Sun Java Communications Suite 5 What's New

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 820–0430
March 2007

Contents

Preface 5

1 **What's New in Sun Java Communications Suite 5** 9

Change in Availability of Communications Suite Products 9

Sun Java Enterprise System Monitoring Framework 10

What's New in This Release of Calendar Server 10

Calendar Server Support in Delegated Administrator Console 11

WCAP Attachment Support 11

Support for LDAP Groups 12

Multiple Domain Mode Only 12

Configuration Program Enhancements 12

Recurrence Details Included in Email Invitations 13

Automatic Backup Process Now a Shared Library 13

Automatic Restart of Services Using Watcher 13

Monitoring Framework Integration 16

Transition to Message Queue for Notification Services 18

Organizers Can Now Receive Reply Notifications 20

Attendees Can Now Modify Their Copy of an Event 20

Rename Tool Enhancement 20

Free-Busy Calculation Change 21

Disabling the Old Calendar Express UI 21

Installing on Mixed Hardware Platforms 21

iTIP Compatibility 21

commdssetup.pl: New Option for a Password File Enhances Security 22

csdb, cscal, csuser Relocated to cal/sbin 22

SSL Changes to ics.conf File 22

What's New in This Release of Messaging Server 22

AXS-One Archiving 23

- Webmail Server Supports IMAP 23
- MeterMaid 24
- Milter 24
- Support of IMAP Standard Extensions 24
- User Lookup and Authentication Improvements 25
- New imsconnutil option 26
- JMQ Notification 26
- Sender Policy Framework 26
- Quota by Type and by Folder 26
- Obtaining Server SSL Certificates 26
- New MMP Features 27
- New MTA Features 27

What's New in This Release of Instant Messaging 34

- Instant Messaging XMPP Redirect Server 34
- Instant Messaging Redeploy Script Changes 34
- Event Notification Service (ENS) Support in Instant Messaging 34
- Legacy SSL and TLS Support for Instant Messaging 34

What's New in This Release of Delegated Administrator 35

- Support for Calendar Groups 35
- Web Server 7.*x* Deployment 36
- Access to Instant Messaging 36
- Debug Log Command for the Delegated Administrator Server 36

What's New in This Release of Communications Express 37

- Support for Attachments in Events/Tasks 37
- Next Available Free Period Button 37
- Address Book Sharing 37
- Support for Multiple Address Book 37
- Preserving Customization 37
- Password Encryption 38
- LDAP Failover Mechanism 38
- Mail Integration into Communications Express 38
- Removal of Access Manager SDK Dependency for Schema 2 Deployment 38

What's New in This Release of Connector for Microsoft Outlook 39

Preface

Sun Java Communications Suite 5 What's New summarizes all features in Sun Java™ Communications Suite 5 that are new or have been enhanced since Sun Java Enterprise System 2005Q4 was originally distributed in October 2005.

Who Should Use This Book

This guide is for individuals who are responsible for assessing and deploying Communications Suite at your site, including:

- Evaluators
- Architects
- System administrators

Before You Read This Book

This guide assumes you are familiar with the following:

- How to design and install enterprise-level software products
- IMAP, POP, HTTP, SMTP, WCAP, LDAP, and XMPP protocols
- Solaris™ Operating System (Solaris OS) system administration and networking

Related Books

The `http://docs.sun.com` web site enables you to access Sun technical documentation online. You can browse the archive or search for a specific book title or subject.

Books in This Documentation Set

For books in the Communications Suite documentation set, go to the following:

- Sun Java System Messaging Server documentation
- Sun Java System Calendar Server documentation

- Sun Java System Instant Messaging documentation
- Sun Java System Communications Express documentation
- Sun Java System Connector for Microsoft Outlook documentation

The following guides have not been updated for this release. However, you can use the previous versions of these guides:

- *Sun Java System Messaging Server 6 2005Q4 MTA Developer's Reference*
- *Sun Java System Messenger Express 6 2005Q4 Customization Guide*
- *Sun Java System Communications Services 6 2005Q4 Schema Migration Guide*

Accessibility Features for People With Disabilities

To obtain accessibility features that have been released since the publishing of this media, consult Section 508 product assessments available from Sun upon request to determine which versions are best suited for deploying accessible solutions. Updated versions of applications can be found at `http://sun.com/software/javaenterprisesystem/get.html`.

For information on Sun's commitment to accessibility, visit `http://sun.com/access`.

Related Third-Party Web Site References

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 or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Training (`http://www.sun.com/training/`)

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`

`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`**
		`Password:`

aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	Prompt
C shell	`machine_name%`
C shell for superuser	`machine_name#`
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell for superuser	`#`

CHAPTER 1

What's New in Sun Java Communications Suite 5

This document summarizes all features in Sun Java Communications Suite 5 that are new or have been enhanced since Sun Java Enterprise System 2005Q4 was originally distributed in October 2005, for the following components:

- Sun Java System Calendar Server 6.3
- Sun Java System Messaging Server 6.3
- Sun Java System Instant Messaging 7.2
- Sun Java Communications Suite 5 Delegated Administrator
- Sun Java System Communications Express 6.3
- Sun Java System Connector for Microsoft Outlook 7.2

This chapter contains the following sections:

- "Change in Availability of Communications Suite Products" on page 9
- "Sun Java Enterprise System Monitoring Framework" on page 10
- "What's New in This Release of Calendar Server" on page 10
- "What's New in This Release of Messaging Server" on page 22
- "What's New in This Release of Instant Messaging" on page 34
- "What's New in This Release of Delegated Administrator" on page 35
- "What's New in This Release of Communications Express" on page 37
- "What's New in This Release of Connector for Microsoft Outlook" on page 39

Change in Availability of Communications Suite Products

Beginning with this release of Communications Suite 5, communications products are being removed from the Sun Java Enterprise System entitlement. Communications products are available as part of the Communications Suite or as individual products. Communications products will no longer be installed through the Java Enterprise System installer. Communications product components continue to interoperate with Java Enterprise System components.

This change in entitlement does not affect the communications products in Java Enterprise System 2005Q4. If you have communication products installed, no change will occur to your entitlement.

Sun Java Enterprise System Monitoring Framework

This release of Communications Suite supports version 2.0 of the monitoring framework. This monitoring framework provides information on the length of time for authentication, message delivery, the number of instant messages sent through the service, and other statistics.

For information on the Sun Java Enterprise System Monitoring Framework, see: *Sun Java Enterprise System 5 Monitoring Guide*.

What's New in This Release of Calendar Server

Calendar Server 6.3 includes the following changes and new features:

- “Calendar Server Support in Delegated Administrator Console” on page 11
- “WCAP Attachment Support” on page 11
- “Support for LDAP Groups” on page 12
- “Multiple Domain Mode Only” on page 12
- “Configuration Program Enhancements” on page 12
- “Recurrence Details Included in Email Invitations” on page 13
- “Automatic Backup Process Now a Shared Library” on page 13
- “Automatic Restart of Services Using Watcher” on page 13
- “Monitoring Framework Integration” on page 16
- “Transition to Message Queue for Notification Services” on page 18
- “Organizers Can Now Receive Reply Notifications” on page 20
- “Attendees Can Now Modify Their Copy of an Event” on page 20
- “Rename Tool Enhancement” on page 20
- “Free-Busy Calculation Change” on page 21
- “Disabling the Old Calendar Express UI” on page 21
- “Installing on Mixed Hardware Platforms” on page 21
- “iTIP Compatibility” on page 21
- “commdssetup.pl: New Option for a Password File Enhances Security” on page 22
- “csdb, cscal, csuser Relocated to cal/sbin” on page 22
- “SSL Changes to ics.conf File” on page 22

Calendar Server Support in Delegated Administrator Console

In the past, provisioning Calendar Server for Schema 2 could be done with the Delegated Administrator Utility, but not with Delegated Administrator Console. Before this release, the Console was the Web graphical user interface for administering only Messaging Server . Now the Console can also be used to administer calendar LDAP entries. With the Console, you can add, delete, or modify LDAP entries for calendar users, groups, resources, and domains. New screens and menu items were added to the Console to support Calendar Server. For directions on how to use the interface, see the Delegated Administrator online help. Some information is also available in the *Sun Java System Calendar Server 6.3 Administration Guide*.

WCAP Attachment Support

Attachment support has been added to WCAP commands with the addition of new parameters and values.

While Communications Express, the Web user interface, does not support attachments yet, users of the Connector for Microsoft Outlook can now put attachments in their events and tasks, and can send attachments with invitations.

As part of attachment support, the following changes have been made to WCAP:

- `fetchattachment.wcap`: a new command has been added to facilitate fetching of attachments. Only the attachment is fetched, not the event or task data itself.
- `deleteattach`: a new argument for the `storeevents` command, used to delete existing attachments from an event or task without deleting the event or task itself.
- `fetchattach`: a new parameter added to all `fetch_by_*` commands so that attachments can be returned as well as the event and task data itself.
- `sendattach`: a new parameter for the `storeevents` command, used to specify whether the actual attachment is sent with the iTIP invitation, or not.
- `X-S1CS-CLIENT-ATTACH-ID`: an X-Token containing the attachment's unique identifier. This X-Token is emitted only if the client supplied the attachment ID when the attachment was stored. Otherwise, the actual attachment is sent with the event.
- The `attachments` argument can store a URL reference to attachments. These attachments are not stored in the data store.

For further information about attachments, see *Sun Java System Calendar Server 6.3 WCAP Developer's Guide*.

Support for LDAP Groups

It is now possible to create LDAP groups using Delegated Administrator. Groups have the following functionality:

- A group is a list of users. The group does not “contain” the listed users. It is not a container.
- A group can have a group calendar.
- Invitations sent to a group reside on all the members' calendars, as well as the group calendar.
- All members of the group share the same access rights to the group calendar.
- There is no primary owner for a group calendar.

Multiple Domain Mode Only

Now all installations are automatically in multiple domain mode. Non-domain mode is not allowed. If your previous Calendar Server deployment did not use multiple domains, or even a single domain, you will now be required to have at least one domain, your default domain.

Configuration Program Enhancements

The configuration program has added screens for:

- “Creating Your Default Domain” on page 12
- “Support of Distributed Calendar Server Databases” on page 12
- “Email Address Field Added to Configuration Wizard Screen” on page 12

Creating Your Default Domain

Starting with this release, there will always be at least one domain under the root. This will be the default domain. Now you can specify the name of the default domain for your multiple domain environment in the configuration program.

Support of Distributed Calendar Server Databases

Now you can specify the names of the front-end and back-end machines for your distributed database environment, that uses the DWP protocol and the CLD plug-in. The calendar databases can be distributed over one or more back-end machines. These machines can be associated with one front-end machine. The new configuration program screens allow you to name the back-end machines and associate them with the front-end machine.

Email Address Field Added to Configuration Wizard Screen

In the default domain screen, a new field was added for the email address of the calendar super user (`calmaster`).

Recurrence Details Included in Email Invitations

For recurring events, email invitations sent to attendees now contain recurrence details.

Automatic Backup Process Now a Shared Library

The `csstored.pl` program is now a shared library.

Automatic Restart of Services Using Watcher

Calendar Server and Messaging Server now use the same stop and start mechanism. The `start-cal` and `stop-cal` commands are wrappers for a new internal service, `csservice`, which was introduced as part of the Watcher implementation. This service starts the Watcher, and then starts all other processes. The `csservice` program is aware of any dependencies the other services have, and in which sequence the services should be started.

Each registered service (process) opens a connection to the Watcher. If a process dies without properly disconnecting, the Watcher automatically restarts it. If the process dies twice in a defined interval, Watcher does not restart it. This timeout interval is configurable.

Additional Watcher information:

- "Calendar Server Services Monitored by Watcher" on page 13
- "Configuring Watcher" on page 14
- "Watcher Logging" on page 14
- "Automatic Restart in High Availability Deployments" on page 14
- "Wrapper Scripts for csservice" on page 14

Calendar Server Services Monitored by Watcher

The Watcher monitors all of the services registered with it. For Calendar Server, the registered processes are: `cshttpd`, `csadmind`, `csdwpd`, `dsnotifyd`.

If `csstored` is enabled, that is, if the configuration parameter `local.store.enable` is set to `"y"`, then `csstored` is also registered with the Watcher. When it is enabled, `csstored` must be successfully started before each service that accesses the store can be started. If it stops, then the dependent processes must be stopped an restarted also.

Configuring Watcher

Watcher is enabled by default. To manage the Watcher process, new parameters were added to the `ics.conf` file:

- `local.watcher.enable = "y"`: the start program (`csservice`) attempts to start the Watcher before any other services. If this parameter is set to `"n"`, then the Watcher program is disabled.
- `service.autorestart = "y"`: the Watcher automatically restarts stopped services. If set to `"n"`, Watcher does not restart stopped services. If this parameter is set to `"n"` , Watcher still monitors the services and sends failure or non-response error messages to the console and the *cal_svr_base*`/data/log` file.
- `local.autorestart.timeout = "600"`: the default time within which a second server failure triggers Watcher to stop trying to do a restart.
- `local.watcher.port`: the default port is `"49994"`; however, if you have Messaging Server, it will also be listening on this port and will be in conflict with Calendar Server. To avoid possible conflict, it is safer to choose a different port for Watcher to listen on.

Watcher Logging

Watcher writes to two logs:

- *cal_svr_base*`/data/log`: watcher sends failure notices and non-response error messages to the console. These messages are also written to this log.
- *cal_svr_base*`/data/log/watcher`: watcher records all server stops and starts in this log file.

Automatic Restart in High Availability Deployments

If a server fails twice within the timeout period, the system stops trying to restart the server. In an HA system, Calendar Server is shutdown and a failover to the other system occurs.

Wrapper Scripts for csservice

The public interfaces to `csservice` are `start-cal` and `stop-cal`. This section shows the usage for each of these wrapper scripts and contains tables with explanations of their options and a list of components to be started or stopped.

start-cal Wrapper Script

The `start-cal` usage is as follows:

```
./start-cal [options...] [components...]
```

The following is the list of options:

`-?` or `--help`	Display this help list.

`-d`	Enable debugging mode.
`-l`	List active services.
`-L`	List enabled services.
`-A`	List all services.

This following is the list of components:

```
watcher
mfagent
ens
store
notify
admin
http
dwp
```

If no components are listed, `start-cal` starts all enabled services.

stop-cal Wrapper Script

The `stop-cal` usage is as follows:

```
./stop-cal [options...] [components...]
```

The following is the list of options:

`-?` or `--help`	Display this help list.
`-d`	Enable debugging mode.
`-f`	Force stop using SIGKILL. (This works only with UNIX® platforms.)

This following is the list of components:

```
watcher
mfagent
ens
store
notify
admin
http
dwp
```

If no components are listed, `stop-cal` stops all enabled services.

Monitoring Framework Integration

This section describes the Calendar Server implementation of the Monitoring Framework and covers the following topics:

- “How the Monitoring Framework is Implemented in Calendar Server” on page 16
- “Configuration of Calendar Server for Monitoring Framework” on page 16
- “Configuring Monitoring Framework for Calendar Server” on page 16
- “Installation Requirements” on page 17

Documentation of the Monitoring Framework and be found at it*Sun Java Enterprise System 5 Monitoring Guide*.

How the Monitoring Framework is Implemented in Calendar Server

Calendar Server and Messaging Server both integrate minimally into the Monitoring Framework for Java Enterprise System. While the Monitoring Framework is running, it periodically checks the following attribute, `operationalStatus` , which can have the status of either `OK`, which means the system is running, or `DOWN`, which means the system is not running.

A new process, the Monitoring Framework agent (`csmfagent`), starts with system start up (`start-cal`). This is the first process started. The process instantiates an application and asserts its status as `OK`. It also catches `SIGTERM` and upon catching one, asserts status `DOWN` and exits.

Similarly, if the Watcher is configured and running, if any part of the system fails or becomes unresponsive, Watcher signals `SIGTERM`, which stops `csmfagent`.

Configuration of Calendar Server for Monitoring Framework

Edit the configuration file, `ics.conf`, to contain the following parameter:

```
local.csmfagent.enable = "y"
```

Configuring Monitoring Framework for Calendar Server

Perform the following two steps:

1. Copy `/opt/SUNWcsgar/config/om.sun.cmm.cs.xml` to `/opt/SUNWmfwk/xml`.
2. Stop and then restart the Manufacturing Framework process.

Installation Requirements

There are two requirements to be able to use the Monitoring Framework:

1. The Java Enterprise System Monitoring Framework (JESMF) must be installed.

   If JESMF is not installed, `csmfagent` won't run.

2. Calendar Server must be able to find the necessary libraries.

   Calendar Server finds the libraries using symbolic links in `/opt/SUNWics5/lib`.

The following are the JESMF libraries:

```
/opt/SUNWmfwk/lib/libMfTransaction.so
/opt/SUNWmfwk/lib/libMfRelations.so
/opt/SUNWmfwk/lib/libMflog4c.so
/opt/SUNWmfwk/lib/libMfMEServer.so
/opt/SUNWmfwk/lib/libmfBeepConnectorServer.so
/opt/SUNWmfwk/lib/libMfRserver.so
/opt/SUNWmfwk/lib/libMfMEInstrum.so
/opt/SUNWmfwk/lib/libMfDiscovery.so
/opt/SUNWmfwk/lib/libMfHashTable.so
/opt/SUNWmfwk/lib/libMflog.so
/opt/SUNWmfwk/lib/libasn1cebuf.so
/opt/SUNWmfwk/lib/libbeepcore.so
/opt/SUNWmfwk/lib/libbeepxmlutil.so
/opt/SUNWmfwk/lib/libbptostransport.so
/opt/SUNWmfwk/lib/libbptosutil.so
/opt/SUNWmfwk/lib/libbptoswrapper.so
/opt/SUNWmfwk/lib/libbputil.so
/opt/SUNWmfwk/lib/libcmm_native.so
/opt/SUNWmfwk/lib/libmfCserver.so
/opt/SUNWmfwk/lib/libmfNotificationProfile.so
/opt/SUNWmfwk/lib/libmfRequestResponseProfile.so
/opt/SUNWmfwk/lib/libmfTimers.so
/opt/SUNWmfwk/lib/libmfTimersJNI.so
/opt/SUNWmfwk/lib/libmfUtils.so
/opt/SUNWmfwk/lib/libmfber.so
/opt/SUNWmfwk/lib/libmfberj.so
/opt/SUNWmfwk/lib/libxmlglobal.so
```

Note – Its possible not all of these files are necessary to implement Calendar Server's part of Monitoring Framework. This is just a list of all the JESMF libraries.

Transition to Message Queue for Notification Services

In this release, there are two notification services for event notifications and alarms: Sun Java System Message Queue (JMQ) and the Event Notification System (ENS). In a future release, the Communications Service products will use JMQ exclusively, and ENS will be removed. However, for this release, the Communications Services products (Messaging Server, Calendar Server, and Instant Messaging) still have internal dependencies on ENS, and you can continue to use ENS for notifications and alarms.

To use JMQ, rather than ENS, you must have Sun Java System Message Queue installed and configured. Install the product using the Sun Java Enterprise System installer. For information about configuring Message Queue, see theMessage Queue Documentation (`http://docs.sun.com/coll/1307.2`).

Calendar Server Configuration Parameters for JMQ

To configure Calendar Server for JMQ, you must add the following lines to the `ics.conf` file:

```
local.server.csmfagent.enable = "yes"
```

```
caldb.serveralarms.jmqlib = "/opt/SUNWics5/cal/lib/libmqcrt.so" (for Solaris)
```

Or,

```
caldb.serveralarms.jmqlib = "/opt/sun/calendar/lib/libmqcrt.so" (for Linux)

caldb.serveralarms.dispatchtype = "jmq"

caldb.serveralarms.jmqhost = "localhost"

caldb.serveralarms.jmqport = "7676"

caldb.serveralarms.jmqUser = "guest"

caldb.serveralarms.jmqPWD = "guest"

caldb.serveralarms.jmqTopic = "JES-CS"
```

Update Notification Properties

Each notification must have the following property: `MQ_MESSAGE_TYPE_HEADER_PROPERTY`. This property identifies what kind of notification it is.

In addition, notifications can have other properties as shown in the following table:

action A string property that indicates the type of action this notification produces. This property can have the following values: `"EMAIL"`, `"AUDIO"`, `"DISPLAY"`, `"PROCEDURE"`, `"FLASHING"`.

aid A string property containing the alarm ID.

calid A string property containing the calendar ID.

comptype A string property indicating the type of component. The value is either `"event"` or `"todo"`.

rid An integer property containing the recurrence ID.

uid A string property containing the component ID, that is either the event ID or the todo ID (task ID)

Update Notification Values

Notifications can be of two types: alarm notifications and update notifications for events and todos.

For alarm notifications, the value of `MQ_MESSAGE_TYPE_HEADER_PROPERTY` is simply `"alarm"`.

For update notifications, the value of `MQ_MESSAGE_TYPE_HEADER_PROPERTY` depends on the type of action that triggered the notification. The following table lists the trigger actions and the corresponding values for this property.

TABLE 1–1 Update Notifications Values

Trigger	Update Notification Value
Deleting a calendar	`DELETECAL`
Modifying an event	`MODIFYEVENT`
Modifying a todo (task)	`MODIFYTODO`
Creating an event	`CREATEEVENT`
Creating a todo (task)	`CREATETODO`
Refreshing an event	`REFRESHEVENT`
Refreshing a todo (task)	`REFRESHTODO`
Replying to an event	`REPLYEVENT`
Replying to a todo	`REPLYTODO`

Organizers Can Now Receive Reply Notifications

Email notifications can now be sent to organizers when an attendee replies to an invitation.

Configure this feature by setting the `ics.conf`parameter `ine.reply.enable`. Set it to `"y"` to enable the feature for the entire system. Set it to `"n"` to disable the feature. The feature is enabled by default.

The three reply types are: accept, decline, tentatively accept. The notification indicates whether the reply is to a single invitation or to an recurring event. The following new message format file parameters were added. The corresponding format files were also added:

- `calmail.imipeventacceptnotification.fname=`
  `"mail_eventacceptnotification.fmt"`
- `calmail.imipeventdeclinenotification.fname=`
  `"mail_eventdeclinenotification.fmt"`
- `calmail.imipeventtentativeacceptnotification.fname=`
  `"mail_eventtentativeacceptnotification.fmt"`
- `calmail.imipeventacceptnotificationrecur.fname=`
  `"mail_eventacceptnotificationrecur.fmt"`
- `calmail.imipeventdeclinenotificationrecur.fname=`
  `"mail_eventdeclinenotificationrecur.fmt"`
- `calmail.imipeventtentativeacceptnotificationrecur.fname=`
  `"mail_eventtentativeacceptnotificationrecur.fmt"`

Note – This feature is not a user preference. That is, it is a system wide configuration parameter, so it applies to all users who send invitations.

For more information about configuring Calendar Server for email notifications, see "To Enable Email Notifications" in *Sun Java System Calendar Server 6.3 Administration Guide*, in the Calendar Server Administration Guide.

Attendees Can Now Modify Their Copy of an Event

Attendees now can modify information in an event on their calendar, including the summary and description.

Rename Tool Enhancement

The Calendar Server utility `rename` now renames deleted events.

Free-Busy Calculation Change

Declined events no longer show up as busy in free-busy calendars.

Disabling the Old Calendar Express UI

With earlier versions of Calendar Server, Calendar Express (the old user interface) was always enabled, even if you did not use the interface. Now it is possible to disable Calendar Express explicitly, using the new `ics.conf` parameter, `service.http.ui.enable`.

If you are upgrading from an earlier version of Calendar Server, the upgrade process adds the parameter to the `ics.conf` file set to `"y"`. This allows the legacy user interface to continue to be used without any changes. However, if you wish to disable it, set this parameter to `"n"`.

Since Calendar Express was deprecated, and is no longer automatically installed in a fresh installation, the parameter does not appear in the `ics.conf` file. The default internal setting is `"n"`.

If you intend to use Calendar Express in a fresh installation, you must install Calendar Express and then add `service.http.ui.enable="y"` to the `ics.conf` file.

Installing on Mixed Hardware Platforms

In the past, for distributed database environments (DWP with CLD Plug-in), front-end and back-end processes had to be installed on the same hardware platform due to big endian-little endian problems. That is no longer true. Front-end and back-end processes can now be installed on different hardware platforms.

For example, a front-end machine could be an X-86 platform machine, while the back-end is a SPARC platform machine.

iTIP Compatibility

Messages sent by Calendar Server are now iTIP compatible (for Microsoft Outlook interoperability).

commdssetup.pl: New Option for a Password File Enhances Security

To enhance security, it is now possible to specify a password file rather than a text password when running `commdssetup.pl`. With the new `-j <passwordfilename>` option, you can protect passwords and enhance security. This is especially useful for scripts. If you have scripts that currently expose the password, and wish to change them, delete the `-w < password>` option and replace it with this new one.

Note – This is a fix for problem #6392093.

---

csdb, cscal, csuser Relocated to cal/sbin

In earlier versions of Calendar Server, csdb, cscal, and csuser were found in the `cal/bin` directory, but now are located in the `cal/sbin` directory.

SSL Changes to ics.conf File

Due to changes in Calendar Server program code, the following changes have been made to the `ics.conf` file:

- `service.http.ssl.certdb.path` deprecated in favor of `local.ssldbpath`. The path given should point to the `config` file (`"/etc/opt/SUNWics5/config"`).
- Instead of including the actual password to the certificate database in the `ics.conf` file, the password now resides in a file (`sslpassword.conf`) inside the `config` directory.

  The proper format for a password in this file is:

  ```
  Internal (Software) Token: password
  ```

What's New in This Release of Messaging Server

The following new features and enhancements were added to the Messaging Server 6.3 release:

- "AXS-One Archiving" on page 23
- "Webmail Server Supports IMAP" on page 23
- "MeterMaid" on page 24
- "Milter" on page 24
- "Support of IMAP Standard Extensions" on page 24
- "User Lookup and Authentication Improvements" on page 25
- "New imsconnutil option" on page 26

- "JMQ Notification" on page 26
- "Sender Policy Framework" on page 26
- "Quota by Type and by Folder" on page 26
- "Obtaining Server SSL Certificates" on page 26
- "New MMP Features" on page 27
- "New MTA Features" on page 27

AXS-One Archiving

Messaging Server supports archiving through the AXS-One archive system. A message archiving system saves all or some specified subset of incoming and outgoing messages on a system separate from Messaging Server. Sent, received, deleted, and moved messages can all be saved and retrieved in an archive system. Archived messages cannot be modified or removed by email users so the integrity of incoming and outgoing is maintained. Message archiving is useful for compliance record keeping, message store management, and message back up. See *Message Archiving Using the AXS-One System* for more information.

Webmail Server Supports IMAP

The webmail server, also known as `mshttpd` (Messaging Server HTTP Daemon), provides email services to the Messenger Express and Communications Express clients. Now, the webmail server accesses the message store through the IMAP server. This provides several advantages:

- Messenger Express and Communications Express clients are now able to access shared folders that are located on different back-end message stores.
- The webmail server no longer must be installed on each back-end server.
- The webmail server can serve as a front-end server performing the multiplexing capabilities previously performed by Messenger Express Multiplexor (MEM).
- MEM is no longer used.
- On the client side, nothing is changed except that users can now access shared folders that are not on their message store. In previous versions, the MEM received HTTP client requests and forwarded it to the appropriate webmail server on the appropriate back-end message store. Because of this, a copy of `mshttpd` had to be installed on every back-end server. Now, the webmail server operates as a front-end server receiving HTTP client email requests. It translates these requests to SMTP or IMAP calls and forwards the calls to either the MTA or the appropriate IMAP server on the back-end message store.

MeterMaid

MeterMaid allows throttling by determining when an IP address has recently connected too often and should be turned away for awhile. MeterMaid represents the officer patrolling the streets, looking for those who have exceeded their allotted amount. It is a repository process that supplants `conn_throttle.so`, providing similar functionality but extending it across the Messaging Server product. In addition, MeterMaid is more configurable than `conn_throttle.so`.

Note – At this time, no further enhancements will be made to `conn_throttle.so` .

Milter

Programs based on the Sendmail Content Management API, also called Milters (short for Mail Filter), can now be run in Messaging Server. Milter provides a plug-in interface for third-party software to validate and modify messages as they pass through the MTA. Milters can process a message's connection (IP) information, envelope protocol elements, message headers, and/or message body contents, and modify a message's recipients, headers, and body. Possible uses for filters include spam rejection, virus filtering, and content control. In general, Milter seeks to address site-wide filtering concerns in a scalable way. See "Using Milter" in *Sun Java System Messaging Server 6.3 Administration Guide*.

Support of IMAP Standard Extensions

- IMAP SORT

  See: `http://www.ietf.org/internet-drafts/draft-ietf-imapext-sort-17.txt`
- IMAP COMPARATOR
- IMAP IDLE

  The IMAP IDLE extension to the IMAP specification, defined in RFC 2177, allows an IMAP server to notify the mail client when new messages arrive and other updates take place in a user's mailbox. The IMAP IDLE feature has the following benefits:

  - Mail clients do not have to poll the IMAP server for incoming messages.

    Eliminating client polling reduces the workload on the IMAP server and enhances the server's performance. Client polling is most wasteful when a user receives few or no messages; the client continues to poll at the configured interval, typically every 5 or 10 minutes.
  - A mail client displays a new message to the user much closer to the actual time it arrives in the user's mailbox. A change in message status is also displayed in near-real time.

> The IMAP server does not have to wait for the next IMAP polling message before it can notify the client of a new or updated mail message. Instead, the IMAP server receives a notification as soon as a new message arrives or a message changes status. The server then notifies the client through the IMAP protocol.

IMAP IDLE is off by default; in future releases, the default may be on.

User Lookup and Authentication Improvements

User lookup and authentication is now performed by a library that all processes should be using. The result is more consistent and faster authentication.

This release supports the MMP implementation. The next release supports implementation in the Message Store and the MTA.

The following interface changes will affect the MMP:

- The MMP now supports user status attributes. Prior to this release, the MMP relied on the back-end servers to enforce user status. This change reduces load on the back-end during user migration scenarios.
- The MMP log messages have been normalized to always include an integer connection id which is not reused during the MMP process lifetime. Previously, the MMP messages used a hex connection context address which could be reused. Furthermore, the `lpool` layer used a different context address that was difficult to correlate. Now the MMP, `hula` and `lpool` layers will all use the same ID.
- The MMP debug log level configuration setting now uses syslog-style log levels rather than unspecified numeric levels. The `LogLevel`option used to default to 1; it now defaults to 5 (LOG_NOTICE). Values below 3 produce no output. Values from 3 (LOG_ERR) to 7 (LOG_DEBUG) provide different quantities of output in the debug log.
- The MMP will now support the following additional MTA options from `option.dat`: `LDAP_DOMAIN_FILTER_SCHEMA1, LDAP_DOMAIN_FILTER_SCHEMA2, LDAP_ATTR_DOMAIN1_SCHEMA2, LDAP_ATTR_DOMAIN2_SCHEMA2, LDAP_ATTR_DOMAIN_SEARCH_FILTER, LDAP_DOMAIN_ATTR_BASEDN, LDAP_DOMAIN_ATTR_CANONICAL, LDAP_DOMAIN_ATTR_ALIAS, LDAP_UID, LDAP_DOMAIN_ATTR_UID_SEPARATOR, LDAP_DOMAIN_ATTR_STATUS, LDAP_DOMAIN_ATTR_MAIL_STATUS, LDAP_USER_STATUS, LDAP_USER_MAIL_STATUS.`
- The `ident` support in TCP access filters was implemented but untested in previous releases. A warning was placed in the manual that `ident` support was deprecated several releases ago. The new code does not implement support for `ident`. Filters which require `ident`will cause authentication to fail with an error.
- Previous versions of MMP permitted user names with any UTF-8 character although this was untested. Correct UTF-8 syntax is now enforced, and overlong encodings and surrogates are fobidden.

New imsconnutil option

The new `-k` option of the `imsconnutil` utility disconnects users from IMAP and POP sessions. Users logged on to Communications Express lose the underlying IMAP connection and, thus, are also disconnected.

JMQ Notification

The JMQ Notification plug-in allows you to deliver notification messages using the Java Messaging Service (JMS) standard. You can now configure plug-ins to send notifications to two different messaging services:

- Sun Java System Message Queue 3.6 or later, which implements the JMS standard
- Event Notification Service

With Message Queue, you can produce topics to a message or a queue, or to both of these delivery methods. Message Queue also provides enhanced load balancing, scalability, and reliability. See Chapter 22, "Configuring the JMQ Notification Plug-in to Produce Messages for Message Queue," in *Sun Java System Messaging Server 6.3 Administration Guide*.

Sender Policy Framework

Sender Policy Framework (SPF) is a technology that can detect and reject forged email during the SMTP dialogue. Specifically, SPF is a method that allows a domain to explicitly authorize the hosts that may use its domain name. In addition, a receiving host may be configured to check this authorization. SPF can thus significantly reduce the instances of forged email. See: Controlling Forged Email Using the Sender Policy Framework

Quota by Type and by Folder

Message store quotas can now be set for specific folders and message types. Message type quotas allow you to specify limits for message type like voicemail and email. Folder quotas set limits on the size of a user's folder in bytes or messages. For example, a quota can be set on the Trash folder. Messaging Server allows you to set default quotas for domains and users as well as customized quotas. See "About Message Store Quotas" in *Sun Java System Messaging Server 6.3 Administration Guide*.

Obtaining Server SSL Certificates

Certificates can no longer be obtained through the Administration Console. Instead, a new command called `msgcert` is used. The old `certutil` command can still be used, but it is much more complicated and is not internationalized. See "Obtaining Certificates" in *Sun Java System Messaging Server 6.3 Administration Guide* for details.

New MMP Features

- Previous versions of the MMP did not look at the `inetUserStatus`, `mailUserStatus`, `inetDomainStatus`, `mailDomainStatus` attributes. The MMP relied on the back-end server to reject connections when accounts were inactive, disabled or deleted. The current version of the MMP now supports these attributes and terminates the connection at the MMP layer if the status is something other than "active", "overquota" or empty. This should improve the scalability of a deployment when migrating users.
- *MMP debug log levels and session ID:* The meaning of the "LogLevel" configuration option for the MMP has been changed to make it follow `syslog` conventions. In previous releases, it was an arbitrary value defaulting to 1. In this release it follows syslog conventions. The default value is 5 (`LOG_NOTICE`), and values from 3 (`LOG_ERR`) to 7 (`LOG_DEBUG`) alter the set of messages displayed and have the same meaning they do for `syslog()` . Also, the messages in the MMP debug log files now use a session/connection id that is numeric and unique within the lifetime of the MMP process.

New MTA Features

The `imsimta cache -change` command allows certain job controller parameter changes to immediately take effect. The allowed formats of this command are:

- `imsimta cache -cache -global -debug=` *integer*
- `imsimta cache -change -global -max_messages=` *integer*
- `imsimta cache -change -channel_template =` *name* `master_job =` *command*
- `imsimta cache -change -channel_template=` *name* `slave_job=`*command*
- `imsimta cache -change -channel=` *name* `master_job=`*command*
- `imsimta cache -change -channel=` *name* `slave_job=`*command*
- `imsimta cache -change -channel=` *name* `thread_depth=`*integer*
- `imsimta cache -change -channel=` *name* `job_limit=`*integer*

Changing parameters for a channel template (such as `tcp_*`) changes that parameter for all channels derived from that template.

The imsimta qm jobs command displays what messages are being processed by what jobs for what channels. Output might be in the following format:

```
channel <channel name>

job <pid>

host <host name>

host <host name>

<count of hosts> HOST BEING PROCESSED BY JOB <pid>

message <subdir/message name>

message <subdir/message name>

processed messages: <# messages successfully dequeued>

failed processing attempts: <# messages reenqueued>

<count of messages> MESSAGES BEING PROCESSES BY JOB <pid>

<count of jobs> JOBS ACTIVE FOR CHANNEL foo

<count of active channels> ACTIVE CHANNELS
```

The following input flags are now available in the FORWARD mapping. In the past they were only available to the various *_ACCESS mappings.

E - Incoming connection used ESMTP/EHLO.

L - Incoming connection used LMTP/LHLO.

F - NOTIFY=FAILURES active for this recipient.

S - NOTIFY=SUCCESSES active for this recipient.

D - NOTIFY=DELAYS active for this recipient.

A - SASL used to authenticate connection.

T - SSL/TLS used to secure connection.

The buffer used for spamfilter verdict destination strings has been increased in size from 256 to 1024 characters. This was done to accommodate the much longer verdict destination strings that Brightmail 6.0 can return.

Two new values now have meaning for the various SPAMFILTERx_OPTIONAL MTA options: 3 and 4. A value of 3 causes spam filter failures to accept the message but queue it to the reprocess channel for later processing. A value of 4 does the same thing but also logs the spam filter temporary failure to syslog.

The ability to log the amount of time a message has spent in the queue has been added to the MTA logging facility. A new option, LOG_QUEUE_TIME , enables this capability. Setting the option to 1 enables queue time logging, while the default value of 0 disables it. The queue time is logged as an integer value in seconds. It appears immediately after the application information string in non-XML format logs. The attribute name in XML formatted logs for this value is qt.

Source channel switching based on user or domain settings is now possible. There are three new settings:

- A new channel keyword userswitchchannel must be present on the initial source channel for user channel switching to occur.
- A new MTA option LDAP_DOMAIN_ATTR_SOURCE_CHANNEL specifies the name of a domain-level attribute containing the name of the channel to switch to.
- A new MTA option LDAP_SOURCE_CHANNEL is a user-level attribute containing the name of the channel to switch to. Additionally, the channel being switched to must be set to allow channel switches, that is, it cannot be marked with the noswitchchannel keyword. Switching is done based on information returned by rewriting the MAIL FROM address. Note that MAIL FROM addresses are easily forged so this functionality should be used with extreme care.

List expansion in the context of the mgrpallowedbroadcaster LDAP attribute now includes all the attributes used to store email addresses (normally mail, mailAlternateAddress, and mailEquivalentAddress). Previously, only mail attributes were returned, making it impossible to send to lists restricted to their own members using alternate addresses.

The default for the GROUP_DN_TEMPLATE MTA option has been changed to "ldap:///$A??sub?mail=*". It used to be "ldap:///$A?mail?sub?mail=*".

The new MTA option LDAP_DOMAIN_ATTR_DEFAULT_MAILHOST specifies a domain-level attribute containing the default mail host for the domain. If set, and the attribute is present on the domain, the mailhost attribute is no longer required on user entries in the domain. This option currently has no default, but preferredmailhost is the logical attribute to use as long as some other, conflicting usage doesn't exist.

New channel keywords generatemessagehash, keepmessagehash, and deletemessagehash. The keyword generatemessagehash , if specified on a destination channel, inserts a Message-hash: header field into the message. The keyword keepmessagehash retains any existing Message-hash: field. The keyword deletemessagehash deletes any existing Message-hash: field. The keyword deletemessagehash is the default. The value placed in Message-Hash: fields is a hash of the message.

New MTA options control how the hash is generated:

- MESSAGE_HASH_ALGORITHM - The hash algorithm. Can be any of "md2","md4", "md5" (the default), "sha1", "md128" (for RIPE-MD128), or "md160" (for RIPE-MD160).
- MESSAGE_HASH_FIELDS - Comma-separated list of fields from the header to hash (in order). Any known header field can be specified. If this option is not specified it defaults to "message-id,from,to,cc,resent-message-id,resent-from,resent-to,resent-cc,resent-bcc,subject,cont

The new MTA option UNIQUE_ID_TEMPLATE specifies a template used to convert an address into a unique identifier. The template's substitution vocabulary is the same as that for delivery options. The resulting unique identifier is intended for use by message archiving tools.

Per-user aliasdetourhost is now possible through the following set of features:

- aliasoptindetourhost channel keyword where detouring only occurs if the user has opted in via the following attribute.
- LDAP_DETOURHOST_OPTIN MTA option specifies the name of an attribute whose presence opts the user in to the detour (assuming of course the source channel has aliasoptindetourhost set).
- ALIASDETOURHOST_NULL_OPTIN MTA option is similar to SPAMFILTERx_NULL_OPTIN in that it specifies a special value which if used in the optin attribute is treated as the same as the attribute being omitted. The default value is "", which means that an empty attribute value is ignored.

Support for a new IP_ACCESS table has been added. This access mapping is consulted during SMTP client operations just prior to attempting to open connections to a remote server. The mapping probe has the following format: source-channel|address-count|address-current|ip-current|hostname

- source-channel is the channel the message is being dequeued from, address-count is the total number of IP addresses for the remote server, address-current is the index of the current IP address being tried.
- ip-current is the current IP address, and hostname is the symbolic name of the remote server.

The mapping can set the following flags:

- $N - Immediately reject the message with an "invalid host/domain error." Any supplied text will be logged as the reason for rejection but will not be included in the DSN.
- $I - Skip the current IP without attempting to connect.
- $A - Replace the current IP address with the mapping result.

The ACCESS_ORCPT MTA option has been changed from a simple boolean (0 or 1) to a bit-encoded value. Bit 0 enables the addition of the ORCPT to all the various access mappings. Bits 1-4 (values 2-16), if set, selectively enable the addition to the ORIG_SEND_ACCESS, SEND_ACCESS, ORIG_MAIL_ACCESS, and MAIL_ACCESS mappings respectively.

The new ACCESS_COUNTS MTA option finds various types of recipient count information in the various recipient *_ACCESS mappings. ACCESS_COUNTS is bit-encoded in the same way as ACCESS_ORCPT . If set, it enables the addition of a set of counts to the end of the access mapping probe string. Currently, the format of the count addition is: RCPT-TO-count/total-recipient-count/ (Note the trailing slash.) All mappings using this information should be coded to ignore anything following the last slash or they may break without warning.

Support has been added for a new caption channel keyword. The caption channel keyword is similar to the existing description channel keyword in that it takes a quoted string as an argument that is intended for use in channel displays. The difference is presumably that a caption is shorter than a description. The Java Enterprise System Monitoring Framework needs both the caption as well as the description.

A new utility routine verifies domain-level Schema 1 and 2 information in the directory. This utility routine is accessible to users through the verify command in imsimta test -domain:

```
% imsimta test -domain
```

```
DOMAIN_MAP> verify
```

This utility verifies canonical domain settings for domains with overlapping user entries. For more information, see “imsimta test -domain” in *Sun Java System Messaging Server 6.3 Administration Reference*

Support for SMTP chunking (RFC 3030) has been added to both the SMTP client and server. This support is enabled by default. Four new channel keywords can be used to control whether or not chunking is allowed.

They are:

chunkingclient - enables client chunking support (default)

chunkingserver - enables server chunking support (default)

nochunkingclient - disables client chunking support

nochunkingserver - disables server chunking support

The log file action field has been extended to indicate whether or not chunking was used to transfer a given message. Specifically, a C will be appended if chunking is used. Note that ESMTP has to be used for chunking to work, so you'll typically see field values like EEC or DEC.

The ability to generate :addresses arguments to sieve vacation via an LDAP autoreply attribute has been added to Messaging Server. The new MTA option LDAP_AUTOREPLY_ADDRESSES provides the name of the attribute to use. This option has no value by default. The attribute can be multi-valued, with each value specifying a separate address to pass to the :addresses vacation parameter.

The new LDAP_DOMAIN_ATTR_CATCHALL_MAPPING can now be used to specify the name of a LDAP domain attribute. This option is not set by default. If set the option specifies the name of a mapping which is consulted when an address associated with the domain fails to match any user entries. The format of the mapping probe is the same as that of the forward mapping, and the USE_FORWARD_DATABASE MTA option controls the format of the probe of this mapping in the same way as the forward mapping. If the mapping sets the $Y metacharacter the resulting string will replace the address being processed.

The MTA now fetches the block limit associated with the envelope return address and will set RET=HDRS if no return policy is specified and the message size exceeds the block limit. This prevents nondelivery reports for large messages from being undeliverable themselves. No new options or settings are associated with this change.

The $E metacharacter in a mapping template indicates an exit after processing the current template. There are cases where it is desirable to exit immediately without interpreting the rest of the template. The $+1E metacharacter sequence now produces this behavior.

The restriction that the same attribute cannot be assigned to multiple slots and hence can have multiple semantics during alias expansion and address reversal.

The internal separator character used to delimit multiple subject line tag additions has been changed from space to vertical bar. This makes it possible to add a tag containing spaces, as some spam filters want to do. This change effectively prevents vertical bars from being used in tags, but such usage is almost certainly nonexistent.

The MIME specification prohibits the use of a content-transfer-encoding other than 7–bit, 8–bit, and binary on multipart or message/rfc822 parts. It has long been the case that some agents violate the specification and encode multi-parts and message/rfc822 objects. Accordingly, the MTA has code to accept such encodings and remove them. However, recently a different standards violation has shown up, one where a CTE field is present with a value of quoted-printable or base63 but the part isn't actually encoded. If the MTA tries to decode such a message the result is typically a blank message.

Messages with this problem have become sufficiently prevalent that two new pairs of channel keywords have been added to deal with the problem: interpretation of content-transfer-encoding fields on multiparts and message/rfc822 parts can be enabled or disabled. The first pair is interpretmultipartencoding and ignoremultipartencoding and the second is interpretmessageencoding and ignoremessageencoding. The defaults are interpretmultipartencoding and interpretmessageencoding.

Several additional error messages the SMTP server either returns or places in DSNs have been made configurable. The new options and their default values are:

ERROR_TEXT_MAILFROMDNSVERIFY
invalid/host-not-in-DNS return address not allowed ERROR_TEXT_INVALID_RETURN_ADDRESS
invalid/unroutable return address not allowed ERROR_TEXT_UNKNOWN_RETURN_ADDRESS invalid/no-such-user
return address ERROR_TEXT_ACCEPTED_RETURN_ADDRESS return address invalid/unroutable but accepted
anyway ERROR_TEXT_SOURCE_SIEVE_ACCESS source channel sieve filter access error
ERROR_TEXT_SOURCE_SIEVE_SYNTAX source channel sieve filter syntax error:
ERROR_TEXT_SOURCE_SIEVE_AUTHORIZATION source channel sieve filter authorization error
ERROR_TEXT_TRANSACTION_LIMIT_EXCEEDED number of transactions exceeds allowed maximum
ERROR_TEXT_INSUFFICIENT_QUEUE_SPACE insufficient free queue space available
ERROR_TEXT_TEMPORARY_WRITE_ERROR error writing message temporary file
ERROR_TEXT_SMTP_LINES_TOO_LONG lines longer than SMTP allows encountered; message rejected
ERROR_TEXT_UNNEGOTIATED_EIGHTBIT message contains unnegotiated 8–bit

Overly aggressive SMTP servers might issue a "5xy bad recipient" response to the first RCPT TO and disconnect immediately, a standards violation. Messaging Server treats the response as a temporary error and tries later, only to get the same result. To work around this server bug, Messaging Server will handle the one recipient as bad and requeue any remaining recipients for a later retry.

Two new actions are available to system sieves: addconversiontag and setconversiontag. Both accept a single argument: A string or list of conversion tags. The addconversiontag action adds the conversion tag(s) to the current list of tags while setconversiontag empties the existing list before adding the new ones. Note that these actions are performed late in sieve processing so setconversiontag can be used to undo all other conversion tag setting mechanisms.

The MTA option, INCLUDE_CONVERSIONTAG, has been added to selectively enable the inclusion of conversion tag information in various mapping probes. This is a bit-encoded value. The bits are assigned as follows: Bit Value Mapping

0 1 CHARSET_CONVERSION - added as ;TAG= field before ;CONVERT

1 2 CONVERSION - added as ;TAG= field before ;CONVERT

2 4 FORWARD - added just before current address (| delim)

3 8 ORIG_SEND_ACCESS - added at end of probe (| delim)

4 16 SEND_ACCESS - added at end of probe (| delim)

5 32 ORIG_MAIL_ACCESS - added at end of probe (| delim)

6 64 MAIL_ACCESS - added at end of probe (| delim)

These tags appear in the probe as a comma-separated list.

The sieve envelope test now accepts "conversiontag" as an envelope field specifier value. The test checks the current list of tags, one at a time. Note that the :count modifier, if specified, allows checking of the number of active conversion tags. This type of envelope test is restricted to system sieves. Also note that this test only "sees" the set of tags that were present prior to sieve processing — the effects of setconversiontag and addconversiontag actions are not visible.

Metacharacter substitutions can now be specified in mgrpModerator , mgrpAllowedBroadcaster and mgrpDisallowedBroadcaster attributes. In particular, the various address-related metacharacter sequences ($A for the entire address, $U for the mailbox part, $D for the domain part) refer to the current envelope from address and can in some cases be used to limit the results returned by the URL to entries that are likely (or guaranteed) to match. This may make authorization checks much more efficient. The new MTA option PROCESS_SUBSTITUTIONS controls whether or not substitutions are performed. This is a bit-encoded value, with the bits defined as follows:

Bit Value

0 1 Enables substitutions in mgrpDisallowedBroadcaster if set

1 2 Enables substitutions in mgrpAllowedBroadcaster if set

2 4 Enables substitutions in mgrpModerator if set

The PROCESS_SUBSTITUTIONS MTA option defaults to 0, meaning that all of these substitutions are disabled by default.

New MTA option LDAP_DOMAIN_ATTR_UPLEVEL. This option specifies the name of a domain-level attribute used to store a domain-specific uplevel value which overrides the value of the DOMAIN_UPLEVEL MTA option for this one domain. Currently only bits 0 and 2 (values 1 and 4) are used from this value; the other bits of DOMAIN_UPLEVEL remain in effect. Note that this attribute is only consulted if the domain is looked up. This means that setting bit 0 of this value to 1 for a domain won't make subdomains of the domain match unless bit 0 of DOMAIN_UPLEVEL is also set. As such, the way to get subdomain matching for some domains but not others is to set bit 0 of DOMAIN_UPLEVEL (this enabling subdomain matches for all domains) then clear bit 0 of the attribute for the domains where you don't want uplevel matching to occur.

Rewrite rules can now be used to override the default `ALIAS_MAGIC` setting. Specifically, a construct in the form `$nT` , where `n` is an appropriate value for the `ALIAS_MAGIC` MTA option, overrides the setting for the domain when the rule matches during alias expansion.

What's New in This Release of Instant Messaging

This section includes the following topics:

- "Instant Messaging XMPP Redirect Server" on page 34
- "Instant Messaging Redeploy Script Changes" on page 34
- "Event Notification Service (ENS) Support in Instant Messaging" on page 34
- "Legacy SSL and TLS Support for Instant Messaging" on page 34

Instant Messaging XMPP Redirect Server

The XMPP redirect server balances the load between servers in a server pool, increasing performance by decreasing the amount of communication required between servers in a single deployment. The XMPP redirect server increases the probability that two users who will likely share presence information and messages end up on the same node. You use a redirect service to optimize resource utilization. The redirect service directs client connections to specific hosts in the server pool.

Instant Messaging Redeploy Script Changes

The redeploy script used to redeploy Instant Messenger resource files has been renamed to iwadmin.

Event Notification Service (ENS) Support in Instant Messaging

In this release there are two notification services for Calendar pop-ups: Sun Java System Message Queue (JMQ) and Event Notification Service (ENS). In a future release, the Communications Services products (Instant Messaging, Calendar Server, and Messaging Server) will use JMQ exclusively and ENS will be removed. However, for this release, you can continue to use ENS.

Legacy SSL and TLS Support for Instant Messaging

TLS support was added to Instant Messaging in the previous release; however, the *Sun Java System Instant Messaging 7 2006Q1 Administration Guide* did not adequately cover instructions for setting up TLS. TLS is used for communication between the server and clients, other servers, and Instant Messaging components such as the XMPP/HTTP Gateway. Legacy SSL is still supported for communication between clients and the multiplexor. Legacy SSL is no longer supported by the server. The *Sun Java System Instant Messaging 7.2 Administration Guide* now provides detailed information about setting up security for your deployment.

As a result of the implementation of TLS in Instant Messaging, you are no longer prompted to enter an SSL port for the server when you run `configure`.

The following `iim.conf` parameters are no longer used:

- *iim_server.sslport* – No separate port is required for TLS connections.
- *iim_server.usesslport* – No separate SSL port.
- *iim_server.secconfigdir* – No longer have NSS key and certificate database for the server.
- *iim_server.keydbprefix* – No longer have NSS key and certificate database for the server.
- *iim_server.certdbprefix* – No longer have NSS key and certificate database for the server.
- *iim_server.coserver1.usessl* – This has been replaced with *iim_server.coserver1.requiressl*.

The following `iim.conf` parameters are new for this release:

- *iim_server.requiressl*
- *iim_server.sslkeystore*
- *iim_server.coserver1.requiressl*

Refer to the *Sun Java System Instant Messaging 7.2 Administration Guide* for information about using these parameters.

The Instant Messenger client uses `imssl.html` and `imssl.jnlp` only for legacy SSL connections. Instant Messenger supports TLS automatically when it connects to a server that is configured to use TLS.

What's New in This Release of Delegated Administrator

Delegated Administrator 6.4 includes the following changes and new features:

- "Support for Calendar Groups" on page 35
- "Web Server 7.*x* Deployment" on page 36
- "Access to Instant Messaging" on page 36
- "Debug Log Command for the Delegated Administrator Server" on page 36

Support for Calendar Groups

Delegated Administrator supports provisioning of calendar groups.

You can use Delegated Administrator to assign calendar service to a group. When the group is first invited to an event, Calendar Server creates a group calendar shared by the users who are members of the group. Invitations to the group appear on the group calendar and on the calendars of the individual members.

The following features implement support for calendar groups:

- In the console, you can assign service packages with calendar service to groups. In the Create Group wizard, a Calendar Service Details panel allows you to specify Calendar attributes for the group. Calendar service details can be modified in the group properties page.
- In the command-line utility, the `commadmin group create` and `commadmin group modify` commands have been enhanced to support calendar groups.

Web Server 7.*x* Deployment

Delegated Administrator can be deployed to Sun Java System Web Server 7.x.

When you run the configuration program, `config-commda`, you can configure the Delegated Administrator server and console to be deployed to Web Server 7.x.

Access to Instant Messaging

Users created in Delegated Administrator will have access to Instant Messaging (IM) service if IM is deployed on your site. Users are automatically assigned basic IM service during user creation.

You must use the Access Manager console to set and manage IM user-access levels. In this release of Delegated Administrator, the Delegated Administrator console does not provide access to IM service and does not provide an interface for managing IM user-access levels.

Debug Log Command for the Delegated Administrator Server

In the command-line utility, the `commadmin debug log` command creates a Delegated Administrator server log that contains debug statements generated by the Delegated Administrator servlets installed on the Web container.

With the `commadmin debug log`command, you must create the log in the `/tmp/` or `/var/tmp/` directory.

The `commadmin debug log` command supersedes the use of the url to enable logging for the Delegated Administrator server. The url used in previous releases can no longer be used for this purpose.

What's New in This Release of Communications Express

Sun Java System Communications Express 6.3 includes the following changes and new features:

- "Support for Attachments in Events/Tasks" on page 37
- "Next Available Free Period Button" on page 37
- "Address Book Sharing" on page 37
- "Support for Multiple Address Book" on page 37
- "Preserving Customization" on page 37
- "Password Encryption" on page 38
- "LDAP Failover Mechanism" on page 38
- "Mail Integration into Communications Express" on page 38
- "Removal of Access Manager SDK Dependency for Schema 2 Deployment" on page 38

Support for Attachments in Events/Tasks

The Calendar component of Communications Express allows users to include attachments to an event or task.

Next Available Free Period Button

Communications Express allows users to check availability of invitees. If the invitee is not available for the day of the event, the next available free period button displays the availability of the invitee in the subsequent six days.

Address Book Sharing

The Address book component of Communications Express allows users to share their address book globally as well as to specific users. You can also assign specific permissions to users who subscribe to your address book. You can also subscribe to other shared address books.

Support for Multiple Address Book

Communications Express allows users to create and maintain more than one address books.

Preserving Customization

Starting this release, the Communications Express upgrade script will preserve all customizations that have been made in the product. This was not possible in earlier releases and all customizations were lost on a patch upgrade.

Password Encryption

Starting this release Communications Express configurator tool enctyps passwords during configuration. This is done transparently by the configuration tool. Communications Express now has a tool to encrypt and manage passwords. Administrators can change passwords by running this script.

LDAP Failover Mechanism

The LDAP failover mechanism in Communications Express balances load between a number of configured master and slave LDAP servers. This increasing performance by decreases the response time. Communications Express contains an LDAP failover Manager module that is responsible to retrieve connections from the master or slave servers. Each load balancing server maintains a pool of available free connections. Whenever a Communications Express component requires a connection to the LDAP server, the LDAP failover manager provides the component with a connection based on the load balancing strategy employed.

Mail Integration into Communications Express

Starting this release, the Webmail related user interface components have been moved to Communications Express. In the earlier releases of Communications Express, the mail related files were resident in the Messaging Server. Also, in previous releases of Communications Express, the webmail and the web container ports had to be available for it to work. As a result of this change, only the web container port needs to be available for Communications Express to work.

Removal of Access Manager SDK Dependency for Schema 2 Deployment

In previous releases, Communications Express used the following APIs and libraries to establish connections and fetch information from an LDAP store:

- Domain MAP API (which a part of Communications Express) if Communications Express was deployed using Schema 1 mode.
- Access Manager SDK if Communications Express was deployed using Schema 2

This made Communications Express dependent on Access Manager in Schema 2 mode even though Access Manager is not mandatory for it to work apart from just connecting and fetching information from the LDAP store. Starting this release, this dependency on Access Manager for Schema 2 has been removed. Communications Express is now shipped with a new Domain MAP API for Schema 2.

Note – As a result of this, users who log in to Communications Express can not log on to Access Manager Console.

What's New in This Release of Connector for Microsoft Outlook

New features in Sun Java System Connector for Microsoft Outlook 7.2 include:

- Polling multiple folders.

  A new option in the Deployment Configuration Program allows multiple mail folders, including Inbox to be checked for new unread messages. This option can be useful if message filters have been set up to automatically move incoming messages to specific folders other than Inbox, or if the direct delivery to a specific folder option has been enabled.
- Creating and sharing multiple calendars and tasks.
- Creating and sharing multiple address books.
- Adding attachments to calendar events. Attachments are saved on server.
- Viewing group memberships within contact details (applies only to the corporate directory).