2

Using an SSL Certificate 3

Setup 4

Setting up DKIM 5

Setup 5

Setting SPF Record (s) 7

Setup 7

Setting up DMARC 7

Office 365 Delivery Issue 9

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. Setting up a DMARC record
6. Using a custom Return-Path (Request from your Account Manager if required)

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.

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.

Subdomains will be what people see in the web address bar when:

- Viewing a web version of an email
- Subscribing to a mail list
- Registering for an event
- Answering a survey
- Viewing a landing page

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.

Using an SSL 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 of the following:

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.

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.

Since October 2018 Google has been warning site visitors that a website is not secure. Swift strongly recommends installing SSL if you have a custom domain.

Setup

1. Send the following certificate ownership information to your on-boarding manager:

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	info@mycompany.com.au	This is the email address that will receive notices to renew the certificate.

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

2. Provide the CSR to your certificate vendor during the purchase process. Be sure to note the expiry date in your calendar. We recommend that you buy the certificate for at least 2 years.

3. Send the resulting text files (containing the certificate for your domain name, as well as the intermediate certificates) to your on-boarding manager. Your certificate provider will give you an option to download the certificate for different type of web servers. Please make sure you download the certificate for Apache. These certificates usually end with ".crt".

4. If you use your own CSR (not generated from Swift Digital) to purchase your SSL certificate you will need to provide the private key as well as the certificate.

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.

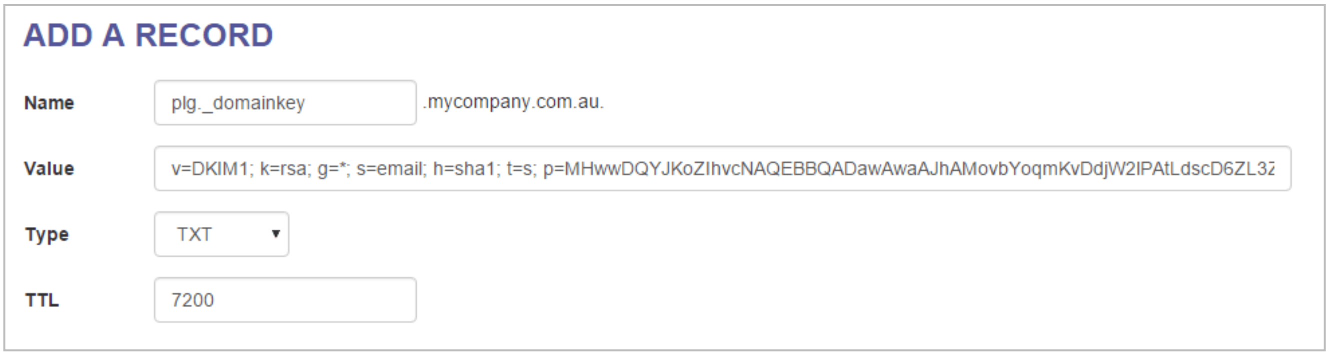
Although we can send emails without DKIM, the recipient mail server and your recipients may assume that your email is a spoof. This will result in reduced readership and is a poor reflection on your brand.

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 on-boarding 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. You will be sent 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.
   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):



ADD A RECORD

Name	plg._domainkey .mycompany.com.au.
Value	v=DKIM1; k=rsa; g=*; s=email; h=sha1; t=s; p=MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAMovbYoqmKvDdjW2IPAtLdscD6ZL3
Type	TXT ▾
TTL	7200

Note that if you are deploying a key that is longer than your DNS tables will allow it is possible to split keys. An example of how to do can be seen here; https://support.symantec.com/en_US/article.TECH123082.html

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

Creating Emails

Using your sending domain please create the following emails: abuse@ and postmaster@. These emails should be forwarded to the corresponding abuse@swiftdigital.com.au and postmaster@swiftdigital.com.au.

This allows us to register for FBL processing (emails marked as spam / complaints from more than 22 most important Email Service Providers), monitor abuse/complaint emails and to add such emails to a suppressed list (to not contact anymore) and to remove many hard bounces from your lists (if postmaster@ is forwarded as many ESPs send bounce emails to postmaster@ email address too).

Some ESPs block delivery if you don't have abuse@ and postmaster@ email addresses (when they send info to these addresses like spam/complaints), these email address are needed if your domain is blacklisted and need to be whitelisted.

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 SPF settings.

You need to add to your current SPF settings as: v=spf1 include:spf.swiftdigital.com.au ~all

As with DKIM, you will need one such record for all the sending domains that you use with Swift Digital. The address will be the same for each.

Setting up DMARC

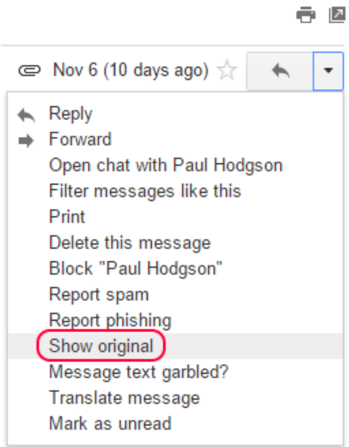
DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance", is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

DMARC needs to start with: v=DMARC1; p=quarantine , you can add any other setting after. Deploy DKIM & SPF as above

Verification

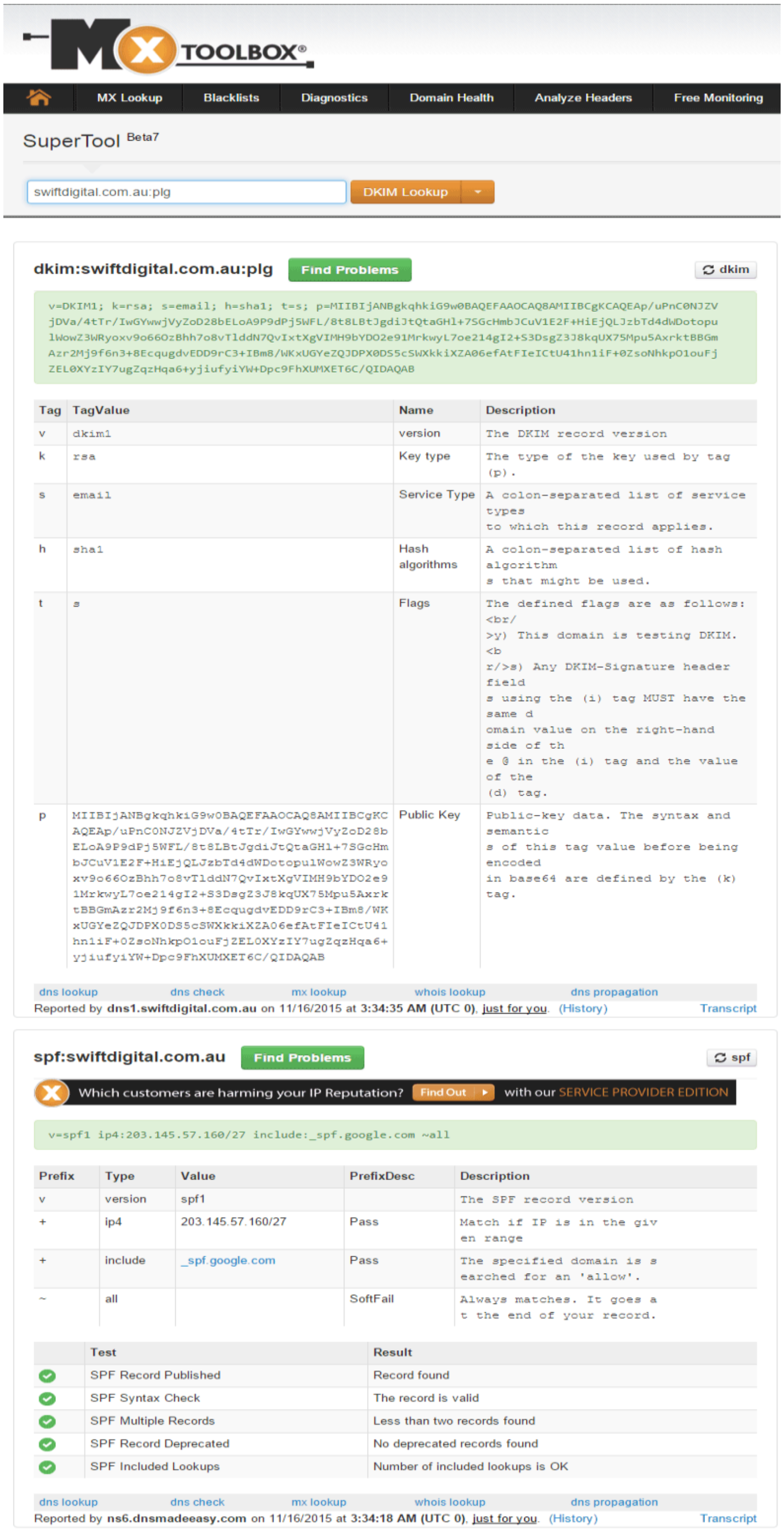
To confirm that these measures are in place, you can either:

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:of



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 algorithms that might be used.
t	s	Flags	The defined flags are as follows:<br/>y) This domain is testing DKIM.<br/>s) Any DKIM-Signature header fields using the (i) tag MUST have the same domain value on the right-hand side of the @ 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 semantics 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

```
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 given range
+	include	_spf.google.com	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at 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

Office 365 Delivery Issue

Summary

- Incoming emails to internal domain from the swift digital system, Suite, are either not received or marked as fraudulent e-mails in Office 365.

Cause

- The issue arises because of Microsoft Anti Spoofing checks to protect from spoof emails.

Resolution

- Important: Office 365 users only.

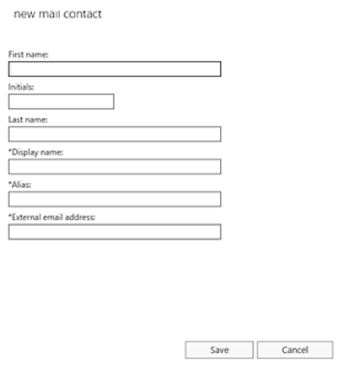
- In order to receive emails in inbox from Swift Digital system when sending to internal users

- Create an Internal mail contact which be used as from address in Swift Digital system.

Login to Office 365 Exchange Online Dashboard

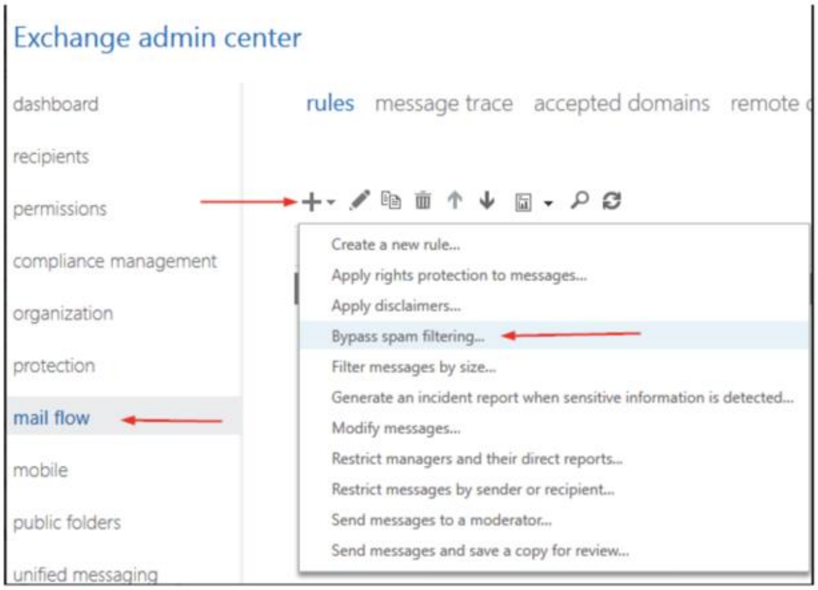
- Under Recipients > Contacts

- Create New Mail contact



Create anti spam bypass message rule

- Under Mail Flow – Message Rule


Exchange admin center
dashboard
recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
unified messaging
rules
message trace
accepted domains
remote
Create a new rule...
Apply rights protection to messages...
Apply disclaimers...
Bypass spam filtering...
Filter messages by size...
Generate an incident report when sensitive information is detected...
Modify messages...
Restrict managers and their direct reports...
Restrict messages by sender or recipient...
Send messages to a moderator...
Send messages and save a copy for review...

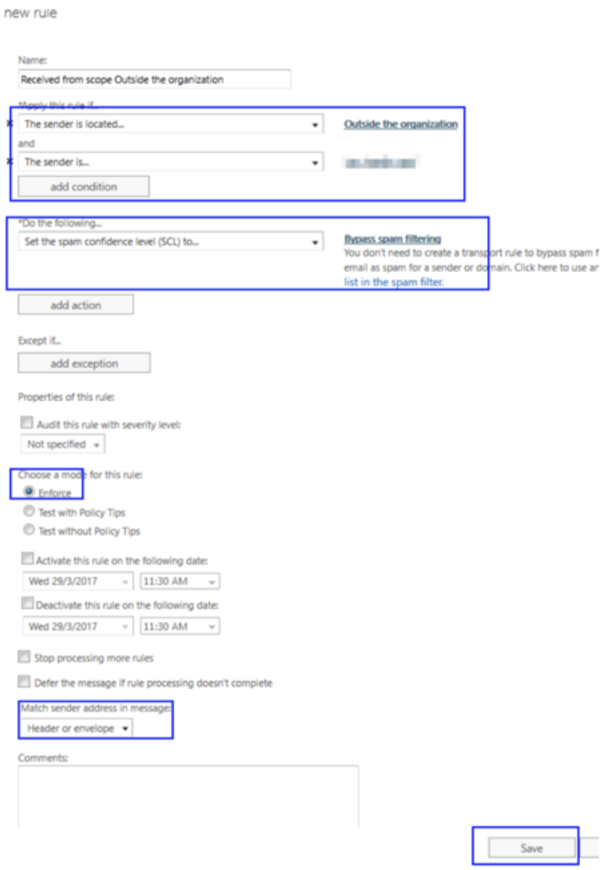
Enter the details in the new spam rule.

- Select the following condition
- The sender is located... outside the organization
- The sender is... the mail contact created above
- Make sure Enforce is selected
- Match sender address is selected to Header or Envelope.

Click Save to close.

- Allow from address in allow bypass list.
- Under protection > spam filter
- Select your spam filter policy and double click to open it.

- Under allow list.
- Add the from address
- Hit save to close.



new rule

Name:
Received from scope Outside the organization

*Apply this rule if...
The sender is located... — Outside the organization
and
The sender is... — [redacted]

*Do the following...
Set the spam confidence level (SCL) to... — Bypass spam filtering

You don't need to create a transport rule to bypass spam f
email as spam for a sender or domain. Click here to use ar
list in the spam filter.

Except if...

Properties of this rule:

□ Audit this rule with severity level:
Not specified

Choose a mode for this rule:
● Enforce
○ Test with Policy Tips
○ Test without Policy Tips

□ Activate this rule on the following date:
Wed 29/3/2017 11:30 AM
□ Deactivate this rule on the following date:
Wed 29/3/2017 11:30 AM

□ Stop processing more rules
□ Defer the message if rule processing doesn't complete

Match sender address in message:
Header or envelope

Comments:

Allow Swift Digital sending domains in connection filtering Allow list.

- Under protection > connection filtering
- Select your connection filtering policy and double click to open it.
- Under connection filtering

Make sure the sending IP address of your system (Swift Digital) are listed in allow list

- Make sure enable safe list is checked
- Hit save to close.

Our domains from where we send emails from:

bouncer.swiftdigital.com.au

parasend1.swiftdigital.com.au

parasend2.swiftdigital.com.au

outmail1.swiftdigital.com.au

outmail2.swiftdigital.com.au

outmail3.swiftdigital.com.au outmail4.swiftdigital.com.au

outmail5.swiftdigital.com.au

outmail6.swiftdigital.com.au

outmail7.swiftdigital.com.au

outmail8.swiftdigital.com.au

outmail9.swiftdigital.com.au

outmail10.swiftdigital.com.au

If any questions in regards to the above please contact:

office365@swiftdigital.com.au and programmers@swiftdigital.com.au