What's New in InterMail 4.0

InterMail 4.0 offers a variety of new features, as well as extensive enhancements to existing functionality. To take full advantage of InterMail's current capabilities, please review this document and the revised manual set included with the software.

1.1 Highlights of the InterMail 4.0 Release

InterMail version 4.0 includes six new servers:

- The Queue Server offers enhanced handling of deferred mail. All transactions involving queued mail are recorded in journal files, providing complete protection against message loss.
- The IMAP server allows clients to view, send, and receive mail via the IMAP4 protocol.
- The Configuration Server supports centralized system configuration, allowing administrators in a multi-host InterMail environment to make changes to a single configuration file and have those changes automatically propagated throughout the system.
- The Manager Server allows remote management of all servers in the system.
- The Web Server supports the SelfCare application, through which administrators can allow end users access to a select set of account information. By allowing end users to perform routine maintenance on their own accounts (changing passwords, forwarding addresses, etc.) overall service can be improved while administrative costs are reduced.
- The SNMP Server provides a means of monitoring InterMail events via a standard SNMP monitoring station.

In addition to six new servers, InterMail version 4.0 offers the following features and enhancements:

- Message aging options that allow administrators to control the length of time that retrieved and unretrieved messages may remain in storage before being deleted.
- Mail throttling options to regulate system load during periods of exceptionally high activity.
- Quotas can be linked to alerts warning users when their mailboxes are approaching maximum capacity.
- MTA filtering (based on the SIEVE scripting language) to assist in the prevention of "junk" e-mail.
- Secure Socket Layer (SSL) support for POP and SMTP traffic.
- Support for Delivery Status Notification (DSN).

For more detailed information on new features and changes to existing functionality, please review the sections that follow.

1.2 Changes in Functionality from 3.2 to 4.0

This section outlines the differences in functionality between InterMail 3.2 to InterMail 4.0. The discussions here cover only *changes* in functionality (i.e., situations where an InterMail function previously existed but now operates in a different manner). To learn more about *new* functionality, please refer to Section 1.3.

1.2.1 Changes to the Directory

In InterMail 4.0, the Directory database was modified to include additional information, which may be shared by multiple Software.com products. The name of the database has been changed to reflect this capability. The database is now known as the Integrated Services Directory.

In previous versions of InterMail, the local domain list was stored in the Directory database and the full domain list was stored in the Configuration Database (the `config.db` file). In InterMail 4.0, all domain information is stored in the Integrated Services Directory.

In previous versions of InterMail, account quota information was stored in the Message Store database and host or system-wide quota settings were specified in the Configuration Database. In InterMail 4.0, there are no host or system-wide quota settings and account quota information is stored in the Integrated Services Directory.

Note: *Quota settings in 4.0 are Class of Service attributes and are set by imdbcontrol at either the Class of Service or the per-account level.*

1.2.2 Changes in Oracle Operation

In previous versions of InterMail, the design of the Oracle database supporting the Message Store Servers dictated that a single MSS process could have only one connection to the Message Store database. InterMail 4.0 includes a multi-threaded Oracle database implementation, allowing a single MSS process to have multiple connections to the Message Store database. This change eliminates the need to run multiple Message Store Servers on a single host.

1.2.3 Changes in Quota Notification

In previous versions of InterMail, users received no notification when they were approaching their maximum allotted mail quota. In InterMail 4.0, a threshold quota can be established (as a percentage of maximum mailbox capacity). When this threshold quota is exceeded, a “near quota” warning will be delivered allowing users to delete mail from their mailbox in order to prevent an over-quota condition.

If a mailbox quota is exceeded, both the sender and the intended recipient can be notified. In earlier versions of InterMail only the sender was notified (via a bounce message). In addition, InterMail 4.0 allows you to indicate the maximum number of times an over-quota notice is sent.

1.2.4 Changes to Mail Blocking Options

In InterMail 3.2, mail blocking policies could only be configured on a per-MTA basis. InterMail 4.0 offers administrators the ability to enable or disable mail blocking policies on a per-account basis. This means that users can either have mail blocked (based on system-wide policies, *not* individually configured options) or they may opt to waive mail blocking and receive all mail.

1.2.5 Changes in Relay Options

In previous versions of InterMail, relay was provided on a per-user or global basis. InterMail 4.0 provides support for relay of mail addressed to non-authoritative domains.

A non-authoritative domain (formerly called a "semi-local" domain) is one over which InterMail does not claim exclusive control. That is to say, InterMail may not recognize all (or even any) of the users in that domain. The establishment of non-authoritative domains allows InterMail to accept mail for a domain, but relay it to another mail host if necessary. Non-authoritative domains can be set to define domains for which your site is an MX backup, or used when InterMail is run in parallel with an existing mail system (i.e., during migration of e-mail accounts from a legacy mail system to InterMail).

One of the conditions for establishing a non authoritative domain is identification of the relay host to which mail should be passed if it cannot be delivered directly. When mail arrives for a known user in a non-authoritative domain, InterMail delivers it to the appropriate local mailbox. When mail arrives for an unknown user in a non-authoritative domain, InterMail passes the message to the designated relay host.

It is assumed that the mail server on the relay host can deliver the message, although InterMail has no way of verifying this. All InterMail needs to know is the IP address of the host to which it should send the mail. From that point forward, the message becomes the responsibility of the receiving mail server.

1.3 New Functionality

In addition to the enhancements described in Section 1.2, InterMail 4.0 incorporates extensive new functionality. The sections that follow provided descriptions of each new feature offered. Additional information on the operation and intended use of each feature can be found in the standard InterMail documentation (the five manuals delivered with the InterMail 4.0 software).

1.3.1 Support for End User Account Access

InterMail version 4.0 includes the SelfCare application, a web-based interface that allows end users to view and modify certain pieces of information related to their e-mail accounts. Access to SelfCare--and individual options within it--can be controlled through the setting of class of service attributes within the Integrated Services Directory. The SelfCare interface can also be customized to include site-specific product information, form text, or user interface presentation.

By default, all end user access is denied, however, administrators may offer end users any or all of the following options:

- the ability to change passwords
- the ability to define a forwarding address
- the ability to enable/disable mail filtering (based on system-wide filtering criteria)
- the ability to set a vacation message

1.3.2 The "Stateless" MTA

InterMail 4.0 includes a "stateless" MTA. With this design the MTA is not responsible for persistent storage of messages. When a message is received by an InterMail MTA, it will either be delivered to the appropriate mailbox or forwarded to a remote server (known as the Queue Server) for temporary storage. Only after one of these two actions has been successfully completed will the sending client be notified that the message has been accepted.

Any outgoing mail queues that are created (in the event that a message was unable to be delivered) are maintained by the Queue Server and can be shared among multiple MTAs. In the event that one MTA is unavailable, any other MTA can process the messages stored in an outgoing mail queue.

1.3.3 IMAP Server

InterMail 4.0 introduces an IMAP Server, enabling IMAP4rev1 clients to send and receive mail in on-line, off-line, and disconnected modes.

Unlike POP clients, IMAP clients are not required to download messages to their local file system to read them (though can do so if they prefer). The IMAP protocol allows for a more "interactive" relationship between client and server, where the client can ask the server for only the headers or the bodies of specific messages, or search for messages that meet specific criteria. Messages in a mailbox can be marked with various flags (e.g., read or answered); and will stay in the mailbox until the user specifically deletes or moves them. In short, IMAP is designed to allow users the ability to manipulate messages on the server as if they were on a local machine.

1.3.4 Enhanced Configuration Functionality

InterMail 4.0 provides enhanced configuration functionality through the addition of the Configuration Server and changes in configuration management. These changes provide administrators with the ability to configure their system through one centralized configuration database and to have these changes automatically propagated throughout the entire system.

Centralized Configuration

Although an InterMail system can consist of numerous hosts and each host contains a local copy of the Configuration Database, InterMail 4.0 system employs a "centralized configuration" method. Configuration changes are entered on one host only, the Master Host.

Dynamic Configuration Propagation

InterMail 4.0 employs a "dynamic configuration" strategy that automatically updates the master Configuration Database, propagates the changes to all other hosts in the InterMail system, and informs the administrator what, if any, actions must be taken on individual servers (stopping and starting of servers) in order for the changes to be recognized.

1.3.5 Message Aging

InterMail 4.0 provides message aging features that allow administrators to define limits on how long retrieved and/or unretrieved mail is allowed to remain in the system.

The ability to age messages is important:

- for users who rarely (if ever) read their mail, and
- for users whose client does not delete mail from the server once it has been retrieved.

When the message aging feature is enabled, InterMail tracks the length of time a message has been stored, and automatically deletes mail older than the allowable lifetime defined.

An aging policy may be enforced on only those messages, which have been retrieved, or on all messages, regardless of whether or not they have been retrieved.

1.3.6 Support for SNMP

InterMail 4.0 enables you to monitor certain events and processes via SNMP (the Simple Network Management Protocol). SNMP is a protocol that provides users the ability to monitor network and system traffic statistics and reportable parameters.

The InterMail SNMP Server provides information such as the number of connections to the POP server since the server was started, the total number of messages that are stored in the MTA, and the total number of messages stored in the Message Store Database.

This information is "sampled" and sent to the user-defined SNMP monitoring station. This data is particularly useful in InterMail because:

- it can be viewed real-time without any script development log parsing,
- it can be viewed with standard SNMP monitoring stations, and
- it provides information about the present state of a server (volumes or numbers of connections at a given time) as well as archived information (accumulated volumes or numbers of connections over a time period).

1.3.7 MTA Filtering

InterMail 4.0 provides a filtering capability using a filtering language based on the SIEVE scripting language. Filters are optionally run on incoming mail and can cause the mail to be rejected, bounced, sidelined, forwarded, thrown away, or delivered normally, based on its content.

Filter actions can be written to detect the presence or absence of certain headers, specific content in headers or body, specific senders, or specific recipients. Message content can be tested by searching for exact string matches or by using simple patterns or complex regular expressions. A filter is set up by establishing an InterMail configuration key with the appropriate set of filter commands.

Note: *Only one filter may be established per MTA, and it applies to all incoming mail; there are no per-user filters.*

1.3.8 Threshold Quotas

InterMail 4.0 allows administrators to set threshold quotas, which alert end-users when their mailboxes are near capacity (i.e., when they have "almost" reached their allotted maximum quota). The content of these warning notices is configurable. The standard text advises users that their mailboxes are nearing capacity, and that messages will soon begin bouncing unless additional space is made available.

The threshold quota setting is always expressed as a percentage of the total configured size of the mailbox. For example, if the threshold quota value is 80, it means that whenever a message arrives that fills a mailbox beyond 80 percent of its allotted capacity, a warning notice will be sent to the end-user.

1.3.9 MTA Extensions

The following functionality extends SMTP-supported commands in InterMail:

Authenticated SMTP

InterMail 4.0 supports SMTP authentication, which helps combat junk mail when the sending of junk mail includes the forgery of sender addresses. By using forged addresses, senders of junk mail can hide their identities. If a sender forges his or her return addresses to include one of your local domains, they may also bypass the relay-prevention and mail blocking policies implemented in InterMail 3.2.

When enabled, the SMTP authentication mechanism requires senders to transmit a username and password at the beginning of the SMTP client session. The client session is allowed to continue only if the given authentication data matches that of an existing account. When messages are transmitted, the sender address--both in the MAIL FROM command and From: header--of the messages are compared to the addresses associated with the account. If the sender address is not valid for the account (that is, the address is a forgery), the message is rejected.

Note: *SMTP authentication requires that the user's e-mail client support the AUTH LOGIN command.*

Support for ETRN

InterMail 4.0 supports the SMTP ETRN command, a mechanism for allowing other SMTP servers to initiate the processing of queued mail for domains that they handle. This is useful in situations where other SMTP servers are accessible for limited periods only (i.e. when a site has dial-up connectivity and wants to initiate the sending of queued mail while they are connected).

Delivery Status Notification (DSN)

InterMail 4.0 includes Delivery Status Notification (DSN), allowing senders to be notified when mail that is sent to another server supporting DSN is delivered, forwarded, or relayed on to another server that does not support DSN. This feature can be set system-wide, but not on a per-user basis.

1.3.10 Header Rewriting

InterMail 4.0 provides the ability to rewrite headers, both for incoming and outgoing mail.

Rewriting Headers for Incoming Mail

In InterMail 4.0, The TO:, CC:, BCC:, FROM:, SENDER:, and REPLY-TO: header fields contain addresses that can be in a variety of formats. Sometimes, the address of a message needs to be modified to ensure that the recipients of the message are able to reply correctly. InterMail 4.0 provides options for rewriting these header fields so that you can control their content and format.

Rewriting Headers for Outgoing Mail

InterMail 4.0 provides the ability to modify headers when messages are destined for a particular domain. For example, when the domain is acting as a gateway to a proprietary system. When a message is being relayed to one of these gateway domains, each address from the header is looked up in the directory.

1.3.11 Remote Control of Servers

In InterMail 4.0, servers in a multi-host configuration can be controlled in a centralized management method through the addition of a Manager Server and the `imctrl` command. Instead of logging on to individual hosts in your InterMail system (as in InterMail 3.2 and earlier versions), you can now issue commands from any host to all servers in the system.

1.3.12 Graceful Server Shutdown

In previous versions of InterMail, the method of shutting down servers (imservctrl) used a UNIX "kill -9." In InterMail 4.0, servers can be shut down "gracefully." There are two new methods in InterMail 4.0 to allow graceful shutdown:

- The `drain` option allows existing connections to cease naturally while all new connections are refused. This method provides "client-friendly" shutdown and allows the servers time to clean up temporary files that may exist.
- The `stop` option causes a server to exit as soon as possible in an orderly fashion. Client sessions may be interrupted, but meaningful information and status messages will be displayed to the client.

1.3.13 Secure POP and SMTP with SSL

InterMail 4.0 offers additional security with the SSL (Secure Socket Layer) in the MTA and POP Servers. MTA and POP using SSL allow both clients and servers to verify authentication in mail transactions by operating on alternate secure ports. In InterMail 4.0, the POP and MTA servers can be configured to listen and accept connections on an alternate secure SSL port in addition to the standard SMTP port (25) and POP3 port (110).

1.3.14 Automated Backup Tools

InterMail 4.0 provides several commands that help in automating the required backup process as well as assist in identifying information that should be included in such a backup.

1.3.15 Additional Logging

The following information describes additional logging and statistical reporting that is recorded in InterMail 4.0.

IMAP Statistics

The following information is gathered by the IMAP server and reported in the imapserv.stat files.

- StatConnections--Current number of IMAP clients connected.
- StatAccumulatedConnections--Total number of IMAP clients that have connected.
- StatFailedConnections--Number of IMAP client connections that have failed.
- StatRejectedConnections--Number of IMAP client connections that have been rejected.
- StatTimedOutConnections--Number of IMAP client connections that have timed out.
- StatFetchRequests--Number of fetch commands that have been serviced.
- CreateRequests--Number of create commands that have been serviced.
- DeleteRequests--Number of delete commands that have been serviced.
- AppendRequests--Number of append commands that have been serviced.
- CopyRequests--Number of copy commands that have been serviced.
- SearchRequests--Number of search commands that have been serviced.
- FetchedVolume--Volume of mail (in KB) fetched by IMAP clients.
- AppendedVolume--Volume of mail (in KB) appended by IMAP clients.
- ExpungedMessages--Number of messages expunged by IMAP clients.