

Exchange Online Protection (EOP) Best Practices and Recommendations

Yes. I said it.

Someone needed to put a line in the sand and today, that person is me. I'm going to say these are some best practices.

But of course, your mileage may vary, depending on your type of organization (users at a local bank or city government will have different threats presented to them than an engineering firm with international customers, for example). Though I work for Microsoft, these *may not necessarily* be Microsoft's best practices. Having migrated hundreds of thousands of mailboxes to the cloud for hundreds of customers over the last 7 years, though, I feel moderately confident that not all of our support engineers would take umbrage with them. Which, if you know support engineers, says a lot.

While there *is no one-size-fits-all* prescriptive guidance from end-to-end, there are still a number of settings and configurations that every organization can use to improve their security posture—and all of the settings merit at least *looking* at to see if they would be of benefit to your organization.

I've also made this available as a PDF, if you want to download it as a cure for insomnia. <https://www.undocumented-features.com/wp-content/uploads/2019/08/EOP-Best-Practices-and-Recommendations.pdf>

- [Introduction](#)
- [Background](#)
- [Mail Hosting Scenarios](#)
- [Domains](#)
 - [Add Your Domains to Office 365](#)
 - [Directory-based Edge Blocking](#)
 - [Disable or enable DBEB](#)
 - [Recommendations](#)
- [DNS](#)
 - [MX Record](#)
 - [MX Configuration and EOP Functionality](#)
 - [IP Reputation](#)
 - [IP Throttling](#)
 - [DNS Record Checks](#)
 - [IP Allow and Block Lists](#)
 - [Recommendations](#)
 - [Sender Policy Framework \(SPF\)](#)
 - [Recommendations](#)
 - [DomainKeys Identified Mail \(DKIM\)](#)
 - [Recommendations](#)

- [Enable DKIM for each custom domain in your tenant](#)
 - [Domain-Based Messaging and Reporting Conformance \(DMARC\)](#)
 - [DMARC Structure](#)
 - [Resources](#)
 - [DMARCAalyzer](#)
 - [DMARC Reporting Service Offering through Valimail](#)
 - [Recommendations](#)
- [Mail Flow Operational View](#)
- [Connectors](#)
 - [Connector Scenarios](#)
 - [Exchange Online Protection Standalone](#)
 - [Exchange Hybrid](#)
 - [Edge Transport Servers](#)
 - [Partner Organizations](#)
 - [Multifunction Devices and Other Relay Scenarios](#)
 - [Recommendations](#)
- [Spam filtering](#)
 - [Anti-spam filter policies](#)
 - [Spam and bulk email actions](#)
 - [Bulk email](#)
 - [Allow lists](#)
 - [Block lists](#)
 - [International spam](#)
 - [Spam properties](#)
 - [Applied to](#)
 - [Recommendations](#)
- [Connection Filter Policy](#)
 - [Recommendations](#)
- [Outbound Spam Filter Policy](#)
 - [Recommendations](#)
- [Exchange Transport Rules](#)
 - [Recommendations](#)
- [Malware Filtering](#)
 - [Anti-malware filter policies](#)
 - [Notes](#)
 - [Recommendations](#)
- [Additional Recommendations](#)
 - [The Last Word on Allow Lists](#)
 - [Enabling End User Quarantine](#)
 - [Reviewing Message Headers](#)
 - [Enabling Multi-Factor Authentication](#)
 - [Configure RFC-Compliant Addresses](#)
 - [Configure the External Postmaster Address in Exchange Online](#)
 - [Configure A Shared Mailbox and Basic Reply Rule](#)
- [Additional Tools](#)
 - [Remote Connectivity Analyzer](#)

- [Report Message Add-In](#)
- [Common Scenarios and Troubleshooting](#)
- [Further Reading](#)

Introduction

Exchange Online Protection (EOP) is the standard signature-based antivirus and antimalware engine that comes with an Office 365 subscription. It is also available as a standalone service for customers who have deployed on-premises mail solutions. Advanced Threat Protection (ATP), a behavior-based heuristic threat protection service, can be added as an integrated or purchased as a standalone service as well.

Background

Before we get into the details on how best to configure Exchange Online Protection and recommendations, I think it would be beneficial to discuss how email works under the hood. The defining protocol for electronic mail communication is the [Simple Mail Transfer Protocol](#), or SMTP. Originally released as an internet standard in 1982, [RFC 821](#) described the mechanisms that would reshape communication as we know it. Like all protocols and specifications, the technical details and capabilities of SMTP continue to be expanded and refined. RFC 821 has had features both deprecated and added, and has continued to evolve for nearly 30 years.

SMTP is the digital evolution of something familiar to us: postal mail. SMTP nomenclature features a lot of words that originate in our traditional vernacular, such as mailbox, gateway, envelope, sender, recipient, and address. Two very important ones that we'll be talking about later, when it comes to email validation, authentication, and the handling of bulk, spam, spoof, and phishing emails, are the Sender and Recipient Headers.

Using postal mail as an example, imagine you are sending a letter. When you create this letter, you'll undoubtedly address it to someone (for example, "Dear Elvis,"), and when you're done, you're going to sign it, ("your biggest fan, Aaron"). These are the RFC 5322 RCPT (recipient) and FROM (duh) fields.

Then, you're going to take that letter, fold it up neatly, and put it inside an envelope. On the outside of the envelope, you address it to "The Elvis Lives Fan Club," and you write your return address in the upper-left hand corner of the envelope. Then, rethinking how you handle disappointment, you decide you don't want to get replies sent to you personally, because you don't want to actually know if your letter makes it to the [Great Valley](#). You erase your return address and write in the address of your mother. She'll know how to break the bad news to you should the need arise. These are the RFC 5321 RCPTTO (recipient) and MAILFROM fields.

Just as you can put any *From* address on the envelope, the same applies to SMTP. This is where some sort of authentication and validation becomes extraordinarily important.

Some of the interchangeable terms you might hear:

Field or Header	Common Names	RFC
FROM	P2 Sender	5322
RCPT	P2 Recipient	5322
MAILFROM	P1 Sender, Return-Path, Envelope Sender	5321
RCPTTO	P1 Recipient, Envelope Recipient	5321

If you really want to dig in and learn more about SMTP structure and workings, head over to the IETF and look up RFC [2822](#), as well as the updates to it and related documents, such as [5322](#), [5335](#), and [5336](#), and [6531](#).

On to the good stuff!

Mail Hosting Scenarios

Office 365 and Exchange Online support three core email hosting scenarios: fully hosted, standalone, and hybrid.

- **Fully hosted** – All mailboxes are hosted in Exchange Online
- **Standalone** – All mailboxes are hosted on-premises (Exchange or otherwise) or another external hosting service
- **Hybrid** – Some mailboxes are hosted in Exchange Online and others are hosted on-premises

In whatever situation you find yourself, the configuration recommendations are going to point to using Exchange Online Protection as your primary ingress point for email, since you'll get the most benefit from the service that way.

Domains

Exchange Online uses domains, like contoso.com, to route email messages and manage messaging options. Most customers choose to use their own domains with Exchange Online and Office 365. While the overall ownership and settings for the domains are managed with a domain registrar or DNS hosting provider, they need to be added to Office 365 so that they are available for use in the service.

When you add a domain for use in Office 365, you're asked to prove ownership of it, which is typically done by inserting a record into your public DNS. After it's been added and verified for use in Office 365, it gets added to Exchange Online as an accepted domain. Accepted domains in Exchange Online, much like Exchange Server, are used to determine which domains you have the authority to answer and accept mail for.

Exchange Online and Exchange Online Protection also have the concept of *remote domains*. These are domains external to your Office 365 or Exchange Online Protection environment, but for which you want to manage some settings. For example, you may want to disable out-of-office messages, disable non-delivery reports, or manage the message format settings for a particular domain.

Add Your Domains to Office 365

1. Go to the admin center at <https://admin.microsoft.com>.
2. Go to the **Setup | Domains** page.
3. Select **Add domain**.
4. Enter the name of the domain you want to add, then click **Next**.
5. Choose a method for how you want to verify that you own the domain.
 1. If your domain is registered and DNS hosted at GoDaddy, 1&1, or one of our other [supported registrars](#), you can choose to allow Office 365 to configure the records automatically. Click **Sign in | Next**, provide your registrar credentials, and Office 365 will set up your records automatically.
 2. You can also have an email sent to the registered administrative contact for the domain with a verification code. This probably isn't the best choice if you don't have access to the email account listed at the registrar. If you have access to the registrar, you can update the WHOIS information, and then come back and try that option after the WHOIS database gets update.
 3. You can use a TXT or MX record to verify your domain. Most organizations select this option, and then use the TXT record method to verify ownership, as they are less intrusive. Select this option, and then click **Next** to see instructions for how to add this DNS record. This can take up to 30 minutes to verify, so it might be a good time to run to the cafeteria for a donut or some kale chips. Just kidding. No one eats kale chips as a first choice.
6. Choose how you want to make the DNS changes required for Office to use your domain.
 1. Select **Add the DNS records for me** if you want Office to configure your DNS (See our [list of supported registrars](#)—your domain must be registered AND have its DNS hosted there. If your domain is registered at one of these registrars but you host your own DNS, you'll have to choose the option to manually add the DNS records yourself).
 2. Select **I'll add the DNS records myself**.
 3. If you chose to add DNS records yourself, click **Next** and you'll see a page with all the records that you need to add to your registrars website to set up your domain. You may not need to configure all of the records for all the domains initially (such as Autodiscover, if you're going to configure Exchange hybrid). At this point, the only thing that you *need* to do is add the TXT record to prove you own the domain.
7. If you've added the records manually, you may need to wait and come back to click the **Verify** button. You can safely click **Skip this step**, and then come back to **Setup | Domains** to verify domains later.

All done! For more information on Domains in Office 365, see [Domains](#).

Directory-based Edge Blocking

When you add a domain to Office 365, it's automatically added as an accepted domain in Exchange Online. When it's added, the domain type is set to *Authoritative*, meaning that if an entry doesn't exist in the Global Address List (GAL) for an email address (user, group, public folder, or other recipient), then it doesn't exist. The GAL becomes the authoritative list of all the addresses available in the domain.

Directory-based Edge Blocking (DBEB, since we have an acronym for literally everything) takes this concept and applies it to the inbound edge with Exchange Online Protection. It uses the Global Address List as a perimeter filter. There are times, though, when this behavior may not be desirable—especially if you have a hybrid Exchange environment or other connected mail environments where all of your protected recipients aren't synchronized or populated inside of Exchange Online's directory. For those times, you may need to disable DBEB.

Disable or enable DBEB

Depending on if your recipients exist in Exchange Online, you may need to enable or disable DBEB.

1. Navigate to <https://admin.microsoft.com>, expand Admin Centers, and select **Exchange**.
2. Go to **Mail flow | Accepted domains**.
3. Select the domain and click **Edit**.
4. Select the domain type.
 1. Set to **Internal relay** to disable DBEB.
 2. Set to **Authoritative** to enable DBEB.
5. Click Save.

For more information on Directory-based Edge Blocking, see [Use Directory-based Edge Blocking to reject messages sent to invalid recipients](#).

Recommendations

1. We recommend adding and verifying all of the domains that you will use for email or sign-in identity to Office 365.
2. Once a domain is verified in Office 365 and added as an accepted domain in Exchange Online, it is automatically configured for Directory-based Edge Blocking. To take advantage of edge filtering, ensure all recipients are configured in Exchange Online and enable DBEB.
3. If you work with partner organizations that use messaging systems that support limited content formats or don't want to deliver certain system messages to them (such as out-of-office replies or non-delivery reports), consider setting up a Remote Domain. For more information on remote domains, see [Manage remote domains in Exchange Online](#).

DNS

Four DNS records control how external entities see and interact with your organization: MX, SPF, DKIM, and DMARC. If you're new to DNS, I'd recommend that stop right now, go read up on our [DNS basics](#) cheat sheet, and then come back here. It will make your life better.

Office 365 has built-in anti-spoofing (pretending to be someone you're not) protections designed to detect legitimate cases of spoofing while protecting your email environment from the illegitimate ones. In the world of postal mail, you could equate spoofing to writing someone else's address in the return address spot on the envelope, in hopes that whoever you sent it to would believe that the "fake" sender you put in the return address spot was the actual sender. Spoofing can sometimes be seen as a way to try to add credibility or legitimacy to mail.

The DNS records we're going to discuss, in regards to spoof and spam intelligence protections, have to do with protecting recipients from emails purporting to be from you.

Mail Exchanger, Sender Policy Framework, DomainKeys Identified Mail, and DMARC are those pieces. These are their stories.

<https://www.undocumented-features.com/wp-content/uploads/2019/08/LO.mp3>

MX Record

A Mail Exchanger (MX) record is a DNS resource record designed to tell mail relay servers where to send email, similar to a postal address. An MX record has three pieces of information: a hostname (the address), a priority or weight, and a time-to-live (how long the record is allowed to be cached by a system).

A stroll down memory lane ...

In the dark ages of the Internet (November 1983, to be more precise), there were three records and a query type that defined how mail would flow and be delivered: the *mail destination* (MD) record, *mail forwarder* (MF) record, and *mail agent* (MAILA) query. These were specified by the (now obsolete) [RFC 833](#). There were several record and query types specified in this RFC. At 73 pages, it's a lengthy read for not much info, but that's what standards typically are.

The MAILA query type was designed to return the mail records for a domain—a mail destination (the eventual mailbox server) as well as mail relays (or mail forwarders) that could be expected to receive or queue mail for the recipient.

The nitty gritty comes down to this:

Let's say the recipient is aaron@contoso.com. A sending message transfer agent (MTA) would perform a MAILA DNS query (like, NSLOOKUP -QTYPE=MAILA -QNAME=contoso.com—don't try this, the record query is deprecated), which might return something like this:

```
contoso.com MD IN mailhost.contoso.com
contoso.com MF IN relay.contoso.com
```

The interpretation is this: *mailhost.contoso.com* would be the best bet to deliver the mail, as it's listed in the MD record, but *relay.contoso.com* could accept it and forward it on.

These records were deprecated in 1986 in favor of the simpler MX record, introduced in [RFC 973](#). The MX Record is simply a hostname of a recipient that can accept mail on a domain's behalf combined with a priority or weight, and a time-to-live (expiration). The mail host designated in the MX record will either:

- Accept the mail on the domain's behalf and either relay it to another stop along the way or deliver it directly to the mailbox (if it is responsible for handling the actual mailbox)
- Reject the mail permanently (permission denied, mailbox full, etc)
- Reject or delay the mail temporarily (such as greylisting or unresponsive destination server)

A domain can have multiple MX records for load-balancing, backup, and distribution. For example, if a domain has a single MX record, regardless of the weight or priority, all traffic will get sent to that host:

Domain: **fabrikam.com**
Hostname: **mail.fabrikam.com**
Priority: **0**
TTL: **1 hour**

This record would indicate that the hostname *mail.fabrikam.com* would be solely responsible for receiving traffic on behalf of fabrikam.com. When you introduce the concepts of multiple MX records and weight or priority, all equally-weighted records are returned in a round-robin fashion (one per query), and then if the queried record does not respond, the sending mail server fails to the next lowest in priority.

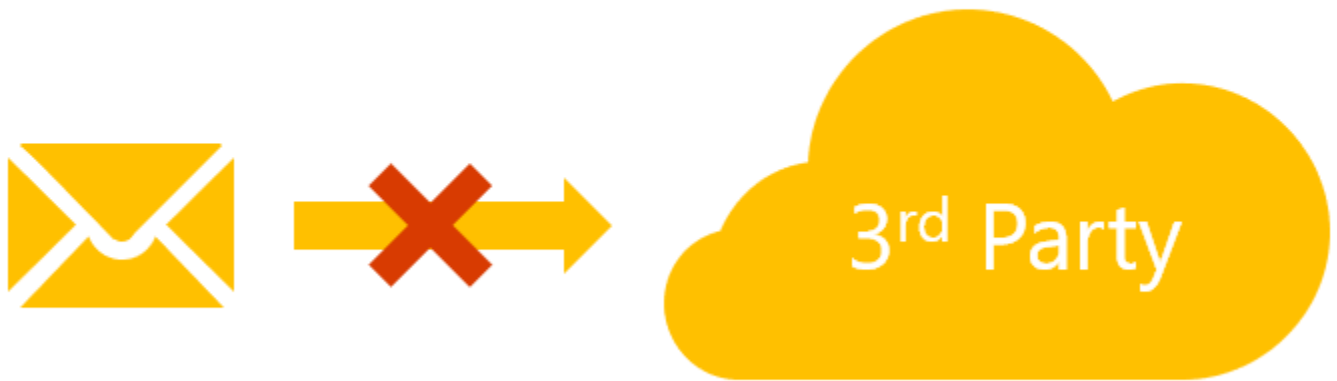
MX Configuration and EOP Functionality

In regards to mail flow, if you are using Exchange Online Protection as part of your spam filtering solution, we recommend that EOP is on the edge, receiving email for your organization. This means setting your MX record to the settings recommended in the Office 365 Admin Center (typically, *domain-com.mail.protection.outlook.com*). There are a number of reasons we recommend this.

IP Reputation

Many of Exchange Online Protection's spam policies rely on IP reputation checks. As mail is processed on the internet (by us and other providers), information regarding spam and phishing messages is gathered and aggregated into a number of databases (both public and private). These databases contain addresses of systems known or likely to send spam. Depending on the literature you read, these databases and services might be referred to as a [Domain Name System Block Lists \(DNSBL\)](#), Real-Time Block Lists (RBL), black lists, or black hole lists. Those (and other ominous terms) typically indicate some sort of automated or curated lists of known and suspected spammers or junk mail senders.

If EOP is the second or third hop after another mail filtering solution (whether it's on-premises or hosted somewhere else), we are making blacklist determinations based on the IP address of the MTA handing off to EOP, and not the original sender. You are reducing the efficacy of EOP, and will instead need to rely on the IP reputation-based filtering settings on the edge MTA or third-party service acting as the first hop.



IP Throttling

Way back in 2014, we introduced IP throttling into Exchange Online Protection. Our IP throttling is a form of [greylisting](#), a reputation-based function designed to delay messages from systems for which there isn't enough information yet to understand if they are legitimate or not. When EOP receives a message from an unknown originating MTA, it issues a 450-level status response (*451 5.7.500-699 (ASxxx) Please try again later*), instructing the sending server to try

again later. Most legitimate systems will retry according to their queue settings; many spam-type systems won't retry and will just move on to the next recipient or host.

If EOP is *not* the MX recipient for your domain, IP throttling and greylisting don't work as designed, as they will be receiving mail from either your on-premises (trusted) environment or third-party (also presumably trusted) environment, and you don't want to delay those.

DNS Record Checks

Exchange Online Protection also makes use of various DNS mechanisms later described (SPF, DKIM, DMARC) to determine the legitimacy of email. If an on-premises or third-party system modifies the message in transit before EOP has a chance to verify those records, the results may end up being invalid.

IP Allow and Block Lists

Like other mail filtering systems, Exchange Online Protection provides mechanisms to block or allow traffic from certain IP addresses. These policies do not work if your MX record is pointing to an on-premises or third-party gateway in front of or instead of EOP. For maximum functionality of IP allow and block lists, EOP should be configured as your MX host. Otherwise, you will need to configure IP allow and block lists in the external systems. *Note: If you have Exchange Transport Rules (ETRs) or spam rules that also rely on IP addresses or PTR lookups, they may not work correctly if Exchange Online Protection is not configured to be your MX host.*

Recommendations

As you've seen, Exchange Online Protection makes use of many IP-based features which require it to be configured as the receiving MX host for your organization. While it is *possible* to use other services in front of Exchange Online Protection, we can't provide support on it, and you'll be reducing the efficacy of the solution. As such, we recommend that you configure EOP as your primary filtering solution.

1. Use Exchange Online Protection as your primary filtering solution by updating your external DNS MX record to point to the value specified in your Office 365 Admin Center (typically *domain-tld.mail.protection.outlook.com*).
2. Don't use backup or lower-priority MX records that point to third-party or on-premises mail systems. Spammers and bulk mail senders typically look for lower-priority MX records in an effort to bypass primary filtering systems, since the configurations are likely not the same.
3. For hybrid Exchange deployments, update your MX record to point to Exchange Online Protection. The TLS inbound and outbound connectors between your on-premises environment will allow mail to be transferred to mailboxes hosted both in-cloud and on-premises.

For further information on configuring mail flow for Office 365, see [Mail flow best practices for Exchange Online and Office 365](#).

Sender Policy Framework (SPF)

The Sender Policy Framework authentication mechanism has its roots way back in 2000. It underwent a few proposals, but eventually emerged as a draft in 2003, and after some hemming and hawing, made its way to *Experimental IETF* status in 2005, and then published as an Experimental [RFC 4408](#). In 2014, SPF's standing was further upgraded to *Proposed Standard* as part of [RFC 7208](#).

Our detailed documentation for setting up SPF is located [here](#), but I'll consolidate and hopefully simplify it for you below.

SPF is configured via a TXT record in your organization's external DNS for a particular domain. You can think of an SPF record as a list of hosts (names, IP addresses, or names and IP addresses listed inside another SPF record) that are allowed to send mail on the domain's behalf.

An SPF record has 2 parts: the **version** information and the **mechanisms** (of which there are 8). We'll use Microsoft's SPF record as an example. Take a look at it below:

```
"v=spf1 include:_spf-a.microsoft.com
include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-
a.microsoft.com
include:spf-a.hotmail.com ip4:147.243.128.24 ip4:147.243.128.26
ip4:147.243.1.153
ip4:147.243.1.47 ip4:147.243.1.48 -all"
```

In the example, **v=spf1** is the version identifier information, and the rest of the record are the mechanisms. Valid mechanisms are:

ALL	Matches always; used for a default result like <code>-all</code> for all IPs not matched by prior mechanisms.
A	If the domain name has an address record (A or AAAA) that can be resolved to the sender's address, it will match.
IP4	If the sender is in a given IPv4 address range, match.
IP6	If the sender is in a given IPv6 address range, match.
MX	If the domain name has an MX record resolving to the sender's address, it will match (i.e. the mail comes from one of the domain's incoming mail servers).
PTR	If the domain name (PTR record) for the client's address is in the given domain and that domain name resolves to the client's address (forward-confirmed reverse DNS), match. This mechanism is discouraged and should be avoided, if possible, per the note in RFC 7208 Section 5.5 . The name of the section is even called "ptr (do not use)," so that gives you an idea of how the IETF feels about it.
EXISTS	If the given domain name resolves to any address, match (no matter the address it resolves to). This is rarely used. Along with the SPF macro language it offers more complex matches like DNSBL -queries.
INCLUDE	References the policy of another domain. If that domain's policy passes, this mechanism passes. However, if the included policy fails, processing continues. To

fully delegate to another domain's policy, the *redirect* extension must be used.

In addition to *mechanisms*, there are also 4 qualifiers:

- + (plus) for a PASS result. This can be omitted; e.g., +mx is the same as mx.
- ? (question mark) for a NEUTRAL result; interpreted like NONE (no policy).
- ~ (tilde) for SOFTFAIL, a debugging aid between NEUTRAL and FAIL. Typically, messages that return a SOFTFAIL are accepted but tagged.
- - (minus) for FAIL; the mail should be rejected.

So, when examining the Microsoft record, you'll see that we use 3 of the mechanisms. We use **INCLUDE** to designate which additional SPF records we'd like ours to reference, we use **IP4** to match individual host IP addresses or ranges of IPs that may not have a DNS record specified, and we use the **ALL** mechanism with the - (minus) qualifier to instruct recipient systems on how interpret senders claiming to send on behalf of microsoft.com: "the addresses listed in the INCLUDE and IP4 statements are authoritative, and we're sure of it. For real."

Frequently, when organizations first start configuring SPF records, they may be unsure of all of the hosts that are sending mail on their behalf, so they may choose to use the ~ qualifier with the **ALL** mechanism, which would instruct the receiving host to check for SPF, but not reject it if it doesn't match. Some spam filtering gateways do have options (non-RFC, mind you) to treat ~ as -. Once you are certain that you have accounted for all your hosts, we recommend you implement the **ALL** mechanism with the - qualifier.

When you are looking at email headers, SPF records are validating the P1 or envelope header (the address specified when the SMTP **MAIL FROM** command is used, per [RFC 5321](#)). From the header's perspective, this is seen as **Return-Path**.

Recommendations

1. Verify all of the hosts (IP address, hostnames, third-party services, web servers, etc.) that are sending mail on your behalf.
2. Implement an SPF record that includes those hosts, as well as the recommended Exchange Online Protection SPF record inclusion (**include:spf.protection.outlook.com**).
3. Use the **ALL** mechanism with the - qualifier. DO NOT USE THE + qualifier with **ALL**, as that is effectively treating all senders as authorized for your domain (*seriously, why even HAVE an SPF record at that point*). If you use the + qualifier, you lose automatically. Do not pass GO. Do not collect \$200.
4. Do not implement more than one SPF TXT record. This is strictly against the RFC, as stated in [Section 3](#):

The SPF record is expressed as a single string of text found in the RDATA of a single DNS TXT resource record; multiple SPF records are not permitted for the same owner name.

For more information, see [How Office 365 uses Sender Policy Framework \(SPF\) to prevent spoofing](#).

DomainKeys Identified Mail (DKIM)

DomainKeys Identified Mail (DKIM) is another authentication mechanism designed to detect spoofing, a technique commonly used in phishing and spam messages make the recipient believe the sender is someone different than they actually are.

DKIM is a form of [public key cryptography](#).

Public key cryptography is a mechanism built from two keys (a **public** key, which is widely distributed and known) and a **private** key (which only the sender/content creator has access to). The content creator *signs* (or creates a cryptographic hash) of selected content with their *private* key. A recipient or viewer of the content can access the sender's *public* key, apply it to the signed or hashed content, and decrypt it and verify its content and source. PKI is kind of like a fingerprint or old-timey [wax seal](#) in that way—it provides [non-repudiation](#), meaning that only the person with this particular private key can generate a hash that can be decoded by this public key.

With DKIM, a sender (usually the sender's email system, as it's typically invisible to the end user) affixes a cryptographic signature of selected hashed content or fields in the header of an email message (for example, the From or Body parts may be hashed). This signature, as with all public key cryptography, is generated with the sender's private key. The recipient system is able to look up that value against the public key denoted in the domain's DKIM selector DNS record. This ensures that the system sending the mail was indeed cryptographically configured to send it, as a form of non-repudiation (as in, you can prove that an email originated from a given domain and sending infrastructure).

DKIM supports multiple keys through the implementation of a tag mechanism called a *selector*. This allows for generating a specific selector/key-pair match for different sending systems. For example, you may configure your internal system to use **selector1/key-pair A**, and you may have a third-party mailing list service that is configured to use **selector2/key-pair B**. In so doing, you are able to verify which system originated a message, and, should a key get compromised, be able to replace that key without affecting other keys in operation.

The values the sender system has chosen to sign influences how further processing of the message could affect the DKIM signature. For example, if the body of the message was hashed and a relaying MTA appends something like **Scanned with X-Ray Vision** at the end of the message, the cryptographic hash for the body has changed, and when the recipient checks the DKIM signature, the message will fail validation.

The DKIM signature tells us *what* fields or properties were used in computing the hash. The valid tags are:

- **v**, version
- **a**, signing algorithm
- **d**, domain
- **s**, selector

- **c**, [canonicalization](#) algorithm(s) for header and body
- **q**, default query method
- **t**, signature timestamp
- **x**, expire time
- **h**, header fields – list of those that have been signed
- **bh**, body hash
- **b**, signature of headers and body

Here is a sample DKIM signature I received:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com;
s=20161025;
h=subject:to:references:from:message-id:date:user-agent:mime-version
:in-reply-to:content-language:content-transfer-encoding;
bh=7vkAPfWWmvsnxoy+A2hlBJnRCGgVb82S4PPbht4k1jk=;
b=BSujkHHL57sLIznA0NfJjzNV0WDq/y1F8+cxCP8dp1GEqSJOJGottfkKdWBtUK3KRQ
wAuXtTDfmb8vEeVEKikmehO6wb9cQsq971BN5h+M3rcWctMOiN80NEgiOMs7kutYXcpn
VbhRbOK8jJNlrWuV6eyVuiMM5YT2eVeqAXzmaYkIzqPwc3mb2z8Xtbzy2/gaGQl/cIzN
bEYootv00ISVh9at58YMiQiZJ36611qxX60Lfz5oM/5r/jQDthPFVDWFIId493sBz439
9j9/Oi2hHlUtvLwlxu1iuUTwwJBsAbB7Xa7tmWpaprui+/d17T1zytSnPXtbB3NA2p
bSAw==
```

Examining the sample DKIM signature I received, we can see the following:

Ta Value/Function

g

v Version: 1

a Algorithm: RSA-SHA256

c Canonicalization: relaxed (header), relaxed (body)

d Domain: gmail.com

s Selector: s20161025

h Header fields: subject, to, references, from, message-id, date, user-agent, mime-version, in-reply-to, content-language, and content-transfer-encoding

bh Body hash: 7vkAPfWWmvsnxoy+A2hlBJnRCGgVb82S4PPbht4k1jk=

b Body and header signature:

```
BSujkHHL57sLIznA0NfJjzNV0WDq/y1F8+cxCP8dp1GEqSJOJGottfkKdWBtUK3KRQ
wAuXtTDfmb8vEeVEKikmehO6wb9cQsq971BN5h+M3rcWctMOiN80NEgiOMs7kutYXc
pn
VbhRbOK8jJNlrWuV6eyVuiMM5YT2eVeqAXzmaYkIzqPwc3mb2z8Xtbzy2/gaGQl/cIzN
bEYootv00ISVh9at58YMiQiZJ36611qxX60Lfz5oM/5r/jQDthPFVDWFIId493sBz439
9j9/Oi2hHlUtvLwlxu1iuUTwwJBsAbB7Xa7tmWpaprui+/d17T1zytSnPXtbB3NA2p
bSAw==
```

When the destination MTA receives the message with a signature, it knows it needs to look up the selector **20161025** for the domain **gmail.com**. The selector DNS record structure is part of the RFC, so the receiving MTA will look up the text record **20161025._domainkey.gmail.com**, for which the value is:

```
"k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAviPGBk4ZB64UfSqWy
AicdR7lodhytae+EYRQVtKDhM+1mXjEqRtP/pDT3sBhazkmA48n2k5NJUyMEoO8nc2r6sUA
+/Dom5jRBZp6qDKJOWjJ5R/OpHamlRG+YRJQqRtqEgSiJWG7h7efGYWmh4URhFM9k9+rmG/
CwCgwx7Et+c8OMlngaLl04/bPmfPjdEyLWyNimk761CX6KymzYiRDZ1MOJOJ7OzFaS4PFb
VLn0m5mf0HVNtBpPwWuCNvaFVflUYxEyblbB6h/oWOPGbzoSgtRA47SHV53SwZjIsVpbq4L
xUW9IxAEwYzGcSgZ4n5Q8X8TndowsDUzoccPFGhdwIDAQAB"
```

This DKIM record has two tags:

Tag Value/Function

k Type of algorithm used in public key (RSA, in this example)
(key type)

p MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAviPGBk4ZB64UfSqWy
(public key) AicdR7lodhytae+EYRQVtKDhM+1mXjEqRtP/pDT3sBhazkmA48n2k5NJUyMEoO8nc2r6sUA+/Dom5jRBZp6qDKJOWjJ5R/OpHamlRG+YRJQqRtqEgSiJWG7h7efGYWmh4URhFM9k9+rmG/CwCgwx7Et+c8OMlngaLl04/bPmfPjdEyLWyNimk761CX6KymzYiRDZ1MOJOJ7OzFaS4PFbVLn0m5mf0HVNtBpPwWuCNvaFVflUYxEyblbB6h/oWOPGbzoSgtRA47SHV53SwZjIsVpbq4LxUW9IxAEwYzGcSgZ4n5Q8X8TndowsDUzoccPFGhdwIDAQAB

Note: The actual string for gmail.com's public key is broken into two TXT records, since it's a 2048-bit key. I concatenated it here for readability.

There are a few more tags available, though not all of them are widely used. The DKIM selector record is formatted much like the authentication signature—with key-value pairs:

Tag Value

- v** Version. OPTIONAL, RECOMMENDED. The version of the DKIM record. The default is DKIM1. The verifiers perform a string comparison on this value, so DKIM1 is not the same as DKIM1.0. DKIM1 is currently the only valid value, but as the standard evolves, new tags and formats may be introduced.
- g** Granularity. OPTIONAL. The default value is “*”. The intent of the tag is to character match the signing address and further restrict the usage of the signing key.
- h** Acceptable Hash Algorithms. OPTIONAL. This field, if present, should contain a colon-separated list of algorithms that might be used. Signers AND verifiers MUST support **sha256**. Verifiers MUST support the **sha1** algorithm as well.
- k** Key Type. OPTIONAL. The default value is RSA. This field, if present, indicates the type of DER-encoded public key exists in the “p=” tag. Signers AND verifiers MUST support the “rsa” type.
- n** Notes. OPTIONAL. Plain-text, human-readable notes. No verifier should use this field; it is meant for administrators.

- p** Public-key data. **REQUIRED**. This value must be base64 encoded. A blank or empty value means the key has been revoked.
- s** Service Type. **OPTIONAL**. The default value is “*”. The current valid potential value is **email**, though it could be expanded should DKIM be used for other services in the future.
- t** Flags. **OPTIONAL**. The default is for no flags to be set. Valid flags include **y**, which indicates the domain is testing DKIM (verifiers **MUST NOT** treat messages flagged as testing differently from unsigned mail, even if the signature fails to verify; and **s**, which indicates a DKIM signature header field using the “i=” tag **MUST** have the same domain on the right-hand side of the @ value in the “i=” tag and the “d=” tag.

Exchange Online establishes two keys for every customer and signs all outbound mail using these keys by default. To ensure alignment, it is recommend that the appropriate DNS entries be created for each custom domain.

Recommendations

The following configurations and steps will allow you to enable DKIM signing for each custom domain in your tenant. We recommend that you configure DKIM for every domain in your organization. Since the DKIM keys are configured and managed in the tenant’s *initial domain* namespace (tenant.onmicrosoft.com), you’ll be creating CNAME records in *your DNS* to point to the records in *our DNS*.

Enable DKIM for each custom domain in your tenant

1. Connect to Exchange Online PowerShell.

2. Show the domains verified in the tenant and their DKIM configuration status:

Get-DkimSigningConfig

```
Windows PowerShell

PS C:\> Get-DkimSigningConfig

Domain                                Enabled
-----                                -
o365ninja.mail.onmicrosoft.com      False
o365ninja.com                        False
o365ninja.onmicrosoft.com           True

PS C:\>
```

3. For one of your custom domains (in my example, I'm going to configure o365ninja.com), run:

Get-DkimSigningConfig -DomainName o365ninja.com | Select Domain,Selector*

```
Windows PowerShell

PS C:\> Get-DkimSigningConfig -Identity o365ninja

Domain : o365ninja.com
Selector1KeySize : 1024
Selector1CNAME : selector1-o365ninja
Selector1PublicKey : v=DKIM1; k=rsa; p=M
                    rm6K3l+Xp9toQCsP6le
                    iL+ysZtFwDfsB6W1nL9
Selector2KeySize : 1024
Selector2CNAME : selector2-o365ninja
Selector2PublicKey : v=DKIM1; k=rsa; p=M
                    H0dfQHIFGAMkSKFxZMN
                    ITzEyyLY9SgtvvXzjJs
SelectorBeforeRotateOnDate : selector2
SelectorAfterRotateOnDate : selector1

PS C:\>
```

*Note: If nothing is returned, you'll need to run **New-DkimSigningConfig -DomainName <domain> -Enabled \$false** first. Office 365 should generate the DKIM selector public keys automatically, however.*

4. Highlight and copy the **Selector1CNAME** value. We're going to use this in a minute.

```
Select Windows PowerShell

PS C:\> Get-DkimSigningConfig -Identity o365ninja

Domain : o365ninja.com
Selector1KeySize : 1024
Selector1CNAME : selector1-o365ninja
Selector1PublicKey : v=DKIM1; k=rsa; p=M
                    rm6K3l+Xp9toQCSP6le
                    iL+ysZtFwDfsB6W1nL9
Selector2KeySize : 1024
Selector2CNAME : selector2-o365ninja
Selector2PublicKey : v=DKIM1; k=rsa; p=M
                    H0dfQHIFGAMkSKFxZMN
                    ITzEyyLY9SgtvvXzjJs
SelectorBeforeRotateOnDate : selector2
SelectorAfterRotateOnDate : selector1

PS C:\> _
```

5. Log into your external DNS. In my case, this domain is hosted at [GoDaddy](#).



Domain Manager



GoDaddy INC. [US] | ht

To see favorites here, select ☆ then ☆, and drag

GoDaddy®



Domain Manager

Domains ▼

Buy & Sell ▼

DNS ▼

Settings

My Domains

Domains ▼

**aaronoffice365lab
.com**

Renews on 1/8/2022

o365ninja.com

Renews on 3/11/2024

6. Once you're in the spot to manage it, you'll want to Add a record. We're going to select **CNAME** as the type, and then use the values from the Get-DkimSigningConfig to populate it.



Domain Manager



GoDaddy INC. [US]

ht

To see favorites here, select ☆ then ☆, and drag

CNAME

CNAME

MX

NS

NS

SOA

SRV

SRV

TXT

Host: **selector1._domainkey** (since we're in the *o365ninja.com* DNS zone, I don't specify that part)

Points to: *value in Selector1CNAME highlighted in Step 4.*

7. Click **Save**.

8. Repeat Steps 4 and 6 for **Selector2**.

9. You should now have resolvable CNAMEs for **selector1._domainkey.<domain>** and **selector2._domainkey.<domain>**.



C:\WINDOWS\system32\cmd.exe

```
C:\>nslookup -q=txt selector1._domainkey.o365ninja.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1
```

```
Non-authoritative answer:
selector1._domainkey.o365ninja.com      ca
selector1-o365ninja-com._domainkey.o365nir
```

```
                "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb
99nM250DwikB04veRT8+sdXsEnzeThORnEWYG5+07+
QAB;"
```

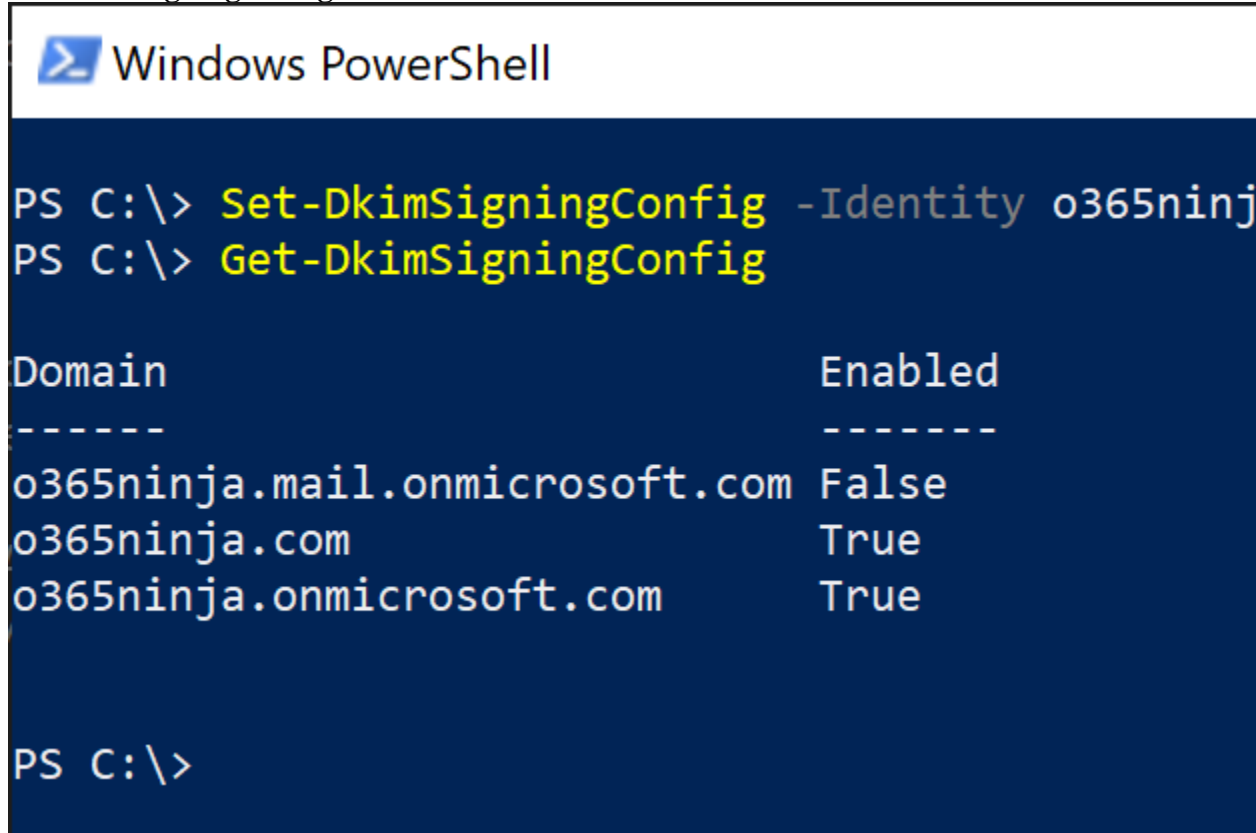
```
C:\>nslookup -q=txt selector2._domainkey.o365ninja.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1
```

```
Non-authoritative answer:
selector2._domainkey.o365ninja.com      ca
selector2-o365ninja-com._domainkey.o365nir
```

```
                "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb
M+587JqMugShB5Srfrrol5aSLw9Si+u0/do6HAsb6c
QAB;"
```

```
C:\>_
```

10. From PowerShell, enable DKIM signing for your custom domain:
Set-DkimSigningConfig -DomainName <domain> -Enabled \$true



```
Windows PowerShell

PS C:\> Set-DkimSigningConfig -Identity o365ninj
PS C:\> Get-DkimSigningConfig

Domain                                Enabled
-----                                -
o365ninja.mail.onmicrosoft.com      False
o365ninja.com                       True
o365ninja.onmicrosoft.com           True

PS C:\>
```

That's it! DKIM is now configured for your custom domain! Woot!

For more information on DKIM with Office 365, see [Use DKIM to validate outbound email sent from your custom domain in Office 365](#).

For more information on how DKIM works, see [DomainKeys Identified Mail \(DKIM\) Signatures](#) and [RFC 6376](#).

Domain-Based Messaging and Reporting Conformance (DMARC)

The purpose of Domain-based Messaging and Reporting Conformance, or DMARC, is to provide another layer of authentication. Like SPF and DKIM, DMARC is a configuration that protects *others* from senders *pretending to be you*. If we could get everyone in the world on-board with doing this, it would go a long way towards reducing or eliminating spoofed phishing mail.

DMARC is really an extension of the two previously discussed mechanisms, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). It allows the owner of a domain to configure a policy in their DNS records to specify which mechanism (DKIM, SPF or both) is

used when sending email from that domain; how to check the From: field (P2 header) presented to end users; how the receiver should deal with failures; and a way to deliver reporting on the actions taken by those policies.

DMARC Structure

The DMARC specification is outlined in [RFC 7489](#). Like SPF and DKIM, DMARC is configured in DNS through the use of a TXT record.

A general DMARC record for fabrikam.com might look something like this:

```
_dmarc.fabrikam.com 3600 IN TXT "v=DMARC1;p=reject;pct=100;
_rua=mailto:d@rua.dmarcdomain.com; ruf=mailto:d@ruf.dmarcdomain.com;
fo=1;sp=quarantine;adkim=r;aspf=s"
```

A DMARC DNS policy record can have several tags. Only three (version, aggregate reporting URI, and policy) are required. The rest (with the exception of the forensics options) have defaults set that will be automatically applied if you don't configure any further options.

Tag	Description	Example
v	Protocol version. (REQUIRED)	v=DMARC1
pct	Percentage of messages to be filtered. If unspecified, default is 100. This applies to messages that <i>fail</i> DMARC only, and is ignored if the p= tag is set to <i>none</i> (monitoring).	pct=50
ruf	Forensic Reporting URI.	ruf=mailto:forensic@domain.com
rua	Aggregate Reporting URI. (REQUIRED). This is where aggregate XML data is sent. Common URI endpoints are mailto: and https:	rua=mailto:aggregate@domain.com or rua=https:aggregate.domain.com/dmarc
p	Policy for domain. (REQUIRED). This applies to messages that <i>fail</i> DMARC. Valid options are <i>none</i> (monitoring mode, used to gather insight into current email flow), <i>quarantine</i> , or <i>reject</i> .	p=reject
sp	Policy for subdomains. By default, inherits settings configured in p= tag.	sp=quarantine
adkim	Alignment mode for DKIM. Valid options are <i>strict</i> and <i>relaxed</i> . In <i>relaxed</i> mode, authenticated DKIM signing domains (d= tag in DKIM policy) that share an organizational domain with the email's FROM domain will pass DMARC. In <i>strict</i> mode, an exact match is required. If unspecified, default setting is <i>relaxed</i> .	adkim=r

- aspf** Alignment mode for SPF. Valid options are `aspf=r` *strict* and *relaxed*. In *relaxed* mode, authenticated SPF domains that share an organizational domain with an email's 'FROM' domain will pass DMARC. In *strict* mode an exact match is required. If unspecified, default setting is *relaxed*.
- rf** Reporting format for forensic reports. Valid options are *afrf* or *iodef*. If none is specified, format is AFRF. `rf=afrf`
- ri** Reporting Interval. This is the number of seconds between aggregate reports. Default is 86,400 seconds. `ri=10600`
- fo** Failure reporting options. Valid options are 0 (generate reports if both DKIM and SPF fail), 1 (generate reports if either DKIM or SPF fails to produce a DMARC pass result), d (generate a report if DKIM fails), or s (generate a report if SPF fails). Default (if unspecified) is 0. `fo=1`

Resources

There are a number of free and paid-for services to help organizations configure, manage, and monitor DMARC. I'm going to list a couple here.

DMARCAalyzer

This service allows organizations to create a DMARC record, as well as configure and view reporting. With a free account, you can use their [DMARC record generator tool](#).

DMARC Reporting Service Offering through Valimail

[In June 2019, we announced a partnership with Valimail](#) to offer free DMARC reporting services for Office 365 customers. Here's a quick run-down of how to configure the service.

1. Go to Valimail's Microsoft landing page: <https://go.valimail.com/microsoft.html>.

2. Sign up.



Free Valimail Monitor fc



<https://go.valimail.com/micro>

To see favorites here, select ☆ then ☆, and drag to t

VALIMAIL

Free Valimail Mon for Office 365

3. After a few minutes, you should receive a few emails in your specified inbox. The first one has an “Accept invitation” link that you’ll need to click on. Click on that link.



Mail - admin@o365ninja.onmicro



https://outlook.office365.com/



Office 365

Outlook

Search Mail and People



New |



Delete



Folders



Favorites

Inbox

2

Sent Items

Drafts



Admin

Inbox

2

Drafts

Sent Items

Deleted Items

Archive

Conversation History

Junk Email

Focused

Other

Next: No events for the next two

Danny

Next Steps | Monitor for O365

Hello Aaron, We have created you



Valimail Support

Welcome to Valimail!

Welcome to Valimail! Hello Aaron

Yesterday

MOD Administrator

MOD Administrator shared "Docu

EXTERNAL Here's the document th

4. You'll be redirected to their website, where you'll be prompted to configure an account. Fill it out, accept the terms of service, and click **Start using Valimail**.



Mail - admin@o365ninja.onmicro



Valimail | V



https://app.valimail.com/users/

VALIMAIL | ENFORC

Welcome to

Password

.....

Password co






.....



I agree to
[Policy](#)



5. Once that has been configured, you can go back to your email and open the second message you received from Valimail. It has configuration details for your DMARC record.

 Reply all |   Delete Junk |  

Next Steps | Monitor for O365



Danny <office365@valimail.com>

Today, 4:03 PM

Admin 

Inbox

Hello Aaron,

We have created your Valimail Monitor for O365 account and it is designed to detect malicious actors abusing your domain for their own nefarious purposes.

Follow these steps to point your DMARC record to the Valimail Cloud Mailbox.

Update your `_dmarc` TXT record.

This allows Valimail to receive your DMARC aggregate reports.

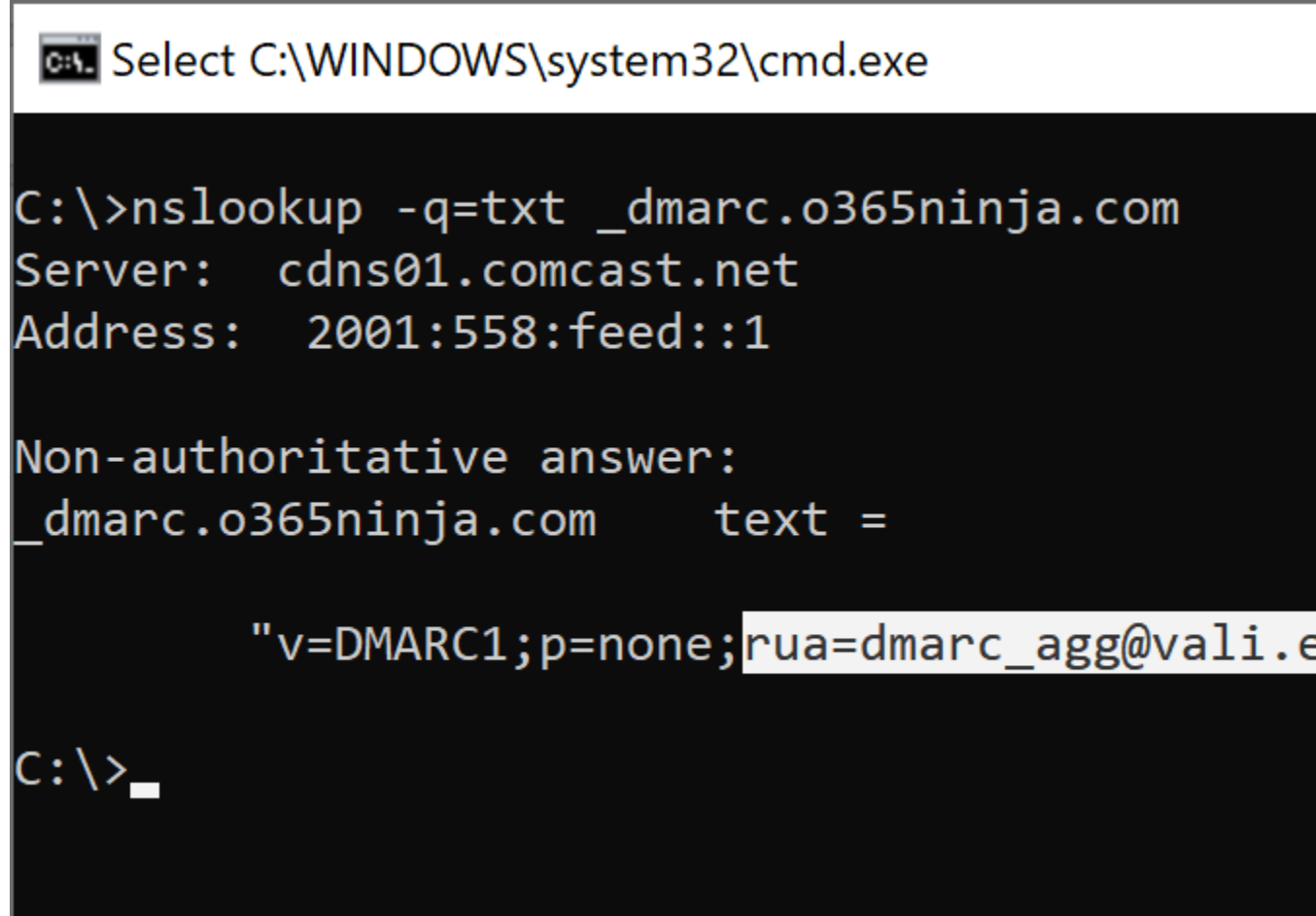
If you already have a `_dmarc` TXT record: add `dmarc_agg@vali.email` to your list of authorized senders.

```
"v=DMARC1; p=none; rua=mailto:dmarc\_agg@vali.email;"
```

The important settings that we're looking for is the value that they're going to give you for **rua=** (the aggregate URI). Take that value, and then add it to your DMARC record (or, if you don't already have one, create a DMARC record for your domain).

6. After you've added or modified your DMARC record, you should be able to look it up via **nslookup**. The syntax is:

nslookup -q=txt _dmarc.domain.com



```
C:\>nslookup -q=txt _dmarc.o365ninja.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
_dmarc.o365ninja.com      text =

                        "v=DMARC1;p=none;rua=dmarc_agg@vali.e

C:\>_
```

That's it! Have your users send mail as usual. You should then, after aggregate reports have started being sent, be able to review the reports in the Valimail console. Ta-da!

Recommendations

There are a number of ways to deploy DMARC, depending on your organization's goals. Once you think you have identified all of your hosts and implemented DKIM and SPF successfully, though, we recommend the following:

1. Sign up for a DMARC monitoring service, such as Valimail.
2. Implement DMARC in monitoring mode, using the **p=none** tag. The DMARC reports will go to the address you configured at the DMARC monitoring service, which will

enable you to get perspective on how much mail you have that is passing or failing DMARC.

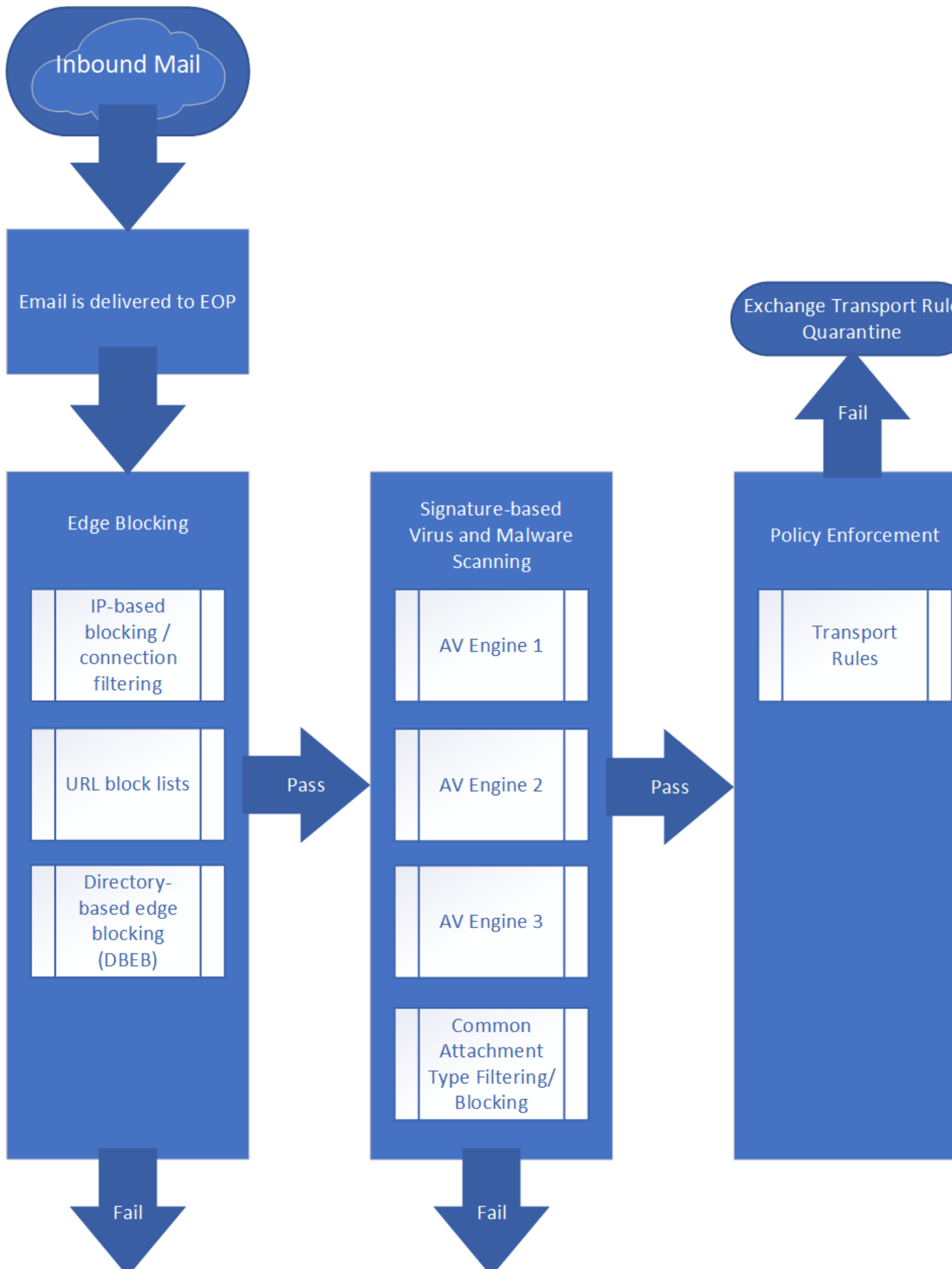
3. Configure your DMARC policy to apply to all mail. Yes, you'll get a ton of messages back, but that's what a monitoring service is for. The policy tag you want is **pct=100**.
4. Once you've been monitoring for a while and have resolved all of the issues that *legitimate* systems had delivering mail, it's time to move your record to the next step: quarantine. You do this by updating your DMARC record policy tag to **p=quarantine**. This will tell receiving systems to take mail that fails validation and put it in the equivalent of a 'spam' or 'junk mail' folder for the recipient. Customers and admins reviewing these messages may make effort to contact you and identify hosts that they either believe they are receiving legitimate mail from (that you may have missed) or to warn you that organizations are attempting to besmirch your good name. I am firmly against besmirching, so you can do what you will with this (such as contacting your legal team to see if they deem it necessary to take action against people fraudulently trying to send mail as you).
5. And, finally, once you have stamped out all of the besmirchers of your name (I was really hoping to get a post where I use *besmirch* at least four times, so thank for you your support), we recommend that you update your DMARC record policy tag to reject all mail that fails validation, using **p=reject**.

For more information on DMARC, head over to [Best practices for implementing DMARC in Office 365](#) and [Enhanced email protection with DKIM and DMARC in Office 365](#).

For more information regarding spoof intelligence, see [Learn more about spoof intelligence](#).

Mail Flow Operational View

In order to best understand where to apply settings and aid in configuring and troubleshooting, I think a view of the processing order for Exchange Online Protection is in order.



It's quite the eye chart. In essence, this is what happens:

1. EOP receives the mail.
2. Edge blocking scenarios take effect:
 1. IP-based blocking (connection filters)
 2. URL-based blocks
 3. Directory-Based Edge Blocking (DBEB)
3. After passing edge blocks, a message goes through malware detection.
 1. Three different signature-based antivirus solutions check the malware. The scanning engines used change periodically. No, we can't tell you what they are, so don't bother asking support. Not even if you have an NDA with us. Any malware automatically triggers the message to quarantine.
 2. If you apply any filters using Common Attachment Type Filtering, those are applied.
4. Next, Exchange Transport Rules are processed. You can do a lot of filtering and processing with transport rules, including filtering based on IPs and content/attachments. You'll notice that there are *two* areas prior to transport rules where IP blocking and attachment blocking can happen.
5. If you've subscribed to [Advanced Threat Protection](#), the Safe Attachments processing happens next. If you don't have an ATP subscription, you just skip step 7. If you have ATP, then go to step 6.
6. If you've subscribed to ATP, now we'll process ATP's spoofing and phishing policies.
7. You've landed at this step, with or without ATP. This is where the spam filtering happens, including SCL and BCL ratings. You'll notice that you can put Safe and Block lists in this step (as you also can with Transport Rules). Take note of where you might want to put them.
8. If a message has made it this far, it's delivered to the next hop (either an Exchange Online mailbox, Exchange on-premises mailbox, or mailbox hosted on a foreign system).
9. For mailboxes hosted in Exchange Online, we also have a process called [Zero-hour Auto Purge](#), which keeps track of messages as they come through the system. If for example, an attachment comes through and is scanned, and we later receive an antivirus signature that includes it, we can go back to the mailbox and process it in accordance with whatever the spam policy is for the user. ZAP is turned on by default.

Connectors

Connectors, in Exchange Online (or EOP, if you're only using the EOP standalone service) are configurations used to direct the flow of mail, typically between your on-premises and cloud environments, but also between other partner organizations.

Connector Scenarios

As soon as you provision your first mailbox in Exchange Online, you'll be able to send and receive mail. No connectors are necessary to begin using the service. If, however, you have more advanced scenarios, you may need to configure them for mail flow to work properly.

Exchange Online Protection Standalone

If you are not going to be using Exchange Hybrid (you are keeping your mail hosted elsewhere or you're not using an Exchange 2010 or later mail system), you'll need to configure connectors to route mail in and out of the service. As I mentioned previously, in order to make the best use of Exchange Online Protection, you'll want Directory-based Edge Blocking, which means you'll want a recipient object in your tenant for every recipient that EOP will be protecting.

For information on configuring standalone connectors, you'll need to review the article, [Set up connectors to route mail between Office 365 and your own email servers](#).

Exchange Hybrid

In this scenario, you've used the Exchange Hybrid Configuration Wizard to establish a relationship between your on-premises Exchange environment and Office 365. When you run the Hybrid Configuration Wizard, a minimum of 4 connectors are created:

- Exchange Online: Inbound
- Exchange Online: Outbound
- Exchange On-Premises: Send Connector (organization-wide)
- Exchange On-Premises: Receive Connector (one per server configured for transport in the Hybrid Configuration Wizard)

Depending on your the version of Exchange deployed on the transport servers, the on-premises receive connectors may be scoped and secured using IP addresses (Exchange 2010) or using a TLS certificate (Exchange 2013 and later). If you have a load-balancer or NAT device in front of your Exchange transport servers and you are using Exchange 2010 on as your transport, then you may need to add the inside virtual IP of the load-balancer appliance to ensure inbound mail from Office 365 reaches your server. *Note: This change, like any other changes you make outside the Hybrid Configuration Wizard, will be overwritten the next time the wizard is run. It is important to document any changes that need to be manually made to the connectors.*

Edge Transport Servers

It is also possible to configure Edge Transport servers with Exchange Online and Exchange Online Protection. While they are supported, I generally recommend customers not use them if at all possible. Just because you can put mustard on chocolate ice cream doesn't make it a good idea.

Exchange Transport Servers can be configured during an Exchange Hybrid configuration as well. Depending on your version of Exchange, you may need to configure them outside of the Hybrid Configuration Wizard.

As to my personal recommendation, from a security perspective, your Client Access Servers (CAS) are already exposed to the internet (usually via some sort of firewall or reverse proxy appliance). We haven't supported a "front-end/back-end" configuration of placing CAS in a

DMZ since 2003 (and even then, I wouldn't say it was well supported—just possible). Edge Transport requires additional certificate deployment, additional servers, and can't co-exist on the same server with other Exchange Server roles. As organizations are making migrations to the cloud, it seems counterintuitive to continue to deploy and support additional on-premises servers.

Partner Organizations

If you conduct a lot of business with a trusted partner, need to ensure certain security requirements, or need to apply special processing rules (such as transport rule-scoped connectors), you may need to deploy custom connectors in Exchange Online to meet these needs. Some of these needs might include ensuring inbound traffic comes from certain IP address ranges or that TLS security is enforced.

For more information on manually configuring connectors for Partner Organizations, see [Set up connectors to route mail between Office 365 and your own email servers](#).

Multifunction Devices and Other Relay Scenarios

A very common scenario that customers face is the need to relay mail through or send mail to Office 365 recipients from third-party or on-premises applications or multifunction devices (such as network scanners). Those can be accomplished in a variety of ways:

- Configure devices to relay through an Exchange Hybrid connector. This is the simplest option, as you'll be able to simply use an anonymous connector in your on-premises environment to route mail to Office 365. Let's say you have your multifunction devices configured on LAN segment 10.0.10.0/24, and your application servers are configured on 10.0.11.0/24, and you want to allow both of those networks to relay to your mailbox recipients in Office 365. In this example, you have an on-premises Exchange server (that has the Transport role configured) named **EXCHANGE2013**. From an Exchange Management Shell, you can run:

```
New-ReceiveConnector -Name "Anonymous Relay" -TransportRole
FrontendTransport -Custom -Bindings 0.0.0.0:25 -RemoteIpRanges
@('10.0.10.0/24','10.0.11.0/24')
Set-ReceiveConnector "Anonymous Relay" -PermissionGroups AnonymousUsers
Get-ReceiveConnector "Anonymous Relay" | Add-ADPermission -User "NT
AUTHORITY\ANONYMOUS LOGON" -ExtendedRights "Ms-Exch-SMTP-Accept-Any-
Recipient"
Set-ReceiveConnector "Anonymous Relay" -AuthMechanism
ExternalAuthoritative -PermissionGroups ExchangeServers
```

You can learn more about configuring an anonymous relay connector in Exchange here: [Allow anonymous relay on Exchange servers](#)

- SMTP Client Submission. This is probably the least popular option, as it requires configuring the sending applications and devices to be configured with a user name and password. Most of my customers avoid it at all costs. It does allow you to send to recipients both inside and outside of the organization. For more information on configure

SMTP client submission, see [Client Submission](#). It requires either port 25 or 587 be available from your client devices.

- **Direct Send.** This is not a popular option, as it only allows you to relay to mailboxes hosted in Office 365. To configure it, you need to update your sending applications and devices to send to your public MX endpoint in Office 365 on port 25, such as **fabrikam-com.mail.protection.outlook.com**. It is highly recommended that you add your network's external NAT to your SPF record to prevent your messages from being flagged as spam.
- **Connector to send mail using Office 365 relay.** This is the most complex to set up, but also most frequently used option (in my experience). If you've already got an Exchange Hybrid configuration in place, you don't need to do anything except enable an anonymous receive connector (if you don't already have one). If you don't have an Exchange Hybrid configuration deployed, you can either do that or follow the steps listed under [Configure a connector to send mail using Office 365 SMTP relay](#).
- **Configure an IIS Server to relay mail.** This is an alternate option to using an Exchange Hybrid configuration to relay mail, designed for customers that don't want Exchange on-premises anymore (though, if you have synchronized identity, the product group as of this writing still only supports using on-premises Exchange to manage the Exchange properties of a user). For more information on configuring IIS for this purpose (spoiler alert: you get to use the IIS 6.0 snap-in), see [How to configure IIS for relay with Office 365](#).

Recommendations

1. Use as few connectors as possible to keep the environment simple and easier to troubleshoot.
2. Use an Exchange hybrid configuration, if possible, if you will be relaying from on-premises systems to Exchange Online or other recipients. Since Exchange Hybrid comprises such a large portion of our install base, if you need to call support, you'll be able to find more resources that understand this configuration.
3. Use a standard method to route on-premises mail to external or Office 365 recipients. Frequently, this will mean configuring an anonymous relay connector in your Exchange hybrid environment so it can relay on your applications' behalf. For your own sake, don't configure some applications with identities, some multifunction devices to use direct send, and some applications to use an Exchange hybrid relay.
4. If you have configured Exchange Hybrid but need to make changes to the default hybrid connectors, be sure you back those changes up (**Get-SendConnector | Export-Clixml** or **Get-ReceiveConnector | Export-Clixml** for on-premises connectors; **Get-OutboundConnector | Export-Clixml** or **Get-InboundConnector | Export-Clixml** for cloud connectors), as making any changes outside of the Hybrid Configuration Wizard will be reverted to the stored configuration the next time the HCW is run. As mentioned previously, you *may* need to manually configure IP address ranges on the receive connectors to add the internal NAT if you have a reverse proxy appliance (such as an F5) in front of your Exchange transport servers). Be sure to back up the configurations before and after you make the changes, and reapply the 'after' IP address ranges if you re-run the Hybrid Configuration Wizard.

5. For the love of all that is holy (as well as my eleven favorite types of cheese and all people named Pete), avoid using Edge Transport servers in your configuration, especially if you are in an older Exchange Hybrid configuration. Edge Transport configurations require additional certificates, which invariably means more work and troubleshooting. They're an SMTP security blanket. If you are on a path to move mailboxes to Office 365, it doesn't make sense to deploy additional hardware and certificates.
6. If you are using custom connectors scoped to certain IP address ranges or domains, make sure they are unique and not overlapping, so as to avoid unintended mail flow consequences. Exchange chooses the *most restrictive or specific* matching connector.

For more information, see [Configure mail flow using connectors in Office 365](#).

Spam filtering

Spam filtering is enabled by default and, in most cases, will provide good coverage and protection for an organization. However as an admin, you can edit the default anti-spam policy so that it's tailored to best meet the needs of your organization. You can also create custom content filter policies and apply them to specified users, groups, or domains in as needed. This may be increasingly necessary if your business or organization is a frequent target of phishing attacks, has a large presence on the internet, or has a lot of publicly available information (such as a government or educational entity).

Custom policies always take precedence over the default policy, but you can change the priority (that is, the running order) of your custom policies.

Every Office 365 tenant has a basic spam filter policy deployed, which you can view in the Security & Compliance Center (<https://protection.office.com/antispam>).



https://protection.office.com/antispa



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management

[Home](#) > Mail filtering

Anti-spam se

Our standard settings co
settings and take advanta
[settings](#)

Standard

Standard

Standard

Spam action

Mark bulk e

Basic spam filter settings include selecting the action to take on messages identified as spam, either place the message into the junk folder or to quarantine the messages. When an email message goes through spam filtering it is evaluated and an individual Spam Confidence Level (SCL) rating is assigned to the message. The service takes actions upon the messages depending upon the spam confidence interpretation of the SCL rating. For more information, see [Spam confidence levels](#).

Anti-spam filter policies

There are several key elements of the Anti-spam filtering policy that can impact your origination. If you need to configure a new policy, you'll need to disable the Standard settings using the slider at the top of the Anti-spam settings page. Once you have disabled that, you have the ability to create a new custom policy.

Below is a list of the key elements and how they can impact filtering in your environment.



Mail filtering - Security & Compliance



https://protection.office.com/antispam



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision

New spam filter

*Name

Description

Spam and bulk actions

Allow lists

Spam and bulk email actions

Expanding **Spam and bulk actions** lets you configure the actions to take for spam, high confidence spam, phishing email, and bulk email. High confidence spam is content that has received an spam confidence level (SCL) rating of 7, 8, or 9. Spam messages have received an SCL rating of 5 or 6. The default delivery location for both spam and high-confidence spam is the user's Junk mail folder. If a message has an SCL rating of 0 or 1, it was evaluated, but judged as "not spam." And finally, an SCL of -1 is applied to mail that meets specific conditions, such as a safe sender or Exchange transport rule. Messages with an SCL of -1, 0, and 1 will be delivered directly to the recipient's Inbox.



Mail filtering - Security & Compliance



https://protection.office.com/antispo



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management

Home > Mail filtering

Anti-spam

Our standard settings and policies for protecting your organization from spam. [View settings](#)

Standard

Custom

+ Create

Spam and blocked senders

Select the actions you want to take on spam and blocked senders.

Spam

Move messages to the Junk folder

High confidence phishing

Move messages to the Junk folder

Phishing emails

Quarantine messages

Bulk email

Move messages to the Junk folder

The actions that you can set for each of these (**spam**, **high confidence spam**, **phishing**, and **bulk**) are:

- **Move message to Junk Email folder.** Sends the message to the Junk Email folder of the specified recipients. This is the default action for both confidence threshold levels.
- **Add X-header.** Sends the message to the specified recipients but adds X-header text to the message header that identifies it as spam. Using this text as an identifier, you can optionally create rules to filter or route the messages as needed. The default X-header text is **This message appears to be spam.**
- **Prepend subject line with text.** Sends the message to the intended recipients but prepends the subject line with the text that you specify in the **Prefix subject line with this text** input box. Using this text as an identifier, you can optionally create rules to filter or route the messages as needed.
- **Redirect message to email address.** Sends the message to a designated email address instead of to the intended recipients. Specify the “redirect” address in the **Redirect to this email address** input box.
- **Delete message.** Deletes the entire message, including all attachments.
- **Quarantine message.** Sends the message to quarantine instead of to the intended recipients. If you select this option, in the **Retain spam for (days)** input box, specify the number of days during which the spam message will be quarantined. (It will automatically be deleted after the time elapses. The default value, 15 days, is the maximum value. The minimum value is 1 day.)

For more information about using the Exchange Admin Center to manage messages that land in the quarantine, see [Quarantine](#) and [Find and release quarantined messages as an administrator](#). Exchange Online Protection also allows end-users to view and release their own spam quarantine. For information about configuring end-user spam notification messages to be sent to end users, see [Configure end-user spam notifications in EOP](#) or [Configure end-user spam notifications in Exchange Online](#).

Bulk email

Bulk mailers vary in their sending patterns, content creation, and list acquisition practices. Some are good bulk mailers that send wanted messages with relevant content to their subscribers (like when you sign up for a specials or deals from a retailer). These messages generate few complaints from recipients.

Other bulk mailers send unsolicited messages that closely resemble spam and generate many complaints from recipients. These lists are frequently gained by through purchasing email lists from unscrupulous suppliers or scraping web sites and chat boards. Office 365 scores each bulk message as either 1 (most likely a good sender) to 9 (spawn of hades who is still trying to reach you about your car's extended warranty).

When managing your spam filter policies, you can select a threshold to treat bulk email as spam. This threshold is based on the bulk complaint level (BCL) of the message. Like a message's SCL, a BCL is also calculated and stamped on the message, where 0 is “not a bulk sender,” 1-3

is “a bulk sender that doesn’t generate many complaints,” 4-6 is “a bulk sender that generates a mixed number of complaints,” and 7-9 is “someone contacting you about your recent magazine subscription.”

You can choose a threshold setting from 1-9 (where a threshold of 1 will treat most bulk email like spam and a threshold of 9 will allow the most to be delivered). The default setting of 7 allows most good bulk messages to be delivered. I’ve found, though, that for most organizations (especially educational institutions or public sector entities that have a lot of public contact information), that lowering the setting to 5 or 6 provides a better end-user experience. The service then performs the configured action, such as sending the message to the recipient’s Junk Email folder.



Mail filtering - Security & Compliance



https://protection.office.com/antispo



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management

Home > Mail filtering

Anti-spam

Our standard settings and recommendations for protecting your organization from spam. [View settings](#)

Standard

Custom

+ Create

Spam and blocked messages

Select the actions you want to take with spam and blocked messages.

Spam

Move messages to the Junk folder

High confidence phishing

Move messages to the Quarantine folder

Phishing emails

Quarantine messages

Bulk email

Move messages to the Junk folder

For more information, see [Bulk Complaint Level values](#) and [What's the difference between junk email and bulk email?](#)

Allow lists

In the **Allow Lists** section, you can specify entries, such as senders or domains, that will always be delivered to the inbox and most filtering is skipped for the messages (malware filtering is always performed).



Mail filtering - Security & Compliance



https://protection.office.com/antispo



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management

Home > Mail filtering

New spam filter

Anti-spam

Our standard settings and settings for your organization.

Standard

Custom

*Name

Description

Spam and blocked

Allow lists



Allow sending

- **Add trusted senders to the Sender allow list.** Click **Edit** next to Allow Sender. In the selection dialog box, add the sender addresses you wish to allow, and then click +. You can separate multiple entries using a semi-colon or a new line. Click

Save to return to the **Allow Lists** page.



Mail filtering - Security & Compli



https://protection.office.com



Office 365 Security & Compliance



Home > M



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision

Anti-s

Our standar
settings and
settings

Sta

Cus

+cr

- **Add trusted domains to the Domain allow list.** Click **Edit** next to Allow Domain. In the selection dialog box, add the domains you wish to allow, and then click +. You can separate multiple entries using a semi-colon or a new line. Click **Save** to return to the **Allow Lists** page.

***Warning:** If you allow top-level domains, it's likely that email you don't want will be delivered to an inbox.*

Block lists

The **Block Lists** settings work exactly like the Allow settings, only in the opposite direction. You can specify entries, such as senders or domains, that will always be marked as spam. The service will apply the configured high confidence spam action on email that matches these entries.

- **Add unwanted senders to the Sender block list.** Click **Edit** next to Block Sender. In the selection dialog box, add the sender addresses you want to block, and then click +. You can separate multiple entries using a semi-colon or a new line. Click **Save** to return to the **Block Lists** page.
- **Add unwanted domains to the Domain block list.** Click **Edit** next to Block Domain. In the selection dialog box, add the domains you want to block, and then click +. You can separate multiple entries using a semi-colon or a new line. Click **Save** to return to the **Block Lists** page.

International spam

On the **International Spam** settings, you can filter out email messages written in specific languages, or sent from specific countries or regions. Office 365 uses information in the message to determine the language and it is recommended to use this to block messages as desired. You can configure up to 86 different languages and 250 different regions. The service will apply the

configured action for high-confidence spam.



Mail filtering - Security & Compliance



https://protection.office.com/antispo



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Home > Mail

New sp

Anti-s

Our standard
settings and
[settings](#)

Sta

*Name

Description

Cus

Spam and b

+Cre

Allow lists

Block lists

- Click **Edit** in the **Filter email messages written in the following languages** area to expand the configuration page. Select the **Filter email messages written in the following languages** checkbox, and then in the selection box, start entering values for a language. Click on a language to add it to the list of languages to filter. For example, if you select to filter messages written in Russian (RU), and **Quarantine message** is your configured action for high confidence spam messages, then any messages written in Russian will be quarantined. Click **Save** to return to the **International Spam** pane (again, ensure that the **Filter email messages written in the following languages** checkbox has been selected on the

page listing the languages you've selected).



Mail filtering - Security & Compliance



https://protection.office.com



Office 365 Security & Compliance



Home > Mail



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Anti-spoofing

Our standard settings and settings

Standard

Custom

+ Create

- Click **Edit** in the **Filter email messages sent from the following countries or regions** area to open the configuration page. Start entering the name of a country or region, and when it is displayed, click it add it to the list. For example, if you select to filter all messages sent from Australia (AU), and **Quarantine message** is your configured action for high confidence spam messages, then any messages sent from Australia will be quarantined. Click **Save** to return to the **International Spam** pane. Just like the languages session, ensure you have the **Filter email messages sent from the following countries or**

regions checkbox selected before you click **Save**.



Mail filtering - Security & Compliance



https://protection.office.com



Office 365 Security & Compliance



Home > Mail



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Anti-spoofing

Our standard settings and settings

State

Custom

+ Create

Note: By default, if no international spam options are selected, the service performs normal spam filtering on messages sent in all languages and from all regions. Messages are analyzed and the configured actions are applied if the message is determined to be spam or high confidence spam.

Spam properties

Under **Spam properties**, you are able to configure the following options (in the Exchange Online Admin Center, they are referred to as Advanced Spam Filtering Options). All of these

settings are disabled by default.



Mail filtering - Security & Compliance



https://protection.office.com/antispo



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Home > Mail filtering

Anti-spam

Our standard settings and custom settings

Standard

Custom

+ Create

Spam properties



Increase spam score
Specify threshold

Image links

☒ Off

URL redaction

☒ Off



Mark as phishing
Specify threshold

Empty reply

☒ Off

JavaScript

☒ Off

Frame o

☒ Off

- **Increase spam score.** These options allow you to specify whether to increase the spam score for messages that include various types of links or URLs. For example, you can choose to increase the spam score if an email has links with IP addresses (such as `Click Here` instead of `Click Here`). If you choose the option to apply a sensitive word list, please note that you cannot view or edit the list. If you want to apply custom content filtering options for your own list of prohibited or sensitive words, you can use an Exchange Transport Rule with a 'matches' condition.
- **Mark as spam.** These options allow you specify whether to mark messages that include various properties as spam. This is also where you can enable or disable the **SPF record: hard fail**, **Conditional Sender ID filtering: hard fail**, and **NDR backscatter** settings. If your mailboxes are hosted in Exchange Online, you most likely won't need to configure the NDR backscatter options (it's really targeted to on-premises mailboxes).

***Important:** I'd recommend you DO NOT ENABLE **SPF record: hard fail** except in extraordinary circumstances, such as under the advice of Premier. It will most likely result in a large number of false positives.*

- **Test mode options.** Let's you configure the test mode options for when a match is made to test the enabled advanced option. Options include the following:
 - **None.** Take no test mode action on the message. This is the default.
 - **Add default X-header text.** Checking this option sends the message to the specified recipients but adds a special X-header to the message that identifies it as having matched a specific advanced spam filtering option. Using the test mode option with an X-header will allow you to search message logs for the specific X-header to gauge a rule's effectiveness.
 - **Send Bcc message.** Checking this option sends a blind carbon copy of the message to the email address you specify in the input box.

For more detailed information, see [Advanced Spam Filtering Options](#).

Applied to

For custom policies only, expand **Applied to** and then click **+Add a condition** create a condition-based rule. You can specify the users, groups, and/or domains for whom to apply this policy. You can create multiple conditions provided that they are unique. Each type (user,

group, domain) can be used only once.



Mail filtering - Security & Compliance



https://protection.office.com/antispo



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Home > Mail filtering

Anti-spam

Our standard settings and configuration for mail filtering. For more information, see [mail filtering settings](#).

Standard

Custom

+ Create

*Name

Description

Spam and blocked

Allow lists

Block lists

International

From this dialog box, you have the ability to select **Recipient domain is** to scope to a domain, **Recipient is** to scope the policy to one or more users, and **Recipient is a member of** to scope the

policy to the members of a group.



Mail filtering - Security & Compliance



https://protection.office.com/antisp



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Home > Mail

Anti-spam

Our standard settings and custom settings

Standard

Custom

+ Create

Description

Spam and block lists

Allow lists

Block lists

Internationalization

Spam properties

After conditions have been added, click **Save** to save the policy.

Recommendations

1. Start off with the default filtering policies and see how they perform. If you have migrated from another filtering solution and are seeing an influx of spam, newsletters, or bulk mail, instruct users to follow the *unsubscribe* links. Many spam filtering services automatically categorize all bulk mail and spam together, when in fact they may come from different types of sources or have been legitimately subscribed to.
2. Leave ZAP turned on.
3. Adjust the Bulk Mail threshold to 6 (from the default threshold of 7) if you find that you are getting more spam than anticipated. You can further ratchet the setting down, but give it a few days in between adjusting the settings and monitor the quarantine.
4. My personal recommendations include configuring the Advanced Spam Filter options to increase the spam score for links with numeric IP addresses and mark empty messages as spam. If you are performing synthetic tests of the mail system, just make sure you put content in the message so the tests don't get dropped.
5. If your organization does not conduct business with international clients or customers, consider implementing
6. When testing out new policies, use the **Applied to** controls to configure a pilot group of users.

Connection Filter Policy

Connection filtering allows you to bypass filtering of messages or block messages from a set of IP addresses or ranges. Using these policies should be used with care as allowing an IP address to send information without filtering could allow spoofing of a domain.

You create an IP Allow list or IP Block list by editing the connection filter policy in the Security & Compliance Center (SCC). The connection filter policy settings are applied to inbound messages only. Refer to the [Mail flow operational view](#) to see where Connection Filters are applied.

1. In the Security & Compliance Center (<https://protection.office.com>), click **Threat management** | **Policy**, then click **Anti-spam**.
2. Click the **Custom** tab on the **Anti-spam settings** page.

3. Expand **Connection filter policy (always ON)**, then click **Edit policy**.



Mail filtering - Security & Compliance



https://protection.office.com/ar



Office 365 Security & Compliance



[Home](#) > Mail filtering



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Anti-spam settings

Our standard settings cover most scenarios. You can customize settings and take advantage of advanced features. [Learn more about anti-spam settings](#)

Standard

Custom settings

[+ Create a policy](#)

Name

4. Create your Allow and/or Block lists by clicking **Edit** as appropriate, and then entering the IP address or CIDR range and clicking +.



Mail filtering - Security & Compliance



https://protection.office.com/ar



Office 365 Security & Compliance



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision

Home > Mail

IP A

Anti-s

Our standard
settings and
settings

Sta

Address

Example

18.4.2

Cus

Allowed

63.42

+Cr

5. Click **Save** when finished.

Important: Adding entries here may be risky and result in other protection schemes being skipped. It is recommended that you review all entries closely. For more information, see [Configure the connection filter policy](#).

Other things to keep in mind:

- If you add an address to both a Connection Filter *Allowed* list and a *Blocked* list, the **ALLOW ENTRY TAKES PRECEDENCE**.
- If you need to create a connection filter for an IP address range larger than /23, you'll need to do it via a Transport Rule. You can do it all in a connection filter, but you'll have to add multiple /24 entries.
- A Connection Filter can have 1,273 entries. Yes, that's a really random number.

Recommendations

1. Limit your use of Connection Filter policies to trusted partners.
2. If you use Connection Filter policies to block connections from certain spammers, be sure to schedule a periodic review of the blocked IPs to make sure they still belong to the entities you're trying to block. You can use the script I provide at [Find Whitelisted Users, Domains, and IPs in Office 365](#) to evaluate your blocked and allowed entries.

Outbound Spam Filter Policy

Outbound filtering checks to make sure your users aren't sending spam. For instance, a user's computer may get infected with malware that causes it to send spam messages, so we build protection against that into the service.

Outbound spam filtering is always enabled. If a customer continues to send spam through the service, they will be blocked from sending messages.

Although outbound spam filtering cannot be disabled or changed, you can use the Security & Compliance Center to configure several company-wide outbound spam settings via the default Outbound spam filter policy.

1. In the Security & Compliance Center, click **Threat management | Policy**, then click **Anti-spam**.
2. Click the **Custom** tab on the **Anti-spam settings** page.

3. Expand **Outbound spam filter policy (always ON)**, then click **Edit policy**.



Mail filtering - Security & Compliance



https://protection.office.com/ar



Office 365 Security & Compliance



[Home](#) > Mail filtering



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Anti-spam settings

Our standard settings cover most scenarios. You can customize settings and take advantage of advanced features. [Learn more about anti-spam settings](#)

Standard

Custom settings

[+ Create a policy](#)

Name

4. On the **Outbound spam filter policy** page, you can select from the following check boxes pertaining to outbound messages, and then specify an associated email address or addresses in the accompanying input box (these can be distribution lists if they resolve as valid SMTP destinations):

- **Send a copy of suspicious outbound email messages to specific people.** These are messages that are marked as spam by the filter (regardless of the SCL rating). They are not rejected by the filter but are routed through the higher risk delivery pool. Note that the recipients specified will receive the messages as a Blind carbon copy (Bcc) address (the From and To fields are the original sender and recipient).
- **Notify specific people if a sender is blocked due to sending outbound spam.** When Office 365 detects a significant amount of spam is originating from a particular user, the user is disabled from sending email messages. The address specified in this setting will be informed that outbound messages are blocked for this user. You can see an example of the notification at [Sample notification](#)

when a sender is blocked sending outbound spam.



Mail filtering - Security & Compliance



https://protection.office.com



Office 365 Security & Compliance



Home > Mail



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Anti-s

Our standard
settings and
[settings](#)

Sta

Cus

+Cre

5. Click **Save**.

Recommendations

1. Configure an entry under **Notify specific people if a sender is blocked due to sending outbound spam** for helpdesk ticketing system-monitored address. That way, it can be routed to service personnel immediately, thereby reducing the potential spread of a compromise situation and helping the affected user's issue get resolved.

Exchange Transport Rules

Exchange Transport Rules (can you guess the acronym?) are a set of steps you can have the system perform based on conditions or logic, such as text or content properties or values in message headers. Exchange Transport Rules are separated into four parts: conditions, exceptions, actions, and properties. **Conditions** are the message properties (sender, IP address, SCL ratings, message header or body content, etc.) that are used to identify which messages to process. **Exceptions** are the message properties that are used to exclude a selected message from a rule (the same components used in Conditions can be used in Exceptions). **Actions** are what the system will do to a message. **Properties** are the leftover things that are not conditions, exceptions, or actions that are related to a transport rule, such as comments, enforcement options, and validity times.

The overall configuration capabilities of ETRs are pretty broad, so we're just going to focus on some common conditions and actions that might be useful from a message hygiene perspective.

One of the most common hygiene scenarios for creating a transport rule is to mark a message as "not spam" by setting the Spam Confidence Level (SCL) rating to -1. If the sending domain has DMARC configured, it's *probably* best to manage via an Exchange Transport Rule (as opposed to the spam filter policy's Allowed domains list), since allowing it with a spam filter rule bypasses spam (duh) as well as phish and spoof rules. Managing it via transport rules gives you much better control and granularity.

For example, if **bobsreallycooltools.com** is a trusted partner, you may have the IP addresses for their main email system allowed in a connection filter. While you do a lot of work with **bobsreallycooltools.com**, maybe you don't want your users receiving promotional or marketing materials from them. Let's say they decided to outsource their promotional and marketing communications to **bigbulkmailsender.com**, and that system uses 5.5.5.5 as their SMTP relay. One of your other partners, **janesrubberducks.com**, also uses **bigbulkmailsender.com** (5.5.5.5) as their SMTP relay for marketing email, and you want to continue receiving their promotional materials. Both of your partner's domains have successfully implemented SPF, DKIM, and DMARC.

In this case, we want to trust bobsreallycooltools.com unless the mail is coming from 5.5.5.5. However, we don't want to block 5.5.5.5 altogether, since we're getting legitimate mail that we want from that IP address on behalf of janesrubberducks.com. We also want to limit our

exposure by ensuring only mail that passes authentication tests is able to bypass the spam filter. So, let's see what we can do.

1. Launch the Exchange Online Control Panel (<https://outlook.office365.com/ecp>) and navigate to **Mail flow**.

2. Click **Rules**, click +, and then select **Bypass spam filtering**.



Policy - Security & Compliance



rules - Microsoft Exchange



https://outlook.office365.com/ExchangeAdminCenter

Admin

Exchange admin center

dashboard

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

rules

message trace



Create a new rule...

Apply Office 365 Message Encryption

Apply custom branding to Outlook

Apply disclaimers...

Bypass spam filtering...

Filter messages by size...

Generate an incident report...

Modify messages...

Restrict managers and their contacts

Restrict messages by sender...

Send messages to a moderation

3. Configure the requirements for the sender's domain to match bobsreallycooltools.com and the Authentication-Results header to match 'dmarc=pass' or 'spf=pass' or 'dmarc=bestguesspass', and configure an exception for the IP address range 5.5.5.5.



new rule

Name:

Bypass spam for bobsreallycooltools.com except from 5.5.5.5

*Apply this rule if...

✕ The sender's domain is...

and

✕ A message header matches...

add condition

*Do the following...

Set the spam confidence level (SCL) to...

add action

Except if...

✕ Sender's IP address is in the range...

add exception

Properties of this rule:

If you really want to up your nerd street cred, you can also do this in PowerShell:

```
New-TransportRule -HeaderMatchesMessageHeader 'Authentication-Results'  
-HeaderMatchesPatterns @('dmarc=pass','spf=pass','dmarc=bestguesspass')  
-SenderDomainIs @('bobsreallycooltools.com')  
-SetSCL "-1" -ExceptIfSenderIpRanges @('5.5.5.5') -Name 'Bypass for  
bobsreallycooltools.com  
except from 5.5.5.5' -StopRuleProcessing:$false -Mode 'Enforce' -  
RuleErrorAction  
'Ignore' -SenderAddressLocation 'HeaderOrEnvelope'
```

4. Click **Save**.

Recommendations

1. Use the [Mail Flow Operational View](#) above to figure out if a Transport Rule is the best place to configure EOP settings.
2. If you are going to use an ETR to configure a bypass spam filtering SCL (-1), you should avoid including large consumer domains, such as outlook.com, hotmail.com, yahoo.com, or gmail.com, since that will increase the risk of spam and phishing attempts that get through to your user mailboxes.
3. Scope your rules appropriately. By default, ETRs are configured to apply to all messages (inbound and outbound), so ensure that you've thought that out. You can apply to all inbound or outbound messages, or all inbound or outbound messages destined to or from certain domains or senders.
4. Mail flow rules are processed sequentially. If you have a message that meets multiple criteria, you may end up taking additional steps unnecessarily. There is a configuration option in a rule to Stop additional processing. For example, rules whose actions are **Block** should probably have **Stop additional processing** enabled, since there's not much else to do except waste CPU cycles.
5. Some actions may take more than one rule to work. For example, if you want to block a message but also forward it to someone's manager, you can't do them both in the same rule. You should configure the message to forward the rule first, and then create another rule immediately following it (with the exact same selection criteria), and configure the additional action.
6. When configuring "Allow" lists, our recommendations are this order:
 - Exchange Transport Rules
 - Outlook Safe Senders list
 - Anti-spam policy: IP Allow Lists
 - Anti-spam policy: Sender/Domain Allow Lists

Malware Filtering

Exchange Online Protection offers multi-layered malware solution that's designed to catch all known malware inbound to or outbound from your organization (known malware being

signature-based things that our rotating malware engines have signature or detection patterns for). Malware filtering is automatically enabled in every tenant via the default anti-malware policy and cannot be deleted or disabled.

You can view and edit some properties of the default anti-malware policy, but you can't delete it. For greater granularity, you can also create custom content filter policies and apply them to specified users, groups, or domains in your organization. Custom policies always take precedence over the default policy, but you can change the priority (that is, the running order) of your custom policies. The default anti-malware policy does not allow you to change the scope of the users.

If malware is detected in an email attachment, the entire message will be quarantined and can only be released by an administrator. By default, no notifications are generated when this happens, though you do have the ability to modify that.

In order to apply more targeted policy settings, you'll need to create custom policies.

Anti-malware filter policies

You need to be assigned permissions before you can perform this procedure. In this case, you must be a member of the Organization Management or Hygiene Management role groups.

1. In the [Security & Compliance Center](#), click **Threat management | Policy | Anti-malware**.



Policy - Security & Compliance



malware f



https://protection.office.com/th



Office 365 Security & Compliance



Home > Policy



Home



Alerts



Permissions



Classifications



Data loss prevention



Records management



Data governance



Supervision



Threat management



Anti-phishing



Protect
phishing
spoofin
tips to v
potenti
messag

Anti-malware



Protect
email fr
includin
take an
malwar

2. On the **Anti-malware** page, do one of the following:
 1. Double-click the default policy in order to edit the company-wide policy.
 2. Click the **+New** icon to create a new policy that can be applied to users, groups, and domains in your organization. You can also edit existing custom policies by double-clicking them.
3. For custom policies only, specify a name for this policy. You can optionally specify a more detailed description as well. You cannot rename the default policy.
4. Click the **Settings** menu option. If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin. In the **Malware Detection Response** section, use the option buttons to configure recipient notifications:



new anti-malware policy

*Name:

Custom Policy

Description:

Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be re

Do you want to notify recipients if their messages are quarantined?

- ☐ No
- ☐ Yes and use the default notification text
- ☒ Yes and use custom notification text

*Custom notification text:

You have quarantined messages. Please log into the end user quarantine or ask your adminis

If you select **Yes** or **Yes and use custom notification text**, the intended recipient will receive email stating that they have quarantined messages. You can customize the notification text if desired. If you select **No**, the message is delivered to the quarantine

silently.

*Note: With Exchange Online Protection, the UI indicates that this messages configured for the malware response will be quarantined. This is different than Exchange Server with the malware filter, and different than the options available in PowerShell. The note at <https://docs.microsoft.com/en-us/office365/securitycompliance/configure-anti-malware-policies> indicates that for **any** option you choose, the result is that the message will be held in the quarantine.*

5. In the **Common attachment types filter** section, choose which file types you want to have the **Malware Detection Response** option selected above applied on. New policies have the most commonly used malicious file types selected to be detected as malware by default. You can only choose from the predefined list in the user interface. If you want to add additional file types to be selectable in the Common attachment types filter area,

you'll need to add them via PowerShell.



new anti-malware policy

*Name:

Custom Policy

Description:

Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be re

Do you want to notify recipients if their messages are quarantined?

- ☐ No
- ☐ Yes and use the default notification text
- ☒ Yes and use custom notification text

*Custom notification text:

You have quarantined messages. Please log into the end user quarantine or ask your adminis

Common Attachment Types Filter

Turn on this feature to block attachment types that may harm your computer.

- ☐ Off
- ☒ On - Emails with attachments of filtered file types will trigger the Malware Detection Resp



6. In the **Notifications** section, you have the option to send a notification email message to senders or administrators when a message is detected as malware and is not delivered. These notifications are only sent when the entire message is deleted.

1. In the **Sender Notifications** section, select the check boxes to **Notify internal senders** (those within your organization) or to **Notify external senders** (those outside your organization) when a detected message is not delivered.
2. Similarly, in the **Administrator Notifications** section, select the check boxes to **Notify administrator about undelivered messages from internal senders** or to **Notify administrator about undelivered messages from external senders**. Specify the email address or addresses of the administrator in their respective **Administrator email address** fields after selecting one or both of these check boxes.

Note: The default notification text is “This message was created automatically by mail delivery software. Your email message was not delivered to the intended recipients because malware was detected.” The language in which the default notification text is sent is dependent on the locale of the message being processed.

3. In the **Customize Notifications** section, you can create customized notification text to be used in place of the default notification text for sender and administrator notifications. Select the **Use customized notification text** check box, and then specify values in the following required fields:

From name. The name you want to be used as the sender of the customized notification.

From address. The email address you want to be used as the sender of the customized notification.

Messages from internal senders. The **Subject** and **Message** of the notification if the detected message originated from an internal sender.

Messages from external senders. The **Subject** and **Message** of the notification if the detected message originated from an external sender.



new anti-malware policy

Notifications

Sender Notifications

Sends a message to the sender of the undelivered message.

☒ Notify internal senders

☒ Notify external senders

Administrator Notifications

Sends a message to the administrator of the undelivered message.

☐ Notify administrator about undelivered messages from internal senders

Administrator email address:

☐ Notify administrator about undelivered messages from external senders

Administrator email address:

Customize Notifications

Create customized notification text to be used in place of the default notification text f

☒ Use customized notification text

*From name:

Malware Response

*From address:

malwareresponse@o365ninja.com

Messages from internal senders

*Subject:

*Message:

*Note: You have to select **Notify internal senders** or **Notify external senders** under the **Notifications** sections in order to be able to customize the respective notifications.*

7. For custom policies only, if you want to scope or target the policy, under **Applied to**, click the drop-down and then create a condition-based rule to specify the users, groups, and/or domains for whom to apply this policy. You can add and set multiple conditions, but can only use each condition type once.
 - To select users, select **The recipient is**. In the subsequent dialog box, select one or more senders from your company from the user picker list and then click **Add**. To add senders who aren't on the list, type an address in the text box next to **Check names** and then click **Check names**. Note: In this box, you can also use wildcards for multiple email addresses (for example: *@domainname). When you are done with your selections, click **OK** to return to the main screen.
 - To select groups, select **The recipient is a member of** and then, in the subsequent dialog box, select or specify the groups. Click **OK** to return to the main screen.
 - To select domains, select **The recipient domain is** and then, in the subsequent dialog box, select the domains. You can only choose domains that are added to your tenant. Click **OK** to return to the main screen.
8. Click **Save**. A summary of your default policy settings appears in the right pane.

Notes

If you need to add additional file extensions or types to be selectable in the Common attachment filter dialog, you'll need to do so through PowerShell.

1. Connect to Exchange Online or Exchange Online Protection via PowerShell.
2. Create a PowerShell array containing the file types to add to the filter. For example, I want to add ZIP and ZI_ to the attachment filter available in the Default policy.

```
[array]$FileTypesAdd = Get-MalwareFilterPolicy -Identity Default |  
Select-Object -Expand FileTypes  
$FileTypesAdd += "zip","zi_"  
Set-MalwareFilterPolicy -Identity Default -EnableFileFilter $true -  
FileTypes $FileTypesAdd
```

Recommendations

1. Only configure company-wide settings in the default anti-malware policy, since it cannot be scoped and will automatically apply to all users.
2. Create custom anti-malware policies to apply certain settings to targeted groups of users.
3. Turn on notifications for recipients so that they know a message was blocked due to malware. This helps alleviate the “I’m expecting mail from” and “why haven’t I received it” questions.
4. If you are configuring an attachment blocking policy, use the [Mail Flow Operational Overview](#) above to determine if the Common Attachment Type Filter blocking is

appropriate as opposed to configuring attachment blocking parameters via Transport Rules. For example, you may want to configure your environment to quarantine messages that have attachments when the message doesn't pass DMARC. That would require a Transport Rule. However, if you just wanted to block .zip files across the board, you could use the Common Attachment Type Filter block to achieve that.

Additional Recommendations

There are a number of additional configurations that don't necessarily fall under configuring policies, but things that are good general practices.

The Last Word on Allow Lists

I mentioned this previously, but any good record deserves another spin.

We provide you *four* mechanisms by which to allow mail to be whitelisted and pass into your environment (listed in order of most preferable to least preferable):

- Exchange Transport Rules
- Outlook Safe Senders
- Anti-spam policy: IP Allow Lists
- Anti-spam policy: Sender/Domain Allow Lists

Using the [mail flow diagram](#) above, you can see that if you add a sender to the anti-spam lists, you are effectively bypassing all of the protections we can offer you.

The most flexible and secure way to ensure you allow legitimate senders is by using a transport rule that checks the authentication headers of a message (looking for the Authentication-Results header to match 'dmarc=pass' or 'spf=pass' or 'dmarc=bestguesspass'), and then setting the SCL to -1 based on that. "SCL -1," as you'll recall, tells EOP to skip spam filtering, since it's now marked as "safe/bypass."

Exchange Transport rules allow the most flexibility (such as allowing sender domain or IP configuration in conjunction with authentication header results), followed by the end-user's Safe Sender's list. If you configure settings in the anti-spam policy, you will be bypassing spam checks solely based on domains or IP addresses and not on additional spam characteristics. Configuring allow rules in the anti-spam policy will bypass many of the safeguards and filtering capabilities of Exchange Online Protection.

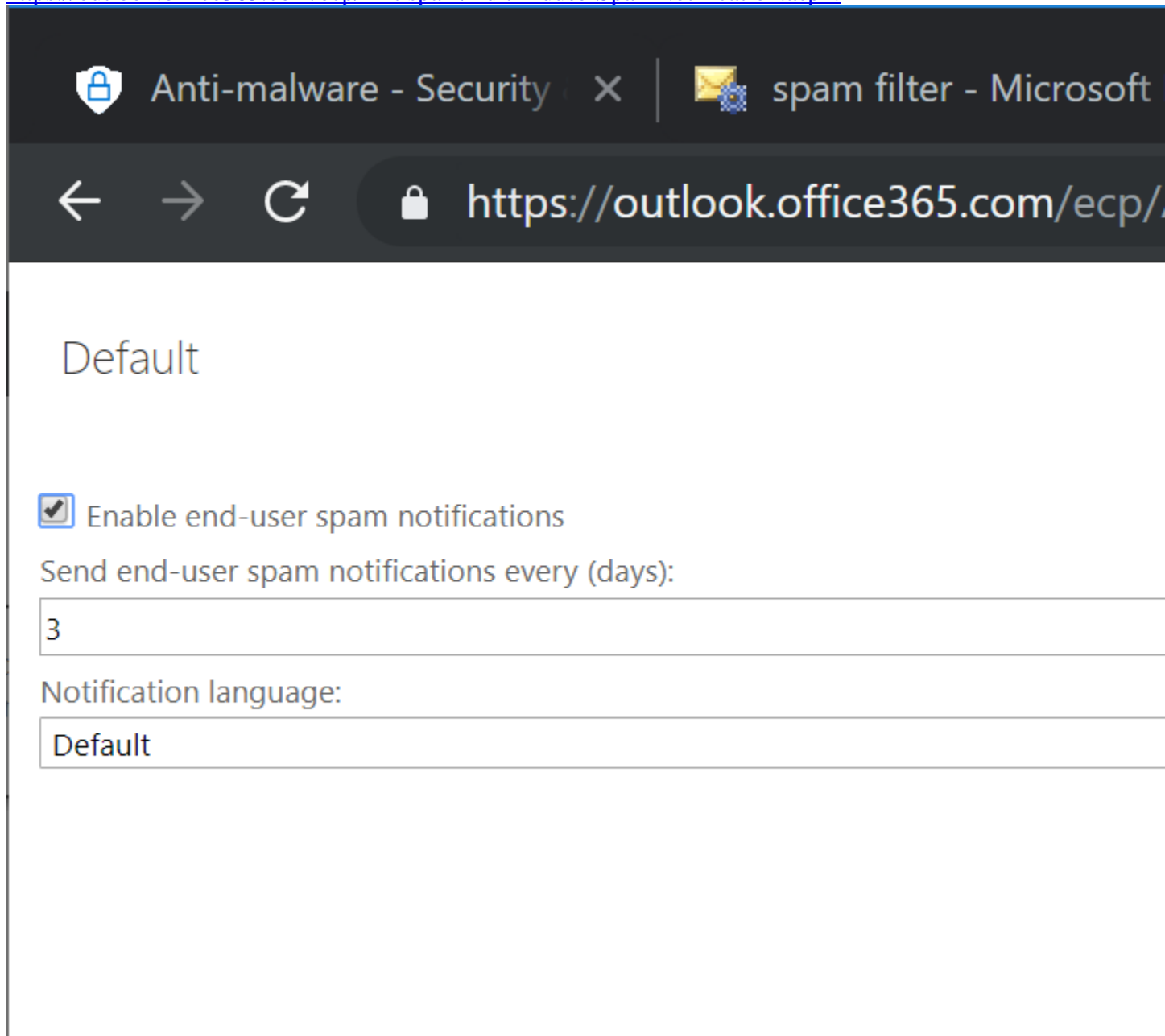
If the sender you're trying to whitelist doesn't have properly configured DMARC, this is a great opportunity to reach out to them, point them to this blog (and other helpful resources), and help improve their security posture for email.

For further reading, check out [Create safe sender lists in Office 365](#).

Enabling End User Quarantine

Many customers choose to enable end-user quarantine, so that users can periodically review and release their own spam-quarantined messages. End users are not able to release malware-quarantined messages. This is a “you do you” type of item, as some of my customers don’t want their end users to have access to this data, while other customers teach their end users to be more self-supporting. Personally, I recommend enabling it and putting the onus on the user to manage their options, and guide them to escalate to a service desk call if necessary.

You can enable end-user quarantine by completing the settings on <https://outlook.office365.com/ecp/Antispam/EditEnduserSpamNotification.aspx>.



The screenshot shows a web browser window with two tabs: 'Anti-malware - Security' and 'spam filter - Microsoft'. The address bar shows the URL 'https://outlook.office365.com/ecp/'. The page content is titled 'Default' and contains the following settings:

- ☒ Enable end-user spam notifications
- Send end-user spam notifications every (days):
- Notification language:

Reviewing Message Headers

When Exchange Online Protection scans an inbound email message it inserts the **X-Forefront-Antispam-Report** header into each message. The fields in this header can help provide administrators with information about the message and about how it was processed. The fields in the **X-Microsoft-Antispam** header provide additional information about bulk mail and phishing. In addition to these two headers, Exchange Online Protection also inserts email authentication results for each message it processes in the **Authentication-results** header.

For information about how to view an email message header in various email clients, see [Message Header Analyzer](#) documentation, or check out this [blog post](#).

You can copy and paste the contents of the message header into the [Message Header Analyzer tool](#). When you select a message in the quarantine in the Exchange admin center, the **View message header** link also easily lets you copy and paste the message header text into the tool. Once in the Message Header Analyzer tool, click **Analyze headers** in order to retrieve information about the header.

For more information, see [Anti-spam message headers](#).

Enabling Multi-Factor Authentication

Users often use a combination of the same password and email address which can be risky, especially when they are used to access resources outside of your organization. To help prevent users' credentials from being compromised, it's recommended that you enable multi-factor authentication (MFA). This isn't necessarily Exchange Online Protection-specific—it's really geared towards any service (Microsoft and otherwise).

For instructions about enabling MFA in Office 365, see [Set up multi-factor authentication for Office 365 users](#).

After you have enabled MFA on your tenant, your users can refer to [Set up 2-step verification for Office 365](#) to set up their second sign-in method for Office 365.

Configure RFC-Compliant Addresses

[RFC 2142](#) lays out a number of addresses that are required for systems hosting domains or mailboxes. They're not configured by default in Exchange Online or Exchange Online Protection; I'd recommend doing so just to be a good internet denizen.

The basic required addresses (from an RFC perspective) are:

Name	Service/Function	Comments	RFC
POSTMASTER	SMTP	postmaster@domain; used to receive comments on usage of domain's email	RFC821 , RFC822

HOSTMASTER DNS		system. hostmaster@domain; address used to receive comments, updates, notifications, complaints, or reports for a domain's DNS zones. It is typically specified in the DNS zone file as well.	RFC1033 , RFC1034 , RFC1035
USENET	USENET/NNTP	usenet@domain; address used to receive comments, updates, complaints, notifications, or reports for a domain's USENET/NNTP services.	RFC977
NEWS	USENET/NNTP	news@domain; synonym or alias for usenet@domain	RFC977
WEBMASTER	WWW/HTTP	webmaster@domain; used for capturing reporting errors or comments for website content.	RFC2068
WWW	WWW/HTTP	www@domain; synonym or alias for webmaster@domain	RFC2068
UUCP	UUCP	uucp@domain; used for receiving reports regarding Unix-to-Unix file copy. It's not been officially deprecated, but still remains a valid RFC.	RFC976
FTP	FTP	ftp@domain; used for receiving reports about file transfer errors.	RFC959
ABUSE	Abuse/Complaints	abuse@domain; used for receiving reports about abusive customers or business practices.	RFC2142
NOC	Network Operations	noc@domain; used for receiving reports about network operations or infrastructure (frequently used for ISPs or other service providers).	RFC2142
SECURITY	Security	security@domain; used for receiving reports about a domain's or organization's security.	RFC2142

No one is going to come knocking on your door if you don't have them (namely, because you don't have a way for anyone to get ahold of you). There are no internet police sending you information superhighway traffic tickets for not having the RFC-required recipients.

When I worked at an ISP, many of these addresses were frequently used and monitored. They do collect a lot of spam, but are also typically the first place people who are familiar with internet standards try to contact you should they experience a problem with your mail system. Nowadays, many of them may be configured to delete items and respond to the sender with a "we received your message, please contact us via this method" and redirect users to a phone number, monitored email address, or web form. Here are some things you can do to be standards-compliant.

Configure the External Postmaster Address in Exchange Online

Exchange Online supports configuring the service to *know* about a postmaster address. You still need to configure the mailbox manually. To configure the address to be used for postmaster, you'll need to connect to Exchange Online via PowerShell and run the following command:

```
Set-TransportConfig -ExternalPostmasterAddress <EmailAddress>
```

You'll still need a mailbox to answer for it, which we'll get to in a minute. For more information on configuring the Postmaster address, see [Configure the external postmaster address in Exchange Online](#).

Configure A Shared Mailbox and Basic Reply Rule

The idea here is to create a shared mailbox with all of those “standard” aliases, and then configure an auto-reply rule to route the sender to a webpage where they can find what they're looking for. This is not the only way to skin this cat, but it is an easy way. You'll need to connect to Exchange Online via PowerShell to run this script. Set \$Domain to whatever your domain is.

```
$Domain = "@o365ninja.com"
New-Mailbox -Shared -Name "Service Mailbox" -DisplayName "Service Mailbox" -
PrimarySmtpAddress "service$($Domain)" -Alias ServiceMailbox
[array]$Addresses = (Get-Mailbox ServiceMailbox).EmailAddresses
Foreach ($address in
("postmaster","hostmaster","usenet","news","webmaster","www","uucp","ftp","ab
use","noc","security")) { $Addresses += "$($address)$($Domain)" }
Set-Mailbox ServiceMailbox -EmailAddresses $Addresses
Foreach ($address in
("postmaster","hostmaster","usenet","news","webmaster","www","uucp","ftp","ab
use","noc","security")) { $Addresses += "$($address)$($Domain)" }
Set-MailboxAutoReplyConfiguration -Identity ServiceMailbox -InternalMessage
"We have received your message. This is an unmonitored mailbox. Please visit
our support page to open a support request." -ExternalMessage "We have
received your message. This is an unmonitored mailbox. Please visit our
support page to open a support request." -ExternalAudience All -
AutoReplyState Enabled
New-InboxRule -Mailbox ServiceMailbox -DeleteMessage
```

Additional Tools

While these might not be totally connected to the EOP service, I feel like they deserve honorable mention.

Remote Connectivity Analyzer

The [Remote Connectivity Analyzer](#) (you're probably pretty good at guessing our acronyms by now—RCA) has several tests that you can use to test mail flow and Autodiscover, and is a good place to start looking if you're experiencing mail flow issues.

Report Message Add-In

We recommend deploying this for the entire tenant as described in this [article](#). Messages that your Office 365 email account marks as junk are automatically moved to users' Junk Email folder. However, spammers and phishing attempts are continually evolving. If you receive a junk email in your inbox, you can use the Report Message add-in to send the message to Microsoft to help us improve our spam filters. If you find an email in your Junk Email folder that's not spam, you can use the Report Message add-in to mark it as a legitimate email, move the message to your Inbox, and report the false positive to help Microsoft improve our spam filters. This add-in works with Outlook 2016 and can be easily deployed for one or all users. To download the add-in, see [Report Message add-in](#). For information about enabling the add-in, see [Enable the Report Message add-in](#).

Note: Before sending samples to Microsoft, refer to [Anti-spam message headers](#) and analyze the message headers from the email that users are receiving. Did these messages get through because of rules (SFV:SKA, SFV:SKN) or user safelist configurations (SFV:SFE)? Before sending samples to Microsoft, refer to [Submitting spam back to Office 365](#).

Common Scenarios and Troubleshooting

This section describes scenarios you should be aware of that are frequently observed in customer deployments.

1. **Compromised users.** Malicious email sometimes originates from users in an organization whose accounts have been compromised. If you have reason to suspect this is happening, you may want to consider configuring [Azure Active Directory Identity Protection](#) to identify the compromised users and mitigate the issue. You can also check out the tools and tips I've provided at <https://www.undocumented-features.com/2018/12/19/checking-for-compromised-email-accounts/>.
2. **Compromised users unable to send mail.** After a user account has been blocked for sending suspicious mail, you'll need to reenable them. See [Removing a user from the Restricted Users portal after sending spam email](#).
3. **Filter tuning.** When managing your spam filter policies, you can select a bulk complaint level (BCL) to treat bulk email as spam. The default setting of 7 allows most good bulk messages to be delivered. However, adjusting to 5 or 6 is a good practice if you feel you are receiving too much spam. Rule of thumb: If there is a high rate of false positives, these may be too sensitive; if there is a high rate of false negatives, these may be not sensitive enough.

Further Reading

From cat videos to uses for the ShamWow, the interwebs have no shortage of reading material. Here's some additional stuff in the Exchange Online Protection vein should you still need help falling asleep.

What is Exchange Online Protection – In case I haven't answered it well enough, here's some other people who basically say the same thing. <https://docs.microsoft.com/en-us/office365/securitycompliance/eop/what-is-eop>

Mail flow rules – This is an enormous read with all of the conditions, exceptions, and actions you can take with transport rules. <https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules>

Common attachment blocking scenarios – There are two core ways to block attachments in Exchange Online: Common Attachment Type Filtering (as part of the malware policy) and Exchange Transport Rules. You have similar capabilities with both, so it's going to be up to you to determine which is going to meet your needs. We've published an extensive guide on configuring attachment blocking options with Exchange Transport Rules here: <https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/common-attachment-blocking-scenarios>

Advanced Threat Protection – I decided to embark upon this post because of the positive feedback I'd received on a similar post for Advanced Threat Protection. Go check it out if you have the service (or are interested in the features it provides): <https://www.undocumented-features.com/2018/05/10/atp-safe-attachments-safe-links-and-anti-phishing-policies-or-all-the-policies-you-can-shake-a-stick-at/>
