APPLICATION BULK EMAIL – BEST PRACTICES

Government applications may use **apps.smtp.gov.bc.ca** for the SMTP server. The **apps.smtp.gov.bc.ca** points to redundant, high capacity servers whose sole purpose is to route government email application traffic.

The following best practices ensure timely delivery of email messages when using this service.

The OCIO will review client applications repeatedly causing delivery issues for other clients or creating undue stress on the service. Applications continuing to negatively impact the service after an OCIO review may have access to this service suspended.

NOTE: To access **apps.smtp.gov.bc.ca** make sure your firewall has the **APPS_SMTP** object.
If you are not using BC Government firewalls, please contact OCIO Messaging for the appropriate firewall rules to add.

All messages using this service are subjected to spam scanning, rate limiting, virus scanning and executable file blocks. There is also a 100MB size attachment restriction on mail going through the messaging environment.

Application owners using the application bulk outbound email SMTP service should follow the best practices outlined below.

UNIQUE and VALID SENDER ADDRESS

Ensure the application is configured to use a unique and valid sender address.

Undeliverable or returned messages without a valid sender address affect performance as they accumulate in the mail queue and are retried until they expire. A valid sender address has a correct prefix and domain suffix, where the domain is legitimate and accepts mail.

Many applications use DoNotReply@gov.bc.ca as their sending address. However, if one application gets rate-limited, it affects the other applications using the same DoNotReply address. OCIO recommends changing the sending address to be unique to the application or ministry so it does not affect other applications or ministries.

- Suggested unique and valid sender address would be donotreplyCITZ@gov.bc.ca or donotreply_application@gov.bc.ca
- An example of an *invalid* sender address is test@example.com.

A valid sender address is required so NDRs (non-delivery receipts) can be reviewed and the application's mailing list updated. More information on this procedure can be found in the section on CLEAN RECIPIENT LISTS.

NOTE: There is no longer a requirement to request that your sender address be added to a whitelist.

TESTING APPLICATION BULK MAILING

Please do not use the production service for testing bulk email applications.

Contact OCIO Messaging for access to the test SMTP service prior to testing a bulk email application.

Before testing and/or evaluating application email performance or determining volume limitations you are encouraged to contact the OCIO Messaging for access to the test environment.

- For bulk mail with a high-failure rate, create a valid Sender address for your application so you can validate email addresses.
- Delete email addresses that fail. The reply-to address should be a valid email address so the owner can review the NDR (non-delivery reciept).
- All applications sending bulk messages to external domains should use a dedicated sender address and associated mailbox in order to monitor any returned mail.

DOUBLE OPT-IN

Applications should be using the double opt-in method of acquiring email addresses. Double opt-in is an industry best practice as outlined in the following legislation Canada's Anti-Spam Legislation (CASL) and CAN-SPAM Act)

Using double opt-in builds a good reputation for bulk email senders.

Double opt-in requires a user to take two actions to sign up for further emails:

a) Once when the user clicks on a previously unchecked check box to opt-in to receive further offers or email messages from the sender.

b) A second time when the sender sends a confirmation email to the user's provided email address asking them to click on a time-sensitive link that will complete their confirmation.

There should be a way of unsubscribing at the bottom of the message and the application should honour that unsubscribe request**.**

THROTTLING

Throttle outbound mail from your application to 30 messages per minute or less.

Notification floods are a common issue. This occurs when a service or application is unable to respond and sends multiple notification emails **per second**, causing mail queues to accumulate thousands of messages. Throttling and using a valid sender address eliminates this issue entirely.

INDIVIDUAL MESSAGES

Configure your application to send individual messages when sending bulk mail. External domains are less likely to identify single-recipient messages as spam. NDRs (non-deliverable report) associated with individual invalid recipients are easier to interpret and handle.

When generating delivery status notification messages, senders should follow the format of a bounce as specified in RFC 3464.

BULK EMAIL LIMITS

Recipient rate limit - To discourage the delivery of unsolicited bulk messages, recipient limits are in place to prevent applications from sending large volumes of email. These limits are applied per-user to all outbound and internal messages.

The current version of Exchange Server On Premises has no recipient limit per day based on sender. It is recommended to send e-mails in batches and/or use distribution groups.

Customers who need to send bulk email over 10,000 recipients (for example, customer newsletters) should use third-party providers that specialize in these services.

5000 recipients per message is the maximum number of recipients allowed in the To: Cc: and Bcc: fields for a single email message. Sending to a distribution group within Active Diretory/GAL counts as one recipient. If sending to a personal distribution lists, each recipient is counted separately.

Individual messages - It is best to configure your application to send individual messages when sending bulk mail. External domains are less likely to identify single-recipient messages as spam. This practice also prevents reply-all storms.

CLEAN RECIPIENT LISTS

High volumes of messages to invalid recipients are increasingly common. This stems mostly from stale address data. Application owners are encouraged to use a mailbox specifically for their application and configure it as the application's sender address. Failed delivery attempts will be returned to the sender address in the form of a non-deliverable report (NDR). The NDR should be reviewed and the invalid recipient should be corrected or updated in the application's mailing list.

Customers are encouraged to have a business process in place to proactively monitor NDRs and update mailing lists to ensure your mailing list is current.

Some external domains have a threshold of invalid recipients they accept and defer further messages when exceeded.

- If delivery attempts to invalid recipients continue, government outbound IP addresses can be blocked temporarily or, with enough volume, permanently.
- Once blocked, everyone using the SMTP service cannot send mail to the external domain via the blocked outbound IP address/addresses.

Suggested methods for managing NDRs (bounced messages)

Example 1: Manual Process

A customer has a mailbox set up for application-generated emails (ORG.Auto-Responder@gov.bc.ca). This mailbox is monitored for non-delivery reports (NDR). The mailbox also gets "out of office" replies, but those are managed with a rule. When NDRs appear, forward to the application owners to correct in their system. These NDRs are often for former employee mailboxes that were automatically receiving system notifications. This ensures applications are up-to-date and aren't sending to stale email accounts.

Example 2: Automated Process

An application uses a valid sender and reply-to address which is monitored by the application. It uses regular expressions to check the body and subject for an error code. If it's a hard bounce (5xx) it is processed further, otherwise the message is ignored, including soft bounces (4xx).

- A record that associates that specific recipient to that specific article (email) is flagged as bounced.
- The total recent bounces for that subscriber is checked, and
    - If the subscriber has more than X bounces in a period of Y days, deactivate the subscription, log it, and update the bounce handler email notification that the subscriber has been removed.
    - If the "X bounces in Y days rule" has not been reached, increment the bounce Count and carry on.
- If the subscriber has even 1 successful email message sent to them, despite any number of bounces, but still within that Y day period, we reset the bounce count back to 0.
- The business area is sent a report summarizing the bounce management activities.

An additional note regarding identifying 500 errors: Look for all 5xx codes and report the specific code in the log/email notification to the business area. There are specific codes (or combination of codes and error messages) that are not always considered permanent: these codes are reported so that manual intervention can occur as needed. You can rely on the "X bounces in Y days rule" to determine which action to take in these cases.

For additional details or clarifications on using the apps.smtp.gov.bc.ca SMTP server, please contact OCIO Messaging Services.