

Sun Java™ System Messaging Server Release Notes

Version 6 2004Q2

Part Number 817-6363-10

These Release Notes contain important information available at the time of release of Sun Java System Messaging Server 6 2004Q2. New features and enhancements, known issues and limitations, and other information are addressed here. Read this document before you begin using Messaging Server 6.

The most up-to-date version of these release notes can be found at the Sun Java System documentation web site: http://docs.sun.com/coll/MessagingServer_04q2. Check the web site prior to installing and setting up your software and then periodically thereafter to view the most up-to-date release notes and product documentation.

These release notes contain the following sections:

- [About Messaging Server 6 2004Q2](#)
- [What's New in This Release](#)
- [Requirements](#)
- [Important Information](#)
- [Known Issues and Limitations](#)
- [Communications Express](#)
- [How to Report Problems and Provide Feedback](#)
- [Additional Sun Resources](#)

Third-party URLs are referenced in this document and provide additional, related information.

NOTE Sun is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

About Messaging Server 6 2004Q2

Messaging Server is a high-performance, highly secure messaging platform that can scale from thousands to millions of users. It provides extensive security features that help ensure the integrity of communications through user authentication, session encryption, and the appropriate content filtering to prevent spam and viruses. With Messaging Server, enterprises and service providers can provide secure, reliable messaging services for entire communities of employees, partners, and customers.

Messaging Server provides a powerful and flexible solution to the email needs of enterprises and messaging hosts of all sizes by using open Internet standards.

This section includes:

- [What's New in This Release](#)
- [Requirements](#)

What's New in This Release

This section includes the following topics:

- [Installation Changes](#)
- [New Features](#)
- [Deprecated Features](#)

Installation Changes

The *Messaging Server Installation Guide* has been discontinued.

If you are installing Messaging Server 6 2004Q2 for the first time, see the *Sun Java™ Enterprise System Installation Guide* (<http://docs.sun.com/doc/817-5760>) for installation instructions.

If you are upgrading from Messaging Server 6 2003Q4 to Messaging Server 6 2004Q2, see “Chapter 8: Upgrading from Java Enterprise System 2003Q4” in the *Sun Java™ Enterprise System Installation Guide* (<http://docs.sun.com/doc/817-5760>) for upgrade instructions.

If you are migrating from an earlier version of Messaging Server to Messaging Server 6 2004Q2, see the *Sun Java™ System Messaging Server Administration Guide* (<http://docs.sun.com/doc/817-6266>) for upgrade information. If you also intend to migrate your LDAP directory data from Schema 1 to Schema 2, read the *Sun Java™ System Communications Services Schema Migration Guide* (<http://docs.sun.com/doc/817-5701>) before you upgrade Messaging Server. For a summary of the directory-migration feature, see [Schema Migration Utility](#).

New Features

This section describes the following new features added to Messaging Server in this release:

- [Product Renamed](#)
- [New Database Version](#)
- [Communications Express Client Software](#)
- [Spanish Dictionary for Web Clients](#)
- [Schema Migration Utility](#)
- [Message Store Enhancements](#)
- [MTA Enhancements](#)

Product Renamed

Beginning with the 6 2004Q2 release, Sun ONE Messaging Server has been renamed Sun Java™ System Messaging Server.

New Database Version

The Messaging Server 6 2004Q2 release uses Sleepycat Berkeley DB version 4.2.

When you apply the upgrade patch to upgrade from Messaging Server 6 2003Q4 to version 6 2004Q2, the patch automatically upgrades the Berkeley DB from version 3.2.9 to version 4.2.

NOTE This note applies to users upgrading from a previous version of Messaging Server to Messaging Server 6 2004Q2.

After you start Messaging Server 6 2004Q2 and the Messaging Server software first updates the data, you cannot revert to a previous version of the Berkeley DB (such as version 3.2.9).

Communications Express Client Software

Messaging Server currently supports two client user interfaces (UI):

- Messenger Express
- Sun Java™ System Communications Express.

Communications Express is new for this release. Going forward, no new features will be added to the Messenger Express user interface. It has been deprecated in favor of the new Communications Express user interface. Sun Microsystems, Inc. will announce an end-of-life timeline for Messenger Express at a future date.

The installation scenario for Communications Express is different depending on how you are installing Messaging Server. There are two scenarios:

- If you are using the Sun Java Enterprise Server installer to install Messaging Server (this is a fresh install, not an upgrade), select Communications Express in the installation program panel along with Messaging Server. This is necessary because Communications Express is a separately selectable component, rather than being installed automatically with Messaging Server.
- If you already have Messaging Server 6 2003Q4 installed, upgrade to Messaging Server 6 2004Q2 using the patchadd process. After you have upgraded your Messaging Server to 2004Q2, use the Sun Java Enterprise System installer to install the Communications Express component.

Both Messaging Server and Communications Express have separate configuration programs that must be run after installation is complete.

For further release note information on this new UI, see

- [Communications Express](#).

In addition, Communications Express offers its own administration, deployment and customization guides, and online help. For a complete list of Communications Express documentation, see Messaging Server 6 2004Q2 Documentation.

Spanish Dictionary for Web Clients

A Spanish dictionary is available for the Messaging Server client user-interfaces, Communications Express and Messenger Express. You can use this feature to spell-check messages in Spanish.

Schema Migration Utility

The new Schema Migration Utility, `commdirmig`, migrates LDAP directory data from Sun Java™ System LDAP Schema 1 (Schema 1) to Sun Java™ System LDAP Schema 2 (Schema 2).

Messaging Server 6 2004Q2 can be configured to use Schema 1 or Schema 2. The Schema Migration Utility provides Messaging Server the following benefits:

- Integration with Sun Java™ System Identity Server, which provides single sign-on (SSO)
- Use of the User Management Utility, `commadmin`, for provisioning the LDAP directory
- Use of a single integrated Directory Information Tree (DIT) for all Sun Java™ Enterprise System products

The Schema Migration Utility performs the following tasks:

- Converts the two-tree DIT structure to a one-tree structure.
- Adds Identity Server object classes, attributes, and ACIs to the domain and user entries. These attributes enable Identity Server to perform single sign-on (SSO) authentication against the LDAP entries.

For information about using the utility to migrate LDAP directory data from Schema 1 to Schema 2, see the *Sun Java™ System Communications Services Schema Migration Guide* (<http://docs.sun.com/doc/817-5701>).

Administration Console

In this release, Messaging Server Administration Console is i18n compliant.

Message Store Enhancements

New Message Store features include the following:

- The `mkbackupdir` utility can now run an `imsasm` script (directive) on each host in a clustered HA deployment. For example, if a deployment clusters the application on two physical hosts, each host can run a separate instance of the `imsasm` script. Each instance of `imsasm` then creates and interprets the data stream for the part of the directory residing on the local host.

The `-a <asm>` option has been added to the `mkbackupdir` utility. `<asm>` specifies the name of the `imsasm` script.

- The `mkbackupdir` utility can perform as a multithreaded process, improving its performance. The `-t <threadnumber>` option has been added to `mkbackupdir`, where *threadnumber* is the number of threads running.
- The `imexpire` utility has a `-v` option that displays maximum (verbose) logging details.
- The `imexpire` utility allows you to specify message-level and mailbox-level logging. The `-v` option allows you to log when old messages are to be removed from the message store for each mailbox or for each message.

- Session locking has been added to the `imexpire` utility.
- The `imquotacheck` utility logs an error when an invalid domain is specified with the `-d` option. Also, if you specify both the `-i` and the `-d` option, `imquotacheck` ignores the `-i` option.
- The `-r` option has been added to the `stored` utility. This option removes old tmp db files.
- Log maintenance and a timestamp have been added to the watcher daemon.
- A debug option has been added to the `imsched` utility.
- The event notification port daemon (`enpd`) can be configured to listen to different port addresses, allowing you to run multiple instances of the `enpd`.

MTA Enhancements

New MTA features include the following:

- Messaging Server no longer replaces the `sendmail` binary when you upgrade or install Messaging Server. For details, see “Handling `sendmail` Clients” in Chapter 1, “Post-install Tasks and Layout” in the *Sun Java System Messaging Server Administration Guide* (<http://docs.sun.com/doc/817-6266>).
- Support for the Windows-125x character set (charset) has been added to Messaging Server.
- Envelope originator and recipient information is provided as `x-envelope-from` and `x-envelope-to` when a file containing the outer message header is requested by a regular conversion entry.
- A nonstandard refuse sieve action has been added.

This action can only be used in system-level sieve scripts. A single string argument is required. If used, this action causes the current message to be immediately rejected at the SMTP level. The string argument is returned as the error string in SMTP. Refuse is incompatible with all other sieve actions except for `discard`.

- If an error occurs in a sieve filter, the sieve owner is notified that the sieve is broken. If it is not a user sieve, the appropriate postmaster is notified of the failure. The incoming mail is filed in the user's inbox. In previous versions of Messaging Server (5.x and earlier), messages were rejected when an error occurred in a sieve filter. (4742425)
- The maximum length of an official host name in the channel table has been increased from 40 to 128 characters.
- Support has been added to the PMDF and SIMS APIs to allow tracking of intermediate addresses. This makes it possible for the `ims-ms` to use sensible addresses in DSNs rather than the internal final addressing forms the `ims-master` channel program requires.

- The "+" subaddress substitution mechanism has always worked with catchall addresses in direct LDAP mode, but the string that was substitute was the subaddress only, not the entire localpart. This has been changed so the entire local part of the original address will be plugged into the catchall address as a subaddress when this construct is used. For example, given an address of the form "foo+bar@domain.com", no local user foo in the domain.com domain, and a catchall address for domain.com of "bletch+*@example.com", the resulting address will now be "bletch+foo+bar@example.com". It used to be "bletch+bar@example.com".
- Support has been added to the low-level logging and message dequeue code to track intermediate addresses. This provides the means for success DSNs to use sensible addresses in DSNs rather than channel-specific private final addressing forms.
- It is now possible to perform the equivalent of a sieve spamadjust operation from the FROM_ACCESS, MAIL_ACCESS, SEND_ACCESS, ORIG_SEND_ACCESS, and ORIG_MAIL_ACCESS mappings. The \$, metacharacter causes an argument to be read from the mapping just prior to any \$N/\$F argument. The argument takes the same form as a spamadjust argument. Note that also some of these mappings are applied on a per-recipient basis any spamadjust operation that is done applies to all recipients. (This is done to allow for tests to see if one of the recipients is a honeypot address.)
- Additional diagnostic detail has been added to SMTP responses that result from failed ETRN commands.
- imsimta cnbuild can handle very large system sieves (RFE 4970618).
- The :copy sieve extension has been implemented.
- The MTA's address rewriting logic has been changed to handle alias expansion errors better. More specifically, address failures in a group or alias that does not override the envelope from would be silently ignored as long as at least one address in the group or alias was valid. The MTA has been changed so that such failures are now reported to the group or alias. A side effect of this change is that groups or aliases that do not contain any valid addresses will not be reported as such and not simply as an invalid address.
- If the SMTP server cannot read the options file or finds an options-file syntax error, the channel program aborts and an error message is written to the log. (4958384)
- New ACCESS_ORCPT MTA option (possible values 1 or 0):
 - Setting the value to 1 adds another vertical bar delimited field to the probe value that is passed to the SEND_ACCESS, ORIG_SEND_ACCESS, MAIL_ACCESS, and ORIG_MAIL_ACCESS mappings containing the original recipient (ORCPT) address.
 - If the message does not have an ORCPT address the original, unmodified RCPT TO address is used instead.

- New `MAX_SIEVE_LIST_SIZE` MTA option: Specify an integer value (*default is 64*) to control how many strings can appear in a list construct in MTA sieve scripts.

NOTE Previously, this MTA option was called `MAX_LIST_SIZE`. The old name was changed because it might be construed as having something to do with mailing lists.

- Enhanced Q log entries to contain additional information about the error(s) causing the entry to be made. (4539521)
- MTA `DELIVERY_OPTIONS` option now supports two new prefix characters:
 - **# (sharp)**: Indicates that the following entry is mailhost-independent, which lets MTA check whether all of a given user's or group's delivery options are independent of the mailhost. If this condition is satisfied, MTA can act on the entry immediately rather than having to forward the message to the mailhost.
 - **/ (slash)**: Causes all addresses produced by the current delivery option to be held, which means the recipient addresses will end up in message files with a `.HELD` extension.

In addition, the `DELIVERY_OPTIONS` default value was updated so the `FORWARD` delivery method is marked as mailhost independent. (4622206)

- New `NOTARY_DECODE` MTA option (4629743): Specify one of the following values
 - **1**: Causes a subset of the original message headers (that are added to the first part of a DSN by the `%H` substitution) to be decoded and converted to match the charset of the first part.

NOTE Use this setting with caution because you can lose information and confusion can result when you convert a rich charset like UTF-8 to a limited charset like ISO-8859-1 or US-ASCII.

- **0 (Default)**: Decodes a subset of encoded-words in the header that match the charset of the first part; no charset conversion is done.
- **-1**: Disables decoding of encoded-words unconditionally.
- A new facility provides the ability to retarget messages that exceed a specified limit for number of recipients, message size, or message lines to an alternate destination channel.

This facility is implemented as a set of new channel keywords (see the following list), which can be placed on any destination channel:

Table 1 New Channel Keywords

Keyword	Description	Default Limits
alternatechannel	Takes a single argument specifying an alternate channel name to use.	Infinite
alternateblocklimit alternatelinelimit alternaterecipientlimit	Accept an integer argument specifying a corresponding threshold.	Infinite

A message that exceeds any of these thresholds will be enqueued to the alternate channel instead of the original destination channel.

- Setting the `LDAP_HOST`, `LDAP_USERNAME`, `LDAP_PASSWORD`, and `LDAP_PORT` MTA options overrides the MTA's use of the `local.ugldaphost`, `local.ugldapbinddn`, `local.ugldapbindcred`, and `local.ugldapport` configutil parameters (respectively) in accessing the LDAP directory server. (4537015)
- Setting the `LINES_TO_RETURN` MTA option to 0 disables partial content return, and instead returns only the message part headers.
- The MTA now checks for 8-bit characters in the local parts of addresses (as well as the received fields it constructs) and replaces those characters with asterisks. (4694916)
- The MTA now creates J records in the log file when a `MAIL FROM` command fails for an administrative reason. J records were previously created only when the failure occurred at the `RCPT TO`.
- The `ALIAS_ENTRY_CACHE_NEGATIVE` option was expanded to work in the general case where no matching LDAP entries are found. Previously this option only worked when a `NO_SUCH_OBJECT` LDAP error was returned.
- The various priority overrides based on size channel keywords (such as `urgentblocklimit`, `normalblocklimit`, and `nonurgentblocklimit`) are now effective for conversion or defragment channels — even when that channel is used implicitly. Previously these keywords only worked when the channel was explicitly included in the message routing.
- New `CACHE_DEBUG` MTA option (Boolean valued 0, 1): Setting this option to 1 tells various MTA components to dump information about the domain, alias, and reverse caches just prior to exiting. (4668998)
- The default value for the `ALLOW_RECIPIENTS_PER_TRANSACTION` TCP channel option was changed from infinite to 128.
- The default value for the `DISABLE_SEND` TCP channel option was changed from 0 (false) to 1 (true).

- The default value for the `HEADER_LIMIT` MTA option was changed from infinite to 2000 (blocks).
- The `REJECT_RECIPIENTS_PER_TRANSACTION` TCP channel option now applies to the `SMTP VRFY` command as well as `RCPT TO`.
- New `HEADER_LIMIT` MTA option: Imposes a limit on the maximum size the primary (outermost) message header can attain. Primary message headers are silently truncated when they reach the specified limit.
- Operations on content type and content disposition parameters no longer invert the order in which the parameters appear.
- New `-[no]reprocessing` qualifier was added to the `imsimta test -rewrite` command to control whether `rewrite_test` acts as if it were the reprocessing channel. In particular, this switch affects whether deferred list expansion is done. Normally, deferred list expansion should be done, so this switch defaults to *on*. Use `-noreprocessing` to disable expansion.
- New `ROUTE_TO_ROUTING_HOST` MTA option (Possible values are 0 or 1):
 - 0 (*Default*): Causes the domain to be treated as non-local when a failure to match an extant `mailRoutingHosts` attribute causes the domain to be treated as non-local; addresses simply will be routed onward according to the rewrite rules. This was the only behavior available in Messaging Server 5.2.
 - 1: Tells Messaging Server to route all addresses associated with the domain to the first host listed in the `mailRoutingHosts` attribute.
- New `LOG_FILTER` MTA option (*Default is 0*): Specify 1 to write the list of active filters enclosed by single quotes into enqueue (E) records in the log file just prior to the diagnostics field. (4672405)
- New `rejectsmtpplonglines` keyword: Adds the option of rejecting messages that contain lines longer than the 1000 characters (including CRLF) allowed by SMTP.

Other options in this area include `wrapsmtplonglines`, which wraps overly long lines and `truncatesmtplonglines`, which truncates overly long lines. (4619953)

NOTE The last two options were available in Messaging Server 5.2, but they were called `wrapsmtp` and `truncatesmtp` respectively. The shorter names are now deprecated, although Messaging Server 6.0 will continue to accept them.

- New `parameterlengthlimit` and `nameparameterlengthlimit` channel keywords (4614439):
 - `parameterlengthlimit` (*Default is 1024*): Controls the points at which general content-type and content-disposition parameters are truncated.

- o **nameparameterlengthlimit** (*Default is 128*): Controls the points at which the `name` content-type and the `filename` content-disposition parameters are truncated.
- New facility for testing sieve scripts is provided as part of Messaging Server.

To activate this facility, use `imsimta test -exp -mm -message=<message-file>`.

Where `<message-file>` is a text file containing the RFC 822 message you want to test against.

NOTE You must use an RFC 822 message only; do not use a queue file.

Table 2 Additional Qualifiers for Testing Sieve Scripts

Qualifier	Description
<code>block</code>	Treats the entire input as a single sieve script. (<i>Default treats each line as a separate script</i>)
<code>from=<addr></code>	Specifies the envelope from address to be used in envelope tests. (<i>Default is the value specified by the RETURN_ADDRESS MTA option.</i>)
<code>input=<file></code>	Reads the input sieve from <code><file></code> . (<i>Default reads test script lines or script blocks from stdin.</i>)
<code>output=<file></code>	Writes results to <code><file></code> . (<i>Default writes script evaluation results to stdout.</i>)

- New MTA options enable you to configure text strings returned by the MTA (*4720378*).

The following table lists these new options and the text strings they override:

New Option	Default Strings the Option Overrides
<code>MISSING_RECIPIENT_GROUP_TEXT</code>	"recipients not specified"
<code>ERROR_TEXT_UNKNOWN_HOST</code>	"unknown host or domain"
<code>ERROR_TEXT_UNKNOWN_USER</code>	"unknown or illegal user"
<code>ERROR_TEXT_UNKNOWN_ALIAS</code>	"unknown or illegal alias"
<code>ERROR_TEXT_ACCESS_FAILURE</code>	"you are not allowed to use this address"
<code>ERROR_TEXT_ALIAS_LOCKED</code>	"list is currently reserved and locked"
<code>ERROR_TEXT_ALIAS_AUTH</code>	"you are not allowed to use this list"
<code>ERROR_TEXT_ALIAS_FILEERROR</code>	"error opening file/URL referenced by alias"
<code>ERROR_TEXT_ALIAS_FILEEXIST</code>	"nonexistent file referenced by alias"
<code>ERROR_TEXT_ALIAS_TEMP</code>	"temporary error returned by alias expansion"
<code>ERROR_TEXT_SEND_REMOTE_ERROR</code>	"no protocol to SEND/SAML"
<code>ERROR_TEXT_SEND_UNKNOWN_ERROR</code>	"do not know how to SEND/SAML"

ERROR_TEXT_BLOCK_OVER	"channel size limit exceeded"
ERROR_TEXT_LINE_OVER	"channel line limit exceeded"
ERROR_TEXT_LIST_BLOCK_OVER	"list size limit exceeded"
ERROR_TEXT_LIST_LINE_OVER	"list line limit exceeded"
ERROR_TEXT_SIEVE_ACCESS	"filter access error"
ERROR_TEXT_SIEVE_SYNTAX	"filter syntax error"
ERROR_TEXT_DISABLED_USER	"user disabled; cannot receive new mail"
ERROR_TEXT_DISABLED_ALIAS	"alias disabled; cannot receive new mail"
ERROR_TEXT_OVER_QUOTA	"user over quota; cannot receive new mail"
ERROR_TEXT_TEMPORARY_FAILURE	"unknown host or domain"
ERROR_TEXT_PERMANENT_FAILURE	"unknown host or domain"
ERROR_TEXT_RECEIPT_IT	"message accepted for list expansion processing"
ERROR_TEXT_INACTIVE_USER	"mailbox temporarily disabled"
ERROR_TEXT_INACTIVE_GROUP	"group temporarily disabled"
ERROR_TEXT_DELETED_USER	"recipient no longer on server"
ERROR_TEXT_DELETED_GROUP	"group no longer on server"
ERROR_TEXT_DUPLICATE_ADDR	"duplicate/ambiguous directory match"
ERROR_TEXT_BRIGHTMAIL_ERROR	"error in Brightmail"

- New `USE_PERMANENT_ERRORS` MTA option (*Default is 0*): Controls whether or not certain errors returned by the MTA are marked as temporary or permanent. Each bit in this option corresponds to a specific error condition and; when set, instructs the MTA to return a permanent error.

The following table lists the `USE_PERMANENT_ERRORS` defined bits:

Table 3 `USE_PERMANENT_ERRORS` Defined Bits

Position	Value	Error
0	1	mailbox temporarily disabled (inactive)
1	2	group temporarily disabled (inactive)
2	4	user over quota; cannot receive new mail
3	8	various alias expansion errors

- MTA now generates message disposition notifications (MDNs) per RFC 2298 in addition to producing delivery status notifications (DSNs) per RFCs 3461-3464 (which MTA could do previously).

MDNs are now used for reject actions in user sieve definitions. An additional mapping was defined to support internationalization of MDNs. This mapping (called the *DISPOSITION_LANGUAGE mapping*) parallels the `notification_language` mapping used to internationalize DSNs. Probes to this mapping take the following form:

```
type|modifiers|source-channel|header-language|return|recipient
```

Where:

- **type** is disposition type, which can be one of the following: `displayed`, `dispatched`, `processed`, `deleted`, `denied`, or `failed`.
- **modifiers** is a comma-separated list of disposition modifiers. The current list is: `error`, `warning`, `superseded`, and `expired`.
- **source-channel** is the source channel producing the MDN.
- **header-language** is the language specified in one of the following: `accept-language`, `preferred-language`, or `x-accept-language`. (MTA uses the first option present.)
- **return** is the address to which the notification is being returned.
- **recipient** is the address that the disposition is about.

The result of the disposition mapping consists of two or three pieces of information separated by vertical bars (`|`). The first piece of information is the directory where the template files for the disposition notification can be found. The second piece of information is the character set into which the standalone disposition text should be forced. (This information is required because some dispositions — notably the dispositions produced by `autoreply echo` or the use of the `:mime` parameter to the `vacation` sieve action — do not employ template files and consequently, cannot inherit the character set from those files.) Finally, the third piece of information is an override subject line for the notification. This information is only used if the `$T` flag is also set by the mapping.

The following additional template files are used to construct MDNs:

- `disposition_deleted.txt` `disposition_failed.txt`
- `disposition_denied.txt` `disposition_prefix.txt`
- `disposition_dispatched.txt` `disposition_processed.txt`
- `disposition_displayed.txt` `disposition_suffix.txt`
- `disposition_option.opt`

Using these template files parallels the use of various `return_*.txt` files for DSNs. (4662616)

- New `imsimta cache -walk -debug=xxx` MTA command: Causes the job controller to write its current state to its log file and/or sets the job controller debug mask to a specified value.
- The default value for the `threaddepth` channel keyword changed from 128 to 10 — resulting from escalations where the common answer was to set `threaddepth` to 10.
- The number of spare LDAP attributes available for substitution in direct LDAP was raised from 2 to 5. `$_nE` or `$_nG` substitutes the *n*th spare. `$_E` subs the first spare and `$_G` subs the second for backwards compatibility.
- The `$_=` metacharacter sequence was added to the set of `$_\ $^, $_` format selector sequences that are available in mappings and rewrite rules. When selected, `$_=` specifies that subsequent substituted characters are to undergo quoting appropriate for insertion into LDAP search filters.
- Symbol substitutions into conversion and character set conversion parameter values (such as `out-dparameter-name-0`) are allowed from the content-type parameter but not from the content-disposition parameter list, which seemed unnecessarily restrictive. Consequently, the ability to substitute things from the content-disposition parameter list was enabled.
- The conversion channel program now defines the following, additional environment symbols:

Table 4 New Environment Symbols

Symbol	Description
<code>PART_SIZE</code>	Size in bytes of the part being processed.
<code>PART_NUMBER</code>	Part number of the current part. (Uses the same format as the <code>PART-NUMBER</code> conversion match parameter.)
<code>ATTACHMENT-NUMBER</code>	Attachment number of the current part. (Uses the same format as the <code>ATTACHMENT-NUMBER</code> conversion match parameter.)
<code>INPUT_CHANNEL</code>	Channel that enqueued the message to the conversion channel. (Corresponds to the <code>IN-CHANNEL</code> conversion match parameter.)
<code>OUTPUT_CHANNEL</code>	Channel to which the message is headed. (Corresponds to the <code>OUT-CHANNEL</code> conversion match parameter.)
<code>CONVERSION_TAG</code>	Current list of active conversion tags. (Corresponds to the <code>TAG</code> conversion match parameter.)

- The `$_nX` metacharacter sequence was added to the MTA's URL template facility. Use `$_nX` to insert the *n*th component of the mailhost. If you omit *n*, the entire mailhost will be inserted.

- The `$nA` metacharacter sequence was added to the MTA's URL template facility. Use `$nA` to insert the *n*th character of the current address. If you omit *n*, the entire address will be inserted.
- New `LDAP_MAX_CONNECTIONS` MTA option (*Default is 1024*): Limits the number of LDAP connections the MTA users can make to the LDAP pool.
- New `logheader` channel keyword (Accepts an integer argument): Overrides the `LOG_HEADER` MTA option on a per-channel basis.
- Messaging Server now checks the `local.imta.schematag configutil` option value or the `LDAP_SCHEMATAG` MTA option value to insure each specified schema name is valid.
- New `personalmap` channel keyword: Added to the `personalinc/ personalomit/ personalstrip` keyword set. If enabled, `personalmap` causes a probe to the `PERSONAL_NAMES` mapping in the general form:

```
name|address
```

Where:

- `name` is the current personal name.
- `address` is the corresponding address.

Additionally, following flags may be set:

- `$I flag`: Set initially if the material is a message ID rather than an address.
- `$R flag`: Set if this is from a "backward pointing" header.
- `$F flag`: Set if this is from a "forward pointing" header.
- `$Y or $T flags`: If an entry matches and sets one of these flags, the mapping result replaces the original personal name.
- New `authrewrite` channel keyword and associated `auth_rewrite` mapping: Added to facilitate modification of header and envelope addresses using addressing information obtained from authentication operations.

The `authrewrite` keyword takes a single integer argument, and possible values are:

- `0`: Does not change anything (*Default*)
- `1`: Adds a `Sender:` or a `Resent-sender:` header field containing the address provided by the authentication operation. The `Resent-` variant is used if other `resent-` fields are present.
- `2`: Adds a `Sender:` header field containing the address provided by the authentication operation.

- **3:** Constructs a probe of the following form `mail-from|sender|from|auth-sender`.

Where:

- **mail-from** is the envelope from address.
- **sender** is the address from the `Sender:` or `Resent-sender:` header field.
- **from** is the address from the `From:` or `Resent-From:` header field.
- **auth-sender** is the address provided by the authentication operation.

The result is run through the `auth_rewrite` mapping, which should return a list of items separated by vertical bars (`|`). These items are consumed (in order) by setting the following flags:

- **\$J or \$K:** Replaces the envelope `from` address for the message.
 - **\$Y or \$T:** Adds an appropriate `Sender:` or `Resent-sender:` header field.
 - **\$Z:** Adds an appropriate `From:` or `Resent-from:` header field. The `Resent-` variants are used if other `resent-` fields are present in the header.
- **4:** Same as 3 except the `resent-` variables are never used.
- The default use for `identnolimited` was changed to `identnonenumeric` in newly generated configurations. The new default avoids DNS lookups out of the box.
 - The `$K` metacharacter was added to the URL determination machinery: Substitutes a search filter that checks the `objectclass` to see if it matches the current criteria established for users or groups. Using this metacharacter in the `REVERSE_URL` MTA option prevents spurious matches against entries such as personal address book entries.
 - The configuration created initially now includes three new entries in the `ORIG_SEND_ACCESS` mapping table. These entries block “external” submission of explicitly source-routed addresses to the `tcp_intranet` channel in an attempt to block relaying “through” “internal” systems. In other words, the entries prevent relay attempts that try to evade normal relay blocking by explicitly source-routing through one or more internal systems.

In addition, the `dequeue_removeoute` channel keyword was added to the `tcp_intranet` channel definition so that “front line” and “back end” system configurations can be uniform. Use this keyword to prevent back end systems from being presented with `@mailhost:user@host` sorts of source-routed addresses by front line systems, thus reducing the need to be certain that back end systems have been properly configured to recognize IP addresses of the front line systems as internal.

Note, however, that this use of `dequeue_removeoute` does imply that back end systems are expected to do message routing (e.g., LDAP lookups) themselves.

- The `USE_ERRORS_TO` and `USE_WARNINGS_TO` MTA options were removed (along with the code to support them) because these options were grossly noncompliant with standards.
- Setting the `mailDomainStatus` attribute to *unused* for a domain tells MTA to ignore the domain entirely.
- The `$(` metacharacter was added to the following access mappings:
 - `ORIG_SEND_ACCESS`
 - `SEND_ACCESS`
 - `ORIG_MAIL_ACCESS`
 - `MAIL_ACCESS`
 - `FROM_ACCESS`

The `$(` metacharacter reads a value from the mapping result and treats it as a set of conversion tags to be applied to the current or, in the case of `FROM_ACCESS`, all recipient(s). `$(` is positioned after `$(` (header addression) in the sequence of arguments read from the mappings.

- The `jettison` sieve action was added to Messaging Server sieve implementation.

`jettison` is similar to `discard` in that it causes messages to be silently discarded. The difference between `jettison` and `discard` is that `discard` does nothing but cancel the implicit `keep`, while `jettison` forces a `discard` to be performed. This behavioral difference is relevant only when multiple sieves are involved. For example, a system-level `discard` can be overridden by a user sieve explicitly specifying `keep`, whereas a system-level `jettison` will override anything done by a user sieve.
- The `$(` metacharacter was added to the following access mappings:
 - `ORIG_SEND_ACCESS`
 - `SEND_ACCESS`
 - `ORIG_MAIL_ACCESS`
 - `MAIL_ACCESS`
 - `FROM_ACCESS`

Using `$(` causes a forced `jettison` to be performed for the all recipient(s).

- Support for RFC 3431, the sieve relational extension, was added to Messaging Server.
- The following new MTA options were added to support Schema 2:
 - `LDAP_SCHEMALEVEL`: Integer value specifying schema level to support.

- 1 = Schema 1 (*Default*)
- 2 = Schema 2
- **LDAP_DOMAIN_FILTER_SCHEMA1** (*Default is (/objectclass=inetDomain)(objectclass=inetdomainalias)*): String specifying filter used to identify Schema 1 domains.
- **LDAP_DOMAIN_FILTER_SCHEMA2** (*Default is an empty string*): String specifying additional filter elements used to identify Schema 2 domains.
- **LDAP_ATTR_DOMAIN1_SCHEMA2** (*Default is sunPreferredDomain*): String specifying attribute used to store the primary domain in Schema 2.
- **LDAP_ATTR_DOMAIN2_SCHEMA2** (*Default is associatedDomain*): String specifying attribute used to store any secondary domains in Schema 2.
- **LDAP_GLOBAL_CONFIG_TEMPLATES** (*Default is an empty string*): String specifying DN where global configuration templates can be found.

CAUTION The `LDAP_GLOBAL_CONFIG_TEMPLATES` attribute should never be used under normal circumstances. Using this attribute to specify an unusual search scheme can result in domain inconsistencies and other problems.

- **LDAP_ATTR_DOMAIN_SEARCH_FILTER** (*Default is inetDomainSearchFilter*): String specifying attribute in the global configuration template area that is used to store the domain search filter template.

NOTE The `LDAP_DOMAIN_FILTER` MTA option is now obsolete and was removed.

- A new facility was added to store information that previously went into the general, forward, and reverse databases into the compiled configuration instead.

A new `USE_TEXT_DATABASES` MTA option was added to control this capability. This option is bit encoded.

- Set bit 0 (value 1) to read the `IMTA_TABLE:general.txt` file as the MTA configuration is initialized and use the information from the `IMTA_TABLE:general.txt` file to replace all uses of the general database.
- Set bit 1 (value 2) to read the `IMTA_TABLE:reverse.txt` file and use the information from this file instead of the reverse database.

- Set bit 2 (value 4) to read the `IMTA_TABLE:forward.txt` file and use the information from this file instead of the forward database.
- A new `overquota` status value was added to the list of possible mail user and mail domain statuses. When set, this new value generates a “user is over quota” error.

NOTE You can use the `USE_PERMANENT_ERRORS` MTA option (described on page 12) to control whether this is a temporary or permanent failure.

- The capability to access per-domain attributes was added to the MTA mapping facility.

The mapping facility uses a metacharacter sequence of the form `$}domain,attribute{`

Where:

- `domain` is the domain in question.
- `attribute` is the attribute associated with the domain.

If the domain exists and has the attribute, its initial value is substituted into the mapping result. However, if either the attribute or the domain does not exist, the mapping entry fails.

- `IMTA_LANG:return_option.opt` (DSN) files and `IMTA_LANG:disposition_option.opt` files can be created to customize translated DSNs and to provide translated Subject: lines for MDNs.

These files can make the internationalization of generated notices more flexible, and they support the following options:

- **RETURN_PERSONAL** (DSN and MDN): Override for the `personal name` field to be used in conjunction with the `From:` field. This field should be RFC 2047 encoded.
- **SUBJECT** (DSN and MDN): Override for the `Subject:` field. This value is used only if the notification did not provide a subject field of its own. This field should be UTF-8 encoded.
- **RECIPIENT_ADDRESS** (DSN): Override for the `Recipient address: text` used in the construction of the per-recipient section in the first part of a DSN. This field should be specified in the same charset that is used for the first part of the DSN.
- **ORIGINAL_ADDRESS** (DSN): Override for the `Original address: text` used in the construction of the per-recipient section in the first part of a DSN. This field should be specified in the same charset that is used for the first part of the DSN.
- **REASON** (DSN): Override for the `Reason:` text used in the construction of the per-recipient section in the first part of a DSN. This field should be specified in the same charset that is used for the first part of the DSN.

- **DIAGNOSTIC_CODE** (DSN): Override for the `Diagnostic code: text` used in the construction of the per-recipient section in the first part of a DSN. This field should be specified in the same charset that is used for the first part of the DSN.
- **TEXT_CHARSET** (MDN): Charset text for the first part and subject of the MDN should be converted to `n.n.n` (DSN).

When constructing the per-recipient part of a DSN, a check is made to see if there is an option whose name matches the numeric per-recipient status. If there is a match, the corresponding text will be inserted into the DSN. Additionally, if the `REASON` option (described above) produces a zero length result, the `REASON` field will not be inserted.

- **HOUR** (DSN): Text to insert for a `%U` or `%u` substitution when `RETURN_UNITS=1` is set. Note that there is no distinction made between `%U` and `%u` (unlike the default case where English “Hour” or “hour” (respectively) would be substituted).
- **DAY** (DSN): Text to insert for a `%U` or `%u` substitution when `RETURN_UNITS=0` (*Default*) is set. Note that no distinction is made between `%U` and `%u` (unlike the default case where English “Day” or “day” (respectively) would be substituted).
- Charset-conversion mapping was extended to provide several additional capabilities:
 - Specify the `IN-CHARSET` option in the output template of a mapping entry to override the charset specified in the encoded-word. Use the `IN-CHARSET` option to set the input charset to `*`, and the charset will be “sniffed” to determine an appropriate label.
 - Specify the `RELABEL-ONLY` option that accepts the following integer values:
 - `1`: `OUT-CHARSET` simply replaces the `IN-CHARSET`.
 - `0`: No relabeling is done.
- New `552_permanent_error_string` SMTP option (goes into the relevant `tcp_*_option` file): Determines if a 552 response should be treated as a permanent error.

Normally (per RFC 2821), 552 responses are treated as if they were 4xx responses and temporary in nature. Some older SMTP servers use the 552 response to indicate a permanent error, so this new SMTP option was added to allow for this behavior.

When a 552 response is received, the text associated with it (including any `xx.xx.xx` extended error code, but excluding any leading spaces) is compared with the value of the `552_permanent_error_string` option. If, and only if, the text matches, the response will be treated as permanent. Otherwise, response will be treated as a retryable error.

- The `ims-ms` channels now support the `master_debug` channel keyword, which is interpreted as equivalent to setting the `DEBUG=4` channel option.
- The `imsimta restart` and `imsimta shutdown` commands now accept Dispatcher services as valid arguments.

For example, `imsimta restart smtp` will restart only the SMTP service (as defined in the Dispatcher configuration). Note that you can only restart a Dispatcher service that is currently running. If you do `imsimta shutdown smtp`, you must restart the Dispatcher to start the SMTP service again.

- The default value for the `MISSING_RECIPIENT_POLICY` MTA option was changed from `1` (do not do anything about illegal headers if they do not contain a `To:`, `Cc:`, or `Bcc:` field) to `0` (add a `To:` field to these headers to make them legal) for consistency and best practice policies.
- Transport and application information strings set by SMTP will be carried through the reprocess channel.
- The `[auth_channel]` and `[cant_channel]` nonpositional alias parameters now accept a list of channel patterns separated by spaces.
- New `disabled` status value was added to the list of possible mail user, mail group, and mail domain statuses. Setting this value generates a `user/group is disabled` permanent failure.
- MTA now caches URL results from look-ups done in rewrite rules and mappings. This new URL result cache is controlled by two new MTA options:
 - `URL_RESULT_CACHE_SIZE` (Default is 10000 entries)
 - `URL_RESULT_CACHE_TIMEOUT` (Default is 600 seconds)
- Asynchronous LDAP look-ups support was added to MTA. Asynchronous look-ups avoid the need to store an entire large LDAP result in memory, which in some cases seems to cause performance problems.

A new `LDAP_USE_ASYNC` MTA option (Bit-encoded value. *Default is 0*): Controls how asynchronous LDAP look-ups are used. Each bit (if set) enables using asynchronous LDAP look-ups with a specific use of LDAP within MTA. The following bits are defined:

Table 5 LDAP_USE_ASYNC Bits

Bit	Value	Description
0	(value 1)	LDAP_GROUP_URL1 (mgrpDeliverTo) URLs
1	(value 2)	LDAP_GROUP_URL2 (memberURL) URLs
2	(value 4)	LDAP_GROUP_DN (UniqueMember) DNs
3	(value 8)	<code>auth_list</code> , <code>moderator_list</code> , <code>sasl_auth_list</code> , and <code>sasl_moderator_list</code> nonpositional list parameter URLs
4	(value 16)	<code>cant_list</code> , <code>sasl_cant_list</code> nonpositional list parameter URLs
5	(value 32)	<code>originator_reply</code> nonpositional list parameter URLs
6	(value 64)	<code>deferred_list</code> , <code>direct_list</code> , <code>hold_list</code> , <code>nohold_list</code> nonpositional list parameter URLs

Table 5 LDAP_USE_ASYNC Bits

7	(value 128)	username_auth_list, username_moderator_list, username_cant_list nonpositional list parameter URLs
8	(value 256)	alias file list URLs
9	(value 512)	alias database list URLs
10	(value 1024)	LDAP_CANT_URL (mgrpDisallowedBroadcaster) outer level URLs
11	(value 2048)	LDAP_CANT_URL inner level URLs
12	(value 4096)	LDAP_AUTH_URL (mgrpAllowedBroadcaster) inner level URLs
13	(value 8192)	LDAP_AUTH_URL inner level URLs
14	(value 16384)	LDAP_MODERATOR_URL (mgrpModerator) URLs

The `LDAP_USE_ASYNC` default (0) disables asynchronous LDAP lookups in the Messaging Server MTA.

- A facility for per-channel message recipient limits was added to Messaging Server.

Two new channel keywords control this facility (Both accept a single integer argument):

- **recipientlimit**: Limits the total number of recipient addresses that will be accepted for the message to the specified value.
- **recipientcutoff**: Compares the total number of recipients presented to the MTA to the specified value. No messages will be accepted for delivery when the number of recipients exceeds the specified limit.
- New Messaging Server MTA facilities enable you to override personal name information associated with header addresses — without having to use LDAP callouts from the `PERSONAL_NAME` mapping. Specifically, you can set a new `LDAP_PERSONAL_NAME` MTA option to the name of the attribute associated with user LDAP entries containing override personal name information.

Note that if 8-bit characters are present in this attribute's value they will be assumed to be UTF-8 and encoded accordingly. No support is implemented or planned for other charsets. You can use conversions to obtain other charsets if you require them.

- You can now use the `mgrpMsgPrefixText` and `mgrpMsgSuffixText` LDAP attributes to insert prefix or suffix text into messages as they undergo group expansion. These are the default attributes used for this purpose; different attributes can be specified using the `LDAP_PREFIX_TEXT` and `LDAP_SUFFIX` text MTA options, respectively.

You can insert text into initial text/plain parts only. The attribute values are given in UTF-8; which is then converted to match the charset of the part into which the text is inserted.

- Added the `$$` metacharacter to the `FROM_ACCESS` mapping. Using this metacharacter causes an additional vertical bar (`|`) separated argument to be read from the mapping result.

This argument is read from the mapping result after any capture argument is read, and consists of from one to three integer values separated by commas.

- The first value establishes a new minimum `blocklimit` for the transaction.
 - The second value establishes a new minimum `recipientlimit`.
 - The third value establishes a new minimum `recipientcutoff`.
- Support for setting `recipientlimit`, `recipientcutoff`, and `blocklimit` based on sender was added to Messaging Server.

You can use the new `LDAP_RECIPIENTLIMIT`, `LDAP_RECIPIENTCUTOFF`, and `LDAP_SOURCEBLOCKLIMIT` MTA options to specify the names of LDAP attributes, which are then used to obtain this information. None of these options have default values.

- Support for setting `recipientlimit`, `recipientcutoff`, and `blocklimit` based on the sender's domain was added to Messaging Server.

You can use new `LDAP_DOMAIN_ATTR_RECIPIENTLIMIT`, `LDAP_DOMAIN_ATTR_RECIPIENTCUTOFF`, and `LDAP_DOMAIN_ATTR_SOURCEBLOCKLIMIT` MTA options to specify the names of domain attributes which are then queried to obtain this information. None of these options have default values.

- The alias processing machinery now keeps track of any personal name information specified in the attribute named by the `LDAP_PERSONAL_NAME` MTA option, and uses this information to construct `From:` fields for any MDNs or vacation replies generated. (4618559)
- The `REJECT_RECIPIENTS_PER_TRANSACTION` SMTP channel option now can be set usefully to values bigger than the `ALLOW_RECIPIENTS_PER_TRANSACTION` SMTP channel option. Also, the code now tracks attempts to add recipients in addition to tracking successful recipient additions, and uses this value in the `REJECT_RECIPIENTS_PER_TRANSACTION` comparison. (4870897)
- MTA now uses specialized machinery to keep track of whether or not a given address expansion result should be employed in DSNs and MDNs as a final recipient address. In addition, if the result should not be so employed, this machinery tracks the address that should be used.

The semantics of the various sorts of address expansions implemented through LDAP are well-defined and set this information automatically. Entries in alias files and databases, however, do not have such clear semantics and, in practice, are used for multiple purposes. A mechanism to explicitly call for a given expansion address to be hidden has therefore been added. Prefixing an expansion address with a colon causes it not to be used in DSNs and MDNs. The address input to the alias expansion operation will be used instead. An example of an alias file entry that uses this facility is:

```
a: :b@example.com
```

- Some useful flags are now set prior to calling the `FROM_ACCESS`, `SEND_ACCESS`, `MAIL_ACCESS`, `ORIG_SEND_ACCESS`, and `ORIG_MAIL_ACCESS` mappings. These flags are:
 - **\$A**: Set if SASL has been used.
 - **\$T**: Set if TLS has been used.
 - **\$S**: Set if success delivery receipts requested (not available in `FROM_ACCESS`).
 - **\$F**: Set if failure delivery receipts requested (not available in `FROM_ACCESS`).
 - **\$D**: Set if delay delivery receipts requests (not available in `FROM_ACCESS`).
- The application information string supplied to the `FROM_ACCESS`, `MAIL_ACCESS`, and `ORIG_MAIL_ACCESS` mappings now includes the system name claimed in the `HELO/EHLO` SMTP command. This name appears at the end of the string and is separated from the rest of the string (normally "SMTP") by a slash (/). (The claimed system name can be useful in blocking some worms and viruses.)
- New `USE_PERSONAL_NAMES` and `USE_COMMENT_STRINGS` MTA options were added to optionally include source and destination channel information in `PERSONAL_NAMES` and `COMMENT_STRINGS` mapping probes.

Setting either option to bit 0 (value 1) will add the usual `source-channel|destination-channel|` prefix to the corresponding mapping probe.

Note that these new options do not control whether the `PERSONAL_NAMES` or `COMMENT_STRINGS` options are used; the `PERSONAL_NAMES` or `COMMENT_STRINGS` options are controlled by various channel keywords.

- Support for RFC 3598, the sieve subaddress extension, was added to Messaging Server.
- New `LDAP_DOMAIN_TIMEOUT` MTA option (Expressed in seconds. Default is 60 * 15 or 15 minutes.): Controls the retention time for entries in the domain map cache.
- The `FILTER_DISCARD` MTA option used to control whether the `filter_discard` channel was used by the `jettison` sieve action. This control was separated out as a new `FILTER_JETTISON` option. The `FILTER_JETTISON` default is taken from the `FILTER_DISCARD` setting, and `FILTER_DISCARD` in turn defaults to 1 (discards go to the bitbucket channel) as it always has.

- The `$#` sequence number generation mapping and rewrite rule metacharacters now accept a fourth argument: an optional modulus. If you specify this fourth argument `m` the value inserted is the sequence number retrieved from the file `mod m` .
- Per-user conversion tags are now applied before mailhost information is considered, which enables front-end systems to perform user-specific conversion operations (RFE 4906355).
- Previously, the simple presence of a spam filter `optin` attribute in a user entry turned on filtering; and all the value could determine was what sort of filtering would be done. This behavior is not compatible with some directory maintenance tools that always provide the attribute, but assume an “off” or “null” value for the attribute is available that does not enable filtering.

As such, a null value facility was added. The new `SPAMFILTER_NULL_OPTIN` MTA option specifies what value a spam filter `optin` attribute must have to be ignored. (Default is an empty string, which means that by default, if an `optin` attribute is present but empty, the attribute will be ignored.)

- The `LDAP_TIMEOUT` MTA option was added (actually re-enabled; formerly part of PMDF): Sets time-outs for LDAP searches performed by MTA. Note that this option does not affect LDAP searches performed by domain map (either the old or new versions). (*4859069*)
- The `$V` metacharacter was added to following access mappings:
 - `ORIG_SEND_ACCESS`
 - `SEND_ACCES`
 - `ORIG_MAIL_ACCESS`
 - `MAIL_ACCESS`
 - `FROM_ACCESS`

If used this metacharacter performs a forced discard for all recipient(s).

- Consolidated new API.
- New MTA vacation and auto-reply facility. The MTA uses message disposition notifications (MDNs) and the SIEVE filtering language for automatically generated responses to email.
- Integration and support of Brightmail and Spamassassin spam filtering utilities.
- LMTP protocol support in a two-tier architecture that enables messages to be sent directly into recipient mailboxes unlike the SMTP protocol, where messages go through an MTA channel queue on the back-end store machine.

- MTA Direct LDAP Lookup, which enables the MTA to interact directly with Sun Java System Directory Server (Directory Server). Messaging Server therefore now requires the use of RFC 2821 standards-compliant email addresses in the directory attributes `mail`, `mailAlternateAddress`, and `mailEquivalentAddress`.
- The SMTP server's default behavior has changed. (4890252). The SMTP server's default behavior permissively accepts various line terminators. Currently, the `smtp` keyword is synonymous to the `smtp_cr_orlf` channel keyword on the `tcp` channels. Not only does this behavior comply with the original SMTP specification (RFC 821), it also now complies with the most recent revision of the SMTP specification (RFC 2821).

Specifically, the `smtp` keyword is synonymous with the `smtp_cr_lf` channel keyword. For more information, see the section on Channel Protocol Selection and Line Terminators in the chapter on Configuring Channel Definitions in the *Messaging Server Administration Guide*.

NOTE The User Management Utility is the recommended mechanism for provisioning Messaging Server and Sun Java System Calendar Server (Calendar Server) users. (See the *Sun Java System Communications Services User Management Utility Administration Guide* (<http://docs.sun.com/doc/817-5703>), for more information.)

The Identity Server Services (as described in the *Sun Java™ Enterprise System Installation Guide* at <http://docs.sun.com/doc/817-5760>) provide only minimal Messaging and Calendar Server LDAP user entry provisioning. Because the Identity Server Services interface does not provide input validation, user entries that cannot receive email or otherwise do not function will be created without reporting any errors. Consequently, we recommend using the Identity Server Services interface for demonstration purposes only.

Deprecated Features

Support for the following features may be eliminated in a future release:

Messenger Express

Going forward, no new features will be added to the Messenger Express user interface. It has been deprecated in favor of the new Communications Express user interface. Sun Microsystems, Inc. will announce an end-of-life timeline for Messenger Express at a future date.

MTA access to database files and the `imsimta` tools to manipulate MTA database files.

Two SSL configuration parameters.

The following configuration parameters are no longer supported:

- `encryption.nscertfile`
- `encryption.nskeyfile`

Direct editing of MTA or MMP configuration files.

A command line tool will be provided in a future release. Although the only current method of editing MTA or MMP configuration files is to use a text editor, the content of the configuration files is not meant to be publicly available indefinitely.

Use of the [PERIODIC_JOB=] sections in the `job_controller.cnf` file. (4907007)

The default entries shipped with iMS have been moved to the new scheduler process and removed from the default `job_controller.cnf` file. Specifically,

- The MTA's default periodic jobs will now be scheduled by the new scheduler process.
- Sites that modify the defaults must apply their changes to the new scheduler process configuration.
- Use of the MTA Job Controller to schedule periodic jobs is deprecated, and this functionality will be removed from the MTA Job Controller in a future release.

Customer supplied plug-ins with IMAP, POP, or Messenger Express.

The Messenger Express authentication plug-in API is supported for this release, but it is preferable to use Identity Server to configure single-sign-on. Client certificate mapping plug-ins are no longer supported.

Support for ident protocol.

Deprecated features include the MTA `ident*` keywords and support for `ident` user names in access control filters. The `indentnone*` keywords continue to be supported.

Delegated Administrator Web command-line interfaces.

These interfaces have been replaced with the new command-line tool, the Communications Services User Management Utility, `commadmin`, which integrates with Identity Server. The User Management Utility enables you to provision against an LDAP directory configured in Schema 2. The User Management Utility does not support provisioning against an LDAP directory configured in Schema 1.

You can continue to use the Delegated Administrator utilities to provision against a Schema 1 directory, but you cannot use Delegated Administrator for Schema 2.

MMP Section option.

The optional `SECTION` option for the `INSTANCENAME` option of the `ServiceList` MMP configuration parameter is deprecated and will be removed in a future release.

imsimta start and imsimta stop commands.

New `start-msg` and `stop-msg` commands have replaced `imsimta start` and `imsimta stop`. The `imsimta start` and `imsimta stop` commands will be removed in a future release.

NOTE For more information about the `start-msg` and `stop-msg` commands, refer to the *Messaging Server Administration Guide*.

Requirements

This section describes the hardware and software required for this release of Messaging Server as follows:

- [Supported Platforms](#)
- [Linux Installation Paths](#)
- [Client Software Requirements](#)
- [Product Version Compatibility Requirements](#)

Supported Platforms

This release supports the following platforms:

- Solaris 8 Operating System with required patches (SPARC® Platform Edition)
- Solaris 9 Operating System Update 2 (SPARC® and x86 Platform Editions) with required patches
- Linux Red Hat EL Advanced Server 2.1 u2 with required patches (glibc 2.2.4-31).

For detailed information about Solaris and Linux requirements, including required upgrade patches and kernel versions, see the

Sun Java Enterprise System Installation Guide (<http://docs.sun.com/doc/817-5760>) and *Sun Java Enterprise System Release Notes* (<http://docs.sun.com/doc/817-5503>).

For a list of the Messaging Server packages, see “Appendix E: List of Installable Packages,” in the *Sun Java Enterprise System Installation Guide* (<http://docs.sun.com/doc/817-5760>).

NOTE The Java Enterprise System installer checks for required platform patches. You must install all required patches or the installation process will not continue.

NOTE The performance of your messaging server depends on many factors, including CPU power, available memory, disk space, file system performance, usage patterns, network bandwidth, and so on. For example, throughput is directly related to file system performance. If you have questions about sizing and performance, contact your Sun Java System representative.

Linux Installation Paths

On the Linux operating system, the Messaging Server core software is installed in the following default path:

```
/opt/sun/messaging
```

During post-installation configuration, Messaging Server data and configuration files are created in the following default path:

```
/var/opt/sun/messaging
```

Messaging Server RPM Names

Messaging Server core software is installed under the following RPM names:

- sun-messaging-core-6.1-9.i386.rpm
- sun-messaging-mta-6.1-9.i386.rpm
- sun-messaging-core-en-6.1-9.i386.rpm
- sun-messaging-sieveui-6.1-9.i386.rpm
- sun-messaging-mmp-6.1-9.i386.rpm
- sun-messaging-install-6.1-9.i386.rpm
- sun-messaging-store-6.1-9.i386.rpm
- sun-messaging-lib-6.1-9.i386.rpm
- sun-messaging-webmail-6.1-9.i386.rpm

Messaging Server localization (l10n) files are installed under the following RPM names:

- sun-messaging-l10n-de-6.1-7.i386.rpm
- sun-messaging-l10n-es-6.1-7.i386.rpm
- sun-messaging-l10n-fr-6.1-7.i386.rpm
- sun-messaging-l10n-ja-6.1-7.i386.rpm
- sun-messaging-l10n-ko-6.1-7.i386.rpm
- sun-messaging-l10n-zh_CN-6.1-7.i386.rpm
- sun-messaging-l10n-zh_TW-6.1-7.i386.rpm

Linux Installation for User Management Utility

User Management Utility (commadmin) software is installed in the following default path:

/opt/sun/comms/commcli

User Management Utility software is installed under the following RPM names:

- sun-commcli-client-1.1-8.i386.rpm
- sun-commcli-server-1.1-8.i386.rpm

Linux Installation for Communications Express

Communications Express software is installed in the following default path:

/opt/sun/uwc

Communications Express software is installed under the following RPM name:

- sun-uwc-6.1-5.i386.rpm

Client Software Requirements

For Messenger Express access, Messaging Server requires a JavaScript-enabled browser. For optimal performance, Sun recommends the browsers listed in [Table 6](#):

Table 6 Messaging Server 6 2004Q2 Client Software Recommendations

Browsers	Solaris 8 for Sparc, Solaris 9 for Sparc, and X86	Windows 98	Windows 2000	Windows XP	Red Hat Linux 7.2	Macintosh OS X
Netscape™ Communicator	7.1	7.1	7.1	7.1	7.1	7.1
Internet Explorer	N/A	6.0 SP1	6.0 SP1	6.0 SP1	N/A	N/A
Mozilla™	1.5	1.5	1.5	1.5	1.5	1.2 or later

Product Version Compatibility Requirements

Messaging Server is compatible with the product versions listed in [Table 7](#):

Table 7 Product Version Compatibility Requirements

Product	Version
Sun Cluster	3.1*
Veritas Cluster Server	1.3, 2.0, 3.5
Sun Java System Directory Server	5.1, 5.2
Sun Java System Identity Server	6.1 (Command-line Interface Only)
Sun Java System Web Server	6.1 (but 6.0 Service Pack 5 if you are using iPlanet™ Delegated Admin)

NOTE* Messaging Server 6 2004Q2 does not support Sun Cluster 3.0 U3 (Update 3).
(4947465)

For more details about product version dependencies, see the *Sun Java Enterprise System Installation Guide* (<http://docs.sun.com/doc/817-5760>) and *Sun Java Enterprise System Release Notes* (<http://docs.sun.com/doc/817-5503>).

Additional Software Requirements

A high quality caching DNS server on the local network is a requirement for a production deployment of Messaging Server. Messaging Server depends heavily on the responsiveness and scalability of the DNS server.

Additionally, ensure in your setup that DNS is properly configured and that it is clearly specified how to route to hosts that are not on the local subnet:

- The `/etc/default/trouter` should contain the IP address of the gateway system. This address must be on a local subnet.
- The `/etc/resolv.conf` exists and contains the proper entries for reachable DNS servers and domain suffixes.
- In `/etc/nsswitch.conf`, the `hosts:` line has the `files`, `dns` and `nis` keywords added. The keyword `files` must precede `dns` and `nis`.
- Make sure that the FQDN is the first host name in the `/etc/hosts` file.

If your Internet host table in your `/etc/hosts` file looks like:

```
123.456.78.910 budgie.west.sesta.com
123.456.78.910 budgie loghost mailhost
```

change it so that there is only one line for the IP address of the host. Be sure the first host name is a fully qualified domain name. For example:

```
123.456.78.910 budgie.west.sun.com budgie loghost mailhost
```

File System

The following file systems are recommended for message stores:

- **LUFS (Logging UFS).**
- **VxFS (Veritas File System).** Veritas File System provides good system performance if configured properly. If you use VxVM, the Veritas Volume Manager, you need to carefully watch that the volumes and the log file for the volumes are set to be regularly striped.
- **HAStoragePlus File System** for Sun Cluster installations. The HAStoragePlus File System provides better performance than the default Sun Cluster Global File System.

The **NFS (Network File System)** is recommended in the following situation:

Though NFS is not supported on machines with message stores, you can use this file system on MTA relay machines, particularly if LMTP is enabled, or for autoreply histories and message defragmentation. (See the *Sun Java™ System Messaging Server Administration Guide* (<http://docs.sun.com/doc/817-6266>) for more information on autoreply). In addition, NFS can be supported on BSD-style mailboxes (`/var/mail/`).

Important Information

This section contains the latest information that is not contained in the core product documentation. This section covers the following topics:

- [Compatibility Issues](#)
- [Redistributable Files](#)
- [Documentation for Messaging Server 6 2004Q2](#)

Compatibility Issues

- iPlanet Delegated Administrator (iDA) is supported by Web Server version 6.0. If your LDAP directory is still in Schema 1, and you want to continue to provision mail users with iDA, use iDA with Web Server 6.0. (Web Server 6.1 does not support iDA.)
- While the preferred single-sign on (SSO) method is the one provided by Sun Java System Identity Server (Identity Server), Messaging Server continues to support the old version of single-sign on.
- The Communications Services User Management Utility, `commadmin`, is the preferred mechanism for provisioning Messaging Server users in an LDAP directory that is compatible with Identity Server.

The Identity Server Services provide only minimal Messaging and Calendar Server LDAP user entry provisioning.

Because the Identity Server Services interface does not provide input validation, user entries that cannot receive email or otherwise do not function will be created without reporting any errors. Consequently, we recommend using the Identity Server Services interface for demonstration purposes only.

- Messaging Server provides two mail filters that work with different user interfaces, as follows:

- The old mail filter provided through the iPlanet Delegated Administrator interface
- A new mail filter provided with Communications Express and Messenger Express

You cannot use both mail filters. If you use the mail filter functionality in Delegated Administrator, disable the mail filter in Communications Express or Messenger Express. Conversely, if you use the Communications Express or Messenger Express mail filter, you cannot use the mail filter functionality in Delegated Administrator.

Redistributable Files

The following redistributable files are provided with Messaging Server 6.0:

- You can redistribute the following files in SOURCE (html and javascript) or binary form (GIF files) within a licensed Messaging Server distribution only:
 - *msg_svr_base*/config/html (and subdirectories)
 - *msg_svr_base*/install/config/html (and subdirectories)

You are not permitted to distribute these files by themselves.

- You can copy and use (but not modify) the following header files solely to create and distribute programs to interface with Messaging Server APIs, to compile customer written code using the documented API to interoperate or integrate with Messaging Server, and only as expressly provided in the Messaging Server documentation:
 - *msg_svr_base*/examples/meauthsdk/expapi.h
 - *msg_svr_base*/examples/tpauthsdk/authserv.h
 - All files in the *msg_svr_base*/include directory (*default location*)
- The following files are provided solely as reference for writing programs that use the documented API to integrate with Messaging Server:
 - *msg_svr_base*/examples/meauthsdk/
 - *msg_svr_base*/examples/tpauthsdk/
 - *msg_svr_base*/examples/mtasdk/

Documentation for Messaging Server 6 2004Q2

Messaging Server Documents

Use the following URL to see all the Messaging Server 6 2004Q2 documentation:

http://docs.sun.com/coll/MessagingServer_04q2

Messaging Server 6 2004Q2 provides the following new and updated documents:

- *Sun Java™ System Messaging Server Release Notes* (this document)
- *Sun Java™ System Messaging Server Deployment Planning Guide*
- *Sun Java™ System Messaging Server Administration Guide*
- *Sun Java™ System Messaging Server Administration Reference*
- *Sun Java™ System Messaging Server Developer's Reference*
- *Sun Java™ System Messaging Server Messenger Express Customization Guide*

Communications Services Documents

Use either one of the following URLs to see the documentation that applies to all Communications Services 6 2004Q2 products:

http://docs.sun.com/coll/MessagingServer_04q2

or

http://docs.sun.com/coll/CalendarServer_04q2

The following documents are available:

- *Sun Java™ System Communications Services User Management Utility Administration Guide*
- *Sun Java™ System Communications Services Enterprise Deployment Planning Guide*
- *Sun Java™ System Communications Services Schema Migration Guide*
- *Sun Java™ System Communications Services Schema Reference*
- *Sun Java™ System Communications Services Event Notification Service Guide*
- *Sun Java™ System Communications Express Administration Guide*
- *Sun Java™ System Communications Express Customization Guide*

Known Issues and Limitations

This section contains a list of the known issues with Messaging Server 6 2004Q2. The following product areas are covered:

- [Installation, Upgrade, and Uninstallation Problems](#)
- [Messaging Server Problems](#)
- [User Management Utility](#)
- [Messenger Express Problems](#)
- [Localization Issues](#)
- [Documentation Issues](#)

Installation, Upgrade, and Uninstallation Problems

This section describes known issues with installing, upgrading, and uninstalling Messaging Server.

If Directory Server is running in a clustered environment, the `comm_dssetup.pl` command does not wait for `stop-slapd` to finish properly. (5020179)

If you are applying the `comm_dssetup.pl` script to a Directory Server cluster configuration, the script may fail because the call to the `stop-slapd` in the generated shell script may take some time to finish even though the call returns immediately.

Workaround

Edit the generated shell script and put in a sleep timeout (such as 10 seconds) after the call to `stop-slapd`.

If you upgrade from Messaging Server 6 2003Q4 to Messaging Server 6 2004Q2 and revert to Messaging Server 6 2003Q4, Messaging Server does not run. (4992042)

This problem occurs if you take the following steps:

- Upgrade from Messaging Server 6 2003Q4 to Messaging Server 6 2004Q2.
- Back out the Messaging Server 6 2004Q2 patch by using the `patchrm` command. This reverts you to Messaging Server 6 2003Q4. You can would then run the `imsimta cnbuild` command to recompile the configuration.
- Attempt to restart the server.

In this scenario, Messaging Server 6 2003Q4 does not start because it cannot read the new version of the Message Store data. Messaging Server 6 2004Q2 upgrades the Sleepycat Berkeley DB to version 4.2.

Workaround

There are two workaround options:

Option 1:

Before you upgrade, copy the Messaging Server database files to a backup location. Then, if you find you must back out the Messaging Server 6 2004Q2 patch, restore the database files before you attempt to back out the new patch.

Option 2:

You can use the following procedure to back out the patch from Messaging Server 6 2004Q2 to Messaging Server 6 2003Q4:

1. Stop the Messaging Server with the `stop-msg` command.
2. Disable the watcher daemon by running the `configutil` command, as follows:


```
configutil -o local.watcher.enable -v no
```
3. Remove the message store database environment files by using the `stored -r` command.

If this command fails to remove the files, use the `stored -R` command. This forces the removal of the files.
4. Enable the watcher daemon as follows:


```
configutil -o local.watcher.enable -v yes
```
5. Remove the log files under the `mboxlist` directory. For example:


```
rm -f /var/opt/SUNWmsgsr/store/mboxlist/log.*
```
6. Remove the Messaging Server 6 2004Q2 package by running the `patchrm <patch id>` command.
7. Run the `imsimta cnbuild` command.
8. Start Messaging Server with the `start-msg` command.

This version of Messaging Server does not support a staged rolling upgrade with minimum downtime in a symmetric HA environment. (4991650)

With Messaging Server 5.2, you could install the Messaging Server more than once on the same machine and patch the different installations separately. This capability enabled support for minimal-downtime staged rolling upgrades. Messaging Server 6 2004Q2 does not provide this capability.

User Calendar Service is not backed out when the User Management Utility (commadmin) upgrade patch is backed out. (4976453)

When the commadmin upgrade patch to version 6.1 (6 2004Q2) is backed out, the UserCalendarService definition does not revert to version 6.0 (6 2003Q4) . The UserCalendarService definition can only be backed out manually.

Workaround

To back out the UserCalendarService definition manually, do the following:

```
# cd /opt/SUNWcomm/lib/services/  
# /opt/SUNWam/bin/amadmin -u admin_login -w password -t deletecaluserAttributes.xml
```

admin_login - Identity Server admin user

password - Identity Server admin password

Note that you have to provide the full path to the amadmin command from the Identity Server bin directory.

If you don't revert the UserCalendarService definition manually and you run the patch twice an error will be logged the second time because the change was already made.

Messaging Server does not start under Sun™ Cluster 3.0 Update 3. (4947465)

Messaging Server cluster agents dump core due to a problem in Sun Cluster 3.0 u\Udate 3. Use Sun Cluster 3.1 to solve this problem.

The installer sets iPlanet Delegated Administrator (iDA) CGI path incorrectly for MS 6. (4929552)

During installation of iDA, the default CGI path is msg-<servername>/Tasks/operation. It should be msg-config/Tasks/operation. The incorrect path causes a throw error when you purge a user from CLI.

Workaround

During installation of iDA, change the default CGI path from msg-<servername>/Tasks/operation to msg-config/Tasks/operation. This will allow you to purge any users rom CLI without causing any errors.

End users cannot manage their mailing lists in Messaging Server 6.0. (4904736)

Sun Java System Messaging Server 6.0 will ship *without* a web-based tool that allows end users to manage their own mailing lists (a regression relative to iPlanet Messaging Server 5.2).

Workarounds

- Install a third-party product for mailing list expansion and management, such as Mailman (<http://www.list.org/>) or Majordomo (<http://www.greatcircle.com/majordomo/>).

- Alternately, do not use Sun Java System LDAP Schema 2, but instead use LDAP Schema 1, which is supported by the graphical user interface found in iPlanet Delegated Administrator for Messaging. Also, in Schema 1, you can provision the directory directly to create Delegated Administrator-compatible LDAP entries, as described in the *iPlanet Messaging Server 5.2 Provisioning Guide* and the *iPlanet Messaging and Collaboration 5.2 Schema Reference*.

Netscape Directory Server 4.16 PAB entries with multi-valued mail attributes cannot be migrated to Directory Server 5.1 because it only accepts single-valued mail attributes. (4869706)

Objectclass violations occur if you try to add these entries.

Workaround

Turn off schema checking if you are porting PAB entries from Netscape Directory Server 4.16 to Directory Server 5.1.

Messaging Server Problems

This section describes known issues in the Messaging Server product.

In `option.dat`, lines starting with #, !, or ; symbols are treated as comment lines. (no bugid)

In `option.dat` files, Messaging Server treats lines beginning with pound sign (#), exclamation point (!), or semicolon (;) characters as comment lines — even if the preceding line has a trailing backslash (\), which means the line is being continued. Consequently, you must be careful when working with long options (particularly delivery options) containing these characters.

There is a workaround for delivery options in which a natural layout could lead to continuation lines starting with a # or !.

Workaround

In delivery options, Messaging Server ignores spaces following the commas that separate individual delivery option types.

For example, instead of:

```
DELIVERY_OPTIONS=\
#*mailbox=@$X.LMTP:$M$_+$2S%$\$2I@ims_daemon,\
#&members=*,\
*native=@$X.lmtpnative:$M,\
*unix=@$X.lmtpnative:$M,\
/hold=$L%$D@hold,\
*file=@$X.lmtpnative:+$F,\
```

```
&@members_offline=*,\  
program=$M$P@pipe-daemon,\  
forward=**,\  
*^!autoreply=$M+$D@bitbucket
```

You can workaroud the problem by adding spaces as follows:

```
DELIVERY_OPTIONS=\  
    #*mailbox=@$X.LMTP:$M$_+$2S%$\$2I@ims_daemon,\  
    #&members=*,\  
    #*native=@$X.lmtpnative:$M,\  
    #*unix=@$X.lmtpnative:$M,\  
    #/hold=$L%$D@hold,\  
    #*file=@$X.lmtpnative:+$F,\  
    #&members_offline=*,\  
    #program=$M$P@pipe-daemon,\  
    #forward=**,\  
    #*^!autoreply=$M+$D@bitbucket
```

DOMAIN_UPLEVEL has been modified. (no bugid)

The DOMAIN_UPLEVEL default value has changed from 1 to 0.

The following characters cannot be used in the User ID: \$ ~ = # * + % ! @ , { } () / < > ; : " ` [] & ? (no bugid)

This constraint is enforced by MTA when operating in direct LDAP mode. Allowing these characters in the User ID can cause problems in the message store. If you want to change the list of characters forbidden by the MTA, set the following option by listing a comma-separated string of the characters' ASCII values:

```
LDAP_UID_INVALID_CHARS=32,33,34,35,36,37,38,40,41,42,43,44,47,58,59,60,61,62,63,64,91,92,93,96  
,123,125,126
```

in the `msg_svr_base/config/options.dat` file. Note that you are strongly advised against relaxing this constraint.

NFS is not supported for mail stores. (no bugid)

The use of NFS is not supported for message stores because certificate on NFS has not been completed.

(msprobe) The default timeout for server response is too small. (5064135)

The default timeout for `msprobe`'s wait for a server response is 10 seconds. This default value, set by the `configutil` parameter `service.readtimeout`, is too small.

In general, this timeout value should be set to at least 30 seconds.

For SMTP, if you configure Messaging Server to perform DNS reverse lookups on incoming connections, but DNS is not working, the SMTP banner takes about two minutes to appear. Therefore, for SMTP, you should set a timeout value of at least 120 seconds.

Workaround:

Set the `configutil` parameter `service.readtimeout` to 2 minutes or to a higher value than your `tcp_ip` stack timeout.

Message creation date/times may be misreported. (5046988)

The name used for messages in the MTA's queue contains an encoded date which is the original creation date for the message. In some cases, this name is being decoded incorrectly. This problem affects the information presented by QM and the message-creation date. The creation date is used to calculate how long a message has been in the system; an incorrect value may cause messages to be returned undelivered prematurely.

When a message store process (such as `mshttpd`) crashes, no core file is created. (5046327)

After installation, Messaging Server directories are owned by `bin` instead of `mailsrv`. As a result, when a process crashes, no core file is created.

Workaround:

1. Start processes from a directory writeable by `mailsrv` such as `/tmp` or the log directory.
2. If `coreadm` is available on your platform, use `coreadm` to redirect core files to a known location (writeable by `mailsrv`).

Cannot log in to Messaging Server from Internet Explorer 6.0 SP1 when using a proxy server. (5043607)

When using an `http` proxy in IE 6.0 SP1 on a PC as a client, you may experience difficulty in logging into Messaging Server. This problem is likely to be due to a non-standard compliant proxy server and cannot be fixed in Messaging Server.

The `msg-admin-xxx` user created by the installer does not have the right to modify the `mailuserstatus` or `maildomainstatus` attribute. (5033014)

The right to modify the `mailuserstatus` and `maildomainstatus` attributes is required by the `msuserpurge` utility and the `mta` quota enforcement mechanism.

Workaround:

Modify the `aci` for the Messaging Server End User Administrators Group to allow write access to the `mailuserstatus` and `maildomainstatus` attributes.

The following sample `ldif` file contains an `aci` that provides the appropriate write access. Replace the string `<local.ugldapbasedn>` with your user/group suffix.

```
# attribute of objectclass top
dn: <local.ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///<local.ugldapbasedn>")
(targetattr="objectclass||mailalternateaddress||mailautoreplymode|
|mailprogramdeliveryinfo||nswmextendeduserprefs||preferredlanguage| | | | |
|maildeliveryoption||mailforwardingaddress||mailAutoReplyTimeout|
|mailautoreplytextinternal||mailautoreplytext||vacationEndDate||vacationStartDate|
|mailautoreplysubject||pabURI||maxPabEntries||mailMessageStore||mailSieveRuleSource|
|sunUCDateFormat||sunUCDateDeLimiter||sunUCTimeFormat||mailuserstatus|
|maildomainstatus")
(version 3.0; acl "Messaging Server End User Administrator Write Access Rights -
product=ims5.0,class=installer,num=101,version=1"; allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
<local.ugldapbasedn>";)
```

SSL breaks when the certificate database is edited using the latest Mozilla browser. (5030342)

Do not attempt to edit the content of the certificate database file (cert8.db) using the Mozilla browser or other NSS tools not built and distributed by Sun Microsystems. Doing so may cause database corruption.

Java Enterprise System 2004Q2 is packaged with NSS version 3.3.x. Messaging Server uses this version of NSS to handle SSL certificates. The cert8.db format does not work well if the cert8.db is created or edited with a Mozilla TIP client, which uses the NSS 3.9 component. This causes the SSL communication to fail.

A malformed pabURI attribute causes coring of mshttpd. (5003127)

Coring of the mshttpd occurs as a result of a malformed pabURI attribute.

Workaround:

Correct the pabURI entry in the LDAP directory.

Correct certmap.conf file content required for client-based SSL. (4967344)

The certmap.conf configuration file specifies how to map a certificate to an entry in the LDAP directory. *By default*, the certificate subject (with two lines commented out) contains the *exact* DN of the LDAP directory entry.

However, a very common alternative behavior is to extract a particular attribute from the subject of the certificate and to search the directory for that attribute.

Workaround:

To achieve this alternative behavior, change:

```
certmap default          default
#default:DNComps
#default:FilterComps    e, uid
```

to:

```
certmap default          default
default:DNComps
default:FilterComps     e
```

NOTE For a complete description of certmap.conf, please refer to the *Sun Java System Server Console 5.2 Server Management Guide*.

Will not see channel is stopped if jobc was recently started. (4965338)

In Messaging Server 5.2, if you issued a `#imsimta qm summarize` command you could view the channels that had been stopped with the `imsimta qm stop <chan>` command.

This behavior changed in 6.0. If you have not used a channel yet, you will not get the 0 lines and you will not see the stopped channels. Messages could be logged without you being aware of it.

imsimta cache -walk -debug=15 issues an error message. (4964696)

The `imsimta cache -walk -debug=15` command works as intended, but issues an “Unknown command specified” error message.

Output from return_debug=1 missing. (4957856)

In previous releases, the output from `return_debug=1` was logged to `job_controller.log`.

In Messaging Server 6.0, the scheduler program runs the `return` job, but does not send the output to any log file.

Korean PAB text corrupt in Internet Explorer 6.0 when auto-select encoding is enabled. (4951813)

Using Internet Explorer 6.0, if you create a user with `preferredlanguage=ko`, select View -> Encoding -> Auto-Select, and log into Webmail as the `ko` user, when you open the Addresses page the text display will be corrupted.

Workaround

Disable Auto-Select and reopen the Addresses page. The text will display appropriately.

NOTE Chinese and Japanese localization's behave properly with Auto-Select enabled.

Warning messages pop up for User Certificate even if the site is not configured for such. (4943648)

This warning message pops up when SSL certificates are installed and all services are enabled to use SSL mode, and you connect to a secured webmail port such as "https://FQDN" and install the site's certificates in your security preferences. The following message pops up: "User Authentication is required." You can press OK and continue the operation.

This is expected behavior. If there is a trusted CA flag on the server certificate in the certificate database, the server asks for client certificates.

Workarounds:

- Remove the root CA from the server or browser's preferences.
- Change the attributes on the Server-Cert so it is not a CA.
- Remove or rename the file `<configdir>/certmap.conf`.

Manage Certificate wizard not creating Secure Sockets Layer (SSL) certificates under Messaging Server/Configuration. (4939810)

When you use the `Manage Certificate` option (Admin Server->Messaging Server->Configuration->Manage Certificate) to create an SSL certificate request, the Manage Certificate wizard should create a certificate and key database in the `Messaging_Server_Base/config` area and not in the `Admin_Server_Root/alias` area. In addition, the file prefixes should change from the `msg-config` value (`msg-config-cert7.db` and `msg-config-key3.db`) to `NULL` (`cert7.db` and `key3.db`).

Workarounds:

- Copy the `msg-config-cert7.db` and `msg-config-key3.db` files from `Admin_Server_Base/alias` area to `Messaging_Server_Base/config` area as `cert7.db` and `key3.db` with proper permissions and ownerships.
- Create soft links for the files under `Messaging_Server_Base/config` area with the proper permissions and ownerships used in the `Admin_Server_Base/alias` area.

Webmail's default behavior for Arabic/Hebrew users has changed since version 5.2. (4933096)

When you log in as a user with `preferredlanguage=ar`, the user interface displays left-to-right instead of right-to-left.

Workaround

1. Create a `/var/msg_svr_base/config/html/ar` directory by copying `/var/msg_svr_base/config/html/en`.
2. Edit `/var/msg_svr_base/config/html/ar/i18n.js` to include

```
i18n['dir'] = 'rtl' (just above i18n['fontface'] = 'PrimaSans BT,Verdana,sans-serif')
```

MMP client certificate lookup supports Schema 1 but not Schema 2. (4918256)

The MMP client certificate mechanism does not support the Schema 2 domain model. Support for the MMP client certificate lookup is limited to a subset of the Schema 1 model created by iPlanet Delegated Administrator. In the supported structure, user entries must be under "ou=People" under the domain node in the Organization Tree, with a pointer to that node in the DC Tree.

imsimta start doesn't start disp and job controller. (4916996)

The `imsimta start`, `imsimta restart`, and `imsimta refresh` commands work only when the watcher process is running.

NOTE New `start-msg` and `stop-msg` commands have replaced `imsimta start` and `imsimta stop`, which are deprecated and will be removed in a future release.

For more information about the `start-msg` and `stop-msg` commands, refer to the *Messaging Server Administration Guide*.

The XSTA, XADR commands are enabled by default. (4910371)

After installation, the SMTP extension commands `XSTA` and `XADR` are enabled by default, which may enable remote and local users to retrieve sensitive information.

Workaround

Add the following lines to the `imta/config/tcp_local_options` file (create this file if necessary) to disable the `XSTA` and `XADR` commands:

```
DISABLE_ADDRESS=1
DISABLE_CIRCUIT=1
DISABLE_STATUS=1
DISABLE_GENERAL=1
```

Searching for a home phone number does not work in the Personal Address Book. (4877800)

A Personal Address Book search based on "Phone #" searches for the work phone number attribute only. You cannot use "Phone #" to search for home or mobile phone numbers.

Cannot Create a User Through the Administration Console (4852026 & 4852004)

Messaging Server no longer supports user or group creation using the Admin Console. User and group entries should be created using the User Management Utilities. The following error messages may appear when logging in as, or sending mail to, a user created using Admin Console:

```
Quota root does not exist
```

```
4.0.0 temporary error returned by alias expansion: . . ."
```

If indirect dependencies already exist between Sun Cluster resources, `scds_hasp_check()` may prevent HAStoragePlus from being supported with those existing configurations. (4827911)

This behavior is observed in Sun Cluster 3.0 Update 3.

Workaround

Create a weak dependency for the existing resources on the HAStoragePlus resource.

Messenger Express Multiplexor (MEM) does not have a configuration option to make use of the OS resolver as well as NSCD. (4823042)

Workaround

Configure system as a caching-only DNS server in order to gain the benefit of caching MX and A records.

MoveUser utility does not work on a mailbox that contains over 25,000 subfolders. (4737262)

It has been reported that the MoveUser utility stops when attempting to move a user's account that has a mailbox containing over 25,000 subfolders.

Access control filters do not work if the short form domain is used in the `/etc/hosts` file. (4629001)

If there is a short form version of a domain name in the `/etc/hosts` file, there will be problems if you use a host name in an access control filter. When the IP address lookup returns a short form version of the domain name, the match will fail. Therefore, you should make sure you use a fully qualified domain name in the `/etc/hosts` file.

Connections aborted with `TCP_IOC_ABORT_CONN` in syslog. (4616287)

If a failover occurs for an HA configuration running Sun Cluster 3.1 on the Solaris 8 U7 or Solaris 9 Operating System and active TCP connections are aborted with the `TCP_IOC_ABORT_CONN` ioctl, messages such as the following are logged on the console and to system logs.

```
Jul 24 16:41:15 shemp ip: TCP_IOC_ABORT_CONN: local = 192.018.076.081:0,  
remote = 000.000.000.000:0, start = -2, end = 6  
Jul 24 16:41:15 shemp ip: TCP_IOC_ABORT_CONN: aborted 0 connection
```

These messages are informational only and should not show up in non-debug mode.

If you use Microsoft Outlook Express as your IMAP mail client, the read and unread flags might not work properly. This is a known problem with the Microsoft Outlook Express client. (4543930)

To enable the workaround, set the following configuration variable:

```
configutil -o local.imap.immediateflagupdate -v yes
```

If, while using the workaround, you experience performance issues, it is recommended that you discontinue using the workaround.

To take effect, changes made using configutil often require a restart of the affected server or servers. (4538366)

Admin Server access control host names are case-sensitive. (4541448)

When you configure “Host Names to allow” for the Admin Server, the access control list is case-sensitive. If the DNS server uses mixed-case host names in the `IN-ADDR` records (used when translating from an IP address to a domain name), the access control list must use the same case. For example, if your host is `test.Sesta.Com`, then the access control list must include `*.Sesta.Com`. Due to this problem, `*.sesta.com` will not suffice.

For example, if the user/group base suffix is `o=isp`, then the DN of the service administrator group is `cn=Service Administrators,ou=groups,o=isp`. To designate the account `uid=ofanning, o=sesta.com, o=isp` as a service administrator, you should add the account’s DN to the group. In the following modify record, the designated user is added as a group member in the LDIF:

```
dn: cn=Service Administrators,ou=groups,o=isp
changetype: modify
add: uniquemember
uniquemember: uid=ofanning, o=sesta.com, o=isp
```

Furthermore, for users to have service administrator privileges, the attribute `memberof` must be added to the user entry and set to the Service Administrator Group, for example:

```
dn: uid=ofanning, o=sesta.com, o=isp
changetype: modify
add: memberof
memberof: cn=Service Administrators, ou=groups, o=isp
```

The MMP `BadGuy` configuration parameter, `BGExcluded`, does not work. (4538273)

Workaround

Deploy separate MMP servers to handle the clients that are excluded from bad guy rules. These servers must have `BadGuy` turned off.

LDAP search performance is slightly impacted by ACIs in Directory Server version 5.x. (4534356)

This issue affects many searches performed by Messaging Server. For faster searches, use directory manager credentials with the following commands to access the directory:

```
msg_svr_base/sbin/configutil -o local.ugldapbinddn -v "rootdn" -l
msg_svr_base/sbin/configutil -o local.ugldapbindcred -v "rootdn_passwd" -l
```

where `rootdn` and `rootdn_passwd` are the credentials of Directory Server’s administrator.

If you enable Sun Cluster 3.0 Update 3, you may encounter a harmless error message. (4490877)

The following harmless error message appears in the Sun Cluster console and also in `/var/adm/messages`, when starting High Availability (HA) services or when switching HA services from one node to another:

```
Cluster.PMF.pmf: Error opening procfs control file </proc/20700/ctl> for tag
<falcon,habanero_msg,4.svc>: No such file or directory
```

User Management Utility

This section describes known issues in Communications Services User Management Utility.

Manual steps are required to enable the `commadmin` utility to run against an LDAP directory in Schema 2 compatibility mode. (5042801)

To enable `commadmin` to work on an LDAP directory in Schema 2 compatibility mode, you must manually take the steps described below.

Workaround

Take the following six steps:

1. Add the following two ACIs to the OSI root. You can find the following two ACIs in the `usergroup.ldif` file, located in the `/opt/SUNWcomm/config` directory.

Be sure to replace `ugldapbasedn` with your `usergroup` suffix. Add the edited `usergroup.ldif` into the LDAP directory.

```
#
# acis to limit Org Admin Role
#
#####
# dn: <local.ugldapbasedn>
#####
dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to org node"; deny
(write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)
```



```
dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*") (version 3.0; acl
"Organization Admin Role access allow read to org node"; allow (read,search) roledn =
"ldap:///cn=Organization Admin Role,($dn),<ugldapbasedn>");)
```

2. Add the following two ACIs to the DC Tree root suffix. You can find the following two ACIs in the `dctree.ldif` file, located in the `/opt/SUNWcomm/config` directory.

Be sure to replace `dctreebasedn` with your DC Tree root suffix and `ugldapbasedn` with your usergroup suffix. Add the edited `dctree.ldif` into the LDAP directory.

```
#
# acis to limit Org Admin Role
#
#####
# dn: <dctreebasedn>
#####
dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to dc node";
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>");)

dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to dc node"; allow
(read,search) roledn = "ldap:///cn=Organization Admin Role,($dn),<ugldapbasedn>");)
```

3. Add the following additional ACIs to the DC Tree root suffix. (These ACIs are not in the `dctree.ldif` file.)

```
dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Proxy user rights"; allow (proxy)
userdn = "ldap:///cn=puser,ou=DSAME Users,<ugldapbasedn>");)
```

```
dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the root suffix";
allow (all) userdn = "ldap:///cn=dsameuser,ou=DSAME Users,<ugldapbasedn>";)
```

```
dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Top-level admin rights";
allow (all) roledn = "ldap:///cn=Top-level Admin Role,<ugldapbasedn>";)
```

4. Set the `com.iplanet.am.domaincomponent` property in the `AMConfig.properties` file to your DC Tree root suffix. For example, modify the following lines in the `<IS_base_directory>/lib/AMConfig.properties` file:

```
from
com.iplanet.am.domaincomponent=o=isp
to
com.iplanet.am.domaincomponent=o=internet
```

5. Enable Identity Server to use compatibility mode. In the Identity Server Console, in the Administration Console Service page, check (enable) the **Domain Component Tree Enabled** check box.

6. Add the `inetdomain` object class to all the DC Tree nodes (such as `dc=com,o=internet`), as in following example:

```
/var/mps/serverroot/shared/bin 298% ./ldapmodify -D "cn=Directory Manager" -
w password
dn: dc=com,o=internet
changetype: modify
add: objectclass
objectclass: inetdomain
```

7. Restart the Web container.

The domain administrator can add and delete services to the domain and can modify domain attributes. (5026945)

The domain administrator should not have the authority to change domain attributes.

If you do a fresh installation of the User Management Utility (`commadmin`) with Java Enterprise System 2004Q2, this problem does not occur. The proper `usergroup.ldif` files are added automatically when you configure `commadmin` with the `config-iscli` program.

This situation occurs if you are using the User Management Utility (`commadmin`) from version 6.0 (6 2003Q4), or if you upgrade `commadmin` from version 6.0 (6 2003Q4) to version 6.1 (6 2004Q2).

Workaround

To obtain the ACIs to properly restrict the privileges of the domain administrator, take the following steps:

1. Open the `usergroup.ldif`, located in the `/opt/SUNWcomm/config` directory, and replace `ugldapbasedn` in the template ldif with your `usergroup` suffix.
2. Add the edited `usergroup.ldif` into the LDAP directory.

If you deploy `commadmin` with Application Server, additional steps are needed to configure `commadmin` after you run the configuration program, `config-iscli`. (5015063)

At the end of the configuration, the configuration utility asks you to manually deploy the war file to the web container used by Identity Server and modify the classpath.

Workaround

To configure `commadmin` properly, using Application Server as the web container, take the following steps:

1. After you complete the `commadmin` configuration, find the `server.xml` file in the Application Server configuration directory. By default, the `server.xml` file should be in the following directory:

```
/var/opt/SUNWappserver7/domains/domain1/server1/config
```

Search for `server-classpath` and add the following to `server-classpath`:

```
app-server-root/domains/domain1/server1/applications/j2ee-modules/commcli_1/WEB-INF/classes
```

2. Deploy the war file as:

```
cd /opt/SUNWappserver7/bin

./asadmin deploy --user "admin user name" --password "admin user password"
--host hostname --port 4848 --name commcli --contextroot
commcli /opt/SUNWcomm/lib/jars/commcli-server.war
```

3. Restart Application Server as follows:

```
cd /var/opt/SUNWappserver7/domains/domain1/server1/bin
./stopserv ; ./startserv
```

Cannot modify non-ASCII groups. (4934768)

If a group is created with a group name that contains non-ASCII characters, it cannot be modified with the `commadmin group modify` command.

For example, if a group with the non-ASCII characters XYZ is specified with the `-G` option in the `commadmin group create` command, an email address of XYZ is automatically added to the group's LDAP entry. Since non-ASCII characters are not allowed in email addresses, modifying the group with `commadmin group modify` fails.

Workaround:

Use the `-E` *email* option when creating a group. This option will specify the group's email address. For example: `commadmin group create -D admin -w password -d siroe.com -G XYZ -S mail \ -E testgroup@siroe.com`.

Creating a group with multiple `-f` options adds only one attribute. (4931958)

If you specify multiple `-f` options for creating dynamic groups in the `commadmin group create` command, only the value specified with the last `-f` option is added to the LDAP entry. The other values are not added.

Workaround:

Do not specify the `-f` option multiple times when using the `commadmin group create` command.

Messenger Express Problems

This section describes known issues in the Messenger Express product.

The Up and Down buttons removed. (no bugid)

The Up and Down buttons used to specify the ordering of your filters have been removed.

Problems may be seen in WebMail on Internet Explorer 6 when proxy server setting is used. (4925995)

Workaround:

Enable or disable "auto-detection" option in Internet Explorer's encoding menu. Use direct connection or switch to different proxy server.

Feature removed from the Advanced Mail Filter Conditions window. (4908625)

The ability to specify a time frame for your filters has been removed from the Advanced Mail Filter Conditions window (of the Mail Filters user interface) for the Messaging Server 6.0 Patch 1 release. The feature was removed because the underlying support is not available.

If you create groups within an existing group, you may encounter the following error:

pab::PAB_ModifyAttribute: ldap error (No Such object). (4883651)

With Directory Server 5.1 or later, you will not be able to enter multiple email IDs for a single contact in the Personal Address Book. (4633171)

Note that Directory Server is exhibiting correct behavior. Due to a problem in Netscape Directory Server 4.x, you are able to enter multiple email IDs.

Localization Issues

The following known issues are not necessarily i18n or l10n specific.

(Linux) Messaging Server console shows an error opening online help. (5054732)

(Linux B11b): Style and device are missing in client-detection edit window. (5053850)

(Linux) Running the configurator in GUI mode displays Simplified Chinese, Traditional Chinese and Korean characters in square or junk chars. (5049404)

J2SE 1.4.2 cannot display certain awt components in Asian Characters in RedHat Advanced Server 2.1

(French) In mail filter, the keywords "any" and "all" are incorrcly translated. (5046722)

In mail filters in Messenger Express, the keyword "all" between conditions behaves as "or." (5046720)

In Communications Express, the mail filters work as they should. This problem only occurs in the now deprecated Messenger Express.

(l10n_ja) Some messages are not updated or not localized in OLH. (5046617)

In the Admin console, the keywords ALL and EXCEPT in access filters must be in English. (5046034)

This issue refers to examples in the Messaging Server Admin console explaining how to define access filters. The keywords ALL and EXCEPT are translated by accident. These keywords must stay in English, as in these examples: "ALL" and "ALL EXCEPT."

Online help for Admin console is not localized in the browser. (5045955)

(l10n-ko) Several search related dialogs fail to load after first time. (5045055)

Workaround:

Clear the temporary internet files

(I10n-ko) "Addresses" page fails to load after first time. (5045050)

Workaround:

Clear the temporary internet files

(i18n) Spell-check for Korean is not supported. (5045043)

(I10n-ko) In the webmail OLH, webmail.gif is not localized. (5045041)

(German)

(German) Group in address book cannot be created. (5044669)

Cannot add contact from search address book window. (5044609)

Workaround:

Add contact to group directly without searching

(ja_only) No indexes to Japanese alphabets in index page of online_help. (5040407)

JS error when you add addresses on msg window invoked from search result. (5038872)

A message pops up when you click the Folders tab. (5038438)

Workaround:

Set preferredLanguage=zh-CN instead of zh

TRASH not localized in mail search dialog. (5035064)

Some untranslated issues in Messaging Server configure CLI in Simplified and Traditional Chinese. (5034466)

Cannot add members to new group through search function. (5032727)

(i18n) New contact page not closed by OK button and javascript error. (5032134)

(i18n) In the Admin Console: message store: you can create aging policy in ja locale, but multibyte chars become garbage. (5031308)

Workaround:

Use only singlebyte chars.

(i18n) Admin with remote directory displays Help Error. (5029459)

(i18n) An unlocalized error message occurs when you enter wrong password for collecting external mail. (5017071)

(i18n) When you composing a new message in HTML text, input method is disabled when you use Bullet/Number list. (5016484)

Workaround:

Move the mouse cursor to a different line where multibyte chars are already entered.

(i18n) Error message is corrupted to sending mail to an unknown email address. (5013576)

(i18n) Under folders tab, default folders are not sorted. (5013572)

(i18n) If Web Server is started under a different locale such as ko, then Korean localized mailfilter page displays for all the users regardless of their preflang setting. (5012270)

Workaround:

Start Web Server under C locale.

The comm_dssetup.pl script is not localized. (4994764)

Corrupt Japanese Delivery Reports. (4985907)

(i18n) Garbled characters in warning dialog box displayed when getting POP msgs. (4951972)

Workaround:

Mozilla browser seems OK.

“New user greeting form” language pull-down menu showing English when you click reset button. (4914441)

(i18n) Initial date format is not Year.Month.Day for an Asian user. (4908619)

Workaround:

Log in to Webmail and change the proper date format under option setting.

(i18n) When you create a new contact, put the Lastname textbox before Firstname for an Asian local user. (4906295)

(i18n) When you compose a new message in HTML text, you need to add local font names to the font list. (4902459)

(i18n) Unable to send mail to a shared multibyte folder. (4887205)

(i18n/I10n) Localized Webmail does not merge some of the folders created by Outlook Express. (4653960)

It is sometimes desired that default “Sent” folder in Webmail can be replaced with “Sent Items” folder created by Outlook Express, hence all the messages sent by both client is copied to “Sent Items” folder. This operation is difficult, particularly in Japanese.

Workaround (in two parts):

1. Edit Japanese `i18n.js` to match Outlook Express’ “Sent Items” translation

```
i18n['sent folder IE'] = 'soushinzumiaitemu'  
fldr['Sent Items'] = 'soushinzumiaitemu'
```

2. End users must log onto Messaging Server using Outlook Express first.

Documentation Issues

This section describes known issues in the Communications Services documentation.

Documentation Incorrectly describes OIDs for two LDAP schema object classes. (5060062)

The *Sun Java System Communications Services 6 2004Q2 Schema Reference* documents incorrect OIDs for the following object classes:

- `icsCalendarUser`
- `icsCalendarResource`

The correct OIDs are as follows:

- `icsCalendarUser` - 1.3.6.1.4.1.42.2.27.9.2.44
- `icsCalendarResource` - 1.3.6.1.4.1.42.2.27.9.2.45

Communications Express

Sun Java™ System Communications Express Version 6 2004Q2 provides an integrated web-based communication and collaboration client that consists of three client modules - Calendar, Address Book and Mail. The Calendar and Address Book client modules are deployed as a single application on any web container and are collectively referred as the Unified Web Client (UWC). Messenger Express is the standalone web interface mail application that uses the HTTP service of the Messaging Server.

This section contains the following topics:

- [Supported Browsers](#)
- [Installation Notes](#)
- [Known Issues and Limitations](#)

Supported Browsers

Communications Express can be viewed using:

- Netscape™ Communicator 6.2.x, 7
- Internet Explorer 5.x, 6.0
- Mozilla™ 1.0 or higher

Installation Notes

The following are the dependent services for Communications Express:

1. **Directory Server.** Install Sun Java™ System Directory Server version 5.2.
2. **Calendar Server.** Install Sun Java™ System Calendar Server Version 6.1.
3. **Web Server.** Install Sun Java™ System Web Server version 6.1 SP2 with JDK version 1.4.2.
4. **Messaging Server.** Install Sun Java™ System Messaging Server 6.1.
5. **Identity Server.** Install Sun Java™ System Identity Server 6.2.

NOTE Communications Express has been tested and is supported only with the server versions mentioned above.

Refer to chapter 1, “Installing and Configuring Communications Express” of *Sun Java™ Systems Communications Express Administration Guide* (<http://docs.sun.com/doc/817-5416>) for instructions on how to install and configure Sun Java System Communications Express.

Refer to chapter 4, “Implementing Single Sign-On” and chapter 5, “Deploying Communications Express and Identity Server” of *Communications Express Administration Guide* (<http://docs.sun.com/doc/817-5416>) for instructions on how to configure Sun Java System Communications Express when Identity Server is deployed.

Known Issues and Limitations

This section contains a list of the known issues with Communications Express. The following product areas are covered:

- [Config Tool Issues](#)
- [Calendar Issues](#)
- [Mail Issues](#)
- [Address Book](#)

General Issues

This section lists general known issues.

Bug no 5008104: Fully qualified host name required in URL even when the user is authenticated.

The domain name is not set in the cookie if the URL is not with FQHN even when the user is authenticated.

Work around

Always access the application using a Fully Qualified Host Name.

Bug no 5025449: The Day and Year formats in the Calendar views are not consistent.

For Asian locales, in the Day View, the Month has the correct format, but the Day and Year fields in the Calendar are not displayed in an Asian format.

Config Tool Issues

This section contains a list of known issues in the configurator and workaround.

Refer to chapter 1, “Installing and Configuring Communications Express” of *Sun Java™ Systems Communications Express Administration Guide* (<http://docs.sun.com/doc/817-5416>) for post-configuration instructions.

No support to modify web-container configuration for IS SDK integration

The configurator does not support modification of web-container configuration, for Identity Server SDK integration.

Workaround

Manually invoke tools provided with Identity Server to modify web container configuration for Identity Server.

Java Enterprise System Unconfigure is not supported

The uwc client does not allow you to undeploy the uwc application, remove files created at config-time, and remove files created during run-time.

Workaround

To unconfigure Communications Express:

1. Remove the Communications Express package. For example on Solaris type
`pkgrm SUNWuwc.`
2. Remove the staging and deploy directories
3. Remove the WEBAPP entry from Web Server or App Server `server.xml` file.

Bug no 4982590: The components for Communications Express are shown to be zero bytes.

The configurator while displaying the Mail and Calendar components for Communications Express shows the component size as 0 bytes.

Bug no 4988408: A wrong error message is displayed when no components are selected in the config tool.

The config tool displays a wrong error message when no components are selected.

The error message says, "You have not selected Components to be configured.

Click Ok and then go to the Directory Selection Panel to specify a different directory or exit configuration."

Bug no 4996723: GUI config input fields should not be right aligned.

The field names and browser buttons are truncated or not visible when the configuration wizard is invoked in a language other than English.

Workaround

Resize the configuration panels to view its contents properly.]

Bug no 5024149: Misleading error message while installing Communication Express from Java Enterprise System 2004Q2.

After installing the following components from Java Enterprise System 2003Q4 installer, Webserver 6.1 SP1 is grayed out when Communication Express is selected from Java Enterprise System 2004Q2 installer:

- Messaging Server
- Calendar Server

- Directory Server
- Administration Server
- Web Server 6.1

The following misleading and incorrect error message is displayed when Web Server 6.1 SP1 is not available for selection and when you click Next in the Component Selection panel:

```
[Sun ONE Web Server 6.1 Service Pack2, Sun ONE Application Server 7.0 Update 3]
```

You must select one of these in the Component Selection panel. Either one of these is required by [Sun Java System Communications Express]

The error message should mention that an older version of Web Server has been detected and that the users are required to uninstall the previous version of Web Server and install the latest version of Web Server from Java Enterprise System 2004Q2 installer.

Bug no 5028906: UWC Configurator: devinstall is dumping core if host aliases are not resolved.

UWC configurator fails to complete the configuration process if your system is not configured for host name aliases.

Workaround

Ensure that you have configured one or more host name aliases for your system.

To configure one or more host name aliases on UNIX systems:

1. Provide the configuration for the `hosts` in `/etc/nsswitch.conf` file:

```
hosts: files dns nis
```

This configuration indicates to the name service the lookup order it should use to resolve host names and host aliases. The name service lookup order is: `files`, `dns`, and `nis`.

2. Ensure that the `/etc/hosts` file contains two or more host names defined against your machine's IP address.

For example, if your system IP address is `129.158.230.64`, then in `/etc/hosts` file, you can configure the IP address as:

```
129.158.230.64    bugie.siroe.varrius.com budgie
```

or

```
129.158.230.64    bugie.siroe.varrius.com  budgie  loghost
```

An example of an incorrect IP address:

```
129.158.230.64    budgie
```

Bug no 5043406: Remove am*.jar from the Communications Express bundle.

When accessing the Communication Express login page, “Server Error” page is displayed.

Workaround

If Communication Express is configured to use Identity Server:

1. Remove `am_sdk.jar`, `am_services.jar`, `am_logging.jar` from `<uwc-deployed-path>/WEB-INF/lib` directory.

For example, `/var/opt/SUNWuwc/WEB-INF/lib`

2. Restart the web container.

Bug no 5043951: Multiple jss3.jar in classloader error when Communications Express installed.

When accessing Communications Express or Identity Server console, the “Server Error” page is displayed. This problem is encountered when Communications Express and Identity Server are deployed in the same web container instance.

Workaround

1. Remove `jss3.jar` from `<uwc-deployed-path>/WEB-INF/lib` directory.

For example, `/var/opt/SUNWuwc/WEB-INF/lib`

2. Restart the web container.

Calendar Issues

Issues with Default Event Status Filter

The Default Event Status Filter in the Options Calendar window specifies the events to be displayed in the day, week, and month calendar views. The options available are: Accepted, Tentative, Declined, No Response.

When only the “accepted” option is selected as the event status, only invitations you have accepted are displayed in the day, week or month calendar views. However, all events created by you are always displayed in the day, week or month calendar views.

In the Options Calendar Window, by default only “Accepted” and “Tentative” are selected, which means as a user, you will not see events you have declined or to which you have not responded as yet.

To view all the events in the Day, Week, Month, and Year views, you should select all the options, that is, Accepted, Tentative, Declined, No Response in the Options Calendar window.

Incompatibility between the semantics used by Sun Java System Calendar Express and Sun Java System Communication Express for First Day of Week.

The next day appears as the “First Day of Week” in the Options Calendar window when you view calendars created using Sun ONE Calendar Express from the Communications Express

For example if “Sunday” is regarded as the First Day of Week in Sun ONE Calendar Express, it appears as “Monday” in Communications Express. Therefore, Communications Express considers “Monday” to be the first day of the Week.

Communications Express and Sun ONE Calendar Express will behave correctly if they are used exclusively (that is if one is used and the other never used). But, if the user transitions from Sun ONE Calendar to Communications Express, or vice-versa, a shift in the “First Day of Week” option would be observed. This is because there is an incompatibility between the semantics used by the two products associated with this particular option.

Bug no 4906250: Calendar grid lines are not visible on Netscape 7.0 run on Solaris 5.9.

When you invoke Communications Express from Netscape 7.0 running on Solaris 5.9, the Calendar grid lines are not visible in the application.

Bug no 4956450: Search for calendars returns all user’s calendars

When calendars with a particular calendar ID is searched for from the Calendar UI, the search results contain the calendars that do not match the criteria.

Workaround

Set `service.calendarsearch.ldap = "no"` in `ics.conf`, the calendar server configuration file and restart the Calendar Server.

Bug no 5019828: Calendar UI does not render html in the calendar description.

All HTML content in calendar description tag are rendered as garbage in the UI.

Bug no 5025016: Edit Calendar Group View fails editing certain calendar groups created in cal_express

The Edit Calendar Group View fails while editing certain calendar groups created in `cal_express`. The character set that pertains to the calendar group name in Laurel is: A-Z, a-z, 0-9 and underscore(_). The character set that pertains to the old calendar express is: A-Z, 0-9, underscore(_), hyphen(-), period(.) and space(.). Laurel does not expand its valid character set and align it to `cal_express`. Due to this, Edit Calendar Group View fails editing certain calendar groups created in `cal_express`.

Bug no 5030757: Locale fallback mechanisms does not work for certain locale names.

Workaround

Create resource bundle directories with "-" instead of "_" when a locale name with an underscore is to be supported.

For example, if locale en_US needs to be supported, create a directory en-US in `<uwc-data-dir>/domain/<domain-name>`.

Bug no 5035906: Search Results are not displayed when you hit 'Enter' key for 'Search for Calendars'

When you click on Search for Calendars, enter any search text and hit 'Enter', the page gets refreshed. However, the Search Results are not displayed.

Bug no 5050108: Clicking Cancel, when deleting an instance of a recurring event in the Week view, deletes the event.

The selected instance of the recurring event is deleted if you delete a recurring event by clicking the delete icon that appears to the left of the event title in the Week view and then decide not to delete the event by selecting Cancel in the Repeating Selections pop-up window.

Mail Issues

If the Sun Java System Messaging Server is installed from Java Enterprise System 2003Q4, apply the following 2 patches:

- 116568-51
- 116570-09

Bug no 5006218: Netscape 7: Sun logo does not appear for mail URL

In Netscape 7, the URL in the browser has Sun logo in the Mast head when Address Book or Calendar is accessed and Java icon when Mail is accessed.

Work around

Copy the `favicon.ico` file from `$UWCDEPLOYDIR/favicon.ico` to `docroot` directory of Web Server where UWC is deployed.

The value of `docroot` can be found in `server.xml`. An example `docroot` entry appearing in `server.xml` is:

```
<PROPERTY name="docroot" value="/opt/SUNWwbsvr/docs"/>
```

Bug no 5032016: Not able to see mail tab or mails in uwc

If user entry in ldap has `inetUserStatus` and `mailUserStatus` set to "Active" the Mail tab is not shown to the user.

Work around

Change the `inetUserStatus` and `mailUserStatus` to "active."

Bug no 5032833: Mail filters: Creating Mail Filter with certain conditions, throws Application Error.

Creating Mail Filter with certain conditions throws the following error page:

Application Error

com.ipplanet.jato.NavigationException: Exception encountered during forward

Root cause = [java.lang.StackOverflowError]

Work around

To be able to create and manipulate large-sized filters, configure the Java thread stack size appropriately.

Bug no 5032888: Mail filters: Settings not saved properly.

The “File message to folder:” and “Forward to email address:” settings are not saved properly when the Mail Filter details are viewed in the Edit mode.

Bug no 5047833: “getinputOBJ is null” error when adding addresses to email using Mozilla 1.4.

The “inputOBJ is null” JavaScript error message is displayed when a user adds addresses from the address book to email To and Cc fields.

Address Book

Bug no 4995472: The address book Name cannot be localized by defaultps/dictionary-<lang>.xml for every session.

This problem exists because the localized value, based on the resolved session language and the domain specific defaultps/dictionary-<lang>.xml, is assigned when the address book is accessed for the first time.

Also the “Name” and “Description” entered in the Address Book Options page are not displayed in the Current Address Book drop-down list that appears on the Address Book tab page.

Bug no 5025048: l18n Strings are to be localized.

Bug no 5052474: Address Book does not use LDAP VLV control even when vlv_paging=true

When you set `vlv_paging=true` in `db_config.properties`, Address Book still does not use the Virtual List View Control while doing an LDAP search. This may affect the performance of Directory Deployments which have VLV indexes setup.

How to Report Problems and Provide Feedback

If you have problems with Sun Java System Messaging Server, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at
<http://www.sun.com/service/sunone/software>

This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.

- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used to reproduce the problem
- Any error logs or core dumps

You might also find it useful to subscribe to the following interest groups, where Sun Java System Messaging Server topics are discussed:

snews://<YourNewsForum>

snews://<YourSecondNewsForum>

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. Use the web-based form to provide feedback to Sun:

<http://www.sun.com/hwdocs/feedback>

Please provide the full document title and part number in the appropriate fields. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the part number of these Release Notes document is 817-6363-10.

Additional Sun Resources

Useful Sun Java System information can be found at the following Internet locations:

- **Documentation for Messaging Server:**
http://docs.sun.com/coll/MessagingServer_04q2
- **Sun Java System Documentation**
<http://docs.sun.com/prod/sunone>
- **Sun Java System Professional Services**
<http://www.sun.com/service/sunps/sunone>
- **Sun Java System Software Products and Service**
<http://www.sun.com/software>
- **Sun Java System Software Support Services**
<http://www.sun.com/service/sunone/software>
- **Sun Java System Support and Knowledge Base**
<http://www.sun.com/service/support/software>
- **Sun Support and Training Services**
<http://training.sun.com>
- **Sun Java System Consulting and Professional Services**
<http://www.sun.com/service/sunps/sunone>
- **Sun Java System Developer Information**
<http://sunonedev.sun.com>
- **Sun Developer Support Services**
<http://www.sun.com/developers/support>
- **Sun Java System Software Training**
<http://www.sun.com/software/training>
- **Sun Software Data Sheets**
<http://www.sun.com/software>

Copyright © 2004 Sun Microsystems, Inc. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

SUN PROPRIETARY/CONFIDENTIAL.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

Use is subject to license terms.

This distribution may include materials developed by third parties.

Portions may be derived from Berkeley BSD systems, licensed from U. of CA.

Sun, Sun Microsystems, the Sun logo, Java and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries.

Copyright © 2004 Sun Microsystems, Inc. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuels relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

Propriété de SUN/CONFIDENTIEL.

L'utilisation est soumise aux termes du contrat de licence.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie.

Sun, Sun Microsystems, le logo Sun, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays.

