Office365 Basic Hygiene Checkup

This brief course covers some "basic hygiene" steps you can take to optimally secure your Office365 tenancy, in leui of Microsoft's "Advanced Threat Protection" service (*which can be costly as the volume of mailboxes scales out*).

Let's set the scene - you've inherited the family business, **Widgets LLC**. You've bought the domain "widgets.com", purchased an Office365 subscription, and you've sent your first email from @widgets.com. Hurrah!

You've read stories about phishing, spear-phishing, "sextorsion", etc., and you suspect that without a rigorous "phishing checkup", your fresh new domain is ripe for abuse (*and you're right!*).

This checkup will guide you through the process of optimally configuring your Office365-hosted domain for email hygine and phishing protection.

Preparation

What do you need to know?

1. First, you can this process to take around a week, depending on the complexity of your email setup.
2. Although email is a "standard", there are countless variations on how providers implement some features, especially the "newer" features like SPIF, DKIM, etc. There will be edge cases where systems won't work "as they should", and some companies you correspond with won't have implemented the same anti-phishing protections that you will. The best you can do is to optimize **your** domain's security profile.

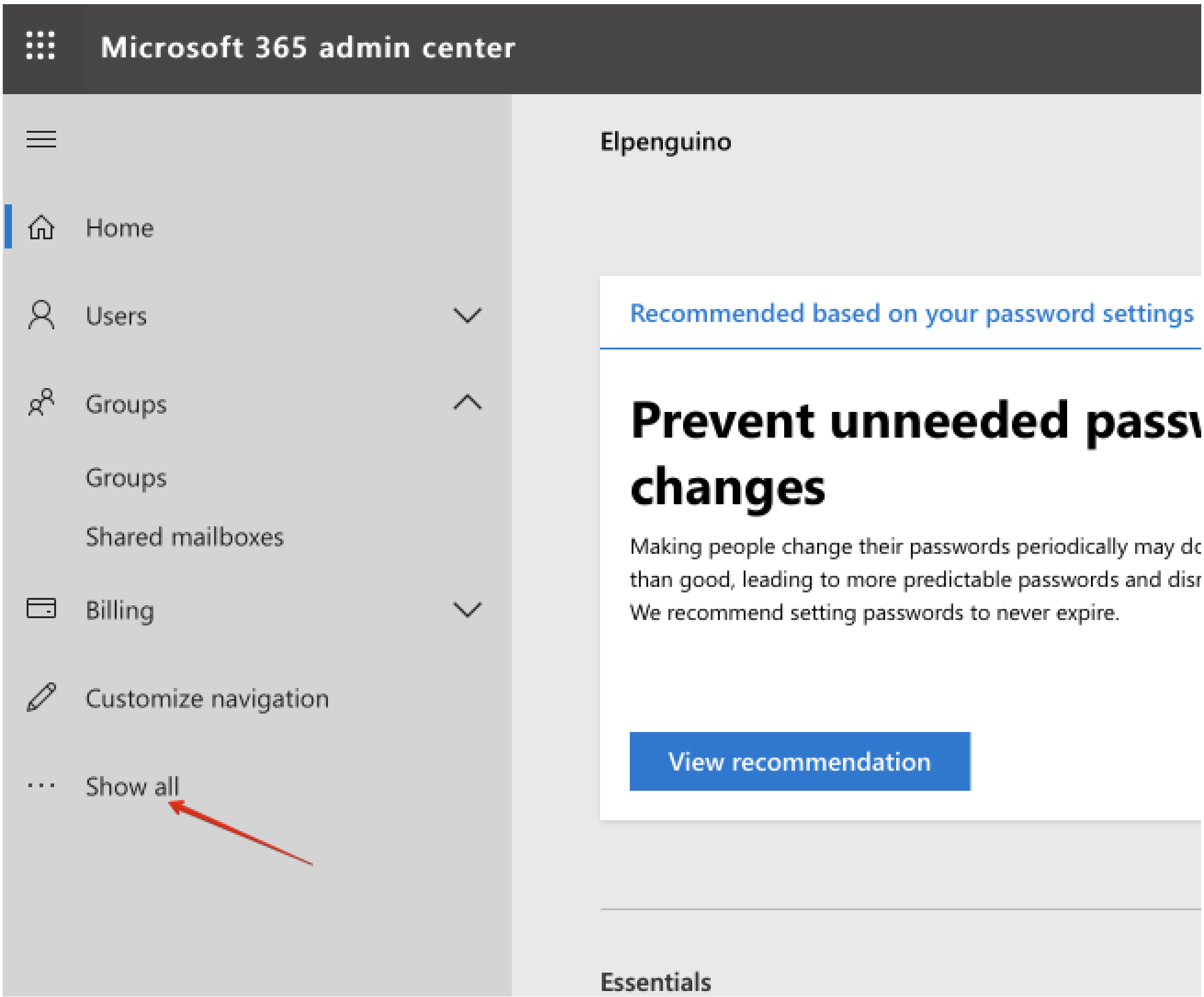
What do you need?

1. You'll need to create DNS records as part of the checkup, so you'll need administrative access to your DNS provider.
2. You'll also want to receive reports of email failures, so ensure that postmaster@yourdomain.com is forwarded to a mailbox you can read.

Basic Navigation (How to find the `Exchange admin center`)

Throughout this tutorial, we'll be using the Office365 "Exchange admin Center". To navigate to the admin center, log into https://admin.microsoft.com/ using your Microsoft Office365 credentials. Your first landing page is `Microsoft 365 admin center`.

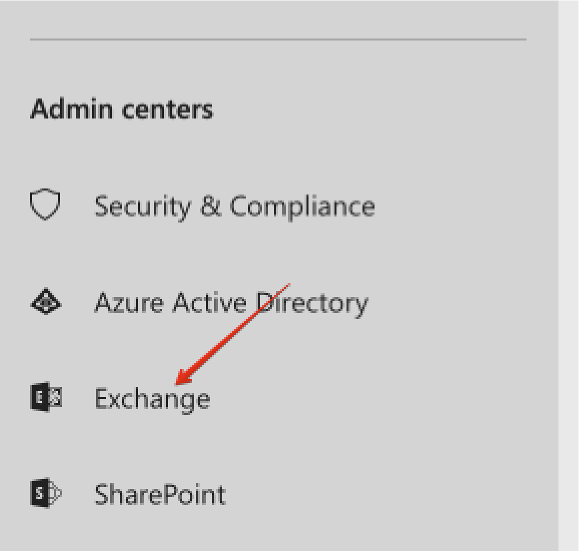
In the navigation panel on the left-hand side, click on `... Show all` to expand navigation:



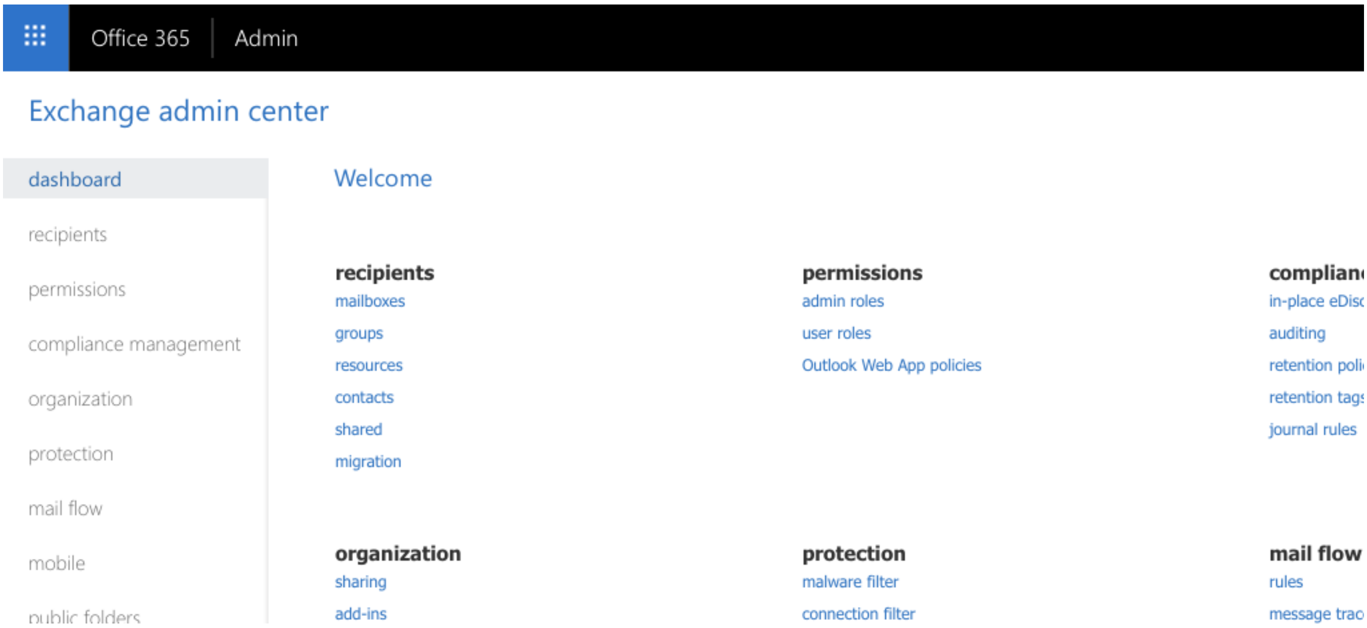
Prevent unneeded passw
changes

Making people change their passwords periodically may dc
than good, leading to more predictable passwords and disr
We recommend setting passwords to never expire.

Under `Admin Centers`, click `Exchange`:



You are redirected to the `Exchange admin center`:



1. Setup a catch-all mailbox

Summary

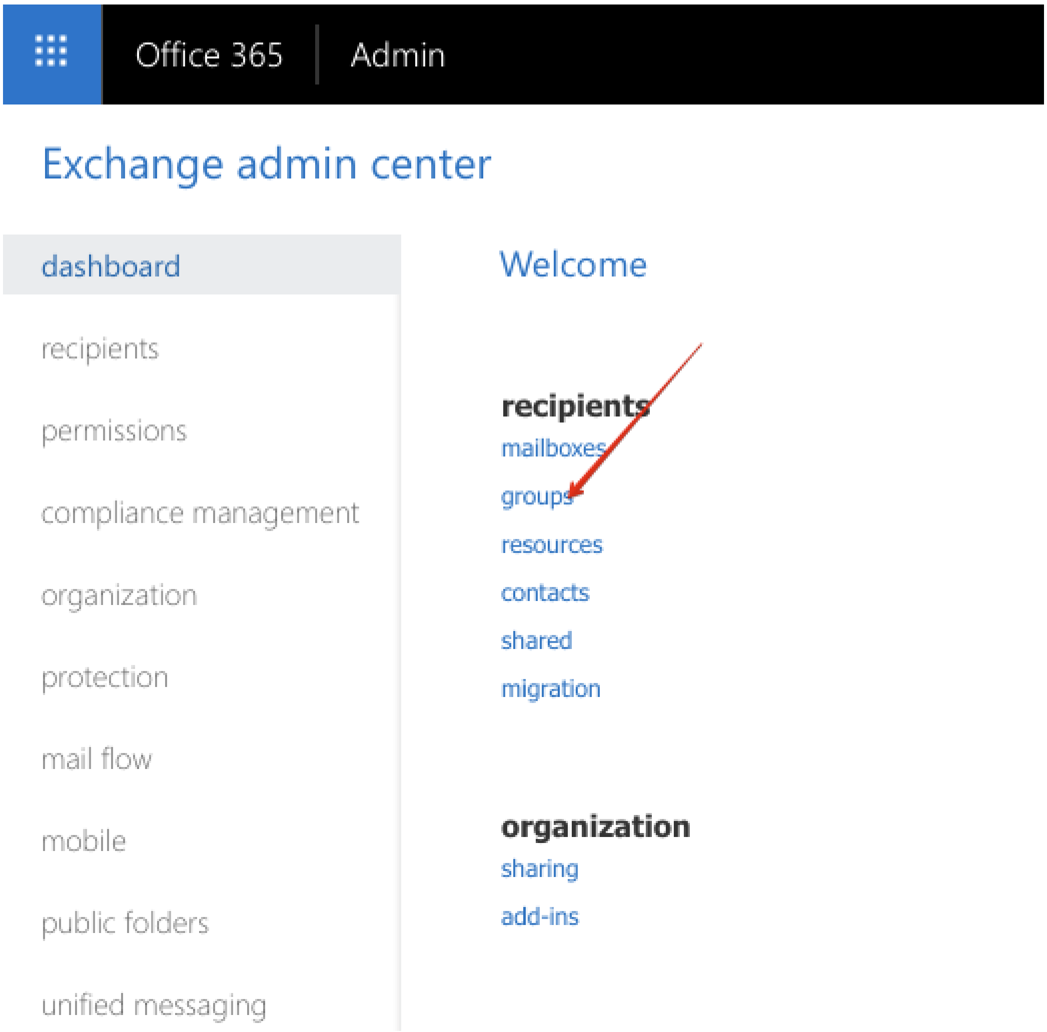
By default, when someone emails a non-existent address at your domain, they receive an mail delivery failure error (*a "**bounce**"*) in response. But if you want total control of incoming email for your domain, and you ***don't*** want to bounce mis-addressed email (*to **accounst@widgets.com**, for example*), you'll want to setup an administrative "catch-all" mailbox.

- Difficulty: Medium
- Risk: Low

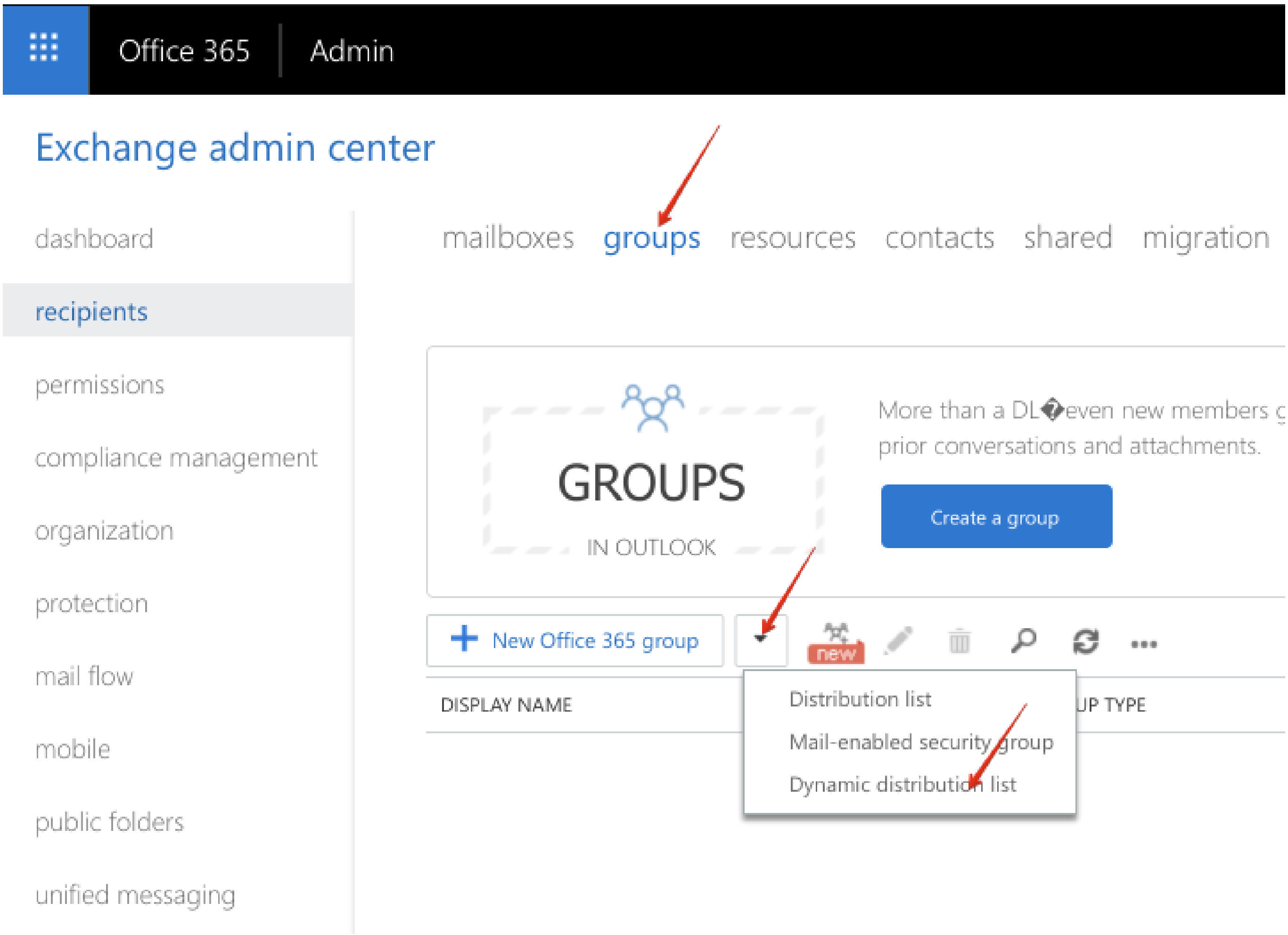
Process

Create dynamic distribution list of all users

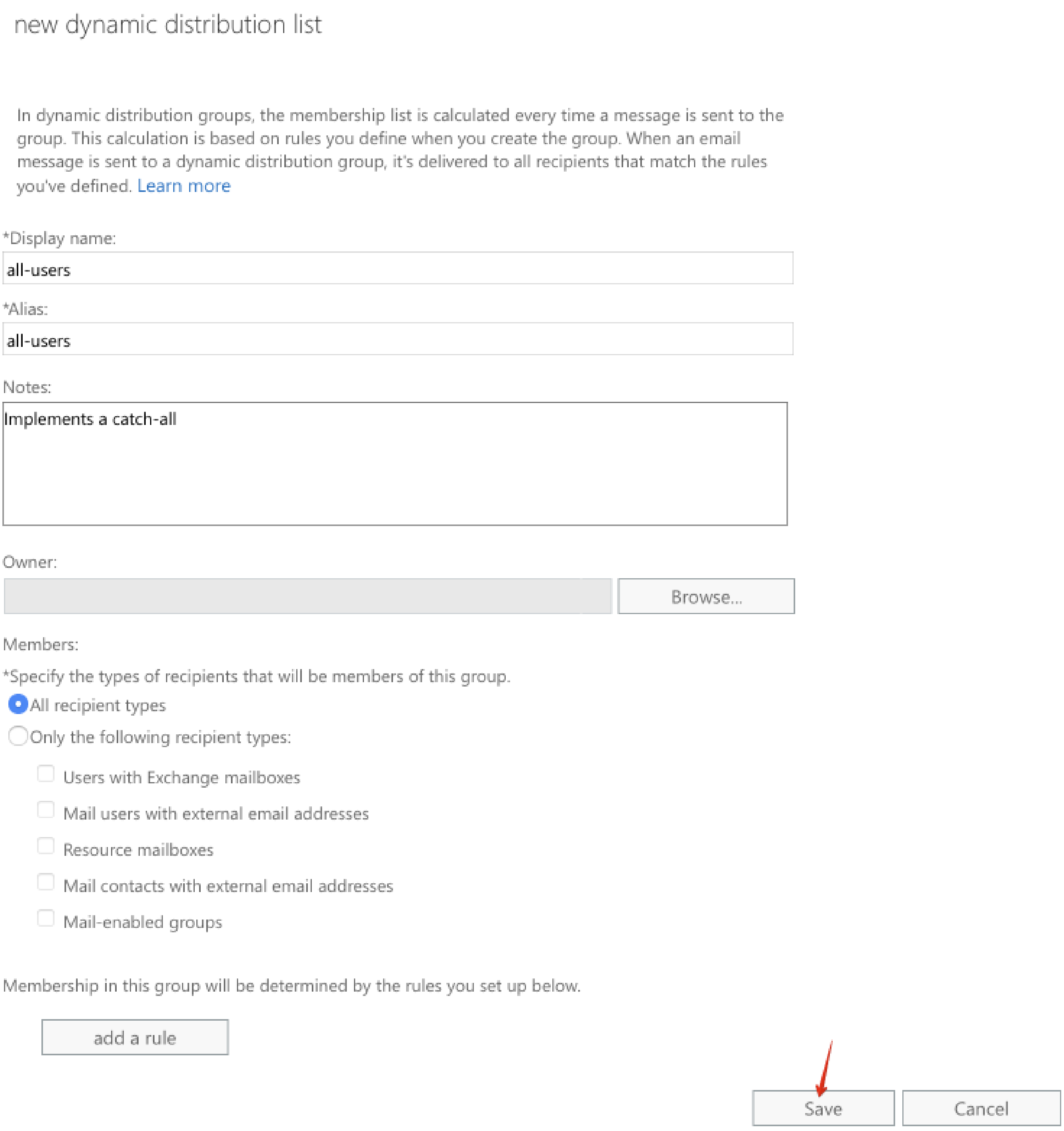
In the `Exchange admin center`, navigate to `recipients` -> `groups`:



Under `groups`, click the arrow on the right of `+ New Ofifce 365 group` to drop down a list of group types, and select `Dynamic distribution list`:



Name your distribution list `all-users` (`Display name` **and** `Alias`), enter a note, and click `Save`:



new dynamic distribution list

In dynamic distribution groups, the membership list is calculated every time a message is sent to the group. This calculation is based on rules you define when you create the group. When an email message is sent to a dynamic distribution group, it's delivered to all recipients that match the rules you've defined. Learn more

*Display name:
all-users

*Alias:
all-users

Notes:
Implements a catch-all

Owner:

Members:

*Specify the types of recipients that will be members of this group.

● All recipient types

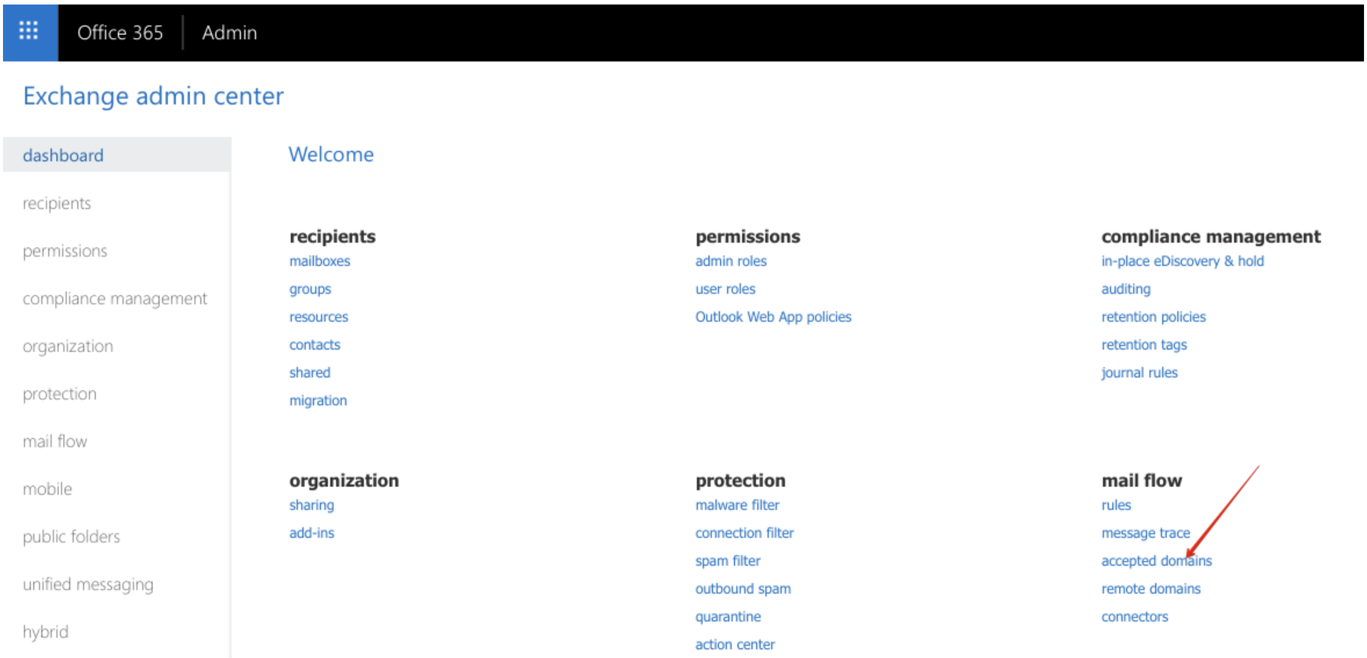
○ Only the following recipient types:

- □ Users with Exchange mailboxes
- □ Mail users with external email addresses
- □ Resource mailboxes
- □ Mail contacts with external email addresses
- □ Mail-enabled groups

Membership in this group will be determined by the rules you set up below.

Alter mail flow

In `Exchange admin center`, navigate to `mail flow` -> `accepted domains`:



Office 365 | Admin

Exchange admin center

- dashboard
- recipients
- permissions
- compliance management
- organization
- protection
- mail flow
- mobile
- public folders
- unified messaging
- hybrid

Welcome

recipients
mailboxes
groups
resources
contacts
shared
migration

permissions
admin roles
user roles
Outlook Web App policies

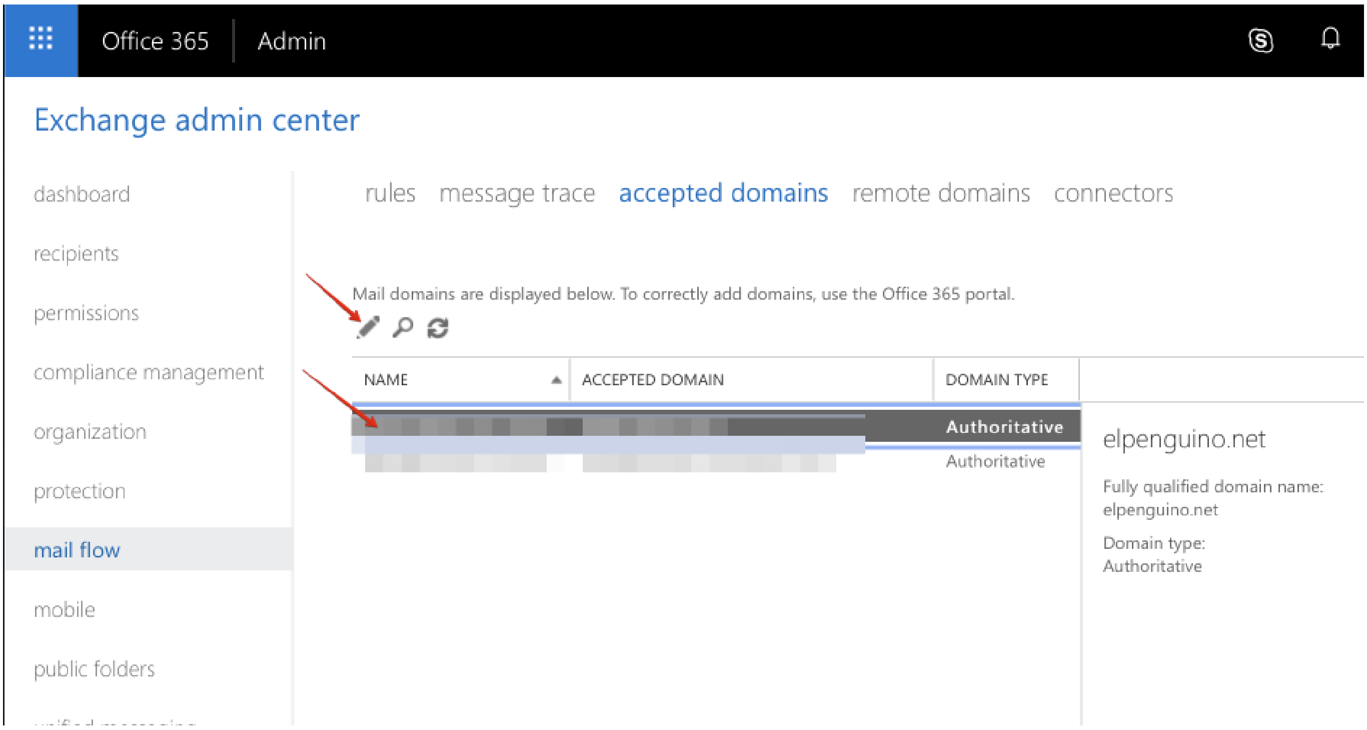
compliance management
in-place eDiscovery & hold
auditing
retention policies
retention tags
journal rules

organization
sharing
add-ins

protection
malware filter
connection filter
spam filter
outbound spam
quarantine
action center

mail flow
rules
message trace
accepted domains
remote domains
connectors

Highlight your domain, and click the pencil icon to edit it:



Office 365 | Admin

Exchange admin center

- dashboard
- recipients
- permissions
- compliance management
- organization
- protection
- mail flow
- mobile
- public folders

rules message trace accepted domains remote domains connectors

Mail domains are displayed below. To correctly add domains, use the Office 365 portal.

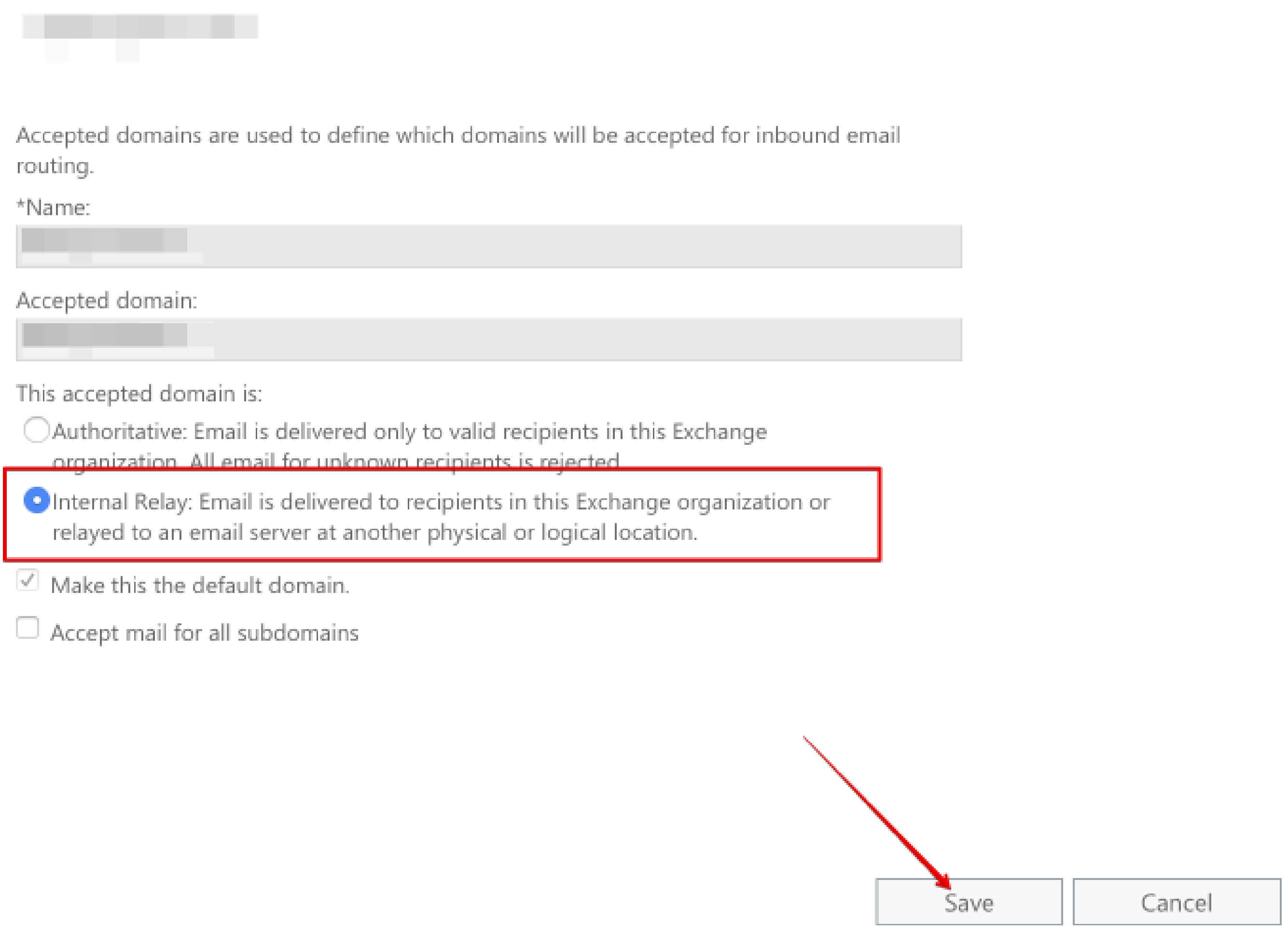
NAME	ACCEPTED DOMAIN	DOMAIN TYPE
[redacted]	[redacted]	Authoritative
[redacted]	[redacted]	Authoritative

elpenguino.net

Fully qualified domain name:
elpenguino.net

Domain type:
Authoritative

Under `This accepted domain is:`, choose `Internal Relay`, and click Save:



[redacted]

Accepted domains are used to define which domains will be accepted for inbound email routing.

*Name:

[redacted]

Accepted domain:

[redacted]

This accepted domain is:

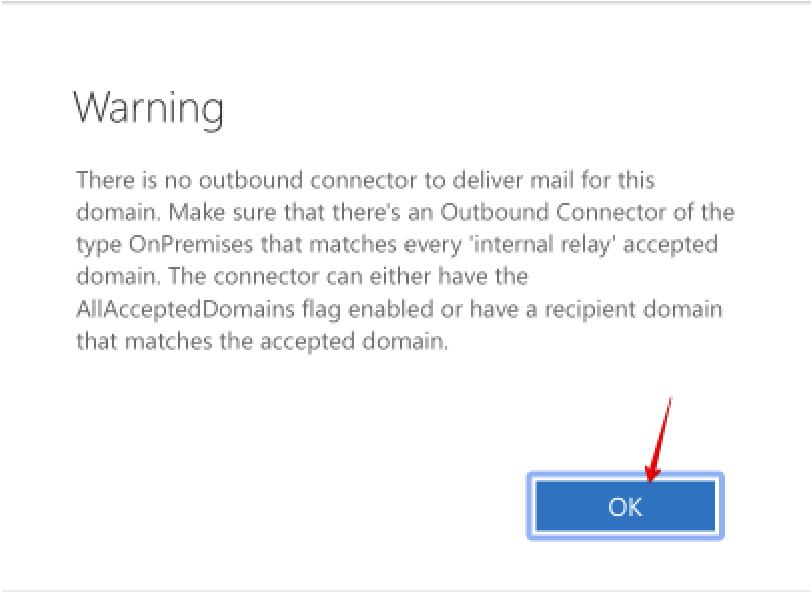
○ Authoritative: Email is delivered only to valid recipients in this Exchange organization. All email for unknown recipients is rejected.

● Internal Relay: Email is delivered to recipients in this Exchange organization or relayed to an email server at another physical or logical location.

☑ Make this the default domain.

□ Accept mail for all subdomains

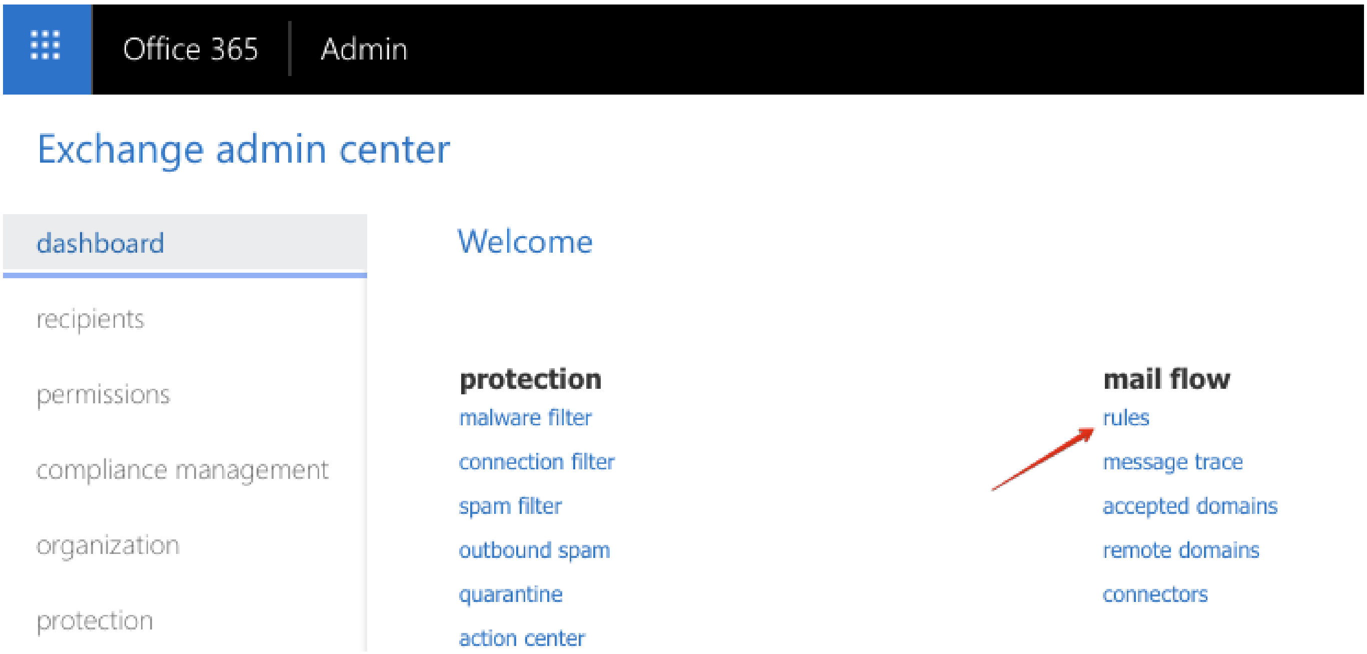
Upon saving, you'll be warned that you don't have an outbound connector for this domain. You can safely ignore this warning - you don't **need** an outbound connector, because you're about to implement a trick to deliver all un-matched email to a local mailbox.



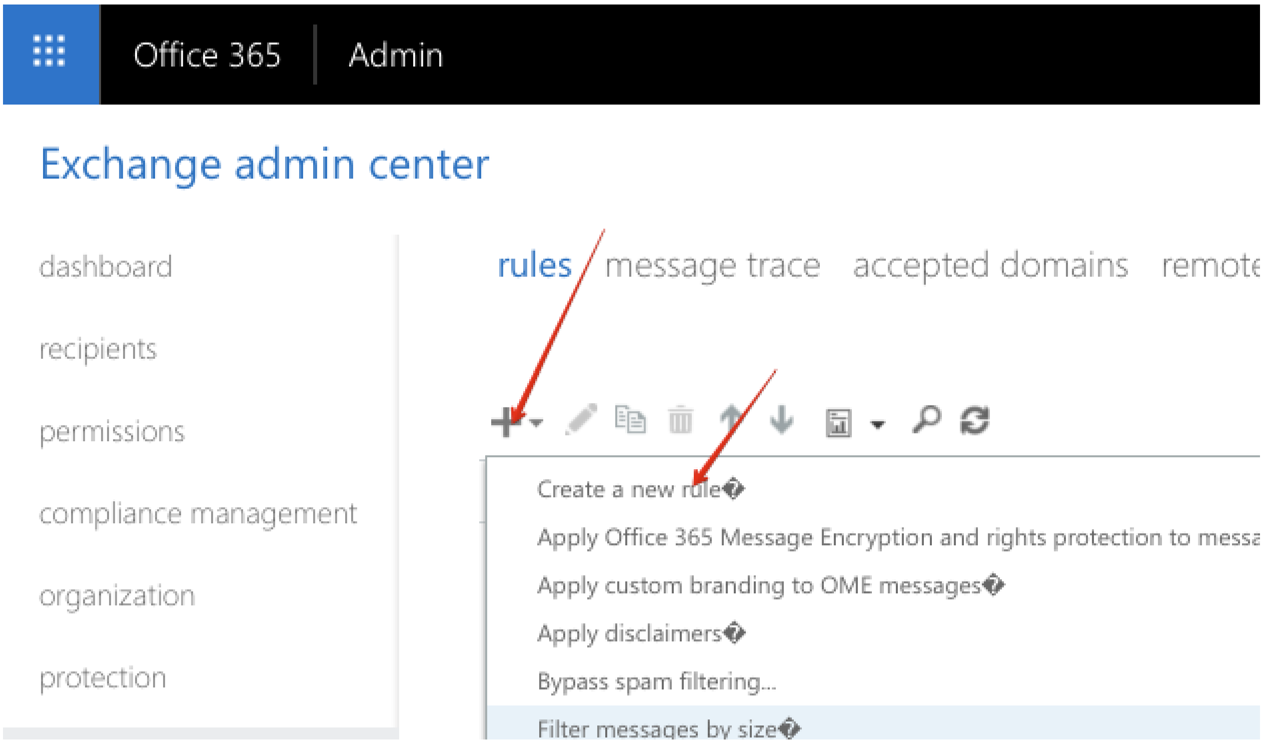
Warning

There is no outbound connector to deliver mail for this domain. Make sure that there's an Outbound Connector of the type OnPremises that matches every 'internal relay' accepted domain. The connector can either have the AllAcceptedDomains flag enabled or have a recipient domain that matches the accepted domain.

Navigate to `mail flow` -> `rules`:



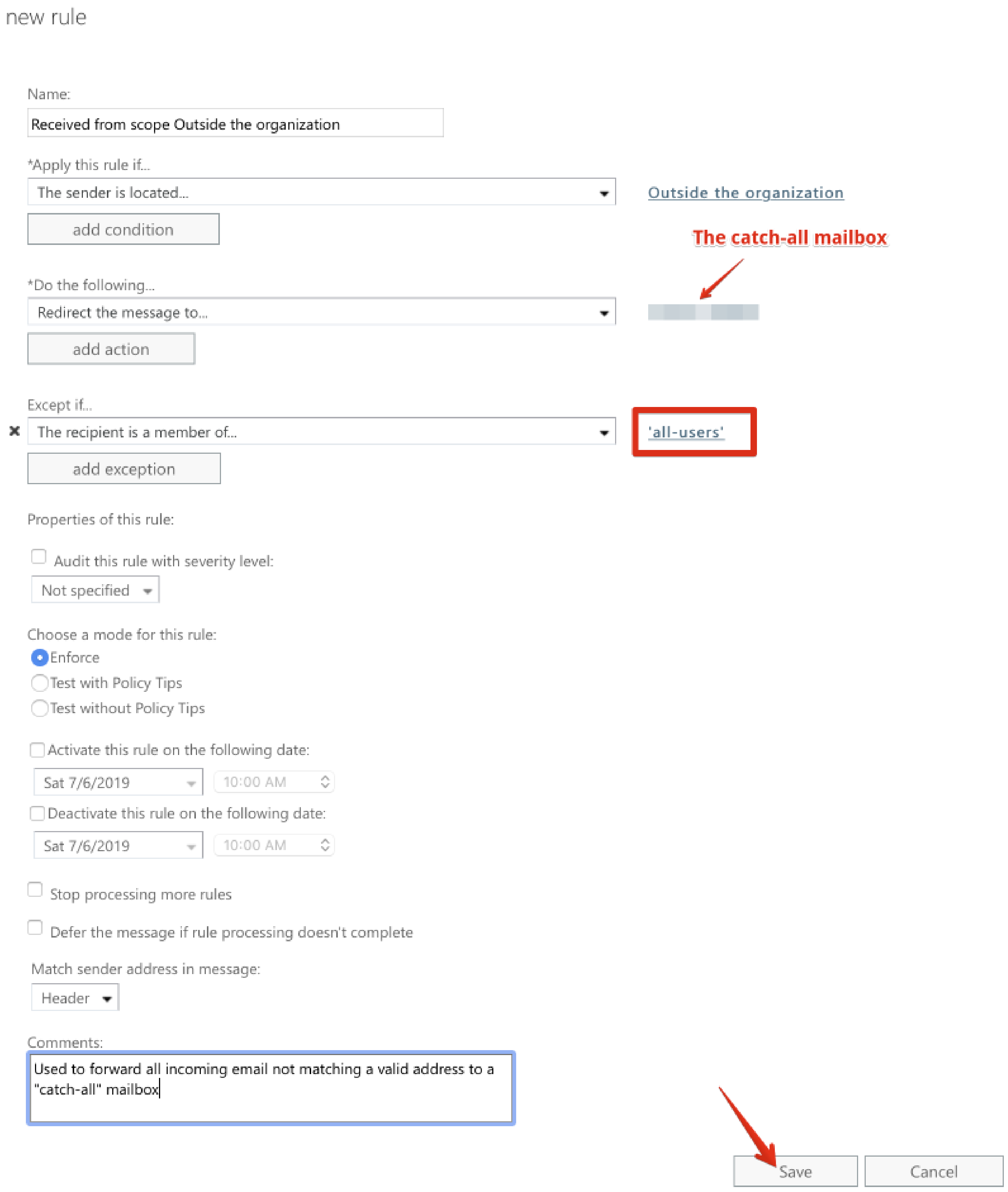
Click the + sign to add a new rule, and choose `Create new rule` from the dropdown:



Use the interface to create a rule with the following:

- Apply this rule if the sender is located.. **Outside the organization**
- Do the following.. **Redirect the message to <your catch-all mailbox>**
- Except if.. **The recipient is a member of all-users** (the dynamic group you created)

Save the rule:



new rule

Name:
Received from scope Outside the organization

*Apply this rule if...
The sender is located... ▾ Outside the organization

add condition

The catch-all mailbox

*Do the following...
Redirect the message to... ▾ [redacted]

add action

Except if...
✖ The recipient is a member of... ▾ 'all-users'

add exception

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:
Sat 7/6/2019 ▾ 10:00 AM

□ Deactivate this rule on the following date:
Sat 7/6/2019 ▾ 10:00 AM

□ Stop processing more rules

□ Defer the message if rule processing doesn't complete

Match sender address in message:
Header ▾

Comments:
Used to forward all incoming email not matching a valid address to a "catch-all" mailbox

Finally, send an email from an outside address to thisaddressdoesntexist@yourdomain.com, and confirm that the message is delivered to the catch-all mailbox.

SPF

What is it?

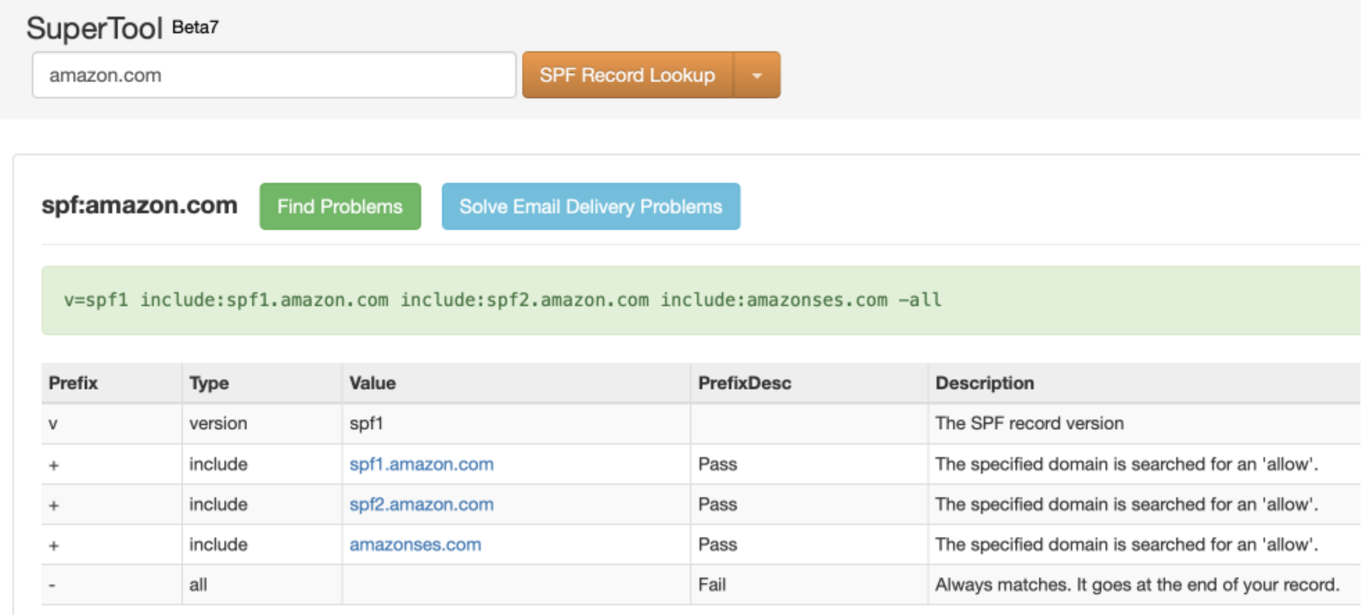
Sender Protection Framework (SPF) is a way to tell the rest of the world which servers are authorized to send email form your domain. (*For example, if your domain is hosted with Office365, recipients should discard any* *emails delivered from spammersrus.com purporting to be sent from your domain!*)

Do I have it?

Enter your domain name into an online SPF testing tool (https://mxtoolbox.com/spf.aspx, for example). For maximum hygine, confirm that:

1. An SPF record exists for your domain
2. The SPF record ends in `-all` (A "hard fail", which instructs receiving mailservers that you do **not** authorize any senders other than those specified, for your domain)

Here's an example of a well-defined SPF record, which hard-fails any unauthorized sources:

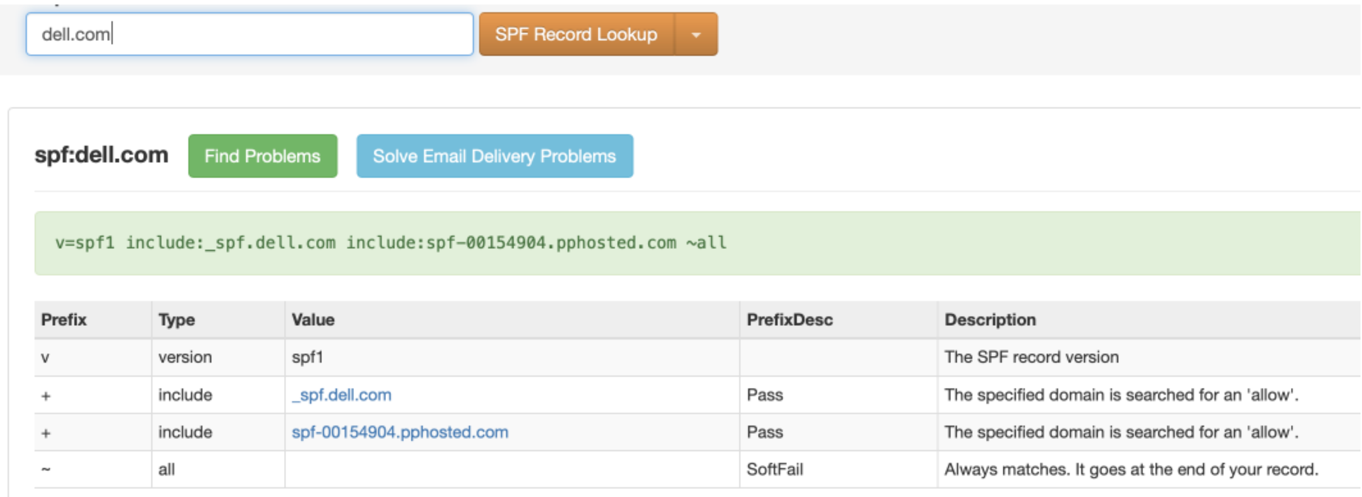


spf:amazon.com

```
v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	include	spf1.amazon.com	Pass	The specified domain is searched for an 'allow'.
+	include	spf2.amazon.com	Pass	The specified domain is searched for an 'allow'.
+	include	amazonses.com	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

Here's an SPF record which, while defined, only soft-fails unauthorized sources (*leaving it up to the receiving mailserver to "make a judgement call"*):

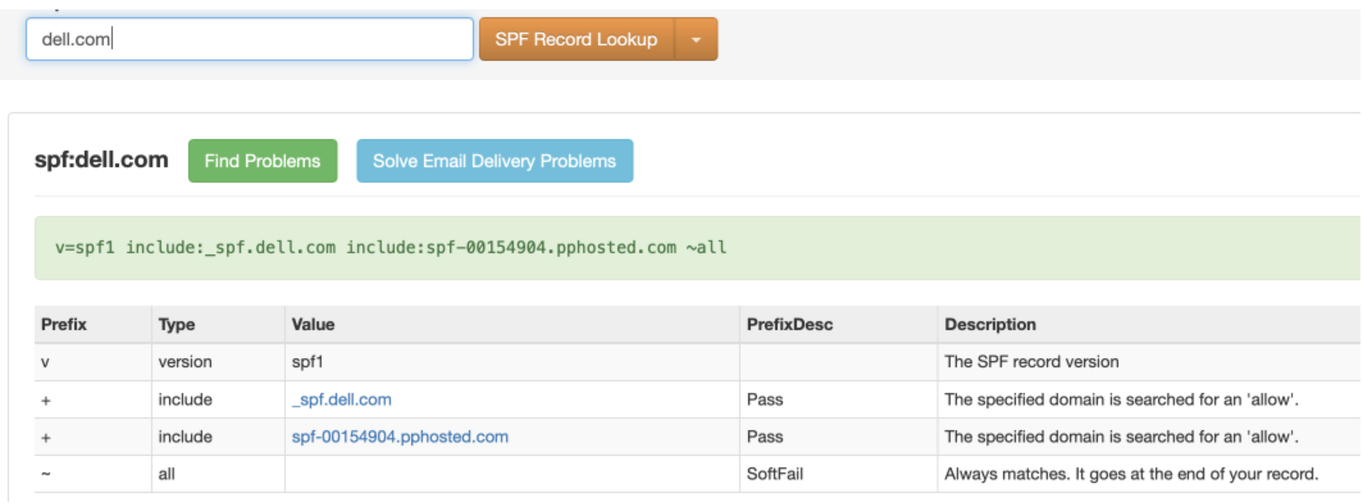


spf:dell.com

```
v=spf1 include:_spf.dell.com include:spf-00154904.pphosted.com ~all
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	include	_spf.dell.com	Pass	The specified domain is searched for an 'allow'.
+	include	spf-00154904.pphosted.com	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

And **here's** an example of a domain with no SPF record:



```
v=spf1 include:_spf.dell.com include:spf-00154904.pphosted.com ~all
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	include	_spf.dell.com	Pass	The specified domain is searched for an 'allow'.
+	include	spf-00154904.pphosted.com	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

How do I get it?

You'll need access to administer your domain's DNS, and you'll want to create a DNS TXT record with the necessary SPF data. Microsoft's support docs explain the process in detail. There are many online SPF record generators, one notable one is https://mxtoolbox.com/SPFRecordGenerator.aspx. If you're fully hosted on Office365, for example, your SPF record could be as simple as `v=spf1 include:spf.protection.outlook.com -all`.

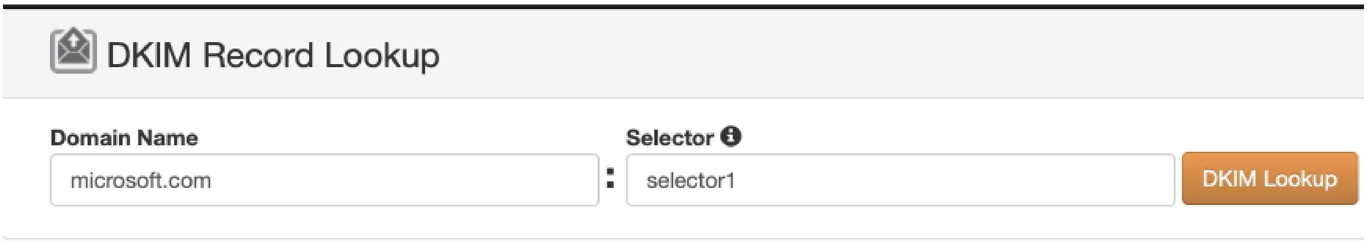
DKIM

What is it?

DomainKeys Identified Mail (DKIM) is another strategy used to prove to the world which servers **should** be allowed to send email for your domain.

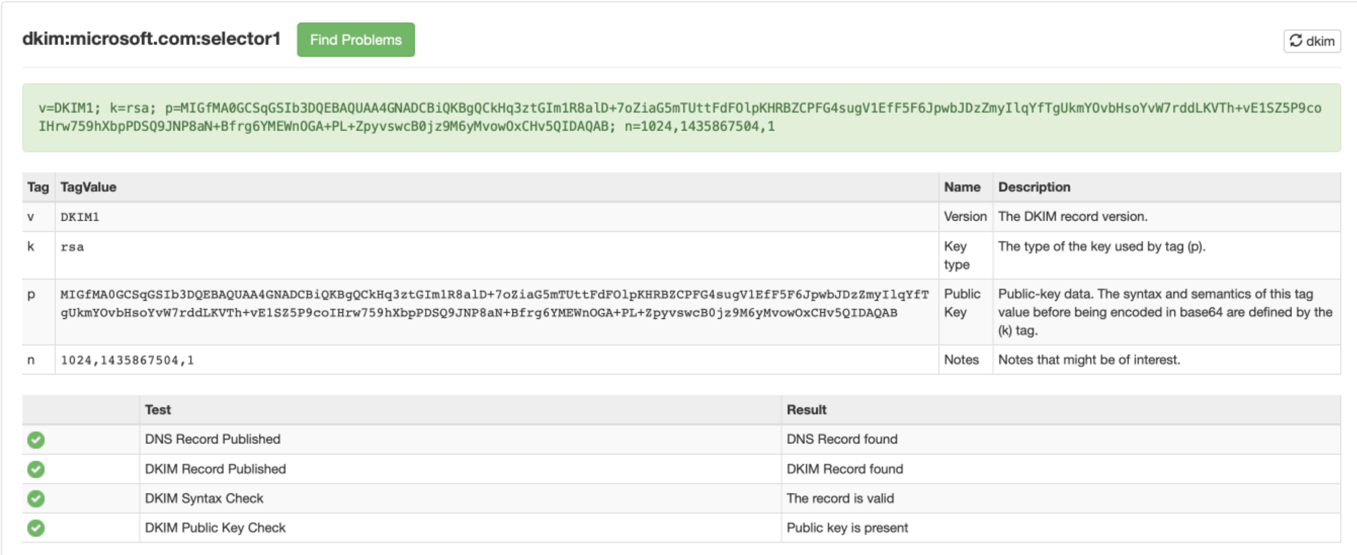
Do I have it?

Confirm that DKIM DNS **records exist** for your domain, by using a DKIM validation tool (https://mxtoolbox.com/dkim.aspx, for example). Supply your domain name and "selector1" as a selector.



Domain Name: microsoft.com
Selector: selector1

Here's an example of a correctly configured domain (Hosted on Office365):



```
v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCkHq3ztGIm1R8alD+7oZiaG5mTUttFdFOlpKHRBZCPFG4sugV1EfF5F6JpwbJDzZmyIlqYfTgUkmYOvbHsoYvW7rddLKVTh+vE1SZ5P9co
IHrw759hXbpPDSQ9JNP8aN+Bfrg6YMEWnOGA+PL+ZpyvswcB0jz9M6yMvowOxCHv5QIDAQAB; n=1024,1435867504,1
```

Tag	TagValue	Name	Description
v	DKIM1	Version	The DKIM record version.
k	rsa	Key type	The type of the key used by tag (p).
p	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCkHq3ztGIm1R8alD+7oZiaG5mTUttFdFOlpKHRBZCPFG4sugV1EfF5F6JpwbJDzZmyIlqYfTgUkmYOvbHsoYvW7rddLKVTh+vE1SZ5P9coIHrw759hXbpPDSQ9JNP8aN+Bfrg6YMEWnOGA+PL+ZpyvswcB0jz9M6yMvowOxCHv5QIDAQAB	Public Key	Public-key data. The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.
n	1024,1435867504,1	Notes	Notes that might be of interest.

	Test	Result
✓	DNS Record Published	DNS Record found
✓	DKIM Record Published	DKIM Record found
✓	DKIM Syntax Check	The record is valid
✓	DKIM Public Key Check	Public key is present

Repeat the test for every domain from which you send email (*if you have more than one domain name*).

Confirm that DKIM **signing** is setup for your domain by following these Microsoft instructions:

1. Sign in to Office 365 with your work or school account.
2. Select the app launcher icon in the upper-left and choose Admin.
3. In the lower-left navigation, expand Admin and choose Exchange.
4. Go to Protection > dkim.
5. Select the domain for which you want to enable DKIM and then, for Sign messages for this domain with DKIM signatures, choose Enable. Repeat this step for each custom domain.

How do I get it?

Microsoft's guide is detailed (*but confusing*).

First, determine your **initial domain**. This domain was created for you when you setup Office365, and it ends in *.onmicrosoft.com*. Typically, your initial domain will be the your actual domain name (*i.e* "*widgets.com*"), with dots removed, followed by "*onmicrosoft.com*". So *widgets.com*'s **initial domain name** will be *widgetscom.onmicrosoft.com*.

Tip: You can also follow the steps above for enabling DKIM in Office365's Exchange Online admin. The resulting page will show you all your configured domains.

Secondly, determine your **domainGUID**. Unless you're a "GCC High" goverment customer, your **domainGUID** will simply be the same as your desired email domain - i.e, "*widgets.com*", with dots replaced with dashes. (*i.e.,* "*widgets-com*").

Now, that you have yoru **initial domain** and **domainGUID**, for every domain you want to protect, create 2 CNAME DNS records:

```
Host name:                      selector1._domainkey
Points to address or value:     selector1-<domainGUID>._domainkey.
<initialDomain>
TTL:                            3600
```

```
Host name:                      selector2._domainkey
Points to address or value:     selector2-<domainGUID>._domainkey.
<initialDomain>
TTL:                            3600
```

In the example of widgets.com, the following 2 records will be created:

```
Host name:                      selector1._domainkey
Points to address or value:     selector1-widgets.com._domainkey.widgets-
com.onmicrosoft.com
TTL:                            3600

Host name:                      selector2._domainkey
Points to address or value:     selector2-widgets.com._domainkey.widgets-
com.onmicrosoft.com
TTL:                            3600
```

Now enable DKIM **signing** for your domain by following these Microsoft instructions:

1. Sign in to Office 365 with your work or school account.
2. Select the app launcher icon in the upper-left and choose Admin.
3. In the lower-left navigation, expand Admin and choose Exchange.
4. Go to Protection > dkim.
5. Select the domain for which you want to enable DKIM and then, for Sign messages for this domain with DKIM signatures, choose Enable. Repeat this step for each custom domain.

(*Note : If the option to enable DKIM signing for your custom domain doesn't exist, you may need to use PowerShell*)

DMARC

What is it?

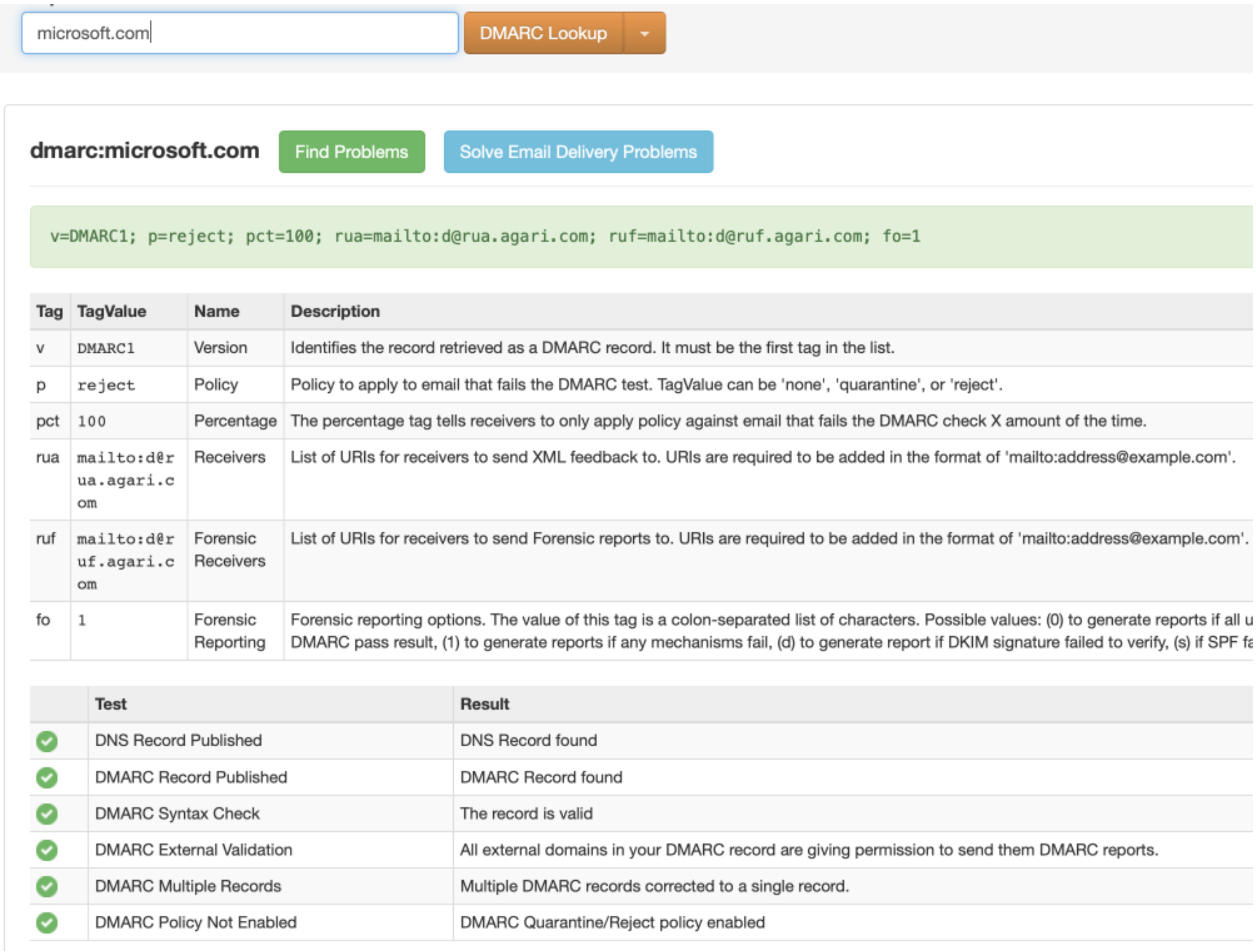
Domain-based Message Authentication, Reporting, and Conformance (DMARC) augments SPF, by testing not only the "envelope sender" of an email (*the address that bounces would go to*), but also the purported "From" address of the sender.

Unlike SPF, DMARC offers far more flexibility regarding what remote mail systems **do** with email which fails validation - you can choose to reject/quarantine a percentage of emails, have delivery reports sent to a nominated email address daily, etc.

Do I have it?

Confirm that DMARC DNS TXT **records exist** for your domain, by using a DMARC validation tool (https://mxtoolbox.com/dmarc.aspx, for example). Supply your domain name and click `DMARC Lookup`.

Here's an example of a correctly configured domain:



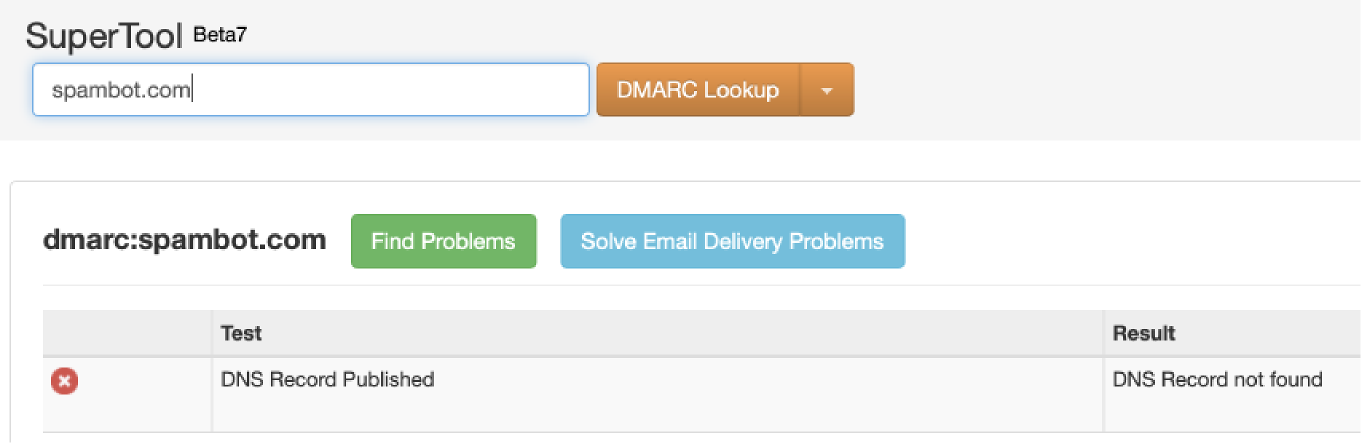
dmarc:microsoft.com

```
v=DMARC1; p=reject; pct=100; rua=mailto:d@rua.agari.com; ruf=mailto:d@ruf.agari.com; fo=1
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. TagValue can be 'none', 'quarantine', or 'reject'.
pct	100	Percentage	The percentage tag tells receivers to only apply policy against email that fails the DMARC check X amount of the time.
rua	mailto:d@rua.agari.com	Receivers	List of URIs for receivers to send XML feedback to. URIs are required to be added in the format of 'mailto:address@example.com'.
ruf	mailto:d@ruf.agari.com	Forensic Receivers	List of URIs for receivers to send Forensic reports to. URIs are required to be added in the format of 'mailto:address@example.com'.
fo	1	Forensic Reporting	Forensic reporting options. The value of this tag is a colon-separated list of characters. Possible values: (0) to generate reports if all u DMARC pass result, (1) to generate reports if any mechanisms fail, (d) to generate report if DKIM signature failed to verify, (s) if SPF fa

	Test	Result
✓	DNS Record Published	DNS Record found
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

And here's an example of an unconfigured domain:



dmarc:spambot.com

	Test	Result
✖	DNS Record Published	DNS Record not found

How do I get it?

To protect your outgoing email with DMARC, setup a DNS TXT record.

Microsoft provides a guide, as does Google. You can also use an online DMARC record generator.

At the most basic (*and harmless*) level, add a TXT record like this to your domain:

```
_dmarc.yourdommain.com --> v=DMARC1; p=none;
rua=mailto:postmaster@yourdomain.com
```

If you want to be more aggressive, and instruct remote servers to **reject** any emails which appear to be spoofed from you, use a record like this:

```
_dmarc.yourdommain.com --> v=DMARC1; p=reject;
rua=mailto:postmaster@yourdomain.com
```

You can also stagger the rollout of DMARC, by instructing remote servers to reject only 10% of your email, and gradually increase this percentage:

```
_dmarc.yourdommain.com --> v=DMARC1; p=none;
rua=mailto:postmaster@yourdomain.com; pct=10
```