

Email Connectivity

CONTACT - EMAIL MESSAGE FLOW OVERVIEW

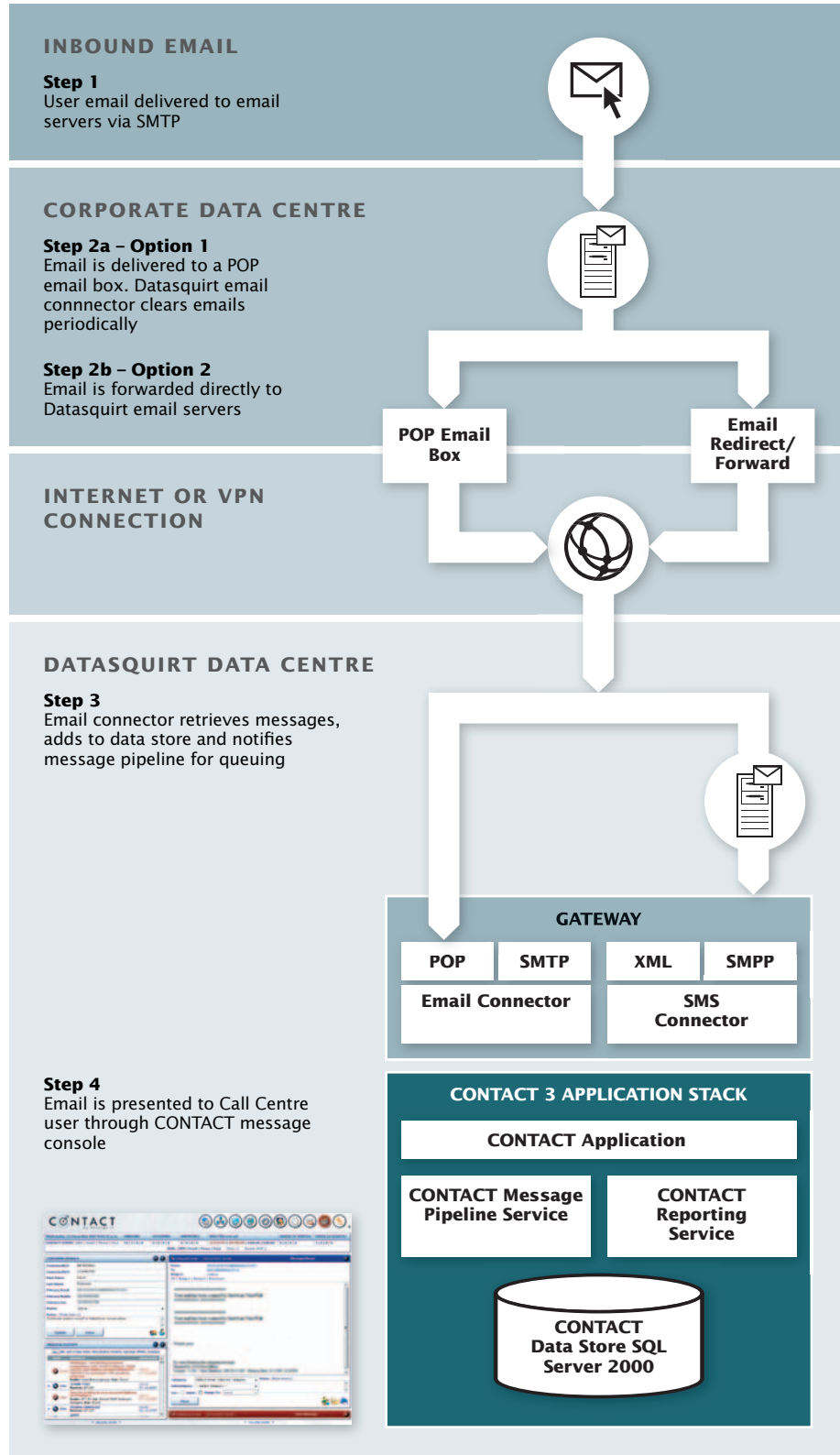


Figure 1: Email message flow overview

CONTACT™ uses standard internet protocols to send and receive email and supports all typical email functionality found in a standard email application.

Inbound email messages are received through clearing POP boxes which are periodically polled.

Outbound messages are sent via our SMTP servers.

Inbound email – forwarding or POP3 mailbox

From an infrastructure perspective, emails are delivered into CONTACT either by setting up a POP3 mailbox for CONTACT to poll and clear periodically, or by forwarding or redirecting one or more email addresses via SMTP to a mailbox that runs within the CONTACT infrastructure.

The messaging service connects to the POP mailbox on a preset time interval. It then downloads and processes the messages and then deletes the original message from the POP mailbox.

Emails are stored in their original format within the CONTACT database to ensure that the messages are correctly preserved for archival and future retrieval purposes.

Outbound – SMTP connectivity

CONTACT directly sends outbound messages via an SMTP server, using customer supplied sender addresses.

Throughputs and delivery guarantees

Due to the large volumes of junk mail now traversing the internet, timely email delivery can be problematic and is often dependent upon the individual ISP's configurations, particularly when you are sending emails to end customers.

Additionally, due to the size difference between plain text email and HTML emails with attachments, it is difficult to guarantee an hourly throughput rate. A guideline of 150-200 messages per minute using an average-sized HTML message with no attachments under optimal conditions (minimal network or server load) can be assumed.

Additionally, there are a couple of specific spam-related issues that need to be highlighted:

SPF – sender policy framework

SPF is a recent development introduced as an attempt to reduce the number of spam networks spoofing organisations' email addresses.

It works by specifying a valid list of SMTP servers that emails for a particular domain can be sent from.

While this technology is not yet broadly supported, it is growing in popularity and large email services such as Google mail do check SPF records.

Therefore, organisations that provide SPF settings within their domain's DNS records will need to add the IP address of the CONTACT SMTP server to their SPF settings; otherwise many servers will reject messages sent from CONTACT.

Grey-listing

Grey-listing is another technique recently implemented by many ISPs to reduce the levels of spam received on their networks.

It works by automatically refusing the first delivery attempt of a message from a new, unknown email server.

Most email servers are configured to retry after a certain interval, however most spam applications are 'dumb' and give up after the first refusal.



When the second or subsequent delivery attempt occurs, it is accepted and the IP address of the new email server is added to a white-list.

The implication of this is that messages may not immediately deliver to an end-user's email address. Instead, they will appear after a period of time; this period of time is solely dependent upon external timeout settings and is beyond our control.

Email features

Support for HTML/plain text – CONTACT supports both HTML and plain text emails and standardised forms of MIME encoding including multipart/alternative, multipart/mixed, etc.

Attachments – Inbound and outbound attachments are supported. Outbound attachments up to 10MB in size are allowed.

These are available from within the application for download or viewing by the CONTACT agent.

Extended character sets – CONTACT supports extended UTF character sets and as such, emails in any language using the various standard MIME encodings.

Avoiding message loops – These may occur where an auto-response is sent to an auto-response. For example, if CONTACT is configured to send auto-responses to all inbound emails, and an address has an out-of-office auto-reply, a loop can occur where CONTACT auto replies to the out-of-office, and the out-of-office then replies to CONTACT.

CONTACT has functionality to stop loops from occurring by limiting the number of auto-responses to a given email address within a certain timeframe. This setting is configurable.

Spam detection – Two methods of spam detection are supported:

- **SMTP interception** – All email messages delivered into our email server are scanned and scored using SpamAssassin. Anything scoring greater than five is discarded as spam.
- **Classification handler** – Can be trained to detect spam and optionally automatically close the message and remove it from the pipeline.

Virus detection – All servers within our infrastructure have enterprise-grade virus detection applications installed and running. Virus signatures are patched as soon as available.

SMTP interception is also used for virus detection; all messages delivered to our email server are scanned and any containing virus attachments are automatically discarded.

