Configuring external email forwarding in Microsoft Office 365

This article is for admins who are unexpectedly receiving the bounce back "`5.7.520 Access Denied – Your administrator has disabled external forwarding`." error message (called a non delivery report (NDR).

External forwarding is controlled by the outbound anti-spam policy and scoped to users based on the configured setting. Currently, 3 settings are supported:

- **Automatic** – This is system-controlled: It allows outbound spam filtering to control automatic external email forwarding. This is the default setting.
- **On** – Automatic external forwarding is allowed and not restricted.
- **Off** – Automatic external forwarding is disabled and will result in an NDR to the end user. See

Configure outbound spam filtering in EOP for more information on how to configure these settings.

Note: Disabling automatic forwarding will also disable Inbox rules that redirect messages to external addresses.

Controlling external email forwarding

As an admin of an organization, you may have company requirements to restrict or control who is able to automatically forward emails using inbox rules, or SMTP forwarding, outside of the organization. Email forwarding can be a useful feature, but can also pose a risk through the potential disclosure of information, even by providing information to attackers that can be leveraged to attack the organization or its partners.

Office 365 doesn't allow automatic external forwarding by either Inbox rules or mail box configuration, which provides a secure default policy. However, the admin can modify these settings for all, or some, users in the organization. Forwarding messages between internal users isn't affected by such a modification.

Note: Disabling automatic forwarding to external addresses in Office 365 is being rolled out in phases with details communicated via Message Center posts. To help administrators prepare for these changes have them modify policies ahead of time to ensure there is no disruption to their users.

More information about users that are using automatic forwarding (inbox rules or SMTP forwarding) in your organization can be found in the auto-forwarded messages report.

How does this policy work with other automatic forwarding controls

As an admin, you may already have other types of controls in place, such as blocking automatic forwarding in remote domains and the use of an Exchange Transport Rule (ETR). Both controls are independent of this particular feature.

For example, if you allow automatic forwarding for a remote domain, but block automatic forwarding via the outbound spam policy the result will be that the automatically forwarded message is blocked.

Similarly, if you allow automatic forwarding in the outbound spam policy, but block it in an ETR or remote domain then the message will be blocked by either of these controls. This allows you to, for example, allow automatic forwarding in the outbound spam policy and use remote domains to control the domains that users can automatically forward messages to.

The blocked email forwarding message

Issue:

When a message is detected as automatically forwarded and the organizational policy blocks that activity, a **Non-delivery report (NDR)** is generated to the end-user. The report indicates the message was not delivered. The NDR has the following format:

```
5.7.520 Access Denied – Your administrator has disabled external forwarding – AS(XXXX)
```

Cause:

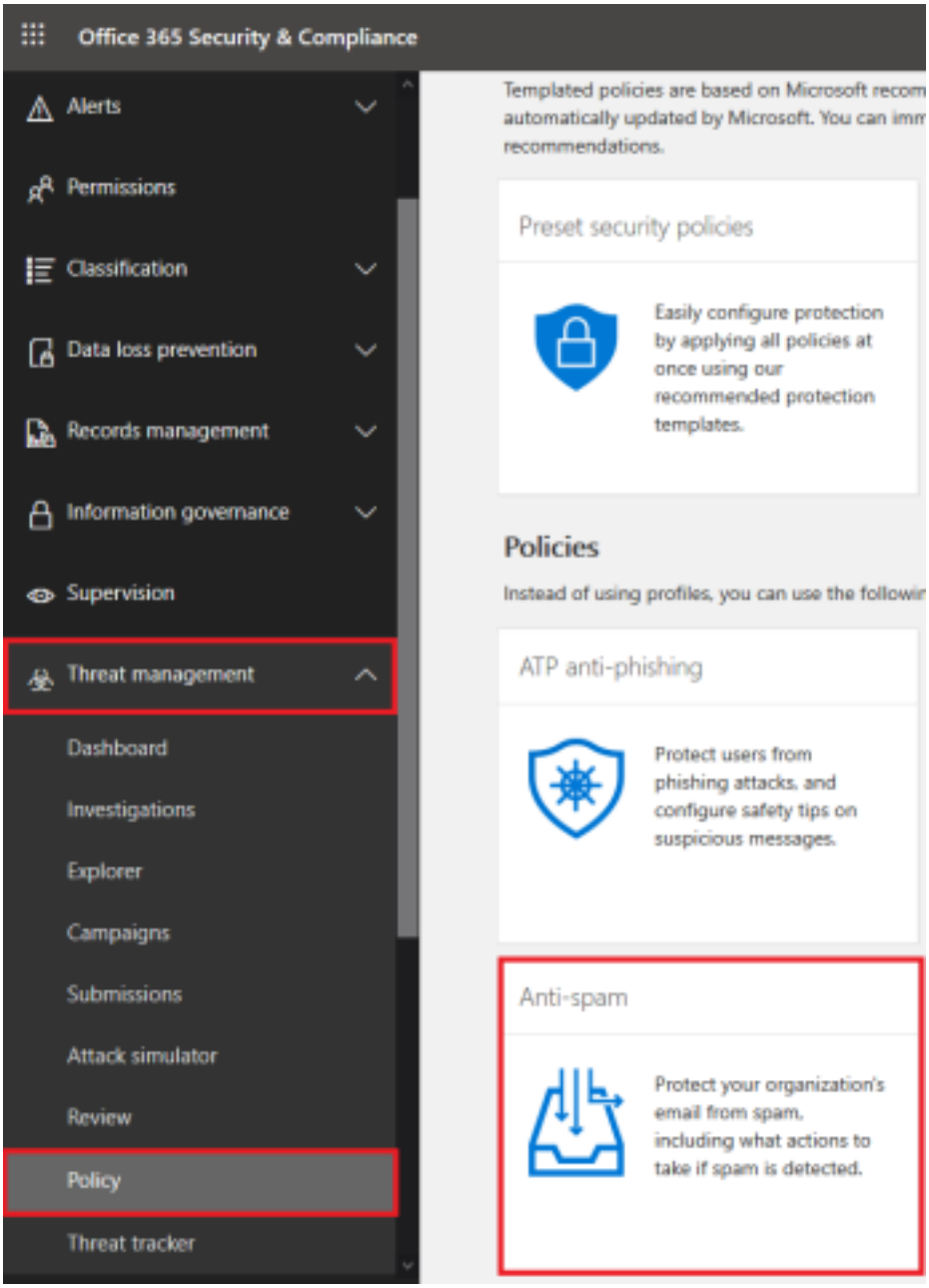
We recently disabled external forwarding by default per the Roadmap item:

- Office 365 ATP: External Email Forwarding Controls

Resolution:

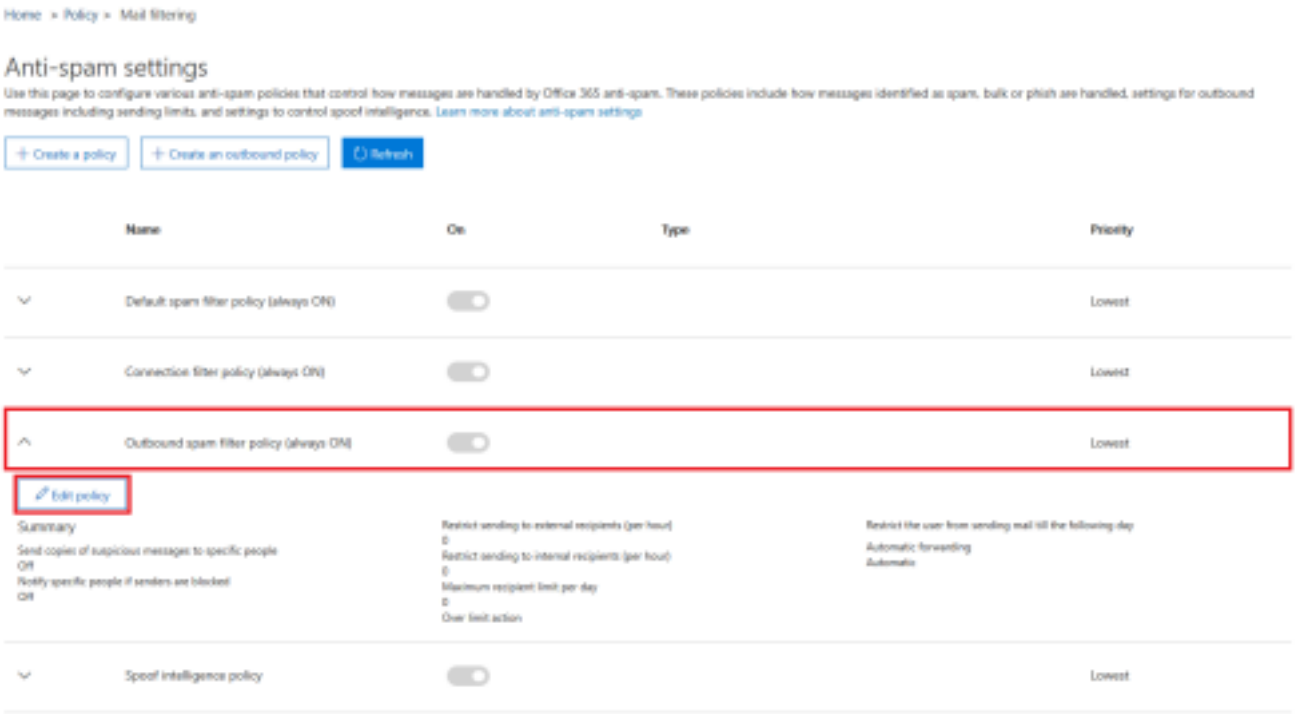
If you want your users to be able to forward externally:

1. Log in to the admin portal and select the "Security" admin center. This will take you to **protection.office.com**.
2. Select **Threat Management** then **Policy.** When the policy window opens, select **Anti-spam**.



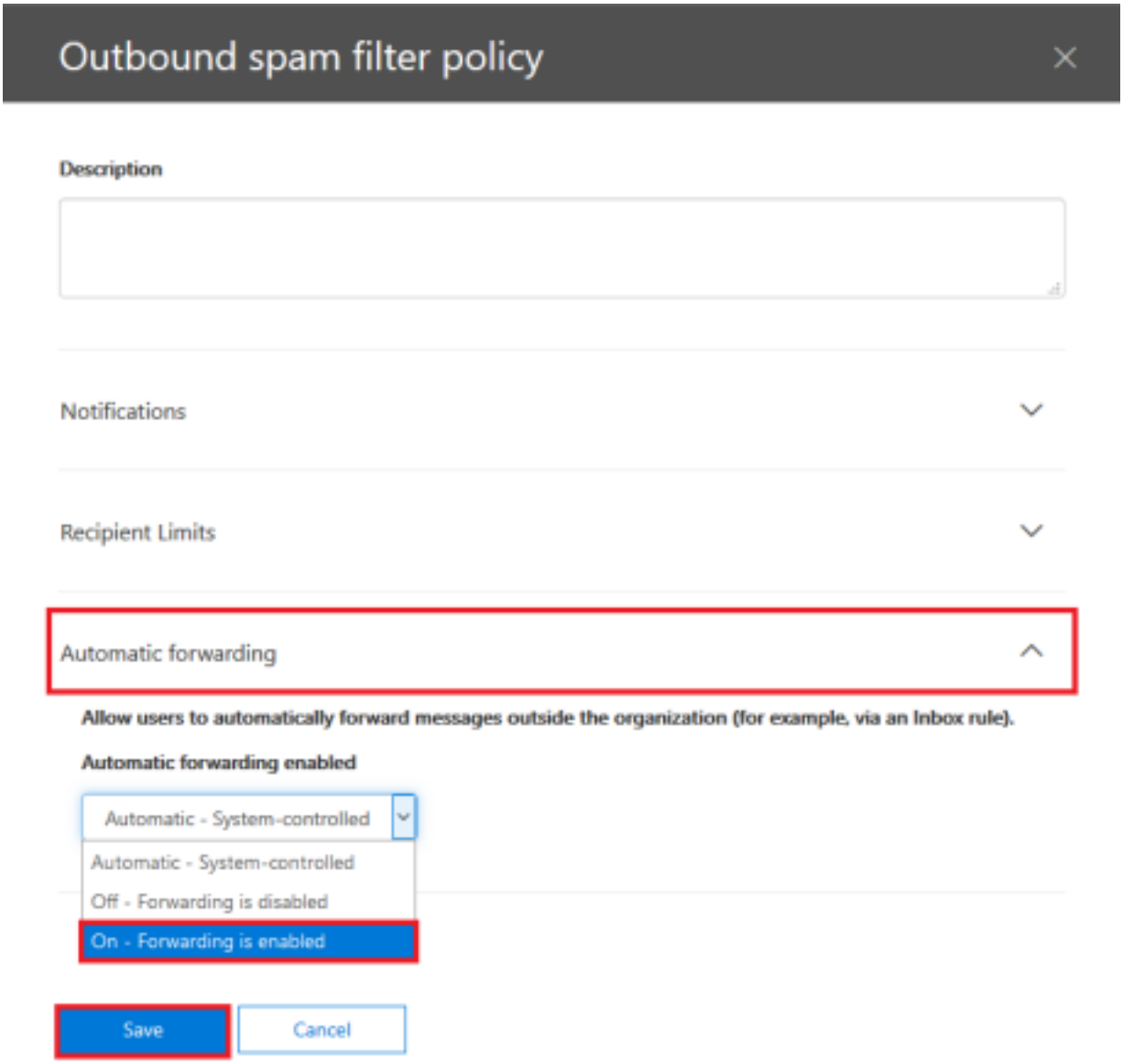
Anti-spam policy settings in threat management center

3. Open the **Outbound spam filter policy (always ON)** then select **Edit Policy.**



Edit policy button in the outbound spam filter policy settings

4. Select **Automatic forwarding** and then on **Automatic – System-controlled**, select **On – Forwarding is Enabled**.



Enable forwarding in the outbound spam filter policy

5. Select **Save**.

Best Practice tip: Alert your email users that you've disabled external forwarding, so they know your organization's policy.