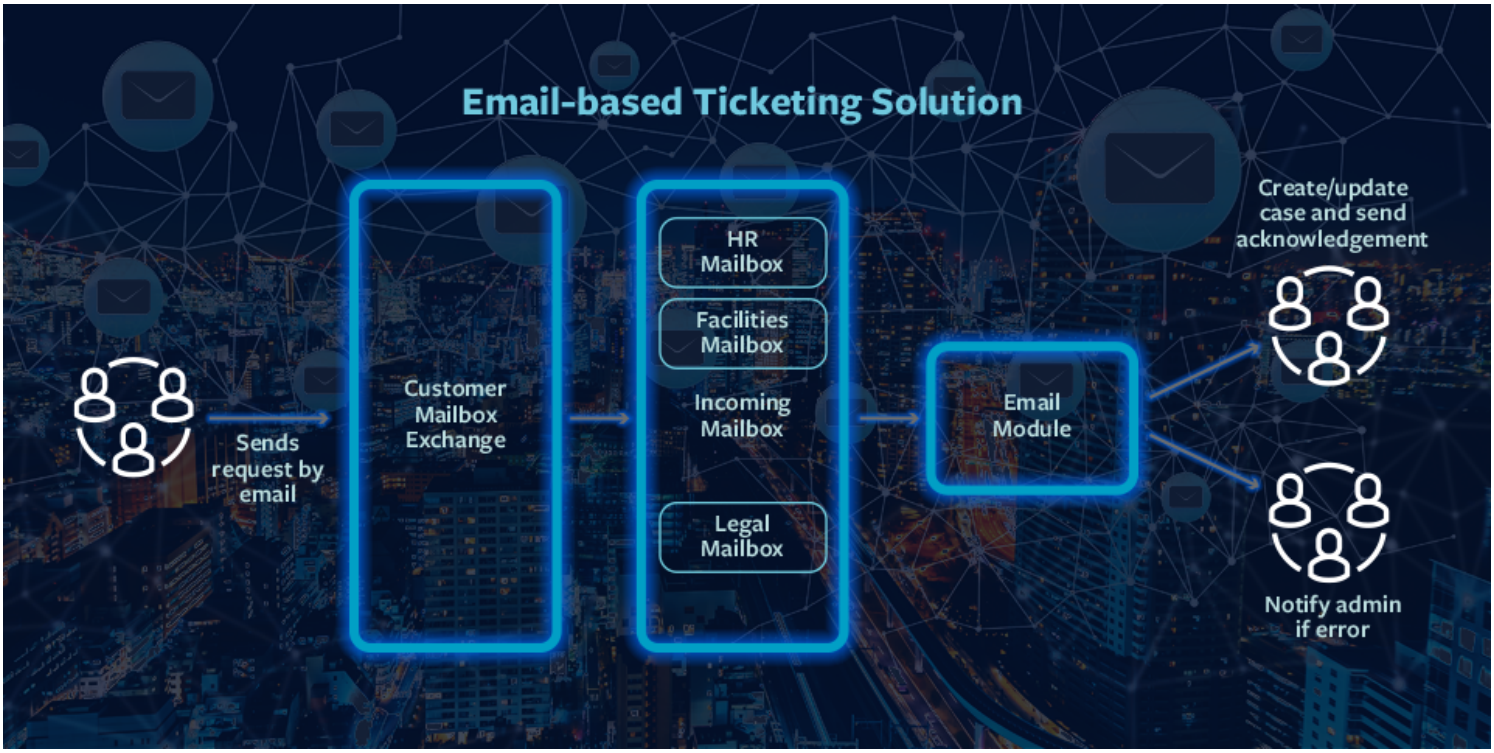
MANAGING “EMAIL FLOOD” IN SERVICE MANAGEMENT SOLUTIONS

Service management solutions have evolved over the years to become truly omni-channel, supporting browser and mobile interfaces and intelligent chatbots, and more. Even so, **email-based ticket creation** remains an important channel.

Although a traditional, email-based ticketing system might seem straightforward, the challenge increases when you have to support external users and public domains. For example, consider the difficulty in intelligently deciphering email content and generating automated replies.

In a traditional email-based ticketing solution, that will look something like this:



Different organizations have different needs—your legal and facilities teams support email-based tickets only from internal employees while your HR team supports emails from both internal and external users, opening your system to the external world and more vulnerabilities. If there are too many unwanted or invalid emails reaching your support system, it will be hard for the support team to manage and prioritize customer conversations efficiently. This flood will lead to more chaos, where the majority of help desk time is wasted cleaning up queues filled with junk or spam emails.

Stop the flood

There are steps you can take to separate legitimate and illegitimate ticket requests and eliminate the causes of email flood to ensure optimal, efficient email processing workflows 24x7.

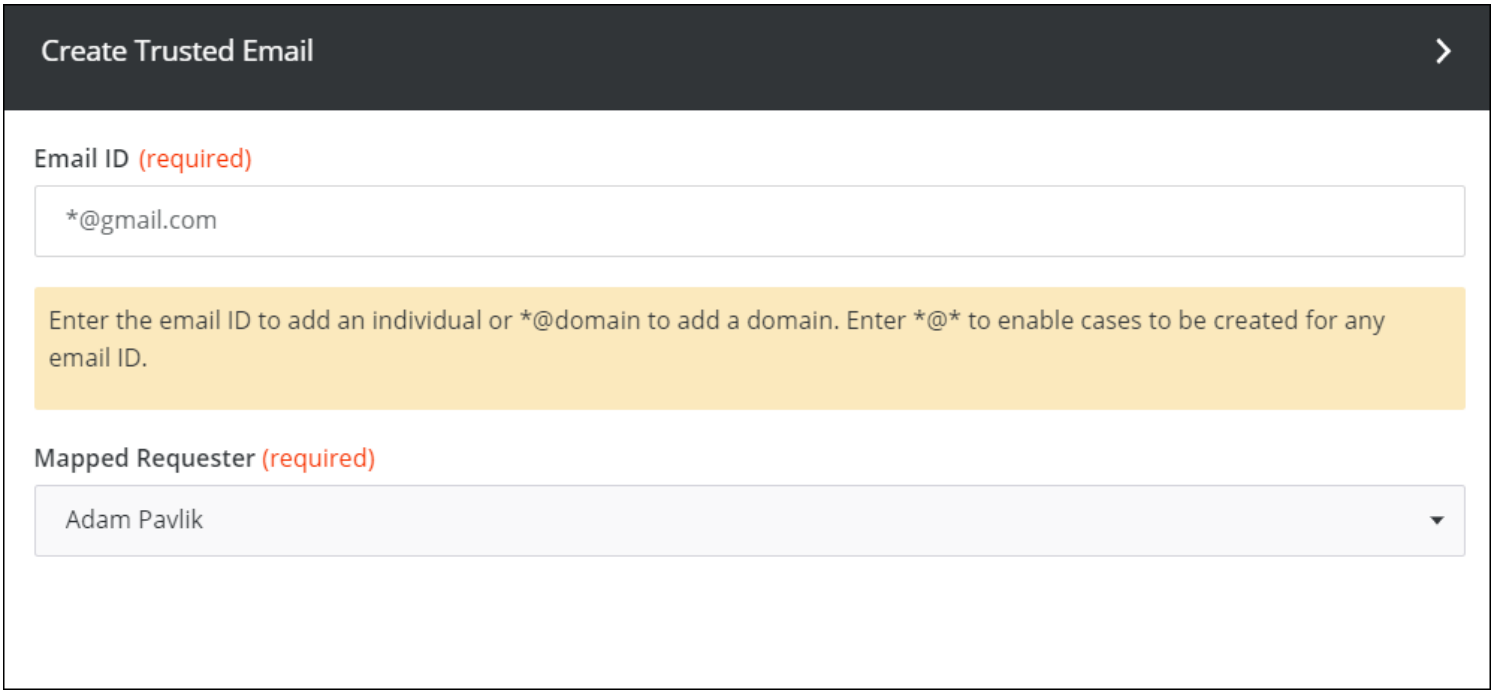
Reduce the noise

First, only allow emails from domains you trust by **setting up trusted domains**: This is one of the safest ways to avoid unnecessary spam emails in your mailbox. Understanding **email whitelisting** best practices can be useful to boost the efficiency of the mailbox processing engine.

Whitelisting and blacklisting

Whitelisting is a quick, one-time-only task to ensure the sender of an email gets added to the trusted domain. This tells your email module that you know this sender and trust them, so the module knows to process the emails and will either create or update the ticket. The emails configured under the trusted domain list will be the only ones able to communicate with your system via emails. All other emails would be automatically discarded.

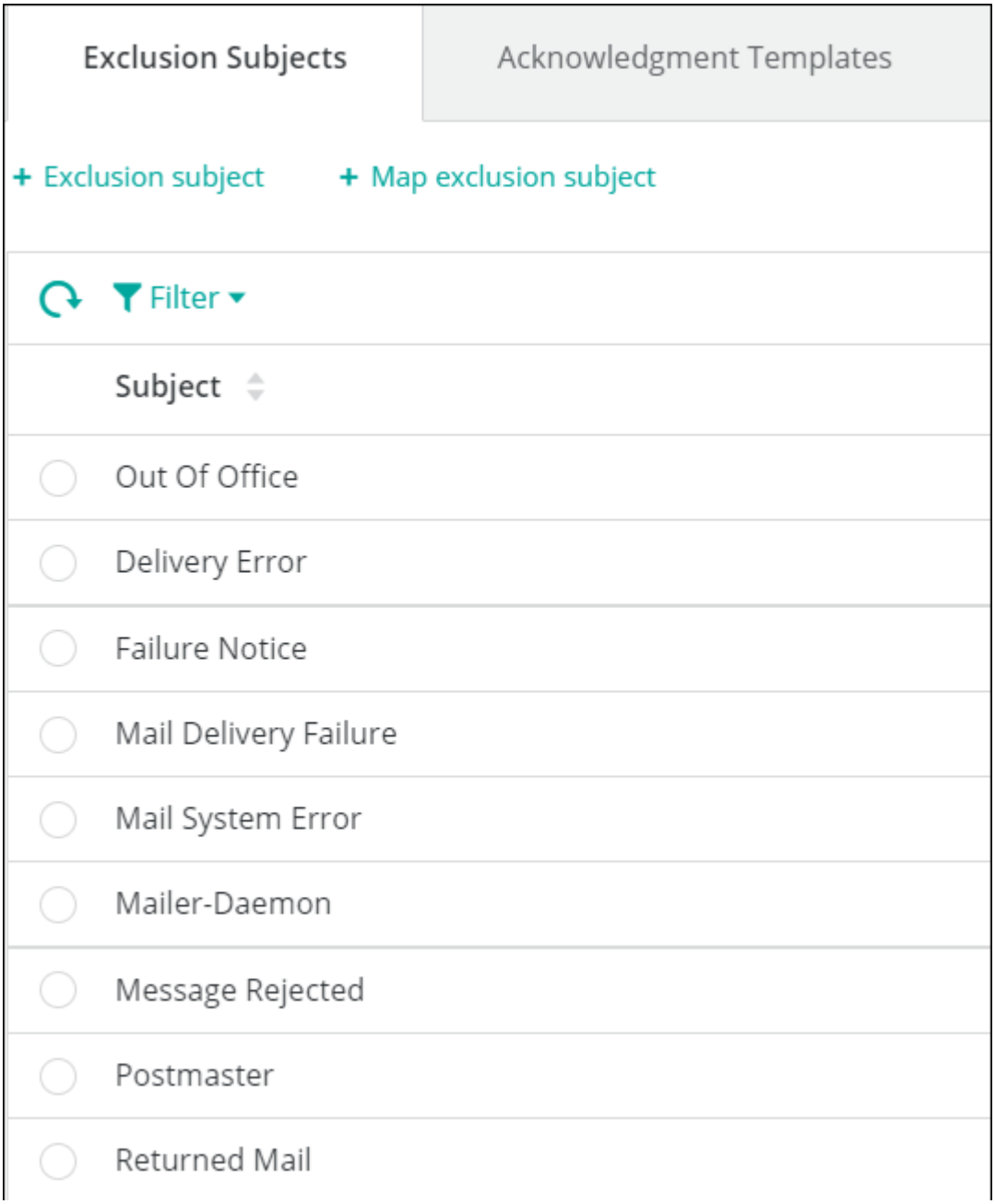
Here is a simple screenshot from BMC Business Workflows, which is a line of business ticketing solution.



Blacklisting is a collection of domains and/or email addresses blocked from sending emails because of spam activity. If your system is receiving spam emails resulting in ticket creation, use the blacklisting feature to ignore them.

Subject exclusion lists

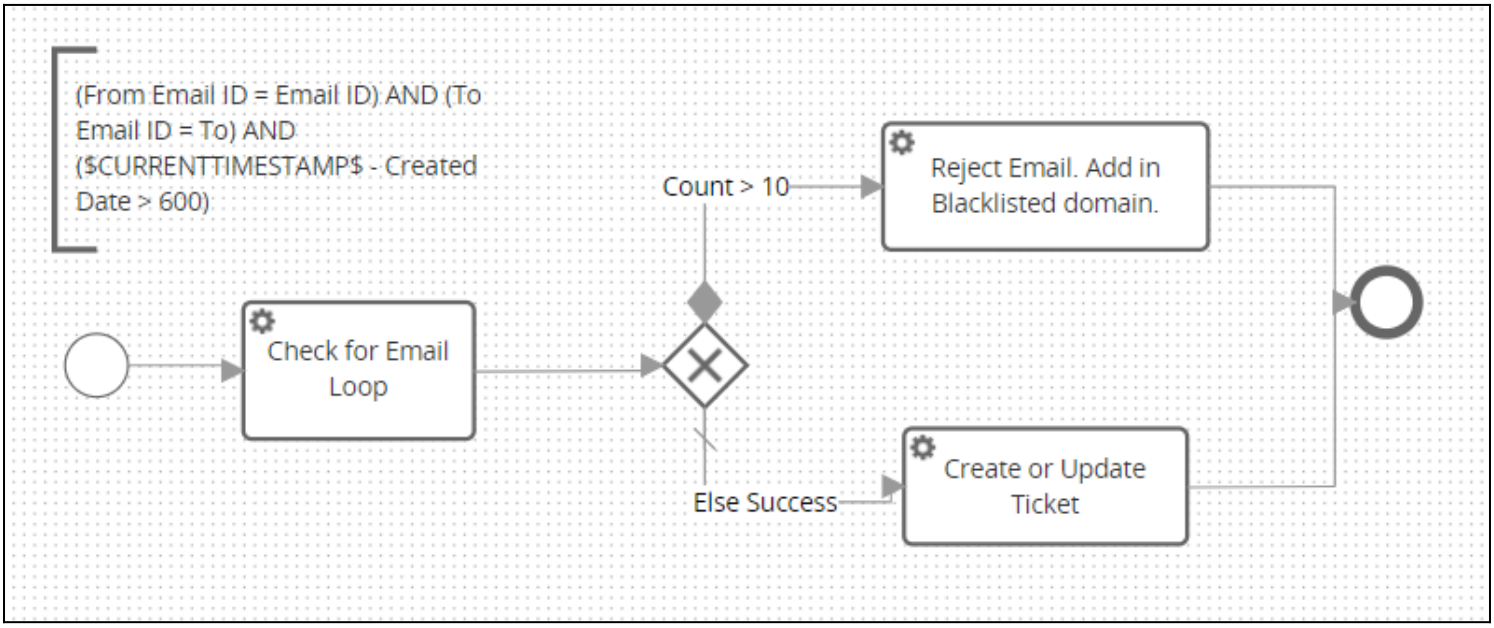
Excluded subjects are words or phrases that appear in the subject line of an incoming email message and cause the email rule engine to reject the message. Incoming messages containing the specified words in the subject field will be discarded, so it is important to review and update the exclusion list. Some commonly used exclusion subjects, which are part of the BMC Business Workflows solution, are listed below.



Detecting email loops

An email loop is an infinite loop phenomenon, resulting from mail servers, scripts, or email clients that generate automatic replies or responses. If one such automatic response triggers another automatic response on the other side, an email loop is created. The process can continue until one mailbox is full or reaches its mail sending limit. In theory, the email loop could last indefinitely. Email loops may be caused accidentally or maliciously, causing denial of service.

Solution: *The email looping algorithm* looks at the sender address , the To email address, and the threshold time interval to detect looping. After receiving more than ten emails in ten minutes from the same sender to the same email address, the loop detection will trigger and stop creating cases within that time span. The sender address will automatically be added to the blacklisted emails and an admin will receive *notification of the potential loop*.



Conclusion

There's no perfect answer to handle email flooding other than to correctly configure your email-based ticketing system to avoid them. If you are able to reduce the noise in the agent's queue, it will improve the productivity. This way, the support agents, who are the unsung champions of the office, are freed up to focus on more engaging, impactful work.