Email Deliverability

Last Modified on 22/01/2024 9:38 am AEST

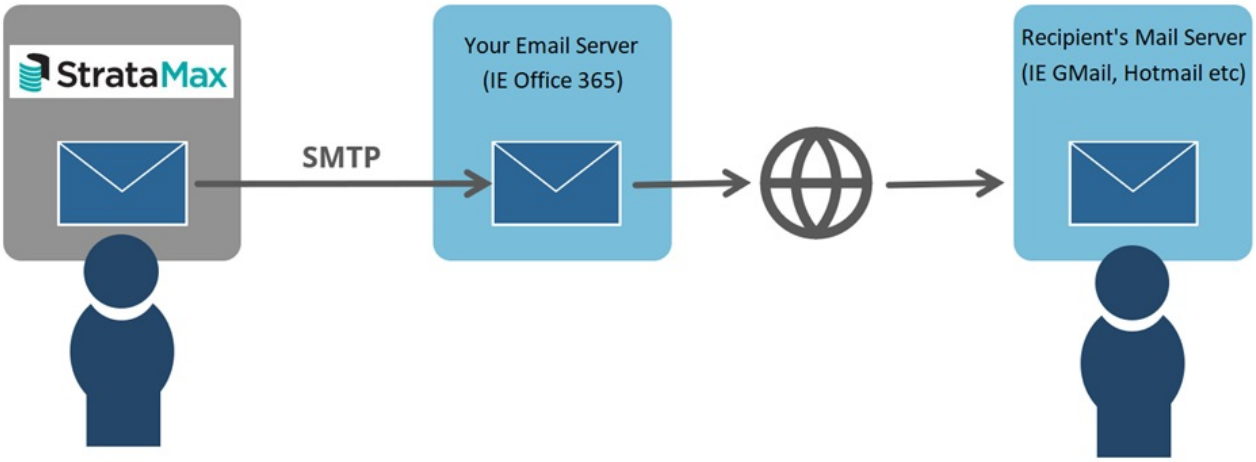
The instructions in this article relates to ***Communication***. The icon may be located on your *StrataMax Desktop* or found using the *StrataMax Search*.

How E-Mails work in StrataMax

StrataMax uses SMTP (Simple Mail Transfer Protocol) relaying to pass emails generated in the application to your nominated mail server.

For most StrataMax clients this is configured within Office 365 via an SMTP receive connector.

Once StrataMax is configured to talk to your mail server, any emails generated from StrataMax (IE Levy Notices) are directed to this mail server instructing it to send the email to the destination recipient.



Email Setup Considerations

Your email recipients (Owners, Committee members, etc) mail servers have advanced recognition and filtering to ensure incoming mail is legitimate and safe.

To prevent your emails being rejected or marked as spam, and increase the chance of successful delivery, it is critically important to ensure your IT team have set up your DNS (domain name system) settings.

The below article details some important areas of consideration to increase the likelihood of emails being delivered successfully.

SPF Records

A Sender Policy Framework (SPF) record is a type of DNS record Mail Administrators use to publish a list of trusted sources of email. This allows domain owners to specify which IP addresses and 3rd-party email vendors are authorized to send email on their behalf.

Spammers often attempt to send emails that appear to come from your domain, which is called spoofing. SPF helps message recipients know where emails from your domain should be coming from and that they aren't spoofed.

Nearly all inbound mail servers use SPF as a primary indicator of deliverability. Formerly, SPF was the only standard an email needed to be largely trusted by mailbox providers. SPF now is complemented with other authentication methods, such as DKIM and DMARC.

Most systems today want to see many indicators that an email is legitimate to better protect their customer from spoofing/phishing and spam, and to help legitimate email have better delivery rates.

SPF Record Example:

```
v=spf1 include:spf.protection.outlook.com -all
```

Office 365 SPF setup instructions: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-spf-configure?view=o365-worldwide

DKIM and DMARC

What is DMARC?

DMARC, which stands for Domain-based Message Authentication, Reporting, and Conformance, is an email protocol that, when published for a domain, controls what happens if a message fails authentication tests (IE the recipient server can't verify that the message's sender is who they say they are). Via those authentication checks (SPF and DKIM), messages purporting to be from the sender's domain are analysed by receiving organizations determining whether the message was actually sent by the domain in the message. DMARC essentially handles the questions: What should happen to messages that fail authentication tests (SPF and DKIM)? Should they be Quarantined? Rejected? Or should we let the message through even if it failed to prove its identity?

In Summary, DMARC acts as a gatekeeper to inboxes and, if set up properly, can prevent phishing and malware attacks from landing in the inbox.

What is DKIM, and how does it improve DMARC?

Becoming DMARC compliant should be the goal of any business that sends email to current or potential customers. DomainKeys Identified Mail (DKIM) is a protocol that contributes to DMARC compliancy and enables a company to take responsibility for sent messages that can be verified by mailbox providers. Essentially, it

allows the outbound domain to digitally sign email to provide legitimacy for the receiver.

StrataMax Communication FAQ

How do I view the emails that have been sent from StrataMax?

Go to the Communications module and into the *File > View Log* menu to search all emails generated in the application.

https://smhelp.stratamax.com/help/communication#view-log

What does the 'Sent' status mean in the Communications Log?

The 'Sent' status in the Communication Log means that your mail server has accepted the email for sending to the recipient. However, this status does not necessarily mean the email has arrived at the destination. If the email has not arrived at your recipient's mailbox, it's possible that the receiving mail server has filtered the email as spam, or rejected it due other reasons, such as blacklisting or the recipient's mailbox being full.

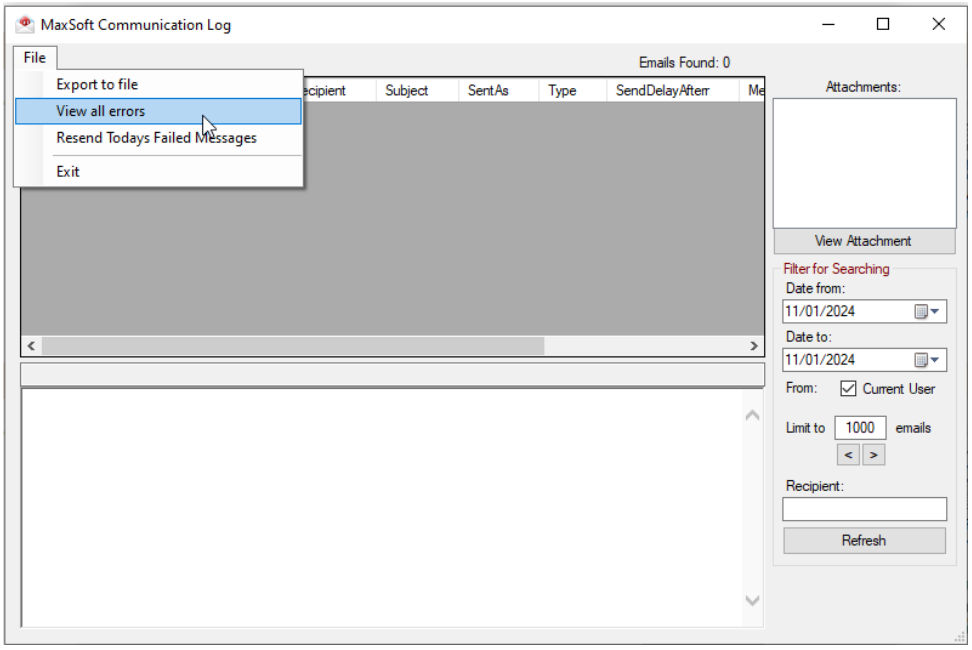
For proof of email delivery to the recipient's email server (IE Gmail), this can normally be arranged through your IT provider who can query your email server logs. These logs should have a record of the handover of the specific email between your email server and your recipient's mail server, at the date and time in the Communication log which will confirm the email was delivered.

I have checked the log, and an email has a state of "Error" state. What should I do?

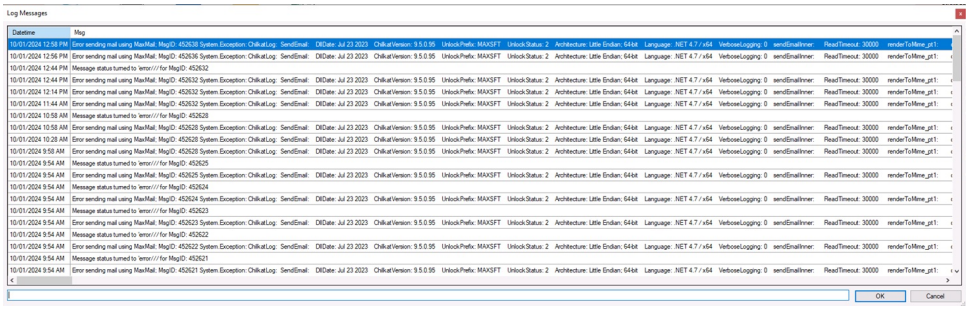
This indicates that the application has been unable to communicate via the relay to the mail server, and further investigation is required by your IT provider as to the reason the email was rejected by your mail server.

Please review the error reasons by opening the Communication Log and clicking *File > View All Errors*.

Communication > File > View Log > File > View All Errors



If you scroll to the far right of this log, it will provide the response reason for the failed email from your mail server. This information should be provided to your IT support to assist in diagnosing the problem.



If your IT team requires further support to resolve the issue, please contact support@stratamax.com.au to log a support case.

I have emails in the log with a status of "Sent", however have not being received by the recipient, what can I do?

These emails have most likely been intercepted by the mail provider's server and or spam/junk mail filtering. We recommend asking the intended recipients to whitelist (or add into the safe senders list) the company's domain, so that any emails from this address are not marked as spam or junk by their mail provider. The process to perform this varies depending on the email provider or system, but usually searching online for something like "Whitelisting Email Domain" for the provider (Gmail, Hotmail, Yahoo, etc.) will provide instructions on how to do this in the desired email application.

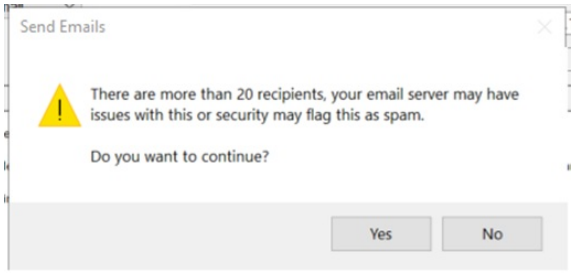
The second consideration is the content contained within the e-mail, such as length, subject line, and number of characters - all areas that can trigger the mail provider's spam/junk mail filter. For example, if emails have short subject lines or included content.

StrataMax allows for customised subject and email content when sending emails from various areas of StrataMax, like levies, work orders, etc. This is an effective way improve the success of StrataMax emails being delivered successfully. This function can be set up in the *Email Template Setup* menu, and is detailed here:

https://smhelp.stratamax.com/help/levy-noticereports#email-template-setup

When trying to send a bulk email, why am I seeing a pop-up message saying 'There are more than 20 recipients, your email server may have issues with this or security may flag this as spam'. How can I avoid this?

You'll see the following advisory in StrataMax when attempting to send a bulk email containing a total of more than 20 recipients within the 'To' or 'BCC' fields.



Mail servers (both sending and receiving) have advanced recognition and filtering to ensure emails sent and received are valid and safe and we receive frequent reports that a single email with many recipients being filtered and blocked by their spam protection, so we have added this alert to ensure you are aware that the email may be rejected.

While this is an advisory only, and your mail can still be relayed on to your outgoing mail server, to increase the likelihood of a successful delivery we'd recommend considering using StrataMax's merge letters functionality to create a distinct email per contact preference, rather than sending a single bulk email to multiple contacts.

You can read more about merge letters in the following article: Merge Letters | Online Help (stratamax.com)

Setting up a Mail Transport Rule (Office 365) to auto BCC an internal mailbox for all outbound emails

This section contains information that can be used to setup rules that will enable specific emails sent from StrataMax to Bcc a specified mailbox; this function is useful to retain a copy of the email in a mailbox so emails can be forwarded to owners and/or agents, or be added to ***DocMax***.

The setup relates to the mail server and therefore would need to be completed by your IT tech. Other methods may be available and it is recommended to discuss options with your IT Tech.

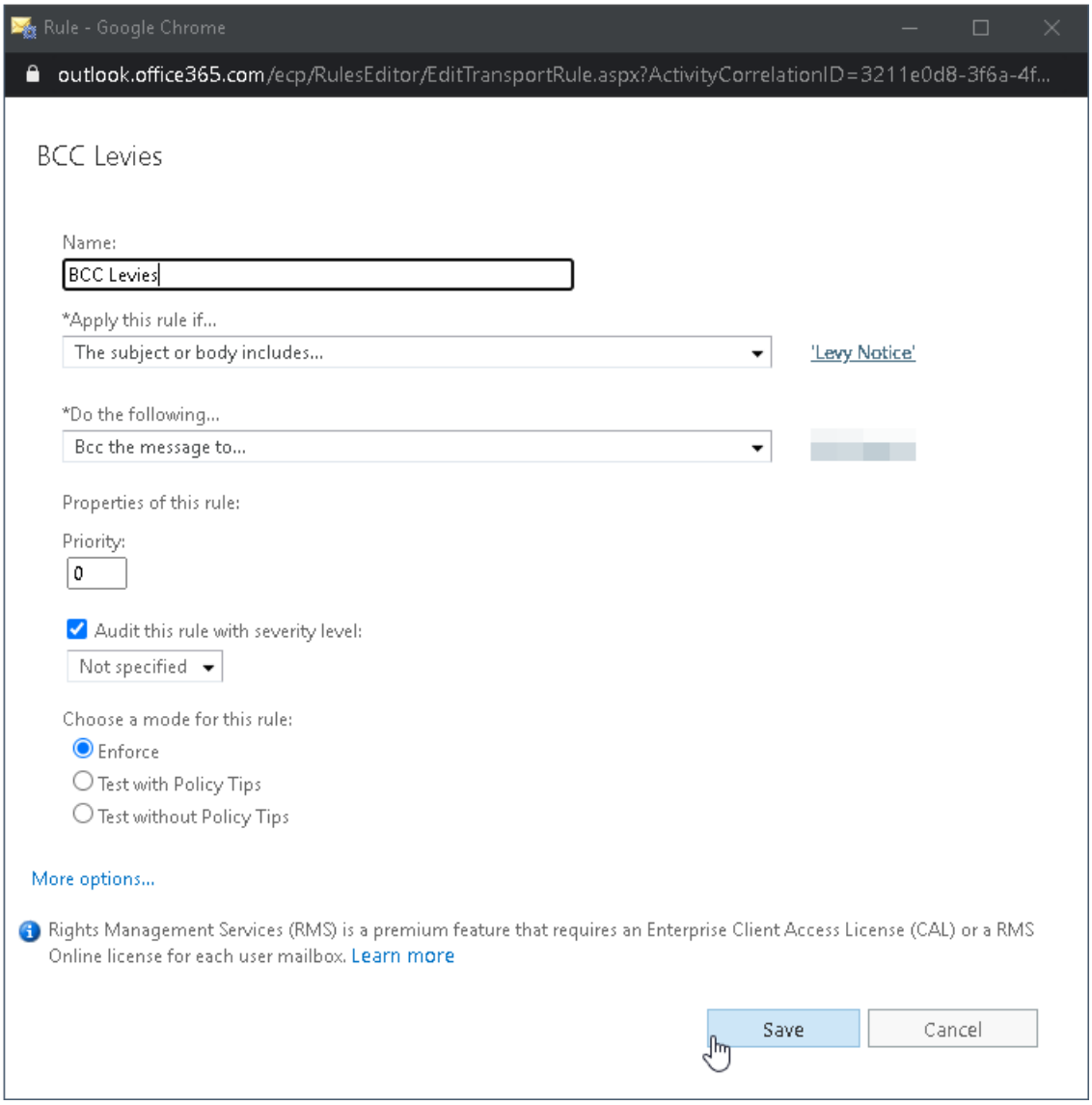
Before setting up a rule to Bcc emails, it is recommended to set up the email subject and body template to contain specific wording that can be used within the rule or alternatively create a rule based on a specific senders email if an email address such as *"levies@abcstrata.com"* is used to send the levy notices.

It is recommended to set up a shared mailbox for all users who need access to the email sent history, and naming it accordingly with a distinctly identifiable name, such as "noreplyhistory."

1. From the main *Admin Portal Center*, go to the *Exchange Admin Center*.
2. Under *Mail Flow* click *Rules*.

3. Click the + icon and select *Create a new rule*.
4. Enter a Name.
5. Modify the criteria of the rule. In the example below *'*Apply this rule if...'* is set to *'The subject or body includes...'* and the key words are set to *'Levy Notice.'* However, the key words are determined by what is setup in the email subject and body template. If wording such as *'Levy Notice'* is used, it is recommend to include an extra space to reduce the likelihood of unwanted emails being Bcc'ed to the mailbox.
6. In the *'*Do the following...'* drop down, select *'Bcc the message to'* and select the appropriate mailbox to Bcc the emails to.
7. Click *Save*.

Once the setup is completed, it is recommended to send a test email from StrataMax, ensuring the email subject or body contains the key words.



Recommended Email Service Providers for StrataMax

- Office 365
    - Office 365 has maximum daily email sending limits. Please consult with your IT provider about whether your emailing needs from StrataMax will exceed these limits.
- SMTP2GO
- SendGrid