

Message Security

Batch Reference Guide

- Google Message Filtering
- Google Message Security
- Google Message Discovery
- Message Security and Discovery for Google Apps Premier Edition

Google™ postini services

Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
www.google.com

Part number: EEBR_R646_00

29 February 2012

© Copyright 2012 Google, Inc. All rights reserved.

Google, the Google logo, Google Message Filtering, Google Message Security, Google Message Discovery, Postini, the Postini logo, Postini Perimeter Manager, Postini Threat Identification Network (PTIN), Postini Industry Heuristics, and PREEMPT are trademarks, registered trademarks, or service marks of Google, Inc. All other trademarks are the property of their respective owners.

Use of any Google solution is governed by the license agreement included in your original contract. Any intellectual property rights relating to the Google services are and shall remain the exclusive property of Google, Inc. and/or its subsidiaries ("Google"). You may not attempt to decipher, decompile, or develop source code for any Google product or service offering, or knowingly allow others to do so.

Google documentation may not be sold, resold, licensed or sublicensed and may not be transferred without the prior written consent of Google. Your right to copy this manual is limited by copyright law. Making copies, adaptations, or compilation works, without prior written authorization of Google, is prohibited by law and constitutes a punishable violation of the law. No part of this manual may be reproduced in whole or in part without the express written consent of Google. Copyright © by Google, Inc.

Postini, Inc. provides this publication "as is" without warranty of any either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Postini, Inc. may revise this publication from time to time without notice. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

GD Graphics Copyright Notice:

Google uses GD graphics.

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 19s99, 2000 Philip Warner.

Portions relating to PNG copyright 1999, 2000 Greg Roelofs.

Portions relating to libtiff copyright 1999, 2000 John Ellson (ellson@lucent.com).

Portions relating to JPEG copyright 2000, Doug Becker and copyright (C) 1994-1998, Thomas G. Lane.

This software is based in part on the work of the Independent JPEG Group.

Portions relating to WBMP copyright 2000 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd 1.8.4, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

Google Compliance Policies Notice:

Google assumes no responsibility in connection with the Compliance Policies lexicon-filtering feature, including any failure to recognize credit card or social security numbers that do not follow an applicable pattern as established in Postini's systems or any failure to encrypt a credit card or social security number.

Contents

Chapter 1: Introduction to Batch Processing	13
About this Book.....	13
Related Documentation	14
About Batch Processing	15
When To Use Batch	15
Batch Validation	16
Submitting Batch Commands for Processing	16
Batch Processing Steps.....	16
Batch Commands Syntax.....	18
Building a Batch File	19
Modifying Users in a Domain Using a List Batch Command	19
Modifying Users in a Domain with Download Users/Settings	21
About EZCommand	22
Setting Up EZCommand	22
Calling EZCommand	23
EZCommand Response Codes	24
EZCommand Example	24
EZCommand Reference	24
Troubleshooting: Batch.....	26
 Chapter 2: Batch Command and Field Quick Summary	 27
About the Batch Command and Field Quick Summary	27
Batch Commands	28
Domain Fields.....	49
Organization Fields.....	52
Report Fields	70
Spool Fields	78
User Fields.....	80
 Chapter 3: Batch Command Quick Summary	 91
About the Batch Command Quick Summary	91
Add Commands	92
Delete Commands	93
Display and Report Commands.....	95
Domain Management Commands	97
IM Security Commands	98

IP Locking Commands.....	100
List Commands.....	100
Message Archiving Message Archiving Commands.....	101
Message Encryption Commands.....	102
Modify Commands.....	103
Notification Commands.....	104
Organization Management Commands	105
Provisional User Management Commands	106
Spooling Commands	107
Test Commands	107
User Management Commands.....	108
Chapter 4: Batch Field Quick Summary	111
About the Batch Field Quick Summary.....	111
Attachment Manager Fields (for Orgs)	111
Default User Fields	112
Domain General Settings Fields	113
Early Detection Quarantine Fields	114
Email Config Fields.....	114
General Org Settings Fields	116
IM Security Fields (for Orgs).....	118
Message Archiving Fields (for Orgs)	119
Message Limits Fields (for Orgs).....	120
Message Limit Fields (for Users).....	120
Notifications Fields (for Orgs)	121
Outbound Compliance Footer.....	121
Quarantine Summary.....	121
Reports, Spam Fields	122
Reports, Traffic Fields.....	123
Reports, Usage Fields	124
Reports, Virus Fields	125
Sender List Fields (for Orgs).....	126
Sender Lists Fields (for Users)	126
Spam Filtering Fields (for Orgs).....	127
Spam Filtering Field (for Users).....	127
System Testing Fields	128
User, Access Fields (for Orgs).....	129
User, General Setting Fields.....	130
Virus Blocking Fields (for Orgs)	133
Virus Blocking Fields (for Users)	134
Chapter 5: Batch Commands	135
About Batch Commands.....	135
Command Reference Page Syntax Notations	135
addalias	137
adddomain	140
addorg.....	142
adduser.....	144

archive_settings display.....	148
archive_settings modify	150
blockprovuser	152
checklatency	153
checkroute	155
deletealias.....	157
deletedomain	160
deleteorg.....	161
deleteprovuser	163
deleteuser	164
displaydomain.....	168
displayorg	170
displayprovuser.....	173
displayspool	175
displayuser.....	178
domain_tls add	180
domain_tls delete.....	182
domain_tls display	184
domain_tls modify.....	186
encryption display_org.....	188
encryption display_user.....	190
encryption list_users	191
encryption modify_org	193
encryption modify_user.....	195
getorgreport	197
help	202
im add	204
im delete	206
im display.....	207
im list.....	209
im listforuser	211
iplock add_range	212
iplock delete.....	216
iplock delete_range.....	218
iplock display	220
iplock set_disposition.....	222
listdomains.....	224
listorgs	229
listprovusers.....	234
listusers.....	238
modifydomain	244
modifyorg	246
modifyuser	249
notification display	252
notification modify	256
org_im_settings display	261
org_im_settings modify.....	263

password force_update	265
password reset	267
password_policy display	269
password_policy update	271
promoteprovuser.....	275
resetuser.....	276
setorgsubstripping	278
showallowedips.....	280
suspenduser	282
testfirewall.....	285
testmail	286
testmx	289
unblockprovuser	292
user_im_settings add.....	293
user_im_settings delete.....	295
user_im_settings display	297
user_im_settings modify	299
Chapter 6: Batch Organization Fields.....	303
About Batch Organization Fields	303
antivirus_sensitivity.....	304
approved_senders (for orgs)	306
archive	308
archive_enable	309
async_bounce.....	311
at_notify_on	312
authentication_data	314
authentication_type.....	316
autocreate_web	318
blatant_spam	319
blocked_senders (for orgs)	321
bounce_fragments	323
company_name	324
create_method (for orgs)	325
created_date.....	326
creator.....	327
custom_journal	328
default_message_limit.....	330
default_user	332
disable_first_spam.....	333
disposition_virus	335
file_transfer_receive	337
file_transfer_send	338
footer_on.....	340
iid	341
im_enable	342
im_external_enable	344
im_proto_enable	345

is_email_config	347
journaling	348
lang_locale (for orgs).....	350
lastmod_date (for orgs).....	351
mail_flow.....	352
max_message_size	353
message_encryption (for orgs).....	355
message_encryption_criteria.....	356
ndr.....	358
non_account_bounce	359
non_account_virus_scan.....	361
nullsender_disposition	363
nullsender_headertag_validation.....	365
orgname.....	367
orgtag.....	369
out_at_notify_on	370
outbound_max_message_size	372
outbound_virus	373
outbound_virus_disposition	375
parent_org	376
qsum_actionable.....	378
qsum_enable	379
qtine_redir_atq.....	380
qtine_redir_ndr.....	382
qtine_redir_out_atq.....	383
qtine_redir_out_virus	384
qtine_redir_spam	386
qtine_redir_virus	387
quarantine_links.....	388
quarsum_links.....	389
remotecmd_secret.....	391
retention_months	392
spam_notify_on	393
standard_journal.....	394
support_contact	396
tagonly_spam	398
timezone (for orgs).....	399
tls_notify_admin.....	400
tls_notify_on.....	402
virus_clean.....	403
virus_notify (for orgs).....	404
welcome_on.....	406
zero_hour_notify_on	407
zero_hour_scan	409
Chapter 7: Batch User Fields.....	411
About Batch User Fields	411
User Field Reference Page Syntax Notations	411

active	412
address.....	413
approved_recipients	414
approved_senders (for users).....	416
blocked_senders (for users)	419
create_method (for users)	421
created_date (for users)	422
created_ts (for users).....	423
filter_adult	424
filter_bulk	426
filter_getrich	427
filter_offers	428
filter_racial	430
im_name	431
initial_password	432
junkmail_filter.....	434
lang_locale (for users)	435
lastmod_date (for users).....	436
message_count	437
message_encrypt (for users).....	438
message_limit.....	440
message_limited.....	441
notice_address	442
orgid.....	444
password	445
primary.....	447
primary_add.....	448
timezone (for users).....	449
TS1	451
TS3	452
uid	453
u_id	454
user_id	455
virus_notify (for users)	456
virus_state	458
weblocked.....	459
welcome_count.....	460
wireless_state.....	461
Chapter 8: Batch Domain Fields	463
About Batch Domain Fields	463
Domain Field Reference Page Syntax Notations	463
alias	464
aliasedfrom	465
aliasedto	465
catchall.....	466
created_ts (for domains).....	468
domainid	469

domainname	470
org (for domains)	471
primary_did	472
primary_dom.....	473
substrip	474
sub_strip	475
Chapter 9: Batch Report Fields	477
About Batch Report Fields.....	477
Report Field Reference Page Syntax Notations	477
acc_messages.....	478
account	479
bad_isp	480
bad_sender.....	481
bulk	482
bytes	483
cleanings.....	485
clean_failures.....	486
commerce	487
customerid	488
customername.....	489
deliveries.....	490
inf_deliveries.....	491
messages	492
mmf.....	494
naughty	495
num_bh_messages	496
num_bytes	497
num_f_messages	498
num_messages	499
num_q_messages	500
num_spams	502
num_viruses	503
pct_bh_bytes	504
pct_bh_messages.....	505
pct_f_bytes	506
pct_f_messages.....	507
pct_q_bytes	508
pct_q_messages.....	509
productid	510
racial	511
recip	513
sellerid	514
ssb	515
stored_size	516
users.....	518

Chapter 10: Batch Spool Fields.....	521
About Batch Spool Fields	521
Spool Field Reference Page Syntax Notations	521
auto_unspool	522
despool_max_connections	523
duration.....	524
org (for spooling).....	525
quota.....	526
spool_delay.....	528
spool_mech	529
status	531
used_pct	532
used_size.....	533
Chapter 11: Examples of Common Tasks.....	535
About Common Task Examples	535
Task Example Syntax	535
Message Center Settings and Password Examples.....	536
Viewing Message Center Settings	536
Editing Message Center Access and Settings	538
Viewing Authentication and Password Settings	540
Editing a PMP Password	541
Notification Examples	542
Viewing Message Center General Notification Settings	542
Editing Message Center General Notification Settings	543
Viewing Quarantine Summary Notification Settings	544
Editing Quarantine Summary Notifications	546
Seeing if a User Has Received a Welcome Notification	547
Resending the Welcome Notification	548
Setting a Virus Notification Interval	549
Org Settings Examples	550
Listing the Organizational Hierarchy	550
Resetting Users	553
Viewing Your Organization's Sender Lists	554
Adding Users and Domains to Sender Lists	555
Viewing Message Limit Policies	558
Editing Your Message Limit Policies	559
Viewing Mail Handling Policies (Non Account Bouncing)	560
Editing Your Mail Handling Policies (Non Account Bounce)	562
Quarantine Summary Example.....	563
Editing the Localized Language Setting	563
Message Archiving Example	564
Editing Message Archiving Settings	564
Message Encryption Example	565
Viewing and Editing Message Encryption Settings	565
IM Security Example.....	566
Viewing and Editing an Org's IM Settings	566
User Settings Examples	566
Listing User Aliases and Primary Addresses	566
Appendix A: Additional Reference Information.....	569
Language and Timezone	569

Chapter 1

Introduction to Batch Processing

About this Book

Welcome to the *Batch Reference Guide* for Message Security. The book components are:

- The Batch Command Line Interface -- The batch commands offer a quick and efficient command line interface to perform a large number of configuration changes.
- The EZCommand Interface -- Is a Perl-based scripting interface that allows administrators to perform a subset of basic administrative tasks. This interface is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

The book is a programming reference and is composed of a:

- Quick reference to all commands' and fields' syntax
- Quick reference to commands listed by common tasks
- Quick reference to fields listed by common tasks
- Command and field reference pages in alphabetical order
- Examples of common batch tasks using several commands

Note: This book assumes you have experience with the Message Security service batch interface and command line scripting. This guide describes how the Message Security service products work with Microsoft Exchange, qmail, and the configurations that the Message Security service recommends. These instructions are designed to work with the most common product scenarios. Any changes to these products' configurations should be made at the discretion of your administrator.

Links to <http://www.microsoft.com/exchange/>, <http://www.qmail.org/> Web sites are provided for your convenience. The links and their content may change without notice, and we disclaim all responsibility for the contents of any such Web sites. Please consult the product's Web site for the latest configuration and support information.

The Message Security service Customer Care does not provide technical support for configuring mail servers or third-party products. In the event of an issue with these products, you should consult with your administrator. Google accepts no responsibility with third-party products. Please contact Postini Professional Services (professionalservices@postini.com) for consulting services. For Message Security and Compliance Help articles, user discussions, and support information, see the [Message Security Help Center](#).

Please send your comments, feedback, and suggestions to postini-doc_comments@google.com.

Related Documentation

For additional information about your Message Security service and optional products, refer to the following related documentation.

Document	Description
<i>The Message Security Release Notes</i>	The latest information about new features in this release, known issues, and resolved issues.
<i>The Message Security Administration Guide</i>	Contains detailed information about using configuration and administering your Message Security service. It's intended for administrators of the Message Security service, and assumes that you are familiar with administering email services for an organization.
<i>Message Center Documentation</i>	On this page, you'll find the <i>Message Center Quick Start</i> user guide and email templates for introducing the service to your users.
<i>Message Security Activation Guide</i>	Instructions for preparing for activation of your Message Security service, completing the online activation form, and testing your activation.
<i>Configuration Guide for Directory Sync</i>	Instructions for setting up your network environment and directory server for Directory Sync, an optional feature of your Message Security service that lets you import user account information to your Message Security service.

Document	Description
<i>Encryption Services Administration Guide</i>	Instructions for setting up Message Encryption to provide policy-based TLS encryption for your organization's email communications.

Document	Description
<i>Postini Message Archiving Administration Guide</i>	Instructions for setting up and administering Message Archiving to provide long-term, immutable storage of your organization's electronic communications.
<i>Postini Message Archiving User's Guide</i>	Instructions for retrieving and exporting email messages, IM conversations, and IM file transfers from your corporate message archive.

About Batch Processing

The standard batch processing is a quick and efficient method to perform a large number of configuration changes by creating, validating and running command scripts in real-time. The batch commands allow you to create, delete, modify and get reports for:

- aliases
- domains
- organizations
- users

Following is a description of how the batch loader works, and key issues in administration.

When To Use Batch

Authority privileges determine which batch commands an administrator can run, just as they determine what parts of the Administration Console an administrator can access. Batch processing is independent of your currently viewed location within the Administration Console, since each batch command contains details about where to apply.

A subset of the batch commands can be run through the EZCommand API. See “About EZCommand” on page 22 for more details.

Configuration changes should be made by batch whenever:

- The number of changes is too great to effectively use the Administration Console.
- The changes can be created by an automated script.

For example, you want to lower spam filter settings from level 4 to level 3 for 100 users. Configuring the Default User with the change will only affect new users. Since changing user configuration for 100 users by Administration Console interface would be repetitive and downright unpleasant, use the batch interface.

Batch Validation

In the Administration Console's Batch page, the batch validator checks either a batch file or batch commands typed in to the batch page for:

- Syntax errors within each command
- Ability to process the command based on the administrator's level or authorization
- Existence of orgs, users, aliases and domains affected by commands

Resulting success and error messages are displayed on the screen. Validation does not process any commands.

Submitting Batch Commands for Processing

When submitted, batch commands are streamlined and immediately processed in the order listed. If using a batch file and the administrator has an active email account, the success and error messages are displayed on the Administration Console screen and mailed to the administrator's address for tracking purposes.

Batch Processing Steps

The Administration Console's Batch page is the definitive resource for batch command syntax and field information. No matter which organization is selected, the Batch page can process commands anywhere in the hierarchy where the administrator has authority.

1. In the Administration Console, go to Orgs & Users > Batch to display the Batch page.

The screenshot shows the 'Batch Upload' interface. It includes fields for creating a file, uploading a file, manual input, validation, and processing. A red error message 'niagra' is displayed in a box.

Batch Upload

Add, delete, and modify groups of accounts with the batch upload tool. See the [Batch Command Reference Guide](#) or [Batch Summaries](#) for more information.

1. Create File Create a text file with your batch commands. (see format below)

2. Upload File

2.5. Manual Input Alternately, enter some commands here:

3. Validate Validate file type and format using the process code.

4. Process Enter the process code (presented in red).

niagra
(process code)

2. Create and enter your batch commands by either of the following methods:

If you need to work with several batch command modifications or lists, create a text file containing the batch commands and browse for that file.

- The file can have any file extension.
- If writing comments in the file begin the comment line with # on a separate line.

#This is an example of a batch command file comment line

- The full command syntax must be on one line. A command broken by a line return will trigger an error.
- If your administrator has a valid email account, when the batch file is processed, the system mails the full success and error output of this session to the administrator.

Note: For more detailed information on building a batch file, see “Building a Batch File” on page 19.

or

If you need a single batch command modification or list, type the batch command directly into the Batch page’s command field.

3. Click Validate to check for syntax errors and return errors as if the batch command were processed. If the system returns errors, correct the syntax mistakes.

4. Click the Back button to return to the Batch page.

After validation, clicking the Back button will clear the selected file to prevent the accidental submission of a mistake-filled batch file.

If you’re using a batch file, browse for the corrected file again, or type your corrected commands in the batch file. You are now ready to submit the batch command.

5. If you’re using a batch file: Copy the process code, paste it into Process Code field, and click the Submit job button. For entering a single batch command, this step is not necessary.

This process code ensures that batch files are not submitted by inadvertently clicking Submit job instead of Validate. If you do not enter the process code, then your batch file will not be uploaded or processed.

6. **For a quick check on your command syntax, use the command line Help feature.**
 - a. Either in your batch file or in the command field, type `help <command>`. For example:
`help displayorg`
 - b. Click the Submit job button. If using a file, copy the process code, paste it into Process Code field, and click the Submit job button.
 - c. Help will return the command's syntax and helpful hints. For example the help for the **displayorg** command is:
`Displayorg`
Syntax: `displayorg <orgname|iid>`
Displays information on <orgname>. Enclose <orgname> in double quotes if it contains an apostrophe.

Batch Commands Syntax

A quick reference to the syntax for batch commands as well as field definitions for user and organizations are listed on the batch page's Summaries link. Access the batch page through the Administration Console by going to Orgs & Users > Batch. Here is the generic batch command syntax using tokens:

`batch-command 1st-argument[, 1st-option][, 2nd-option]`

or

`batch-command 1st-argument,1st-field=1st-value[,2nd-field=2nd-value`

Objects inside “[]” (square brackets) are optional. Using the Administration Console syntax, commas (',') are used between batch command arguments, within arguments use '\,'.

Following are the batch command syntax tokens:

- `batch-command` -- The name of the batch command to process.
- `1st-argument` -- The domain, organization, user, or alias being acted upon by the batch command.
- `1st-option` -- The first batch command optional argument which modifies the behavior of the batch command.
- `2nd-option` -- The second batch command optional argument which modifies the behavior of the batch command.
- `1st-field` -- The first field being assigned by the batch command.
- `1st-value` -- The value being assigned to the first field by the batch command.
- `2nd-field` -- The first field being assigned by the batch command.
- `2nd-value` -- The value being assigned to the first field by the batch command.

Building a Batch File

Batch files allow you to run several commands at once. Below are two examples. The first example shows how to modify all users in a domain by using a listing batch command. The second example shows how to use the Administration Console Batch page and the Download Users/Settings page.

Modifying Users in a Domain Using a List Batch Command

To modify all users in a domain, download the list of all users and craft it into a batch file using the `listusers` and `modifyuser` batch commands. If you want to delete all the users in the domain, use the `deleteuser` command.

1. In the Administration Console, go to Orgs & Users > Batch to display the Batch page.
2. Type this command in the command field to get a list of user addresses associated with the domain you wish to modify.

This example uses the ‘Sales’ organization which has two domains, ‘@sales.jumboinc.com’ and ‘@support.jumboinc.com’. It returns all of the users whose addresses end with ‘sales.jumboinc.com’.

```
listusers sales.jumboinc.com$, targetOrg=Sales, aliases=0,  
childorgs=1, sort=ADDRESS:a, fields=ADDRESS
```

- The **listusers** command searches for all user addresses that end with ‘sales.jumboinc.com’. The \$ flag targets the search to text ending with the given address string ‘sales.jumboinc.com’.
- The command searches all users in the Sales organization.
- This list includes no aliases. It returns the primary user addressees only.
- It searches all sub-organizations (childorgs).
- It returns a list sorted by ascending user addresses.
- And it returns only the address fields instead of the default addresses and orgname fields.

3. Select and copy all of the lines in the Executed section of the Batch Results page.

4. Open a text editor (if using Microsoft Notepad, turn word-wrap off) and paste the text. Save the file using the file extension “.csv”.

5. Start Excel or any other spreadsheet application, and open the .csv file saved in step 4.

- a. Create a column with the email addresses.
- b. Add a column to the left of the addresses column.
- c. Fill that column with the command: modifyuser
- d. For each field you wish to modify, create a column to the right of the addresses column. In each column row, type in the <field name> = <the new value>. These are called *field-value pairs*.
- e. Save the file again as a .csv file.

Note: See “modifyuser” on page 241 or “listusers” on page 230 for more information. In the Administration Console, click the Batch Command Reference link on the Orgs and Users > **Batch** page for a link to **modifyuser** command. This command reference page lists links to all user fields you can modify. In turn, each batch field reference page lists the different values you can give to the field=value pairs.

6. Load the file into a text editor.

Replace all occurrences of “modifyuser,” with “modifyuser ” to remove the comma and add a space. Make sure there is a comma between the user’s address and the fields, and between each field=value pair. The result should look something like this example:

```
modifyuser msmith@sales.jumboinc.com, junkmail_filter=0,  
virus_notify=9
```

7. Save the result as a .txt file.

8. You can now validate this file and upload it as a batch file as described in “Batch Processing Steps” on page 16.

Modifying Users in a Domain with Download Users/Settings

An alternative to using the list commands is to use the Download Users/Settings. To modify all users in a domain, download the list of all users and craft it into a batch file using the **modifyuser** batch command.

1. Open the Administration Console and select the Orgs and Users tab.
2. Click the Users link and select your Account org from the Choose Org pull-down list.
3. Type in the “%” character and then the domain name in the Find User field and click Search.

[This performs a search across all of your organizations for user addresses using that domain, returning the first 15,000 users.]
4. Click Download Users/Settings.
5. Select and copy all of the lines that have email addresses on them.
6. Open a text editor (if using Microsoft Notepad, turn word-wrap off) and paste the text. Save the file using the file extension “.csv”.
7. Start Excel or any other spreadsheet application, and open the .csv file saved in step 6.
 - a. Delete all columns except the one containing the email addresses.
 - b. Add a column to the left of the addresses column.
 - c. Fill that column with the word: modifyuser
 - d. In as many columns as necessary to the right of the addresses column, type in field-value pairs.
 - e. Save the file again as a .csv file.

Note: Click the Users link on the Orgs and Users > Batch page for a link to user field and value information.

8. Load the file into a text editor.

Replace all occurrences of “modifyuser,” with “modifyuser “ to remove the comma and add a space. Save the result as a .txt file.

You can now validate this file and upload it as a batch file as described in “Batch Processing Steps” on page 16.

About EZCommand

EZCommand is a Perl-based scripting interface that allows administrators to perform basic tasks without having to log in to the Administration Console. EZCommand facilitates the integration of various administrative functions with the administrator's tools and applications.

Note: This interface is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

The EZCommand commands, which are a subset of the batch commands available through the Administration Console, perform user-related tasks:

- adduser
- modifyuser
- deleteuser
- addalias
- deletealias
- suspenduser

Setting Up EZCommand

The following steps are required to successfully use the EZCommand interface:

1. **You must be proficient in Perl programming and have the ability to generate valid cross-authentication (XAuth) strings.**

See The Message Security Administration Guide, “Cross-Authentication” for information on cross authentication. Enabling Cross authentication or EZCommand requires programming knowledge.

2. **Set a Shared Secret for each organization that contains an administrator.**

An “EZCommand Shared secret” must be submitted for an org in order to process commands by an Administrator in that org.

- a. In the Administration Console, go to Orgs & Users > Orgs.
- b. Choose the organization from the Choose Org pull-down, or click the name in organization list.
- c. In the Organization Management page, scroll to the Organization Settings section and click General Settings.
- d. On the General Settings page, enter the shared secret in the EZCommand Shared Secret field and click Save.
- e. Add shared secrets to other organizations that contain administrators who will submit EZCommands. With EZCommand, the shared secret must be set for each organization; the shared secrets are not inherited down the organization hierarchy.

Note: You can create or modify this shared secret using the **modifyorg** command and the **remotecmd_secret** field. For example:

```
modifyorg sales, remotecmd_secret=swordfish
```

3. Check and set administrator privileges for the organizations you plan to work with.

EZCommands are only limited by the authorization for the administrator who processes the. See *The Message Security Administration Guide*, “Administrators” chapter for details on authorization.

Calling EZCommand

Commands are sent to EZCommand via a secure, cross-authenticated HTTP request to the host name of the web cluster which serves your Administration Console pages:

```
https://hostname/exec/remotecmd?auth=authstring&cmd=cmdstring
```

Note: SSL is required

hostname

The host name listed in the URL after a successful log in to the Administration Console. It will be of the form ac-sN.postini.com.

The N is the system in Message Security service which processes your mail traffic.

To locate your system, login to the Administration Console.

- **Administration Console** -- Log in to your Administration Console. The URL will show which system holds your account. In the URL, the system corresponds to the s<number> in ac-sN.postini.com.

authstring

The authstring is a URL-escaped XAuth string made by combining an administrator account and the EZCommand Shared Secret field on the org containing the administrator. (See *The Message Security Administration Guide*, “User Authentication” chapter for details on the scripting necessary to generate an authstring.). **cmdstring**

The cmdstring is a URL-escaped command to execute (described in next section).

EZCommand Response Codes

The HTTP response will contain a two-part return value: <status> <message>

- *status*: 1 for success or 0 for failure
- *message*: contains additional details

EZCommand Example

For example, to add the user, agoodman@jumboinc.com using the privileged account administrator@jumboinc.com, at host name ac-s8.postini.com.

Submit:

```
https://ac-s8 .postini.com/exec/  
remotecmd?auth=3X2dLdwfb9BLKtmr%2F5f4hOn82rsRLWGadministrator%40ju  
mboinc.com&cmd=adduser%20agoodman%40jumboinc.com
```

Upon successful completion, the following response would be returned:

```
1 Created new user agoodman@jumboinc.com in organization Jumbo Org 1
```

WARNING: Do not use ac-s8.postini.com unless that is your appropriate host name, as described in the “Calling EZCommand” section above. For example, your host name may be ac-s5.postini.com. Using the wrong hostname will guarantee your EZCommand processing will fail.

EZCommand Reference

For detailed information on the commands and fields discussed below, go to each EZCommand-enabled command and field reference page in this Guide, or, online, log in to the Administration Console. Go to the Orgs & Users > **Batch**, and review the Batch Command and User fields pages in *The Message Security Batch Reference Guide* linked on that page.

This interface is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Note: All EZCommand-enabled commands must be URL-escaped in order to be properly submitted. For example, URL-escaping the command:

```
adduser agoodman@jumboinc.com
```

changes it to:

```
adduser%20agoodman%40jumboinc.com
```

Since EZCommand is an HTTP interface, all non-alphanumeric characters appearing in the command must be URL-escaped or the system will not recognize them. An example of the full URL string:

```
https://ac-s<N>.postini.com/exec/  
remotecmd?auth=<authstring>&cmd=adduser%20agoodman%40jumboinc.com%  
2c%20welcome%3d1
```

where N is the system number and <authstring> is the SHA1-encrypted shared secret/username pair.

Note that this includes *all* non-alphanumeric characters, not just URL special-meaning characters as defined by RFC2396. According to RFC2396, the following list of characters have a special meaning in URLs:

```
";;" | "/" | "?" | ":" | "@" | "&" | "=" | "+" | "$" | ","
```

addalias

Syntax and Example:

```
addalias username, targetalias  
addalias user@jumboinc.com, useralias@jumboinc.com
```

adduser

Syntax and Examples:

```
adduser username [, field=value]...  
adduser user@jumboinc.com  
adduser user@jumboinc.com, org=jumboinc.com sales  
adduser user@jumboinc.com, welcome=1  
adduser user@jumboinc.com, org=jumboinc.com sales, welcome=1
```

deletealias

Syntax and Example:

```
deletealias targetalias  
deletealias useralias@jumboinc.com
```

deleteuser

Syntax and Example:

```
deleteuser username  
deleteuser agoodman@jumboinc.com
```

modifyuser

Syntax:

```
modifyuser username [field=value]...
```

suspenduser

Syntax:

```
suspenduser username [notify] [hardSuspend] [deliver]
```

- **suspend:** All filtering services are turned off.
- **notify:** User receives mail explaining the suspension.
- **hardSuspend:** User is flagged as not allowed to log into the web site.
- **deliver:** Any quarantined email for the user is delivered. Virus infected email is not cleaned.

Troubleshooting: Batch

Batch validation fails because a Batch command argument contains the comma “,” character.

In the Administration Console, the comma character, is used to delimit different arguments passed to a batch command, as described in “Batch Commands Syntax” on page 18. Within a batch command argument, include double quotes in a comma delimited value list, so that the comma will not be used as a delimiter.

Examples:

```
modifyuser ted@jumboinc.com, approved_senders="+yahoo.com,+aol.com"  
modifyorg "Jumbo, Inc", support_contact=support@jumboinc.com
```

Batch Validation fails although command syntax is correct.

The batch validator does not take into account previous changes made within a batch file. This implies that the following batch command sequence will cause a validation error.

```
adduser username1@jumboinc.com  
addalias username1@jumboinc.com, username2@jumboinc.com
```

If the syntax is correct, then these batch commands can be processed in this sequence without error.

Chapter 2

Batch Command and Field Quick Summary

About the Batch Command and Field Quick Summary

This index is a quick summary for the batch commands and fields. Each command and field is listed with a simple description, the command's or field's syntax, and an example.

For other quick reference information, see the “Batch Command Quick Summary” on page 91, “Batch Field Quick Summary” on page 111, and the “Additional Reference Information” on page 569.

Batch Commands

addalias

The addalias command associates an additional address with a user's primary email address. The alias receives the same filtering and shares the same User Quarantine as the user's primary email address.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
addalias <user address>, <alias> , [ confirm ]
```

```
addalias msmith@jumboinc.com, mary@jumboinc.com, confirm
```

adddomain

The adddomain command adds a domain to your organization hierarchy.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
adddomain <org name | iid>, domain=<domain name>
```

```
adddomain "Jumbo's Western Region", domain=jumboinc.com
```

addorg

The addorg command adds a sub-organization to your organizational hierarchy.

Batch Command Syntax and Example:

```
addorg <org name>, parent=<parent org> [, <field>=<value>, ...]
```

```
addorg "Jumbo's Org", parent="Jumbo, San Carlos",  
max_message_size=250
```

adduser

The adduser command adds users to the Message Security service.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
adduser <user address> [, <field>=<value>, ...], [org=<org name>],  
[welcome=<1 | 0>]  
  
adduser jim@jumboinc.com, approved_senders=+hugeisp.com, welcome=1
```

archive_settings display

The archive_settings display command displays the archive settings for an organization.

Batch Command Syntax and Example:

```
archive_settings display org=<org name>  
  
archive_settings display org="Jumbo's ABC, Santa Clara"
```

archive_settings modify

The archive_settings modify command edits the archive settings for an organization.

Batch Command Syntax and Example:

```
archive_settings modify org=<org name>, archive_enable=<on | off>,  
mail_flow=<on | off>, journaling=<on | off>  
  
archive_settings modify org=Jumbo ABC, archive_enable=on,  
mail_flow=on, journaling=on
```

blockprovuser

The blockprovuser command sets a provisional user as permanently blocked from being added to the Message Security service. This occurs when using SmartCreate mail handling policy.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
blockprovuser <user address>  
  
blockprovuser john@jumboinc.com
```

checklatency

The checklatency command measures the connection delay between the email data center and your email server. This is the Latency Test.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
checklatency <email config org>, mailhost=<mail server>
```

```
checklatency sales email config, mailhost=my.mailserver.com
```

checkroute

The checkroute command, or Traceroute Test, traces the network route from the server to the input mail server.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
checkroute <email config org>, mailhost=<mail server | IP address>
```

```
checkroute salesemailconfig, mailhost=mailserver.jumboinc.com
```

deletealias

The deletealias command removes a user's alias completely from the Message Security service.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
deletealias <alias>
```

```
deletealias myalias@jumboinc.com
```

deletedomain

The deletedomain command removes the domain from your organizational hierarchy.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
deletedomain <domain name | domain id>
```

```
deletedomain jumboinc.com
```

deleteorg

The deleteorg command removes an organization from the Message Security service.

Batch Command Syntax and Example:

```
deleteorg <org name | iid>
```

```
deleteorg "Jumbo's Western Region"
```

deleteprovuser

The deleteprovuser command removes a provisional user that is known to be illegitimate. It won't appear on your bill.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
deleteprovuser <user address>
```

```
deleteprovuser john@jumboinc.com
```

deleteuser

The deleteuser command removes users from the Message Security service.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
deleteuser <user address | user_id> [ , deactivate] [ , purge] [ , confirm ]
```

```
deleteuser msmith@jumboinc.com
```

If the user being deleted is an administrator, use confirm:

```
deleteuser admin@jumboinc.com, confirm
```

displaydomain

The displaydomain command displays all of the selected domain's settings information.

Batch Command Syntax and Example:

```
displaydomain <domain name | domain id>
displaydomain jumboinc.com
```

displayorg

The displayorg command displays all the selected organization's settings information.

Batch Command Syntax and Example:

```
displayorg <org name | org's iid>
displayorg "Jumbo's Western Region"
```

displayprovuser

The displayprovuser command shows the active list of provisional users.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
displayprovuser <email address>
displayprovuser john@jumboinc.com
```

displayspool

The displayspool command shows the Spool Manager settings for your email config organization.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
displayspool <email config org>  
displayspool jumboemailconfig
```

displayuser

The displayuser command shows all the user's settings information.

Batch Command Syntax and Example:

```
displayuser <user address | u_id>  
displayuser msmith@jumboinc.com
```

domain_tls add

The domain_tls add add command adds Policy-Enforced TLS to organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
domain_tls add org=<email config orgtag | ID>, hop=<ib_sender |  
ob_recipient>, domain=<domain name>  
domain_tls add org=<Salesemailconfig, hop=ib_sender,  
domain=jumboinc.com
```

domain_tls delete

The domain_tls delete command deletes the organization's Policy-Enforced TLS settings which identify domain names that require inbound and outbound message traffic to be sent via a TLS connection.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
domain_tls delete org=<email config orgtag | ID>, hop=<ib_sender |  
ob_recipient>, domain=<domain name>  
domain_tls delete org=<Salesemailconfig, hop=ib_sender,  
domain=jumboinc.com
```

domain_tls display

The domain_tls display command displays Policy-Enforced TLS settings for organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
domain_tls display org=<email config orgtag | ID>, hop=<ib_sender |  
ob_recipient>  
  
domain_tls display org=<Salesemailconfig, hop=ib_sender
```

domain_tls modify

The domain_tls modify command edits settings for Postini Policy-Enforced TLS.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
domain_tls modify org=<email config orgtag | ID>, hop=<ib_sender>,  
domain=<domain name | _default><cert_validation=<encrypt | verify | trust |  
domain>  
  
domain_tls modify org=Salesemailconfig, hop=ib_sender,  
domain=_default, cert_validation=verify
```

encryption display_org

The encryption display_org command displays an organization's encryption information.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
encryption display_org, orgtag=<org name>  
  
encryption display_org, orgtag=Sales
```

encryption display_user

The encryption display_user command displays user specific encryption information.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
encryption display_user, address=<user address>  
encryption display_user, address=msmith@jumboinc.com
```

encrypton list_users

The encryption list_users command lists all encryption users in this organization.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
encryption list_users, orgtag=<org name>, [ext_encrypt=<on | off | match>]  
encryption list_users, orgtag=Sales, ext_encrypt=on
```

encryption modify_org

The encryption modify_org command lists all encryption users in this organization.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
encryption modify_org, orgtag=<org name>, service=<on | off | match |  
default> [ ,criteria=header string] [ ,cascade=1]  
encryption modify_org, orgtag=Sales, service=on
```

encryption modify_user

The encryption modify_user command modifies encryption settings for a user.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
encryption modify_user, address=<user address>, service=<on | off | match |  
default>  
encryption modify_user, address=msmith@jumboinc.com, service=on
```

getorgreport

The getorgreport command builds a traffic, virus, spam, or usage report for a selected organization.

Batch Command Syntax and Example:

```
getorgreport <org name>, report=<report type>, date=<date>, [top=<integer>]  
getorgreport sales, report=traffic_summary, date=20060916-20060901  
getorgreport sales, report=spam_summary, date=20060331, top=10  
getorgreport sales, report=usage_summary, date=20060331
```

help

The help command lists the syntax, example, and quick tips for a command.

Batch Command Syntax and Example:

```
help <command>  
help displayorg
```

im add

The iplock add_range command creates an IM record using the user's IM screen name.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
im add im_name=<protocol:screen name>, address=<user address>  
im add im_name=MSN:kristie_kerns@hotmail.com,  
address=kkerns@jumboinc.com
```

im delete

The im delete command deletes the IM record associated with the user's IM screen name.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
im delete im_name=<protocol:screen name>  
im delete im_name=MSN:kristie_kerns@hotmail.com
```

im display

The im display command displays an IM record for an IM screen name.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
im display im_name=<protocol:screen name>
im display im_name=MSN:kristie_kerns@hotmail.com
```

im list

The im list command displays IM screen names for a specific organization.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
im list orgtag=<org name>, im_regex=<regular expression>, suborgs=<yes | no>, page=<page number>, pagesize=<page size>
im list orgtag=sales, im_regex=%joe%, suborgs=yes, page=1,
pagesize=5
```

im listforuser

The im listforuser command displays the complete list of IM screen names associated with a user's email address.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
im listforuser address=<user address>
im listforuser address=msmith@jumboinc.com
```

iplock add_range

The iplock add_range command allows emails from specific domains with specific IP addresses to be delivered to an organization and its sub-organizations.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
iplock add_range org=<email config org name>, domain=<domain name>, range=<IP address>[/<CIDR subnet>]
```

Single Domain and IP Address/CIDR Subnet

```
iplock add_range org=sales_email_config, domain=jumboinc.com, range=64.18.0.0
```

```
iplock add_range org=sales_email_config, domain=jumboinc.com, range=64.18.0.0/16
```

iplock delete

The iplock delete command removes all domains with IP limitations configured in the specified email configuration organization.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
iplock delete org=<email config org name>
iplock delete org=sales_email_config
```

iplock delete_range

The iplock delete_range command removes either one IP limitation or all IP limitations for one domain configured in the specified email config organization.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Examples:

```
iplock delete_range org=<email config org name>, domain=<domain name>, range=<<IP address [/CIDR subnet]> | all>
```

If the domain has multiple IP limitations (63.18.0.0/16, 64.18.0.0/16), this example removes both IP limitations from this domain:

```
iplock delete org=sales_email_config, domain=jumboinc.com, range=all
```

To delete a specific IP limitation for the domain, this example removes only the limitation for 64.18.0.0/16.

```
iplock delete org=sales_email_config, domain=jumboinc.com, range=64.18.0.0/16
```

iplock display

The iplock display command lists all allowed sending domains and associated IPs configured in an email config organization.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Examples:

```
iplock display org=<email config org name>
```

```
iplock display org=sales_email_config
```

iplock set_disposition

The iplock set_disposition command configures the IP lock's response behavior when a message does not match the IP range.

Note: This command is not available in this version. The default disposition is to 'reject' the message if it does not match a domain's IP lock. The message is bounced with a 500 error.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
iplock set_disposition org=<email config org name>, domain=<domain name>,  
disposition=<reject | ignore | quarantine>
```

The default behavior is to reject with a 550 error any message that does not match the IP range:

```
iplock set_disposition org=sales_email_config, domain=jumboinc.com,  
disposition=reject
```

listdomains

The listdomains command returns a list of domains in an organization. The list can be all domains or it can be sorted and filtered.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
listdomains <domain name qstring | ALL> , targetOrg=<org name>
[,orgtaggs=<orgtag qstring> ]
[, primaryqs=<primary domain qstring> ]
[,aliases=<0 | 1> ]
[,childorgs=<0 | 1> ]
[,sort=<sortspec> ]
[,fields=<fieldlist> ]
[,start=<startindex> ]
[,end=<endindex> ]

listdomains ALL, targetOrg=sales, childorgs=1, sort=ORGTAG:a
```

listorgs

The listorgs command returns a list of organizations. The list can be all organizations or it can be sorted and filtered.

Batch Command Syntax and Example:

```
listorgs <orgtag gstring | ALL> , targetOrg=<org name>
[ , childorgs=<0|1> ]
[ , sort=<sortspec> ]
[ , fields=<fieldlist> ]
[ , start=<starindex> ]
[ , end=<endindex> ]

listorgs ALL, targetOrg=sales, sort=IID:nd
```

listprovusers

The listprovusers command returns a list provisional users. The list can be all provisional users or it can be sorted and filtered.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```

listprovusers <org name>
[, subset=ALL | BLOCK | UNBLOCK]
[, addressqss=<match spec>]
[, childorgs=0 | 1]
[, sort=<sortspec> ]
[, fields=<fieldlist> ]
[, start=<startindex> ]
[, end=<endindex> ]

listprovusers My Company, subset=ALL, sort=TS1:d,
fields=ADDRESS|TS1|TS3

```

listusers

The listusers command returns a list of users. The list can be all users or it can be sorted and filtered.

Batch Command Syntax and Example:

```

listusers <user address qstring | 'ALL' , targetOrg=<org name>
[, orgtagqss=<orgtag qstring>]
[, primaryqss=<primary address qstring>]
[, aliases=<0 | 1>]
[, childorgs=<0 | 1>]
[, sort=<sortspec>]
[, fields=<fieldlist>]
[, start=<startindex>]
[, end=<endindex>]
[, type_of_user=<im | all>]

listusers ALL, targetOrg=sales, sort=ADDRESS:a

```

modifydomain

The modifydomain command can move a domain, set subdomain stripping, and modify domain aliases.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
modifydomain <domain name>, [neworg=<org name> | substrip=<yes | no> |  
alias=<alias name> | -alias name>]  
  
modifydomain jumboinc.com, substrip=no
```

modifyorg

The modifyorg command modifies an organization's settings.

Batch Command Syntax and Example:

```
modifyorg <org name> [,field=<value>, ...]  
  
modifyorg sales, im_enable=on
```

modifyuser

The modifyuser command modifies a user's settings.

Batch Command Syntax and Example:

```
modifyuser <user address> [, <field>=<value>, ...]  
  
modifyuser msmith@jumboinc.com, junkmail_filter=0
```

notification display

The notification display command displays an organization's notification information.

Batch Command Syntax and Example:

```
notification display  
  
type=<all | attachment_manager_inbound | attachment_manager_outbound |  
early_detection_quarantine | first_spam | password_reset |  
quarantine_summary | spam | suspension | virus | welcome_user>,  
org=<target Org>  
  
notification display type=virus, org=sales
```

notification modify

The notification modify command creates, modifies, and deletes notifications associated with an organization.

Syntax and Examples Per Notification Type:

```

notification modify type=attachment_manager_inbound, org=<org name> [ , <state=<user | quarantine redirect | both | off>> ] | [ , text=link:<the org name which shares the notification text> | unlink | default ]

notification modify type=attachment_manager_inbound, org=sales, state=user, text=default

notification modify type=attachment_manager_outbound, org=<org name> [ , state= user | quarantine redirect | both | off ] | [ , text=link:<the org name which shares the notification text> | unlink | default ]

notification modify type=attachment_manager_outbound, org=sales, state=user, text=link:engineering_org

notification modify type=early_detection_quarantine, org=<org name> [ , state=< on | off > ] | [ , text=link:<the org name which shares the notification text> | unlink | default ]

notification modify type=early_detection_quarantine, org=sales, state=on, text=default

notification modify type=first_spam, org=<org name> [ , state=< on | off > ] | [ , text=link:<the org which shares the notification text> | unlink | default ] | [ , cc=<user address> ]

notification modify type=first_spam, org=sales, state=on, text=unlink, cc=<mssmith@jumboinc.com>

notification modify type=password_reset, org=<org name> [ , text=link:<the org which shares the notification text> | unlink | default ]

notification modify type=password_reset, org=sales, text=default

notification modify type=quarantine_summary, org=<org name> [ , state=<on | off> ] | [ , inbox_delivery=<on | off> ] | [ , delivery_hour=<4 thru 21 which is an hour between 4 a.m. and 9 p.m> ] | [ , subject_links=<on | off> ] | [ , text=default ]

notification modify type=quarantine_summary, org=sales, state=on, inbox_delivery=off, delivery_hour=6, subject_links=on, text=default

notification modify type=spam, org=<org name> [ , state=<on | off> ] | [ , text=link:<the org name which shares the notification text> | unlink | default ] | [ , cc=<user address> ] | [ , frequency=< 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 > ]

notification modify type=spam, org=sales, state=on, text=default, cc=<mssmith@jumboinc.com>, frequency=3

notification modify type=suspension, org=<org name> [ , <text=link:<the org which shares the notification text> | unlink | default > ]

notification modify type=suspension, org=sales, text=default

notification modify type=virus, org=<org name> [ , state=<immediately | one per day | organization default | off> ] | [ , text=link:<the org which shares the notification text> | unlink | default ] | [ , cc=<user address> ]

notification modify type=virus, org=sales, state=immediately, text=default, cc=<mssmith@jumboinc.com>

```

```
notification modify type=welcome_user, org=<org name> [ , state=<on | off> ]  
| [ , text=link:<the org name which shares the notification text> | unlink |  
default ] | [ , cc=<user address> ]  
  
notification modify type=welcome_user, org=sales, state=on,  
text=default, cc=msmith@jumboinc.com
```

org_im_sesttings display

The org_im_settings display command displays all of the IM settings for an organization.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
org_im_settings display orgtag=<org name>  
org_im_settings display orgtag=sales
```

org_im_settings modify

The org_im_settings modify command modifies an organization's IM settings.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
org_im_settings modify orgtag=<org name>, disposition=<null | off | archive |  
standard_journal | custom_journal>, [disposition_email=<user address>] [  
file_transfer_receive=< off | internal_only | include_external >] [  
file_transfer_send=< off | internal_only | include_external >]  
  
org_im_settings modify orgtag=sales,  
disposition="archive,standard_journal"
```

password force_update

The password force_update command forces a user or all users in an organization to change their passwords the next time the user logs into the system. This command is used with an organization using the PMP password policy configuration.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
password force_update user=<user address>
password force_update org=<org name> [, cascade= <yes | no>]
password force_update user=msmith@jumboinc.com
password force_update org=Sales
password force_update org=Sales, cascade=yes
```

password reset

The password reset command resets a user's password. This command is used with an organization using the PMP or PMP password policy configuration.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
password reset user=<user address> [, password=<text>] [, notify=<yes | no>]
password reset user=msmith@jumboinc.com
password reset user=msmith@jumboinc.com, password=a8f2KTT*#, notify=yes
```

password_policy display

The password_policy display command displays the password policy for an organization. This command is used with an organization using the PMP password policy configuration.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
password_policy display <org=<org name>> | <iid=<org ID>>
password_policy display org=Sales
```

password_policy update

The password_policy update command creates a password policy for a new organization or updates the password policy for an existing organization. This command is used with an organization using the PMP password policy configuration.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
password_policy update <org=<org name>> | <iid=<org ID>>
[, min_length=<1 - 10> | null ]
[, required_complexity=<no | yes | null>]
[, max_login_attempts=<1 - 10 | null>]
[, lockout_period=<1 - 999 number of minutes | null>]
[, max_password_age=<1 - 999 number of days | null>]
[, password_history=<0 | 1 - 24 | null>]
[, cascade= <no | yes | null>]

password_policy update org=Sales, min_length=6,
required_complexity=yes, lockout_period=60
```

promoteprovuser

The promoteprovuser command adds a provisional user to the Message Security service and removes the provisional user record. This command is used with SmartCreate.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
promoteprovuser <user address>
promoteprovuser provuser@jumboinc.com
```

resetuser

The resetuser command resets most of a user's policy settings to the settings of the organization's Default User. This command can be used with any user, and is commonly used to reset a suspended user.

Batch Command Syntax and Example:

```
resetuser <user address>
resetuser msmith@jumboinc.com
```

setorgsubstripping

The setorgsubstripping command enables domain stripping for all domains in an organization.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
setorgsubstripping <org name | iid>,<on/1 | off/0>
setorgsubstripping sales,1
```

suspenduser

The suspenduser command suspends a user by disabling all filtering and the user's access to the Message Center.

Batch Command Syntax and Example:

```
suspenduser <user address> [ , notify] [ , hardSuspend] [ , deliver]
suspenduser msmith@jumboinc.com, hardSuspend
suspenduser msmith@jumboinc.com, notify, hardSuspend, deliver
```

testfirewall

The testfirewall command tests whether your firewall allows email traffic from IP addresses outside of the Message Security service IP range.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
testfirewall <user address>
testfirewall jumbomailserver@jumboinc.com
```

testmail

The testmail command verifies whether your email server can receive a message. This is the SMTP Message Test.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
testmail <user address>, mailtype=<1 | 0>
testmail msmith@jumboinc.com, mailtype=1
```

testmx

The testmx command tests your MX records. This is the MX Record Test.

Batch Command Syntax and Example:

```
testmx <domain name>  
testmx mailserver.jumboinc.com
```

unlockprovuser

The unlockprovuser command unblocks provisional users who have been blocked from becoming regular users. Provisional users are created with SmartCreate.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
unlockprovuser <user address>  
unlockprovuser msmit@jumboinc.com
```

user_im_settings add

The user_im_settings add command adds an IM settings record for a given user email address.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
user_im_settings add address=<user address>, external_enable=<on | off>,  
proto_enable=< + | - >all | aim | msn | yahoo | google>  
user_im_settings add address=msmith@jumboinc.com,  
external_enable=on, proto_enable=+all
```

user_im_settings delete

The user_im_settings delete command deletes an IM settings record for a given user email address.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
user_im_settings delete address=<user address>  
user_im_settings delete address=msmith@jumboinc.com
```

user_im_settings display

The user_im_settings display command displays IM settings for a given user email address.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
user_im_settings display address=<user address>
user_im_settings display address=msmith@jumboinc.com
```

user_im_settings modify

The user_im_settings modify command modifies IM settings for a given user email address.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Batch Command Syntax and Example:

```
user_im_settings modify address=<user address>, external_enable=<on | off>, protot_enable=< + | - >all | aim | msn | yahoo | google> [, file_transfer_receive=< off | internal_only | include_external >] [, file_transfer_send=< off | internal_only | include_external >]
user_im_settings modify address=msmith@jumboinc.com, external_enable=on, proto_enable=+all, file_transfer_receive=internal_only, file_transfer_send=off
```

Domain Fields

alias

The alias field holds the domain's aliases.

Syntax and Example:

```
alias = <alias>, ...
modifydomain jumboinc.com, alias=jumboalias.com
```

aliasedfrom

The aliasedfrom field lists a domain's aliases.

Syntax and Example:

```
aliasedfrom < domain's alias >, ...
aliasedfrom "hugeisp.com, jumboincwest.com"
```

aliasedto

The aliasedto field lists the domain associated with this alias.

Syntax and Example:

```
aliasedto <primary domain name>
aliasedto jumboinc.com
```

created_ts (for domains)

The created_ts (for domains) field holds the domain's creation timestamp.

Syntax and Example:

```
aliasto <primary domain name>
created_ts 1145962000
```

domainid

The domainid field holds the domain's unique

Syntax and Example:

```
domainid = < domain ID >
domainid 100001012
```

domainname

The domainname field holds the name of the domain.

Syntax and Example:

```
domainname=<string>  
domainname jumboinc.com
```

org (for domains)

The org (for domains) field holds the organization associated with the domain.

Syntax and Example:

```
org = <org name>  
org sales
```

primary_did

The primary_did field holds the primary domain ID.

Syntax and Example:

```
primary_did = <domain ID>  
primary_did 100001012
```

primary_dom

The primary_dom field holds the primary domain name associated with a domain alias.

Syntax and Example:

```
primary_dom = < primary domain name >  
primary_dom jumboinc.com
```

sub_strip

The sub_strip field enables subdomain substripping for the domain.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
sub_strip=< on/1 | off/0 >
```

```
sub_strip=on
```

substrip

The substrip field enables subdomain stripping for the domain.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
substrip=< on/1 | off/0 >
```

```
substrip=on
```

Organization Fields

approved_senders (for orgs)

The approved_senders (for orgs) field holds an email address or domain to be added or removed from the organization-level Approved Senders list.

Syntax and Example:

```
approved_senders=< [+] | -email address>, ... | < [+] | -domain name>, ... |<empty>
```

```
modifyorg sales, approved_senders=+jim@hugeisp.com
```

archive

The archive field lists whether archiving is on or off for an organization.

Syntax and Example:

```
archive=<on/1 | off/0 | NULL ()>
```

```
archive 1 (on)
```

archive_enable

The archive_enable field enables archiving to be on or off for an organization.

Syntax and Example:

```
archive_enable=<on | off | NULL>  
archive_settings modify org=Jumbo ABC, archive_enable=on,  
mail_flow=on, journaling=on
```

async_bounce

The `async_bounce` field lists whether the Connection Manager's Asynchronous Bouncing control is activated for inbound traffic. This control is for email servers that issue "unknown user" bounce messages asynchronously and require added security.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
async_bounce=on | off | NULL ()  
modifyorg sales, async_bounce=on
```

at_notify_on

The `at_notify_on` field shows the recipient notification status for messages quarantined by the Inbound Attachment Manager.

Syntax and Example:

```
at_notify_on=< 0 | 1 | 2 | 3 | NULL ()>  
modifyorg sales, at_notify_on=1
```

authentication_data

The `authentication_data` field holds the text `authstring` used for non-PMP authentication of users and administrators when logging into the Message Center or Administration Console.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
authentication_data= <XAuth string | NULL>  
authentication_data=<POP mail server | NULL>  
authentication_data=<POP mail server, < @ | +domain extension>>  
authentication_data=<POP mail server, <@ | +USERDOMAIN>>  
modifyorg sales, authentication_data="mypopserver"  
modifyorg sales, authentication_data="mypopserver, @jumboinc.com"
```

```
modifyorg sales, authentication_data="mypopserver, +jumboinc.com"
modifyorg sales, authentication_data="mypopserver, @USERDOMAIN"
modifyorg sales, authentication_data="mypopserver, +USERDOMAIN"
```

authentication_type

The authentication_type field holds the type of authentication protocol used by an organization.

Syntax and Example:

```
authentication_type = < 1 | 4 | 5 >
authentication_type 1 (PMP)
```

autocreate_web

The autocreate_web field determines whether users can be automatically created when the organization is using POP authentication. This is the Web Autocreate feature. After an organization's Authentication Method is set to POP and the Authentication Data is configured, an administrator can either enable user autocreation or not. For this autocreation method, a user is added automatically to the Message Security service when first logging in to the Message Center.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
autocreate_web=<off/0> | <on/1>
modifyorg sales, autocreate_web=off
```

blatant_spam

The blatant_spam field lists the activation status for Blatant Spam Blocking which bounces or blackholes (deletes) obvious spam before it reaches your email servers.

Syntax and Example:

```
blatant_spam=<OFF | blackhole | ERROR 571 Message Refused | NULL>
modifyorg sales, blatant_spam=blackhole
```

blocked_senders (for orgs)

The blocked_senders (for orgs) field lists an email address or a domain to be added or removed from the organization-level Blocked Senders list. All messages from these senders or domains will be quarantined.

Syntax and Example:

```
blocked_senders=<[+] | -emailaddress> | <[+] | -domain name | empty>,...  
modifyorg sales, blocked_senders=+jim@hugeisp.com
```

bounce_fragments

The bounce_fragments field enables partial message fragments to be quarantined or bounced.

Syntax and Example:

```
bounce_fragments=<on | off | NULL ()>  
modifyorg sales, bounce_fragments=on
```

company_name

The company_name field holds the company or entity name that is used in email notifications.

Syntax and Example:

```
company_name=<text>  
modifyorg sales, company_name=Jumbo Inc
```

create_method (for orgs)

The create_method (for orgs) field shows how an organization was created.

Syntax and Example:

```
create_method= 2 | 3  
create_method=2
```

created_date

The created_date field holds the creation time stamp for an organization.

Syntax and Example:

```
created_date=<date>  
created_date=1145962000
```

creator

The creator field lists the ID of the administrator who created the organization.

Syntax and Example:

```
creator=<user address | NULL (none)>
```

```
creator msmith@jumboinc.com
```

custom_journal

The custom_journal field is an on/off switch for IM conversations sent to the IM administrator's email address.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
custom_journal= < on | off >
```

```
org_im_settings modify orgtag=sales,  
disposition="archive,custom_journal"
```

default_message_limit

The default_message_limit field holds the maximum number of messages each registered user or alias in an organization can receive per day.

Syntax and Example:

```
default_message_limit=<0 - 99999999 | NULL>
```

```
modifyorg sales1, default_message_limit=1000
```

default_user

The default_user field lists the name of the organization's Default User template used when creating a new user in this org.

Syntax and Example:

```
default_user=pdefault@<domain> | postinidefault@<domain>  
<name>@<domain>
```

```
default_user 200122277 (pdefault@jumboinc.com)
```

disable_first_spam

The disable_first_spam field is an organization-level activation switch for a new user's notification telling the user the first spam message has been quarantined in the user's Message Center.

Syntax and Example:

```
disable_first_spam=<0/on | 1/off | NULL ()>  
modifyorg sales, disable_first_spam=1
```

disposition_virus

The disposition_virus field holds the disposition status of an email containing a virus. The disposition can be either redirected, deleted, quarantined, or tagged as a virus in the message email headers.

Syntax and Example:

```
disposition_virus=<redirect | quarantine | blackhole | tagonly | NULL ()>  
modifyorg sales, disposition_virus=blackhole
```

file_transfer_receive

The file_transfer_receive field enables receiving IM file transfers internally within the organization or to everyone.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
file_transfer_receive=< off | internal_only | include_external >  
org_im_settings modify orgtag=sales,  
file_transfer_receive=internal_only
```

file_transfer_send

The file_transfer_send field enables sending IM file transfers internally within the organization or to everyone.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
file_transfer_send=< off | internal_only | include_external >  
org_im_settings modify orgtag=sales,  
file_transfer_send=internal_only
```

footer_on

The footer_on field holds the activation status for an organization-level outbound Compliance Footer which describes an email policy or legal compliance.

Syntax and Example:

```
footer_on=<on | off>  
modifyorg sales, footer_on=on
```

iid

The iid field lists the unique sequential database assigned key for this organization.

Syntax and Example:

```
iid=<database key number>  
iid 100050344
```

im_enable

The im_enable field is an organization-level switch enabling IM Security.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
im_enable=<off/0 | on/1 | NULL ()>  
modifyorg= sales, im_enable=on
```

im_external_enable

The im_external_enable field is an organization-level IM Security switch which enables IM users to communicate with external users.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
im_external_enable=<off/0 | on/1 | NULL ()>  
modifyorg sales, im_external_enable=on
```

im_proto_enable

The im_proto_enable field lists what IM protocols are allowed for the organization.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
im_proto_enable=<+ | -protocol>,... | NULL  
modifyorg sales, im_proto_enable=+yahoo,-AIM
```

is_email_config

The is_email_config field states whether a configuration is the email config organization or not.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
is_email_config=<no | yes | undef>  
modifyorg jumboemailconfig, is_email_config=yes
```

journaling

The journaling field enables message archive journaling for an organization.

Syntax and Example:

```
journaling = <on | off>  
archive_settings modify org=Jumbo ABC, archive_enable=on,  
mail_flow=on, journaling=on
```

lang_locale (for orgs)

The lang_locale (for orgs) field enables organization-level language localization in the Quarantine Summary's static text, the default top text, character sets, and date format.

Syntax and Example:

```
lang_locale=<language code string | NULL>  
modifyorg sales, lang_locale=en_us.utf8
```

lastmod_date (for orgs)

The lastmod_date (for orgs) field holds the date the organization was last modified.

Syntax and Example:

```
lastmod_date=<time stamp>
```

```
lastmod_date 1145962000
```

mail_flow

The mail_flow field turns on or off the inbound and outbound archiving.

Syntax and Example:

```
mail_flow=<on | off>
```

```
archive_settings modify org=Jumbo ABC, archive_enable=on,  
mail_flow=on, journaling=on
```

max_message_size

The max_message_size field holds the organization-level maximum size of inbound attachments-per-message that users can receive.

Syntax and Example:

```
max_message_size=<1 - 300 (MB) | NULL (200M)>
```

```
modifyorg sales, max_message_size=20
```

message_encryption (for orgs)

The message_encryption (for orgs) field enables outbound organization-level messages to be encrypted and sent to a secure portal.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
message_encryption=<on | off | match | NULL ()>
```

```
modifyorg sales, message_encryption=on
```

message_encryption_criteria

The message_encryption_criteria field holds a header or subject string identifying outbound organization-level messages that need to be encrypted.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
message_encryption_criteria=<string> | NULL  
modifyorg sales, message_encryption_criteria=This message is  
encrypted
```

ndr

The `ndr` field holds outbound mail configuration (block or blackhole) for undeliverable bounce messages generated by the organization's mail server. This is the control for Undeliverable Bounce Message handling.

Syntax and Example:

```
ndr=<off | blackhole | quarantine | NULL ()>  
modifyorg sales, ndr=quarantine
```

non_account_bounce

The `non_account_bounce` field is a switch for Non-Account Bouncing. When on, messages are bounced if not addressed to a registered user or alias.

Syntax and Example:

```
non_account_bounce=<on/1 | off/0 | NULL ()>  
modifyorg sales, non_account_bounce=on
```

non_account_virus_scan

The `non_account_virus_scan` field enables virus scanning for non-account messages.

Syntax and Example:

```
non_account_virus_scan=<on/1 | off/0 | NULL ()>  
modifyorg sales, non_account_virus_scan = on
```

nullsender_disposition

The `nullsender_disposition` field holds a Non-Delivery Report/Receipt (NDR) message disposition, allowing organizations to filter inbound valid and spam NDRs. This functionality is available for the Message Filtering, Message Security, and Message Discovery products.

Syntax and Example:

```
nullsender_disposition=<quarantine | blackhole | <errstr> | ERROR <errstr> |  
NULL >  
  
addorg Sales, parent="Jumbo, San Carlos",  
nullsender_disposition=quarantine  
modifyorg Sales, nullsender_disposition=blackhole  
modifyorg Sales, nullsender_disposition="511 Refused - no sender"  
addorg Sales, parent="Jumbo, San Carlos",  
nullsender_disposition="ERROR 499 Deferred - no sender"
```

nullsender_headertag_validation

The nullsender_headertag_validation field holds the number of hours an NDR or “bounce” message will be accepted by the system for any outbound message sent with a header containing a digital signature. This functionality is available for the Message Filtering, Message Security, and Message Discovery products.

Syntax and Example:

```
nullsender_headertag_validation=< 1 - 336 | 0 | NULL >  
  
modifyorg Sales, nullsender_headertag_validation=120
```

orgname

The orgname field lists the name of the current organization.

Syntax and Example:

```
orgname=<text string>  
  
modifyorg sales, orgname=Hugeisp
```

orgtag

The orgtag field lists the name of the current organization. It is equivalent to the orgname field.

Syntax and Example:

```
orgtag=<text string>  
  
orgtag sales
```

out_at_notify_on

The out_at_notify_on field holds the notification recipient for messages quarantined for Outbound Attachment Manager rules.

Syntax and Example:

```
out_at_notify_on=<0 | 1 | 2 | 3 | NULL ()>  
modifyorg sales, out_at_notify_on=1
```

outbound_max_message_size

The outbound_max_message_size field holds the maximum size of attachments-per-message that users in the organization can send.

Syntax and Example:

```
outbound_max_message_size=<1 - 300 (MB) | NULL (200M)>  
modifyorg sales, outbound_max_message_size=200
```

outbound_virus

The outbound_virus field holds the activation status for outbound virus scanning.

Syntax and Example:

```
outbound_virus=<on/1 | off/0>  
modifyorg sales, outbound_virus=1
```

outbound_virus_disposition

The outbound_virus_disposition field lists the disposition (bounce or redirect) of an outbound email containing a virus.

Syntax and Example:

```
outbound_virus_disposition=<1 | 2>  
modifyorg sales, outbound_virus_disposition=2
```

parent_org

The parent_org field lists the organization that is one level up in the org hierarchy.

Syntax and Example:

```
parent_org=<text string>  
modifyorg sales, parent_org=Hugeisp
```

qsum_actionable

The qsum_actionable field determines if Quarantine Summary links are available.

Syntax and Example:

```
qsum_actionable=<"not actionable" | "basic delivery">  
modifyorg sales, qsum_actionable="not actionable"
```

qsum_enable

The qsum_enable field is a switch that sends the Quarantine Summary notifications.

Syntax and Example:

```
qsum_enable=<on | off>  
modifyorg sales, qsum_enable=on
```

qtine_redir_atq

The qtine_redir_atq field holds Attachment Manager Quarantine Redirect administrator address for inbound attachments.

Syntax and Example:

```
qtine_redir_atq=<valid user address | NULL (none)>  
modifyorg sales, qtine_redir_atq=msmith@jumboinc.com
```

qtine_redir_ndr

The qtine_redir_ndr field holds the user email address for the quarantined outbound Undeliverable Bounce Messages. When an outbound message is quarantined as an undeliverable Bounce message, the message is stored in this Message Center.

Syntax and Example:

```
qtine_redir_ndr=<valid user address | NULL (none)>  
modifyorg sales, qtine_redir_ndr=ndruser@jumboinc.com
```

qtine_redir_out_atq

The qtine_redir_out_atq field holds the user address for the Attachment Manager quarantined email for this organization. When an outbound message is quarantined by Attachment Manager, the message is stored in this Message Center.

Syntax and Example:

```
qtine_redir_out_atq=<valid user address | NULL (none)>
```

```
modifyorg sales, qtine_redir_out_atq=support@jumboinc.com
```

qtine_redir_out_virus

The qtine_redir_out_virus field holds the email address for the user receiving outbound virus email quarantine for an organization. When an outbound message is quarantined as a virus, the message is stored in this Message Center.

Syntax and Example:

```
qtine_redir_out_virus=<valid user address | NULL (none)>
```

```
modifyorg sales, qtine_redir_out_virus=support@jumboinc.com
```

qtine_redir_spam

The qtine_redir_spam field holds email address for the user receiving inbound spam email quarantine for an organization. When an outbound message is quarantined as spam, the message is stored in this Message Center.

Syntax and Example:

```
qtine_redir_spam=<valid user address | NULL (none)>
```

```
modifyorg sales, qtine_redir_spam=support@hugeisp.com
```

qtine_redir_virus

The qtine_redir_virus holds the email address for the user receiving inbound virus email quarantine for an organization. When an outbound message is quarantined as a virus, the message is stored in this Message Center.

Syntax and Example:

```
qtine_redir_virus=<valid user address | NULL (none)>
```

```
modifyorg sales, qtine_redir_virus=support@hugeisp.com
```

quarantine_links

The quarantine_links field is a switch to enable quarantine message links to be available in the Message Center.

Syntax and Example:

```
quarantine_links=<off/0 | on/1>  
modifyorg sales, quarantine_links=0
```

quarsum_links

The quarsum_links field is a switch enabling Quarantine Summary message links to be available.

Syntax and Example:

```
quarsum_links=<0/off | on/1 | NULL ()>  
modifyorg sales, quarsum_links=0
```

remotecmd_secret

The remotecmd_secret field holds the shared secret for digitally signing EZCommand URLs.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
remotecmd_secret=<string | NULL>  
remotecmd_secret swordfish
```

retention_months

The retention_months field holds the number of months archived messages are retained for an organization. This field applies to Postini Message Archiving, which is only used with Message Security installations.

Syntax and Example:

```
retention_months <number of months integer>
```

In the Administration Console, the field is returned as output with a different label:

```
Archive Retention Months: 3
```

spam_notify_on

The spam_notify_on field is a switch enabling the sending of spam quarantine notifications.

Syntax and Example:

```
spam_notify_on=<on/1 | off/0 | NULL ()
```

```
modifyorg sales, spam_notify_on=on
```

standard_journal

The standard_journal field is an on/off switch enabling IM conversations to be sent to all participants in the user's organization.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
standard_journal= <on | off >
```

```
org_im_settings modify orgtag=sales,  
disposition="archive,standard_journal"
```

support_contact

The support_contact field holds the address of the support contact for the organization. This address is used for all help links, and is the sender for notifications.

Syntax and Example:

```
support_contact=<support user address>
```

```
modifyorg sales, support_contact=support@hugeisp.com
```

tagonly_spam

The tagonly_spam field enables adding header tags to a spam email instead of forwarding the email to quarantine.

Syntax and Example::

```
tagonly_spam=<off/0 | on/1 | NULL ()>
```

```
modifyorg sales, tagonly_spam=off
```

tls_notify_admin

The `tls_notify_admin` field lists the administrator who receives the email config organization's Policy-Enforced TLS alerts.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
tls_notify_admin = <admin user address | NULL>
modifyorg Sales tls_notify_admin = msmith@jumboinc.com
```

tls_notify_on

The `tls_notify_on` field enables Policy-Enforced TLS alerts for an email config organization. It also acts as a throttle for the alert notifications by designating how much time elapses before additional notifications.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
tls_notify_on = <0 | 1 - 86400>
modifyorg Sales tls_notify_on = 600
```

timezone (for orgs)

The `timezone (for orgs)` field holds the user's timezone, a UNIX TZ string used in Message Center II.

Syntax and Example:

```
timezone=< UNIX TZ string >
timezone America/Los_Angeles ((GMT-8:00) Pacific Time (US &
Canada); Tijuana)
```

virus_clean

The `virus_clean` field is a flag indicating whether a virus cleaning is allowed for this organization.

Syntax and Example:

```
virus_clean=<off/0 | on/1>
modifyorg sales, virus_clean=1
```

virus_notify (for orgs)

The virus_notify (for orgs) field specifies how frequently virus notification email will be generated for the organization.

Syntax and Example:

```
virus_notify=<0 | 1 | 9 | NULL ()>  
modifyorg JumboInc virus_notify=9
```

welcome_on

The welcome_on field allows the system to send out welcome notifications. It shows whether a message should receive a welcome message at some point within the next 24 hours.

Syntax and Example:

```
welcome_on=on/1 | off/0  
welcome_on 1 (on)
```

zero_hour_notify_on

The zero_hour_notify_on field enables an Early Detection Quarantine virus notification sent to the message's recipient.

Syntax and Example:

```
zero_hour_notify_on=on/1 | off/0  
• When the field is returned as output:  
  zero_hour_notify_on 1 (on)  
• To change the setting:  
  modifyorg sales, zero_hour_notify_on=on
```

zero_hour_scan

The zero_hour_scan field enables or disables the Early Detection Quarantine feature.

Syntax and Example:

```
zero_hour_scan=1 | 0  
• When the field is returned as output:  
  zero_hour_scan 1 (on)  
• To change the setting:
```

```
modifyorg sales, zero_hour_scan=1
```

Report Fields

acc_messages

The acc_messages field holds the number of email messages sent to accounts or aliases registered in the Message Security service for the Traffic Report.

Syntax and Example:

```
acc_messages = <string of total number of message>
```

```
acc_message 2
```

account

The account field holds the user account for spam and virus messages in the org-level Spam and Virus Reports.

Syntax and Example:

```
account = <account name>
```

```
account Jumbo Inc
```

bad_isp

The bad_isp field holds the total number of quarantined messages due to a Blocked Senders listed domain. Used in the Spam Report.

Syntax and Example:

```
bad_isp= <total number string>
```

```
bad_isp 3
```

bad_sender

The bad_sender field holds the total number of quarantined messages due to the sender being listed on the Blocked Senders list either at the org or user level. Used in the Spam Report.

Syntax and Example:

```
bad_sender= <total number string>
```

```
bad_sender 3
```

bulk

The bulk field holds the total number of messages quarantined by the general category for junk email filtering for the Spam Report

Syntax and example:

```
bulk= <total number string>
```

```
bulk 3
```

bytes

The bytes field holds the total number of quarantined spam or virus messages in bytes for the Spam or Virus Report.

Syntax and Example:

```
bytes= <total number string>
```

```
bytes 3
```

cleanings

The cleanings field holds the number of viruses cleaned for the Virus Report.

Syntax and Example:

```
cleanings= <total number string>
```

```
cleanings 3
```

clean_failures

The clean_failures field holds the number of viruses cleaning failures for the Virus Report.

Syntax and Example:

```
clean_failures= <total number string>
```

```
clean_failures 3
```

commerce

The commerce field holds the number of filtered special offers for the Spam Report.

Syntax and Example:

```
commerce= <total number string>  
commerce 3
```

customerid

The customerid field holds unique identifying number for an Message Security service account customer. Used in the Usage Report.

Syntax and Example:

```
customerid=<unique id>  
customerid 11111101
```

customername

The customername field holds the name of the customer. Used in the Usage Report.

Syntax and Example:

```
customername=<customer name>  
customername Jumbo Inc
```

deliveries

The deliveries field holds the number of spam messages delivered from Quarantine to the user's mailbox for the Spam Report.

Syntax and Example:

```
deliveries= <total number string>  
deliveries 3
```

inf_deliveries

The inf_deliveries field holds the total number of infected deliveries from quarantine virus messages for the Virus Report.

Syntax and Example:

```
inf_deliveries= <total number string>  
inf_deliveries 3
```

messages

The messages field holds the total number of messages for the Usage Report.

Syntax and Example:

```
messages = <number of messages>
```

```
messages 11
```

mmf

The mmf field holds the total number of Get Rich messages for the Spam Report.

Syntax and Example:

```
mmf= <total number string>
```

```
mmf 3
```

naughty

The naughty field holds the total number of messages triggering the Sexually Explicit junk email filter for the Spam Report.

Syntax and Example:

```
naughty= <total number string>
```

```
naughty 3
```

num_bh_messages

The num_bh_messages field holds the total size of blackholed messages for the Traffic Report.

Syntax and Example:

```
num_bh_messages= <total number string>
num_bh_messages 3
```

num_bytes

The num_bytes field holds the total size of messages in bytes for the Traffic Report.

Syntax and Example:

```
num_bytes= <total number string>
```

```
num_bytes 3
```

num_f_messages

The num_f_messages field holds the total number of messages delivered directly to your mail server for all addresses in the server's domain for the Traffic Report. This is Forward Acct Messages.

Syntax and Example:

```
num_f_messages= <total number string>
num_f_messages 3
```

num_messages

The num_messages field holds the total number of messages passed through the Message Security service for the Traffic Report.

Syntax and Example:

```
num_messages= <total number string>
num_messages 3
```

num_q_messages

The num_q_messages field holds the total number of quarantined messages for the Traffic Report.

Syntax and Example:

```
num_q_messages= <total number string>
num_q_messages 3
```

num_spams

The num_spams field holds the number of quarantined spam for the Spam Report.

Syntax and Example:

```
num_spams= <total number string>
num_spams 3
```

num_viruses

The num_viruses field holds the total number of quarantined viruses for the Virus Report.

Syntax and Example:

```
num_viruses = <total number string>  
num_viruses 3
```

pct_bh_bytes

The pct_bh_bytes field holds the total percent of blackholed messages in bytes for the Traffic Report.

Syntax and Example:

```
pct_bh_bytes= <total number string>  
pct_bh_bytes 3
```

pct_bh_messages

The pct_bh_messages field holds the total percent of blackholed messages for the Traffic Report.

Syntax and Example:

```
pct_bh_messages= <total number string>  
pct_bh_messages 3
```

pct_f_bytes

The pct_f_bytes field holds the total percent of bytes delivered to your mail server for the account in bytes for the Traffic Report.

Syntax and Example:

```
pct_f_bytes= <total number string>  
pct_f_bytes 3
```

pct_f_messages

The pct_f_messages field holds the total percent of messages delivered to your mail server for the account for the Traffic Report.

Syntax and Example:

```
pct_f_messages= <total number string>  
pct_f_messages 3
```

pct_q_bytes

The pct_q_bytes field holds the total percent of quarantined messages in bytes for the Traffic Report.

Syntax and Example:

```
pct_q_bytes= <total number string>
```

```
pct_q_bytes 3
```

pct_q_messages

The pct_q_messages field holds the total percent of quarantined messages for the Traffic Report.

Syntax and Example:

```
pct_q_messages= <total number string>
```

```
pct_q_messages 3
```

productid

The productid field holds the Message Security service product name for the Usage Report.

Syntax and Example:

```
productid=<name of product>
```

```
productid ee
```

racial

The racial field holds the number of messages triggering the Racially Insensitive junk email filter for the Spam Report.

Syntax and Example:

```
racial= <total number string>
```

```
racial 3
```

recip

The recip field holds the email address of the recipient account for the Traffic Report.

Syntax and Example:

```
recip= <email address>  
recip msmith@jumboinc.com
```

sellerid

The sellerid field holds the unique identifying number of the Message Security service seller for the Usage Report.

Syntax and Example:

```
sellerid=<seller's id>  
sellerid 11111801
```

ssb

The ssb field holds the number of messages impacted by the Blatant Spam Blocking for the Spam Report.

Syntax and Example:

```
ssb= <total number string>  
ssb 3
```

stored_size

The stored_size field holds the total number of stored message bytes in the archive for the last month for the Usage Report.

Syntax and Example:

```
stored_size=<number of messages in bytes>  
stored_size 0
```

users

The users field holds the total number of users in the Usage Report.

Syntax and Example:

```
users=<number of users>  
users 11
```

Spool Fields

These fields are applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

auto_unspool

The auto_unspool field is the on/off switch for automatically delivering spooled messages.

Syntax and Example:

```
auto_unspool=<off/0 | on/1>  
auto_unspool '0'
```

despool_max_connections

The despool_max_connections field holds the maximum number of dedicated connections which will deliver your spooled mail when an outage is complete. This is the Unspooling Connection Rate.

Syntax and Example:

```
despool_max_connections=<number of dedicated connections string>  
despool_max_connections 5
```

duration

The duration field holds the amount of time since spooling was last activated, or the amount of time that spooling has been activated.

Syntax and Example:

```
duration=<duration time in seconds >  
duration 1800
```

org (for spooling)

The org (for spooling) field holds the name of the email config organization managed by Spool Manager.

Syntax and Example:

```
org=<email config name>  
org jumboemailconfig
```

quota

The quota field holds the assigned space available for spooling for this email config managed by Spool Manager.

Syntax and Example:

```
quota=<assigned space in bytes>
```

```
quota 5242880
```

spool_delay

The spool_delay field, in conjunction with connection failures, determines how many seconds before spooling starts.

Syntax and Example:

```
spool_delay=<900 | 1800 | 3600>
```

```
spool_delay 900
```

spool_mech

The spool_mech field holds the initiation mechanism that starts spooling.

Syntax and Example:

```
spool_mech=<“Automatic” | “Start Manually” | “Suspend” | “Spool Delay”>
```

```
spool_mech “Suspend”
```

status

The status field holds email config organization's status managed by Spool Manager.

Syntax and Example:

```
status=<“Not Provisioned” | Suspended | “Standing By” | Spooling |  
Unspooling>
```

```
status Suspended
```

used_pct

The used_pct field is the percentage of the assigned spooling space that has been used.

Syntax and Example:

```
used_pct= < total number string>
```

```
status Suspended
```

used_size

The used_size field holds the used amount of allocated spool storage for an email config managed by Spool Manager.

Syntax and Example:

```
used_size=< total amount in bytes >
```

```
used_size 3.00
```

User Fields

active

The active field indicates whether the user has ever logged into the Message Center.

Syntax and Example:

```
active=<no/0 | yes/1>
```

```
active 1 (yes)
```

address

The address field holds the email address of the user or the user's alias.

Syntax and Example:

```
address=<legal email address>
```

```
modifyuser msmith@jumboinc.com, address=msmith@hugeisp.com
```

approved_recipients

The approved_recipients field holds an email address or domain to be added or removed from the Approved Recipients list which is also known as the Approved Mailing list located in the user's Message Center.

Syntax and Example:

```
approved_recipients=<[+] | -user address><[+] | -domain name>,... | 'empty'  
modifyuser msmith@jumboinc.com, approved_recipients=-  
newupdates@hugeisp.com
```

approved_senders (for users)

The approved_senders (for users) field holds an email address or domain to be added or removed from the user-level Approved Senders list in the user's Message Center.

Syntax and Example:

```
approved_senders=<[+] | -user address>, ... | <[+] | -domainname>,... |  
<empty>  
modifyuser msmith@jumbocinc.com, approved_senders=+jim@hugeisp.com
```

blocked_senders (for users)

The blocked_senders (for users) field lists an email address or a domain to be added or removed from the user-level Blocked Senders list. All messages from these senders or domains will be quarantined in the user's Message Center.

Syntax and Example:

```
blocked_senders=<[+] | -emailaddress> | <[+] | -domain name> | <empty>,...  
modifyuser msmith@jumboinc.com, blocked_senders=-jim@hugeisp.com
```

create_method (for users)

The create_method (for users) field shows how a user is created.

Syntax and Example:

```
created_date = <date in UNIX seconds>  
create_method 2
```

created_date

The created_date field shows when the user was created in UNIX seconds.

Syntax and Example:

```
created_date = <date in UNIX seconds>  
created_date = 1145962000
```

created_ts (for users)

The created_ts (for users) field holds the date the im_map record was created.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
created_ts=<user creation date>  
created_ts: 2006/04/14 00:36:28 GMT
```

filter_adult

The filter_adult field holds the sexual content filter settings for the user.

Syntax and Example:

```
filter_adult=<numeric | text string>  
modifyuser msmith@jumboinc.com, filter_adult=moderate
```

filter_bulk

The filter_bulk field holds the general spam filter setting for the user. This filter handles the bulk of the spam being blocked.

Syntax and Example:

```
filter_bulk=<number | text>  
modifyuser msmith@jumboinc.com, filter_bulk=aggressive
```

filter_getrich

The filter_getrich field holds the Get Rich Quick category filter setting for the user.

Syntax and Example:

```
filter_getrich=<number | text>  
modifyuser msmith@jumboinc.com, filter_getrich=lenient
```

filter_offers

The filter_offers field holds the Special Offers category filter setting for the user.

Syntax and Example:

```
filter_offers=<number | text>  
modifyuser msmith@jumboinc.com, filter_offers=moderate
```

filter_racial

The filter_racial field holds Racially Insensitive category filter setting for the user.

Syntax and Example:

```
fitler_racial=<number | text>  
modifyuser msmith@jumboinc.com, filter_racial=moderate
```

im_name

The im_name field holds the IM user's im screen name.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
im_name=<protocol : IM screen name>  
im add im_name=MSN:kristie_kerns@hotmail.com,  
address=kkerns@jumboinc.com
```

initial_password

The initial_password field holds the PMP password assigned to this user when the user was first added to the service.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
initial_password=<8 printable characters | NULL>  
modifyuser msmith@jumboinc.com, initial_password=ducksoap
```

junkmail_filter

The junkmail_filter field is an on/off switch for Spam Filtering.

Syntax and Example:

```
junkmail_filter=<off/0 | on/1>  
modifyuser msmith@jumbocinc.com, junkmail_filter=on
```

lang_locale (for users)

The lang_locale (for users) field enables user-level language localization in Message Center II's static text, the default top text, character sets, and date format.

Syntax and Example:

```
lang_locale=<language code string | NULL>  
modifyuser msmith@jumboinc.com, lang_locale=en_us.utf8
```

lastmod_date (for users)

The lastmod_date (for users) field shows the last time the user record was modified.

Syntax and Example:

```
lastmod_date=<time stamp>  
lastmod_date 1145962000
```

message_count

The message_count field holds the approximate number of messages received by this user within one day.

Syntax and Example:

```
message_count=<0 - 99999999>  
message_count 16
```

message_encrypt (for users)

The message_encrypt (for users) field enables outbound user messages to be encrypted and sent to a secure portal.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
message_encryption=<on | off | match | NULL ()>  
modifyuser msmith@jumboinc.com, message_encryption=on
```

message_limit

The message_limit field holds the maximum number of messages allowed per day for this user.

Syntax and Example:

```
message_limit=<0 - 99999999> | NULL
```

```
modifyuser msmith@jumboinc.com, message_limit= 1000
```

message_limited

The message_limited field is yes/no switch showing the user has reached the daily message limit.

Syntax and Example:

```
message_limited=<no/0 | yes/1>
```

```
message_limited 0 (no)
```

notice_address

The notice_address field holds the address where notifications for this user are sent.

Syntax and Example:

```
notice_address=<legal email address | NULL>
```

```
adduser jim@jumboinc.com, notice_address=support@jumboinc.com
```

orgid

The orgid field holds a unique ID for the organization containing the user.

Syntax and Example:

```
orgid=<IID | orgtag>
```

```
orgid 100001012 (sales)
```

password

The password field holds the encrypted PMP user password.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
password=<printable characters>  
modifyuser msmith@jumboinc.com, password=3pds9999
```

primary

The primary field holds the primary user's unique identifying ID.

Syntax and Example:

```
primary = <user ID>
```

```
primary 202846402
```

primaryadd

The primary_add field holds the primary user address.

Syntax and Example:

```
primary_add = < user name >
```

```
primary_add msmith@jumboinc.com
```

timezone (for users)

The timezone (for users) field holds the user's timezone, a UNIX TZ string. This is used in Message Center's scheduling of "quiet times," when messages should not be forwarded to the user's mobile device.

Syntax and Example:

```
timezone=<UNIX TZ string | NULL>
```

```
timezone MST7
```

TS1

The TS1 field holds the most recent timestamp for a good email message to a provisional user.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
TS1= < time in UNIX seconds >
```

```
TS1 1145962000
```

TS3

The TS3 field holds the timestamp for the oldest email message to a provisional user.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

TS3= < time in UNIX seconds >

TS3 1145962000

uid

The uid field holds the user's unique ID.

Syntax and Example:

uid = < user ID >

uid 202846402

u_id

The u_id field holds a unique ID for this user.

Syntax and Example:

u_id=<user ID>

u_id 202846402

user_id

The user_id field holds a unique ID for this user, and is useful when escalating an issue to your service representative or Customer Care.

Syntax and Example:

user_id=<database generated ID>

user_id 2001122283

virus_notify (for users)

The virus_notify (for users) field holds frequency of a user's virus notifications.

Syntax and Example:

```
virus_notify=<0 | 1 | 9 | NULL ()>  
modifyuser msmith@jumboinc.com, virus_notify=1
```

virus_state

The virus_state field is an on/off/unavailable switch for virus scanning functionality.

Syntax and Example:

```
virus_state=<0/on | 1/off | 2/unavailable>  
modifyuser msmith@jumboinc.com, virus_state=on
```

weblocked

The weblocked field is an on/off switch giving Message Center access for the user.

Syntax and Example:

```
weblocked=<0/no | 1/yes>  
modifyuser msmith@jumboinc.com, weblocked=1
```

welcome_count

The welcome_count field holds whether a welcome message have been sent.

Syntax and Example:

```
welcome_count=<1 | 0>  
welcome_count 1
```

wireless_state

The wireless_state field is an on/off/unavailable switch for Wireless Forwarding which allows the user to forward messages to a text-enabled phone, PDA, or other mobile device.

This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax and Example:

```
wireless_state=<0/on | 1/off | 2/unavailable>  
modifyuser msmith@jumboinc.com, wireless_state=0
```


Chapter 3

Batch Command Quick Summary

About the Batch Command Quick Summary

This index is a quick summary mapping commands to categories of common tasks. Several commands create, display, or modify the data fields. Use this quick reference to discover which commands are specialized for a particular task, and to decide the best way to automate your organization management.

Add Commands

Domains

`adddomain` -- The `adddomain` command adds a domain to your organization hierarchy. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Domain Aliases

`modifydomain` -- The `adddomain` command adds a domain to your organization hierarchy. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

IM Security

`iplock add_range` -- The `im add` command creates an IM record using the user's IM screen name. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`user_im_settings add` -- The `user_im_settings add` command adds an IM settings record for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

IP Locking

`iplock add_range` -- The `iplock add_range` command allows emails from specific domains with specific IP addresses to be delivered to an organization and its sub-organizations. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Organizations

`addorg` -- The `addorg` command adds a sub-organization to your organizational hierarchy.

Policy Enforced TLS, Message Encryption

domain_tls add -- The domain_tls add command adds Policy-Enforced TLS enablement to organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Users

adduser -- The adduser command adds users to the Message Security service. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

User Aliases

addalias -- The addalias command associates an additional address with a user's primary email address. The alias receives the same filtering and shares the same User Quarantine as the user's primary email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Delete Commands

Domains

deletedomain -- The deletedomain command removes the domain from your organizational hierarchy. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

IM Security

im delete -- The im delete command deletes the IM record associated with the user's IM screen name. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

user_im_settings delete -- The user_im_settings delete command deletes an IM settings record for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

IP Locking

iplock delete -- The iplock delete command removes all domains with IP limitations configured in the specified email configuration organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

iplock delete_range -- The iplock delete_range command removes either one IP limitation or all IP limitations for one domain configured in the specified email config organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Organizations

deleteorg -- The deleteorg command removes an organization from the Message Security service.

Policy Enforced TLS, Message Encryption

domain_tls delete -- The domain_tls delete command deletes the organization's Policy-Enforced TLS settings which identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Provisional Users

deleteprovuser -- The deleteprovuser command removes a provisional user that is known to be illegitimate. It won't appear on your bill. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Users

deleteuser -- The deleteuser command removes users from the Message Security service. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

User Aliases

deletealias -- The deletealias command removes a user's alias completely from the Message Security service. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Display and Report Commands

Domains

`displaydomain` -- The `displaydomain` command displays all of the selected domain's settings information.

Help

`help` -- The `help` command lists the syntax, example, and quick tips for a command.

IM Security

`im display` -- The `im display` command displays an IM record for an IM screen name. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`org_im_settings display` -- The `org_im_settings display` command displays all of the IM settings for an organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`user_im_settings display` -- The `user_im_settings display` command displays IM settings for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

IP Locking

`iplock display` -- The `iplock display` command lists all allowed sending domains and associated IPs configured in an email config organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Message Archiving

`archive_settings display` -- The `archive_settings display` command displays the archive settings for an organization.

Notifications

`notification display` -- The `notification display` command displays an organization's notification information.

Organizations

displayorg -- The displayorg command displays all the selected organization's settings information

PMP Passwords

password_policy display -- The password_policy display command displays the password policy for an organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Policy Enforced TLS, Message Encryption

domain_tls display -- The domain_tls display command displays Policy-Enforced TLS settings for organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

encryption display_org -- The encryption display_org command displays an organization's encryption information. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

encryption display_user -- The encryption display_user command displays user specific encryption information. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Provisional Users

displayprovuser -- The displayprovuser command shows the active list of provisional users. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Reports

getorgreport -- The getorgreport command builds a traffic, virus, spam, or usage report for a selected organization.

Spooling

displayspool -- The displayspool command shows the Spool Manager settings for your email config organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Users

displayuser -- The displayuser command shows all the user's settings information.

Domain Management Commands

Add Domains

adddomain -- The adddomain command adds a domain to your organization hierarchy. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Delete

deletedomain -- The deletedomain command removes the domain from your organizational hierarchy. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Display

displaydomain -- The displaydomain command displays all of the selected domain's settings information.

List

listdomains -- The listdomains command returns a list of domains in an organization. The list can be all domains or it can be sorted and filtered.

Modify

modifydomain -- The modifydomain command can move a domain, set subdomain stripping, and modify domain aliases. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Policy Enforced TLS, Message Encryption

`domain_tls add` -- The `domain_tls add` command adds Policy-Enforced TLS enablement to organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`domain_tls delete` -- The `domain_tls delete` command deletes the organization's Policy-Enforced TLS settings which identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`domain_tls display` -- The `domain_tls display` command displays Policy-Enforced TLS settings for organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`domain_tls modify` -- The `domain_tls modify` command edits settings for the Policy-Enforced TLS. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Substripping

`setorgsubstripping` -- The `setorgsubstripping` command enables domain stripping for all domains in an organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

IM Security Commands

Add

`iplock add_range` -- The `im add` command creates an IM record using the user's IM screen name. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`user_im_settings add` -- The `user_im_settings add` command adds an IM settings record for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Delete

im delete -- The im delete command deletes the IM record associated with the user's IM screen name. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

user_im_settings delete -- The user_im_settings delete command deletes an IM settings record for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Display

im display -- The im display command displays an IM record for an IM screen name. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

org_im_settings display -- The org_im_settings display command displays all of the IM settings for an organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

user_im_settings display -- The user_im_settings display command displays IM settings for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Lists

im list -- The im list command displays IM screen names for a specific organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

im listforuser -- The im listforuser command displays the complete list of IM screen names associated with a user's email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Modify

org_im_settings modify -- The org_im_settings modify command modifies an organization's IM settings. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

user_im_settings modify -- The user_im_settings modify command modifies IM settings for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

IP Locking Commands

Add

iplock add_range -- The iplock add_range command allows emails from specific domains with specific IP addresses to be delivered to an organization and its sub-organizations. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Delete

iplock delete -- The iplock delete command removes all domains with IP limitations configured in the specified email configuration organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

iplock delete_range -- The iplock delete_range command removes either one IP limitation or all IP limitations for one domain configured in the specified email config organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Display

iplock display -- The iplock display command lists all allowed sending domains and associated IPs configured in an organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Edit

iplock set_disposition -- The iplock set_disposition command configures the IP lock's response behavior when a message does not match the IP range. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

List Commands

Domains

listdomains -- The listdomains command returns a list of domains in an organization. The list can be all domains or it can be sorted and filtered.

IM Security

im list -- The im list command displays IM screen names for a specific organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

im listforuser -- The im listforuser command displays the complete list of IM screen names associated with a user's email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Organizations

listorgs -- The listorgs command returns a list of organizations. The list can be all organizations or it can be sorted and filtered.

Policy Enforced TLS

encryption list_users -- The encryption list_users command lists all encryption users in this organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Provisional Users

listprovusers -- The listprovusers command returns a list provisional users. The list can be all provisional users or it can be sorted and filtered. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Users

listusers -- The listusers command returns a list of users. The list can be all users or it can be sorted and filtered.

Message Archiving Message Archiving Commands

Display

archive_settings display -- The archive_settings display command displays the archive settings for an organization.

Modify

`archive_settings modify` -- The `archive_settings modify` command edits the archive settings for an organization.

Message Encryption Commands

Policy Enforced TLS

`domain_tls add` -- The `domain_tls add` command adds Policy-Enforced TLS enablement to organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`domain_tls delete` -- The `domain_tls delete` command deletes the organization's Policy-Enforced TLS settings which identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`domain_tls display` -- The `domain_tls display` command displays Policy-Enforced TLS settings for organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`domain_tls modify` -- The `domain_tls modify` command edits settings for the Policy-Enforced TLS. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`encryption display_org` -- The `encryption display_org` command displays an organization's encryption information. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`encryption display_user` -- The `encryption display_user` command displays user specific encryption information. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`encryption list_users` -- The `encryption list_users` command lists all encryption users in this organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`encryption modify_org` -- The `encryption modify_org` command modifies encryption settings for an organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`encryption modify_user` -- The `encryption modify_user` command modifies encryption settings for a user. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Modify Commands

Domains

`modifydomain` -- The `modifydomain` command can move a domain, set subdomain stripping, and modify domain aliases. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

IM Security

`org_im_settings modify` -- The `org_im_settings modify` command modifies an organization's IM settings. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`user_im_settings modify` -- The `user_im_settings modify` command modifies IM settings for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Message Archiving

`archive_settings modify` -- The `archive_settings modify` command edits the archive settings for an organization.

Message Encryption

`encryption modify_org` -- The `encryption modify_org` command modifies encryption settings for an organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`encryption modify_user` -- The `encryption modify_user` command modifies encryption settings for a user. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Notifications

`notification modify` -- The `notification modify` command creates, modifies, and deletes notifications associated with an organization.

Organizations

modifyorg -- The modifyorg command modifies an organization's settings.

PMP Passwords

password force_update -- The password force_update command forces a user or all users in an organization to change their passwords when logging into the system. This command is used with an organization using the PMP password policy configuration. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

password reset -- The password reset command resets a user's password. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

password_policy update -- The password_policy update command creates a password policy for a new organization or updates the password policy for an existing organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Policy Enforced TLS

domain_tls modify -- The domain_tls modify command edits settings for the Policy-Enforced TLS. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Users

modifyuser -- The modifyuser command modifies a user's settings.

Notification Commands

Display

notification display -- The notification display command displays an organization's notification information.

Modify

notification modify -- The notification modify command creates, modifies, and deletes notifications associated with an organization.

Organization Management Commands

Add

`addorg` -- The addorg command adds a sub-organization to your organizational hierarchy.

Delete

`deleteorg` -- The deleteorg command removes an organization from the Message Security service.

Display

`displayorg` -- The displayorg command displays all the selected organization's settings information.

`org_im_settings display` -- The org_im_settings display command displays all of the IM settings for an organization.

List

`listorgs` -- The listorgs command returns a list of organizations. The list can be all organizations or it can be sorted and filtered.

Modify

`modifyorg` -- The modifyorg command modifies an organization's settings.

`org_im_settings modify` -- The org_im_settings modify command modifies an organization's IM settings.

Notifications

`notification display` -- The notification display command displays an organization's notification information.

`notification modify` -- The notification modify command creates, modifies, and deletes notifications associated with an organization.

PMP Passwords

password force_update -- The password force_update command forces a user or all users in an organization to change their passwords when logging into the system. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

password reset -- The password reset command resets a user's password. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

password_policy display -- The password_policy display command displays the password policy for an organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

password_policy update -- The password_policy update command creates a password policy for a new organization or updates the password policy for an existing organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Provisional User Management Commands

Block

blockprovuser -- The blockprovuser command holds the provisional user who is permanently blocked from being added to the Message Security service. This occurs when using SmartCreate mail handling policy. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

List

listprovusers -- The listprovusers command returns a list provisional users. The list can be all provisional users or it can be sorted and filtered. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Promote

promoteprovuser -- The promoteprovuser command adds a provisional user to the Message Security service and removes the provisional user record. This command is used with SmartCreate. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Unblock

unlockprovuser -- The unlockprovuser command unblocks provisional users who have been blocked from becoming regular users. Provisional users are created with SmartCreate. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Spooling Commands

Display

displayspool -- The displayspool command shows the Spool Manager settings for your email config organization. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Test Commands

Firewalls

testfirewall -- The testfirewall command tests whether your firewall allows email traffic from IP addresses outside of the Message Security service IP range. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Latency Delays

checklatency -- The checklatency command measures the connection delay between the email data center and your email server. This is the Latency Test. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Mail Flow

testmail -- The testmail command verifies whether your email server can receive a message. This is the SMTP Message Test. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

MX Records

testmx -- The testmx command tests your MX records. This is the MX Record Test.

Traceroute

checkroute -- The checkroute command, or Traceroute Test, traces the network route from the server to the input mail server. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

User Management Commands

Add

adduser -- The adduser command adds users to the Message Security service. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

iplock add_range -- The im add command creates an IM record using the user's IM screen name. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

addalias -- The addalias command associates an additional address with a user's primary email address. The alias receives the same filtering and shares the same User Quarantine as the user's primary email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Delete

deletealias -- The deletealias command removes a user's alias completely from the Message Security service. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

user_im_settings delete -- The user_im_settings delete command deletes an IM settings record for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

deleteprovuser -- The deleteprovuser command removes a provisional user that is known to be illegitimate. It won't appear on your bill. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

deleteuser -- The deleteuser command removes users from the Message Security service. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Display

displayuser -- The displayuser command shows all the user's settings information.

`user_im_settings display` -- The `user_im_settings display` command displays IM settings for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

List

`listusers` -- The `listusers` command returns a list of users. The list can be all users or it can be sorted and filtered.

`im listforuser` -- The `im listforuser` command displays the complete list of IM screen names associated with a user's email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

`displayprovuser` -- The `displayprovuser` command shows the active list of provisional users. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Modify

`modifyuser` -- The `modifyuser` command modifies a user's settings.

`resetuser` -- The `resetuser` command resets a suspended user to most settings of the organization's Default User.

`suspenduser` -- The `suspenduser` command suspends a user by disabling all filtering and the user's access to the Message Center.

`user_im_settings modify` -- The `user_im_settings modify` command modifies IM settings for a given user email address. This is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Chapter 4

Batch Field Quick Summary

About the Batch Field Quick Summary

This index is a quick summary mapping fields to categories of common tasks. Use this quick reference to discover which fields are specialized for a particular task, and to decide the best way to automate your organization management.

Attachment Manager Fields (for Orgs)

Inbound

- Disposition

Fields -- Related Commands

- at_notify_on -- displayorg, modifyorg
- Redirect Address

Fields -- Related Commands

- qtine_redir_atq -- displayorg, modifyorg
- qtine_redir_ndr -- displayorg, modifyorg

Outbound

- Quarantine Notification Recipient

Fields -- Related Commands

- out_at_notify_on -- displayorg, modifyorg
- Redirect Address

Fields -- Related Commands

- qtine_redir_out_atq -- displayorg, modifyorg
- qtine_redir_out_virus -- displayorg, modifyorg

Default User Fields

Default User

- Name

Fields -- Related Commands

- default_user -- displayorg, displayuser, modifyuser

Spam

- Spam on/off

Fields -- Related Commands

- junkmail_filter -- displayuser, modifyuser

Virus

- Virus on/off

Fields -- Related Commands

- virus_state -- displayuser, modifyuser

Filters

- Adult Settings

Fields -- Related Commands

- filter_adult -- adduser, displayuser, modifyuser

- Spam Blocking Settings

Fields -- Related Commands

- filter_bulk -- adduser, displayuser, modifyuser

- Get Rich Settings

Fields -- Related Commands

- filter_getrich -- adduser, displayuser, modifyuser
- Offers Settings

Fields -- Related Commands

- filter_offers -- adduser, displayuser, modifyuser
- Racial Settings

Fields -- Related Commands

- filter_racial -- adduser, displayuser, modifyuser

Domain General Settings Fields

IDs and Name

- Alias related domain

Fields -- Related Commands

- primary_dom -- listdomains
- Domain alias

Fields -- Related Commands

- alias -- deletedomain, displaydomain, listdomains
- ID

Fields -- Related Commands

- aliasedfrom -- deletedomain, displaydomain, listdomains
- aliasedto -- deletedomain, displaydomain, listdomains
- domainid -- deletedomain, displaydomain, listdomains
- iid -- listdomains
- primary_did -- listdomains

- Name

Fields -- Related Commands

- domainname -- adddomain, deletedomain, displaydomain, listdomains, (For more cmd info, see **domainname** page)
- Org name

Fields -- Related Commands

- org (for domains) -- displaydomain

Substripping

- On/Off

Fields -- Related Commands

- substrip -- displaydomain
- sub_strip -- Administration Console-Domain Download/Settings

Early Detection Quarantine Fields

- On/Off

Fields -- Related Commands

- zero_hour_scan -- displayorg, modifyorg
- Notification

Fields -- Related Commands

- zero_hour_notify_on -- displayorg, modifyorg

Email Config Fields

Disaster Recovery/Spooling

- On/Off

Fields -- Related Commands

- auto_unspool -- displayorg
- Org name

Fields -- Related Commands

- org (for spooling) -- displayspool
- Start mechanism

Fields -- Related Commands

- spool_mech -- displayspool
 - Time last activated
- Fields -- Related Commands*
- duration -- displayspool
 - Remaining space

Fields -- Related Commands

- quota -- displayspool
- Time before spooling

Fields -- Related Commands

- spool_delay -- displayspool
- Email Config status

Fields -- Related Commands

- status -- displayspool
- Unspooling connection rate

Fields -- Related Commands

- despool_max_connections -- displayspool
- Used allowed space

Fields -- Related Commands

- used_pct -- displayspool
- Allocated space

Fields -- Related Commands

- used_size -- displayspool

IP Locking

- Add

Fields -- Related Commands

- orgname, domainname -- iplock add_range
- Clear all domain locks

Fields -- Related Commands

- orgname -- iplock delete_range
- Delete

Fields -- Related Commands

- orgname, domainname -- iplock delete
- Edit

Fields -- Related Commands

- orgname, domainname -- iplock set_disposition
- Show all sending domain:IPs

Fields -- Related Commands

- orgname -- iplock display

Message Encryption

(See User, General Setting Fields)

- External On/Off Match

Fields -- Related Commands

- message_encryption (for orgs) -- displayorg, modifyorg
- Header text

Fields -- Related Commands

- message_encryption_criteria -- displayorg, modifyorg
- Policy-Enforced TLS administrator

Fields -- Related Commands

- tls_notify_admin -- displayorg, modifyorg
- Policy-Enforced TLS alert

Fields -- Related Commands

- tls_notify_on -- displayorg, modifyorg

Org Type

- Yes/No

Fields -- Related Commands

- is_email_config -- displayorg

General Org Settings Fields

Authentication

- POP, XAuth's auth.string

Fields -- Related Commands

- authentication_data -- displayorg, modifyorg
- Type of authentication

Fields -- Related Commands

- authentication_type -- displayorg
- EZCommand secret

Fields -- Related Commands

- remotecmd_secret -- displayorg, modifyorg

General Info

- Creation method

Fields -- Related Commands

- create_method (for orgs) -- displayorg
- Creation date

Fields -- Related Commands

- created_date -- displayorg
- Modify date

Fields -- Related Commands

- lastmod_date (for orgs) -- displayorg

Org ID and Names

- ID

Fields -- Related Commands

- iid -- adddomain, deleteorg, displayorg, modifyorg, (for more cmds, see [iid page](#))

- Name

Fields -- Related Commands

- org (for spooling) -- displayspool
- orgname -- displayorg, modifyorg, (for more cmds, see [orgname page](#))
- orgtag -- listorgs, (for more cmds, see [orgtag page](#))
- parent_org -- addorg, displayorg

People/Support

- Administrator

Fields -- Related Commands

- support_contact -- displayorg, modifyorg
- Account ID

Fields -- Related Commands

- customerid -- getorgreport
- Creator of org

Fields -- Related Commands

- creator -- displayorg
- Notification name

Fields -- Related Commands

- company_name -- displayorg, modifyorg

Org Management

- Add an org

Fields -- Related Commands

- orgname -- addorg
- Delete an org

Fields -- Related Commands

- orgname -- deleteorg
- Edit/Move an org

Fields -- Related Commands

- orgname -- modifyorg
- List orgs

Fields -- Related Commands

- orgtag, orgname -- listorgs

IM Security Fields (for Orgs)

IM Security

- On/Off

Fields -- Related Commands

- im_enable -- modifyorg, org_im_settings modify, displayorg, org_im_settings display

Fields -- Related Commands

- im_external_enable -- displayorg, org_im_settings display

Fields -- Related Commands

- custom_journal -- org_im_settings modify, org_im_settings display

Fields -- Related Commands

- standard_journal -- org_im_settings modify, org_im_settings display

- Protocols on/off

Fields -- Related Commands

- im_proto_enable -- displayorg, org_im_settings display

- Receiving file transfers

Fields -- Related Commands

- file_transfer_receive -- org_im_settings modify, org_im_settings display

- Sending file transfers

Fields -- Related Commands

- file_transfer_send -- org_im_settings modify, org_im_settings display

Message Archiving Fields (for Orgs)

Message Archiving

- Inbound, outbound On/Off

Fields -- Related Commands

- mail_flow -- archive_settings display, archive_settings modify

- On/Off

Fields -- Related Commands

- archive -- displayorg, modifyorg, org_im_settings display

- archive_enable -- archive_settings display, archive_settings modify

- journaling -- archive_settings display, archive_settings modify

- Retention length

Fields -- Related Commands

- retention_months -- archive_settings display

Message Limits Fields (for Orgs)

Inbound

- Attachment Size

Fields -- Related Commands

- max_message_size -- displayorg, modifyorg
- Msg. Limit (per day)

Fields -- Related Commands

- default_message_limit -- displayorg, modifyorg

Outbound

- Attachment size

Fields -- Related Commands

- outbound_max_message_size -- displayorg, modifyorg

Message Limit Fields (for Users)

Limits

- Limit allowed

Fields -- Related Commands

- message_limit -- adduser, modifyuser, displayuser
- Limit reached, yes/no

Fields -- Related Commands

- message_limited -- displayuser
- One day total messages

Fields -- Related Commands

- message_count -- displayuser

Notifications Fields (for Orgs)

Notifications

- On/Off

Fields -- Related Commands

- disable_first_spam -- displayorg, modifyorg
- welcome_on -- displayorg, modifyorg

Outbound Compliance Footer

Compliance

- Compliance footer's related organization

Fields -- Related Commands

- iid -- adddomain, deleteorg, displayorg, modifyorg, setorgsubstripping, imdisplay, listdomains, listorgs, listusers

- On/Off

Fields -- Related Commands

- footer_on -- displayorg, modifyorg

Quarantine Summary

Notification

- Where to send notification

Fields -- Related Commands

- notice_address -- adduser, displayuser, modifyuser

Reports, Spam Fields

Inbound

- Name

Fields -- Related Commands

- account -- getorgreport
- Quarantined messages from Blocked Senders list

Fields -- Related Commands

- bad_isp -- getorgreport
- Quarantined senders from Blocked Senders list

Fields -- Related Commands

- bad_sender -- getorgreport
- Total Blatant Spam Blocked messages

Fields -- Related Commands

- ssb -- getorgreport
- Total Get Rich messages

Fields -- Related Commands

- mmf -- getorgreport
- Total junk in quarantine

Fields -- Related Commands

- bulk -- getorgreport
- Total from quarantine to user's mail account

Fields -- Related Commands

- deliveries -- getorgreport
- Total quarantine

Fields -- Related Commands

- num_spams -- getorgreport
- Total racially insensitive junk mail

Fields -- Related Commands

- racial -- getorgreport
- Total sexually explicit junk mail

Fields -- Related Commands

- naughty -- getorgreport
- Total spam in quarantine in bytes

Fields -- Related Commands

- bytes -- getorgreport
- Total special offers

Fields -- Related Commands

- commerce -- getorgreport

Reports, Traffic Fields

Inbound

- Forward Acct. msgs

Fields -- Related Commands

- num_f_messages -- getorgreport
- Name

Fields -- Related Commands

- recip -- getorgreport
- Percentage blackholed

Fields -- Related Commands

- pct_bh_messages -- getorgreport
- Percentage blackholed in bytes

Fields -- Related Commands

- pct_bh_bytes -- getorgreport
- Total delivered

Fields -- Related Commands

- pct_f_messages -- getorgreport
- Total delivered in bytes

Fields -- Related Commands

- pct_f_bytes -- getorgreport
- Total mail flow

Fields -- Related Commands

- num_messages -- getorgreport
- Total of mail going to accounts

Fields -- Related Commands

- acc_messages -- getorgreport
- num_bh_messages -- getorgreport
- Total msgs in bytes

Fields -- Related Commands

- num_bytes -- getorgreport
- Total quarantined

Fields -- Related Commands

- num_q_messages -- getorgreport
- pct_q_messages -- getorgreport
- Total quarantined in bytes

Fields -- Related Commands

- pct_q_bytes -- getorgreport

Reports, Usage Fields

Inbound

- Customer ID

Fields -- Related Commands

- customerid -- getorgreport
- Customer Name

Fields -- Related Commands

- customername -- getorgreport
- Product ID

Fields -- Related Commands

- productid -- getorgreport
- Seller ID

Fields -- Related Commands

- sellerid -- getorgreport
- Total messages

Fields -- Related Commands

- messages -- getorgreport
- Total users

Fields -- Related Commands

- users -- getorgreport
- Usage amount in bytes

Fields -- Related Commands

- stored_size -- getorgreport

Reports, Virus Fields

Inbound

- Name

Fields -- Related Commands

- account -- getorgreport
- Total failed viruses cleanings

Fields -- Related Commands

- clean_failures -- getorgreport
- Total quarantined

Fields -- Related Commands

- num_viruses -- getorgreport
- Total quarantined virus msgs delivered to admin mail box

Fields -- Related Commands

- inf_deliveries -- getorgreport
- Total viruses cleaned

Fields -- Related Commands

- cleanings -- getorgreport
- Total virus msgs in quarantine in bytes

Fields -- Related Commands

- bytes -- getorgreport

Sender List Fields (for Orgs)

Approved Senders

- Addresses, domains

Fields -- Related Commands

- approved_senders (for orgs) -- displayorg, modifyorg

Blocked Senders

- Addresses, domains

Fields -- Related Commands

- blocked_senders (for orgs) -- displayorg, modifyorg

- Total blocked ISPs

Fields -- Related Commands

- bad_isp -- getorgreport

- Total blocked senders

Fields -- Related Commands

- bad_sender -- getorgreport

Sender Lists Fields (for Users)

Approved

- Addresses, domains

Fields -- Related Commands

- approved_recipients -- adduser, modifyuser, displayuser
- approved_senders (for users) -- adduser, modifyuser, displayuser

Blocked

- Addresses, domains

Fields -- Related Commands

- blocked_senders (for users) -- adduser, modifyuser, displayuser

Spam Filtering Fields (for Orgs)

Inbound

- Disposition

Fields -- Related Commands

- blatant_spam -- displayorg, modifyorg
- On/Off header tags

Fields -- Related Commands

- tagonly_spam -- displayorg, modifyorg
- On/Off quarantine notify

Fields -- Related Commands

- spam_notify_on -- displayorg, modifyorg
- Redirect address

Fields -- Related Commands

- qtine_redir_spam -- displayorg, modifyorg

Spam Filtering Field (for Users)

Inbound

- Filter settings

Fields -- Related Commands

- filter_adult -- adduser, modifyuser, displayuser
- filter_bulk -- adduser, modifyuser, displayuser
- filter_getrich -- adduser, modifyuser, displayuser
- filter_offers -- adduser, modifyuser, displayuser
- filter_racial -- adduser, modifyuser, displayuser
- On/Off

Fields -- Related Commands

- junkmail_filter -- adduser, modifyuser, displayuser

System Testing Fields

Testing

- Firewall

Fields -- Related Commands

- address -- testfirewall
- Latency

Fields -- Related Commands

- orgname (emailconfig org) -- checklatency
- MX records

Fields -- Related Commands

- domainname -- testmx
- SMTP message

Fields -- Related Commands

- address -- testmail
- Traceroute

Fields -- Related Commands

- orgname (email config org) -- checkroute

User, Access Fields (for Orgs)

Message Center

- On/Off

Fields -- Related Commands

- quarantine_links -- displayorg, modifyorg
- quarsum_links -- displayorg, modifyorg

- Language

Fields -- Related Commands

- lang_locale (for orgs) -- displayorg, modifyorg

- Time

Fields -- Related Commands

- timezone (for orgs) -- modifyorg

Unrecognized addresses

- On/Off

Fields -- Related Commands

- async_bounce -- displayorg, modifyorg
- blatant_spam -- modifyorg
- non_account_bounce -- displayorg, modifyorg

- Outbound disposition

Fields -- Related Commands

- ndr -- displayorg, modifyorg

- Total blocked messages

Fields -- Related Commands

- num_bh_messages -- getorgreport

Quarantine summary

- Disposition

Fields -- Related Commands

- qsum_actionable -- displayorg, modifyorg

- Language

Fields -- Related Commands

- lang_locale (for orgs) -- displayorg, modifyorg
- NDR

Fields -- Related Commands

- ndr -- displayorg, modifyorg
- nullsender_disposition -- addorg, displayorg, modifyorg
- nullsender_headertag_validation -- displayorg, modifyorg
- On/Off

Fields -- Related Commands

- qsum_enable -- displayorg, modifyorg

User, General Setting Fields

General User Settings

- Creation method

Fields -- Related Commands

- create_method (for users) -- displayuser
- Modify date

Fields -- Related Commands

- lastmod_date (for users) -- displayuser

IDs and Names

- ID

Fields -- Related Commands

- primary -- listusers
- uid -- listusers
- u_id -- listusers, im display, user_im_settings display
- user_id -- modifyuser, displayuser

- Name

Fields -- Related Commands

- primary_add -- listusers
- Name, alias

Fields -- Related Commands

- address -- adduser, modifyuser, displayuser (For more cmd, see **address** page)
- Name, ID

Fields -- Related Commands

- orgid -- adduser, modifyuser, displayuser

Message Center

- Yes/No

Fields -- Related Commands

- active -- displayuser
- weblocked -- adduser, modifyuser, displayuser

Message Encryption

- External on/off match

Fields -- Related Commands

- message_encrypt (for users) -- adduser, modifyuser, displayuser

Passwords

- First password, set by system

Fields -- Related Commands

- initial_password -- displayuser
- PMP password

Fields -- Related Commands

- password -- adduser, modifyuser, displayuser

Provisional User

- Promoted Timestamp

Fields -- Related Commands

- TS3 -- listprovusers
- Received Timestamp

Fields -- Related Commands

- TS1 -- listprovusers

Time/Language

- Creation timestamp

Fields -- Related Commands

- created_ts (for users) -- listdomains, im display
- Quarantine Summary language

Fields -- Related Commands

- lang_locale (for users) -- adduser, modifyuser, displayuser
- Timezone for Message Center II & Message Center Classic (for scheduling wireless forwarding timezone only)

Fields -- Related Commands

- timezone (for users) -- adduser, modifyuser, displayuser

User management

- Add a user

Fields -- Related Commands

- address -- adduser
- Delete a user

Fields -- Related Commands

- address -- deleteuser
- Edit a user

Fields -- Related Commands

- address -- modifyuser
- List users

Fields -- Related Commands

- address -- listusers
- Reset

Fields -- Related Commands

- address -- resetuser
- Suspend

Fields -- Related Commands

- address -- suspenduser
- User alais

Fields -- Related Commands

- address -- addalias, deletealias, displayuser, listusers

Wireless Forwarding

- On/Off/Unavailable

Fields -- Related Commands

- wireless_state -- addalias, deletealias, displayuser

Virus Blocking Fields (for Orgs)

Inbound

- Disposition

Fields -- Related Commands

- disposition_virus -- displayorg, modifyorg

- Message frgments

Fields -- Related Commands

- bounce_fragments -- displayorg, modifyorg

- Non-account messages

Fields -- Related Commands

- num_bh_messages -- getorgreport

- Non-account msgs enable

Fields -- Related Commands

- non_account_virus_scan -- displayorg, modifyorg

- Notification frequency

Fields -- Related Commands

- virus_notify (for orgs) -- displayorg, modifyorg

- On/Off

Fields -- Related Commands

- virus_clean -- displayorg, modifyorg
- Redirect address

Fields -- Related Commands

- qtine_redir_virus -- displayorg, modifyorg
- Sensitivity

Fields -- Related Commands

- antivirus_sensitivity -- displayorg, modifyorg

Outbound

- Disposition

Fields -- Related Commands

- outbound_virus_disposition -- displayorg, modifyorg
- On/Off

Fields -- Related Commands

- outbound_virus -- displayorg, modifyorg

Virus Blocking Fields (for Users)

Inbound

- Frequency of notification

Fields -- Related Commands

- virus_notify (for users) -- adduser, modifyuser, displayuser
- On/Off/Unavailable

Fields -- Related Commands

- virus_state -- adduser, modifyuser, displayuser

Chapter 5

Batch Commands

About Batch Commands

The batch commands let you automate the management of large organizational configurations. These commands can add, delete, display, list, modify, test, and report on your organization configurations.

Command Reference Page Syntax Notations

Each command's syntax section uses notation and punctuation to show you where to put your specific information, and what information is required or optional:

The reference pages use the Administration Console syntax and have an example for each command:

- The command name and commas are required.
- Information between '< >' symbols means you need to add your specific information here. (for example: <user address> becomes `jim@hugeisp.com`)
- Information between '[']' square brackets mean this type of information is optional. (for example: [, <field>=<value>, ...] becomes `,approved_senders=+mary@hugeisp.com, filter_getrich=lenient`)
- A choice of values are separated by '|'. (for example: `welcome= <1 | 0>` means you have a choice of `welcome=1` or `welcome=0`)

Below are two examples of the adduser command. The command requires at least the user address. If needed, optional fields and parameters can be used.

```
adduser <user address> [, <field>=<value>, ...][, org=<org name>]  
[,welcome=<1|0>]
```

```
adduser msmith@jumboinc.com
```

```
adduser jim@hugeisp.com, approved_senders=mary@hugeisp.com,  
org=Sales, welcome=1
```

See “Batch Command and Field Quick Summary” on page 27 for an overall syntax summary, and see “Batch Command Quick Summary” on page 91 for more information.

addalias

The addalias command associates an additional address with a user's primary email address. The alias receives the same filtering and shares the same User Quarantine as the user's primary email address.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
addalias <user address>, <alias> , [confirm]
```

Example

```
addalias msmith@jumboinc.com, mary@jumboinc.com, confirm
```

Description

Batch Interface Description for addalias

Adds <alias> as an alias of <user address>, and requires a `confirm` parameter at the end of the command.

- <user address> -- The user's primary address associated with the alias.
Note: Enclose <user address> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.
- <alias> -- The alias address for the user's primary address.

If <alias> is an existing alias for another user, the alias will be transferred to the new <user address>.

If <alias> is an existing user's primary address:

- The existing user's primary address is deleted. This primary address name becomes an alias for the new user's primary address.
 - Any associated aliases for the existing user will be deleted and will become aliases for the new user's primary address.
 - The existing user's messages will be transferred before creating the alias.
- For example:

```
addalias operations@jumboinc.com, support@jumboinc.com, confirm
```

In this organization, support@jumboinc.com already exists as a user's primary address with an existing alias, helpdesk@jumboinc.com.

After the **addalias** command is run, operations@jumboinc.com has 2 new aliases, support@jumboinc.com and helpdesk@jumboinc.com. And the primary address support@jumboinc.com is removed.

- confirm -- A required positional parameter if an existing user address is being overwritten to become an alias address. The text confirm must be at the end of the command. There is no numeric equivalent.

EZCommand Description for addalias

See the Batch Interface Description for addalias for general usage details.

When used as an EZCommand, the command must be URL-escaped in order to properly submitted.

Example:

```
addalias msmith@jumboinc.com, mary@jumboinc.com, confirm
```

changes to

```
addalias%20msmith%40jumboinc.com%20mary%40jumboinc.com%20confirm
```

Errors

Possible batch command error messages include:

```
'No such user 'username' (unknown administrator address supplied).'  
'String authorization failed.'  
'No commands to process.'  
'Command not recognized: command.'  
'You don't have permission to insert users into org name.'  
'No such organization 'org name'.'  
'No default user available for organization org name.'  
'No secret key in database'.'
```

If the alias is not added successfully, the possible batch command error messages are:

```
'No arguments supplied'  
'No domain record exists for targetalias. Please add the domain first  
and then add aliases.'  
'Invalid address (reason) =>The targetAlias is not valid'  
'No user 'username'.'  
'You don't have permission to add aliases to username.'  
'Please don't alias accounts to themselves.'  
'Can't alias username; in use as an admin.'  
'targetalias cannot be assigned to username because targetalias already  
exists as a user which you are not authorized to delete.'  
'That alias aliasname already exists for that user username.'  
'Adding an alternate account (alias) cannot be performed at this time.  
This feature may be disabled for up to 14 days during system  
maintenance. Please retry in a few days. We apologize for any  
inconvenience.'  
'Differing mail hosts'
```

If merging two recently migrated users so that one address is an alias for the other user:

```
"Adding an alternate account (alias) cannot be performed at this time.  
This feature may be disabled for up to 14 days during system  
maintenance. Please retry in a few days. We apologize for any  
inconvenience."
```

Return Values

- When using the Batch Interface, if the `helpdesk@jumboinc.com` alias for `msmith@jumboinc.com` was added, this string would be returned:

```
'Added alias helpdesk@jumboinc.com to user msmith@jumboinc.com.'
```
- When used as an EZCommand, the HTTP response will contain a two-part return value: <status><message>
 - status -- 1 for success, or 0 for failure
 - message -- Contains errors and additional details

Authorization

- Read: Email Aliases
- Write: Email Aliases

Classification

Batch user management; EZCommand-enabled

Notes

- To view a user's associated aliases or to get a user's address from an alias:

```
listusers ALL, primaryqs=jim@jumboinc.com, targetOrg=100046262,  
childorgs=1, aliases=1
```

```
listusers =alias4mary@jumboinc.com, targetOrg=200046262,  
childorgs=1, aliases=1, fields=ADDRESS|PRIMARY_ADD
```

- A deactivated user can be added as an alias to another user. In the instance of an alias creation, the deactivated user's record is purged from the system. For more information about deactivated users, see "deleteuser" on page 164.
- When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: deletealias, displayuser, listusers

Related Fields

Input: address

See Also

"Building a Batch File" on page 19

"About EZCommand" on page 22

"Listing User Aliases and Primary Addresses" on page 566

The Message Security Administration Guide, "Users and Quarantines."

adddomain

The adddomain command adds a domain to your organization hierarchy.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
adddomain <org name | iid>, domain=<domain name>
```

Example

```
adddomain sales, domain=jumboinc.com  
adddomain "Jumbo's Western Region", domain=jumboinc.com
```

Description

Adds the domain record <domain name> to the organization <org name>

- <org name> -- The organization where you wish to add the domain.
 Enclose <org name> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.
- <domain name> -- The name of the domain being added.

Errors

- Add the domain before routing the DNS MX entries to the Message Security service. Otherwise the traffic will be bounced with the SMTP fatal error:

554 No relaying allowed - psmtsp.

- If extra parameters are used when calling the command, for example substrip and 'alias', this error message is returned:

Invalid parameters: 'substrip', 'alias' are not supported via batch 'adddomain'. Please use 'modifydomain'

Return Values

When using the Batch interface, if the `western.sales.jumboinc.com` domain was added to the `Sales` organization, this string would be returned:

`'Added domain western.sales.jumboinc.com to organization Sales.'`

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Classification

Batch domain and organization management

Notes

- Confirm the domain is already associated with an email config. If not, add the domain to the email config.
- A domain must be added below its associated email config organization.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: deletedomain, displaydomain, listdomains, listorgs, modifydomain, setorgsubstripping

Related Fields

- Input: domainname, orgname
- Related: alias, created_ts (for domains), domainname, iid, org (for domains), primary_did, primary_dom, substrip

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "Domains"

addorg

The addorg command adds a sub-organization to your organizational hierarchy

Syntax

addorg <org name>, parent=<parent org> [, <field>=<value>, ...]

Example

```
addorg sales, parent=execs
```

```
addorg "Jumbo's Org", parent="Jumbo, San Carlos", max_message_size=250
```

Description

Creates a new organization, <org name>, underneath the parent organization, <parent org>.

- <org name> -- The name of the sub organization being added.

Enclose <org name> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

- parent -- The new organization's parent.

Errors

When using the Administration Console Batch page and you forget a comma ',' before the 'parent=' parameter, the parent=<parent org> becomes part of the <org name> and this error will result:

```
'Please pick a parent for ''.
```

Note: If you include a read-only field with this command, the system will return an error.

Return Values

When using the Batch Interface, if the Sales organization was added under the JumboInc parent organization, this string would be returned:

```
'Created new organization Sales under organization JumboInc.'
```

Authorization

- Read: Create Organizations
- Write: Create Organizations

Classification

Batch organization management

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: deleteorg, displayorg, getorgreport, listorgs, modifyorg, org_im_settings display, org_im_settings modify, setorgsubstripping

Related Fields

- Input: orgname
- Optional field input: approved_senders (for orgs), archive, async_bounce, at_notify_on, authentication_data, blatant_spam, blatant_spam, blocked_senders (for orgs), company_name, creator, default_user, disable_first_spam, disposition_virus, message_encryption (for orgs), footer_on, iid, im_enable, im_external_enable, im_proto_enable, is_email_config, lang_locale (for orgs), lastmod_date (for orgs), max_message_size, ndr, non_account_bounce, nullsender_disposition, orgname, out_at_notify_on, outbound_max_message_size, outbound_virus, outbound_virus_disposition, parent_org, qsum_actionable, qsum_enable, qtine_redir_atq, qtine_redir_ndr, qtine_redir_out_atq, qtine_redir_out_virus, qtine_redir_spam, qtine_redir_virus, quarantine_links, quarsum_links, remotecmd_secret, spam_notify_on, support_contact, tagonly_spam, timezone (for orgs), virus_clean, virus_clean, virus_notify (for orgs), welcome_on

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “Organization Management.”

adduser

The adduser command adds users to the Message Security service.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
adduser <user address> [, <field>=<value>, ...], [org=<org name>], [welcome=<1/true | 0/ false>]
```

Example

Batch command interface examples:

- Add a user, add to the user's approved_senders list, and send out an immediate welcome notification:

```
adduser jim@jumboinc.com, approved_senders=+hugeisp.com, welcome=1
```

- If the org is not included, the command adds the user to the organization associated with the user's domain. This is the default behavior:

```
adduser msmith@jumboinc.com
```

- Adds a user to the Company Sales organization:

```
adduser msmith@jumboinc.com, org=Company Sales
```

Description

Batch Interface Description for adduser

Adds a user, <user address> to an organization.

- <user address> -- The new user's mail address.

Enclose <org name> in double quotes or preceded with a '\> symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

- <field>=<value> -- Any user field for which you have write privileges.
- org -- Explicitly specified <org name> to associate with the <user address>

Default: If no organization is specified, the organization is looked up from the domain part of the user's address and the user is placed in the domain's associated organization.

- welcome=1/true -- Sends a welcome notification immediately to the new user. This is an optional parameter.
- welcome=0/false -- Sends a welcome notification within 24 hours in the default notification batches.

Default: welcome=false

EZCommand Description for adduser

See the Batch Interface Description for adduser for general usage details.

When used as an EZCommand, the command must be URL-escaped in order to properly submitted.

Example:

```
adduser msmith@jumboinc.com
```

changes to

```
adduser%20msmith%40jumboinc.com
```

WARNING: Do not add a distribution list or a mailing list as a user account unless you have included these lists in your contracted user count. Doing so may cause you to incur additional costs. Consider adding the lists as aliases to an existing user account designed for this purpose.

Errors

- Possible batch command errors include:

```
'No such user 'username' (unknown administrator address supplied).'  
'String authorization failed.'  
'No commands to process.'  
'Command not recognized: command.'  
'You don't have permission to insert users into org name.'  
'No such organization 'org name''  
'No default user available for organization org name'  
'No secret key in database.'
```

Note: This means "no secret key" was found in the EZCommand Shared Secret. The secret code must exist in the organization in which the administrator account resides.

- If adding the user was not successful, some of the batch command errors could be:

```
'No arguments supplied'  
'Invalid address: 'username' (reason)'  
'username' clashes with an existing address or alias'  
'No domain record exists for domain. Please add the domain first  
and then add users'  
'You don't have permission to insert users into org name'  
'No such organization 'org name''  
'No default user available for organization org name'
```

- If using the Administration Console and you see an "Invalid Pattern" error message, confirm all commas are present and in the correct location.
- If you include a read-only field with this command, the system will return an error.

Return Values

- When using the Batch Interface, if `msmith@jumboinc.com` was added to the Finance organization, this string would be returned:

'Created new user msmith@jumboinc.com in organization Finance.'

- When used as an EZCommand, the HTTP response will contain a two-part return value: <status><message>
 - status -- 1 for success or 0 for failure
 - message -- Contains errors and additional details

Authorization

- Read: Add Users
- Write: Add Users

Classification

Batch user management; EZCommand-enabled

Notes

- The user's email account must be set up on your email server.
- The user's domain must be added to the Message Security service.
- A user's name must be unique and can contain any ASCII character except: <>()\';:@ "#='', which must be either in double quotes or preceded by a '\' symbol.
- Users must be added to your hierarchy below the email config mapped to the user's email server.
- Notification files (your welcome notification) are limited to 500 KB.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: deleteuser, displayuser, listusers, modifyuser, resetuser, suspenduser

Related Fields

Input: address

Related: active, address, approved_senders (for users), approved_recipients, blocked_senders (for users), message_encrypt (for users), message_encrypt (for users), filter_adult, filter_bulk, filter_getrich, filter_offers, filter_racial, initial_password, junkmail_filter, lang_locale (for users), message_count, message_limit, message_limited, notice_address, orgid, password, timezone (for users), timezone (for users), user_id, virus_notify (for users), virus_state, weblocked, welcome_count, wireless_state

See Also

“Building a Batch File” on page 19

“About EZCommand” on page 22

“Editing Message Archiving Settings” on page 564

“Resending the Welcome Notification” on page 548

The Message Security Administration Guide, “Users and Quarantines”

archive_settings display

The archive_settings display command displays the archive settings for an organization. This command applies to Postini Message Archiving, which is only used with Message Security installations.

Syntax

```
archive_settings display org=<org name>
```

Example

```
archive_settings display org="Jumbo's ABC, Santa Clara"
```

Description

Displays the archives' settings for an organization.

Enclose <org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Errors

Some of the possible errors include:

If your archive feature is not enabled, this error message is returned:

```
archive_settings display error: select * from archive_configs where  
iid=<iid name>; no rows selected
```

Note: In the Administration Console's go to the Archive settings page for your organization to configure this organization's archive functionality.

Return Values

If the Sales organization had archiving enabled, in the Administration Console this command would return:

```
Message Archiving Settings for Sales:  
Archive Enable: on  
Mail Flow: on  
Journaling: off  
Archive Retention Months:12
```

Authorization

- Read: Advanced Applications/Message Archiving
- Write: Advanced Applications/Message Archiving

Classification

Batch Message Archiving

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: archive_settings modify, displayorg, org_im_settings display, org_im_settings modify

Related Fields

- Input: orgname
- Related: archive, archive_enable, custom_journal, retention_months, standard_journal

See Also

“Building a Batch File” on page 19

“Editing Message Archiving Settings” on page 564

Postini Message Archiving Administration Guide

archive_settings modify

The archive_settings modify command edits the archive settings for an organization. This command applies to Postini Message Archiving, which is only used with Message Security installations.

Syntax

```
archive_settings modify org=<org name>, archive_enable=<on | off>,
mail_flow=<on | off>, journaling=<on | off>
```

Example

```
archive_settings modify org=Jumbo ABC, archive_enable=on,
mail_flow=on, journaling=on
```

Description

Archive settings can only be made on a user org (not account or email config orgs).

- org -- The name of the organization associated with this archive. Enclose <org name> in double quotes or preceded with a '\> symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols. In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.
- archive_enable -- Turns archiving on or off for this organization. This field must be enabled for mail_flow and journaling to be modified.
- mail_flow -- If archive_enable is on, this turns on or off inbound and outbound archiving.
- journaling -- If archive_enable is on, this enables the archiving of journaled messages. Also, If you choose the journaling option, you must also set up journaling on your mail server.

Note: When archiving is enabled, mail_flow and/or journaling must be on. If you use both inbound/outbound and journal archiving, Message Archiving stores two copies of each inbound and outbound message.

Return Values

If the Sales organization's archive settings was modified in the Administration Console, the command would return:

```
Archive settings successfully updated for 'Sales'.
```

Authorization

- Read: Advanced Applications, Message Archiving
- Write: Advanced Applications, Message Archiving

Classification

Batch organization management, Message Archiving

Related Commands

Batch Commands: archive_settings display

Related Fields

- Input: orgname
- Related: archive, archive_enable, custom_journal, retention_months, standard_journal

See Also

“Building a Batch File” on page 19

“Editing Message Archiving Settings” on page 564

Postini Message Archiving Administration Guide

blockprovuser

The blockprovuser command sets a provisional user as permanently blocked from being added to the Message Security service. This occurs when using the SmartCreate user management feature.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

blockprovuser <user address>

Example

```
blockprovuser john@jumboinc.com
```

Description

Blocks the provisional user from being added to the org.

Note: Enclose <user address> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Authorization

- Read: Delete Users
- Write: Delete Users

Classification

Batch user management

Notes

- Do this for users you don't want to provide Message Security for, or for a user who has left your company but continues to receive email.
- Used with SmartCreate, newly added users are unconfirmed provisional users. These users are promoted to regular user after verified as associated with someone in your org by receiving 3 legitimate emails within a week. Or the user can be blocked or unblocked from being added to the Message Security service. Once the email criteria is met, the user is added to service. Otherwise the user is deleted.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `deleteprovuser`, `displayprovuser`, `listprovusers`, `promoteprovuser`, `unblockprovuser`

Related Fields

Input: address

See Also

[“Building a Batch File” on page 19](#)

[“Editing Your Mail Handling Policies \(Non Account Bounce\)” on page 562](#)

[*The Message Security Administration Guide*, “Users and Quarantines”](#)

checklatency

The `checklatency` command measures the connection delay between the email data center and your email server. This is the Latency Test.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
checklatency <email config org>, mailhost=<mail server>
```

Example

```
checklatency sales email config, mailhost=my.mailserver.com
```

Description

Measures the time to open the SMTP connection with the target email server, <mail server>.

- <email config org> = Name of the email config containing the mailhost
Enclose <email config org> in double quotes or preceded with a '\> symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.
- mailhost = The name of the mail server to check

Errors

If the server you are attempting to test does not have DNS entries, this error is returned. The example is for mailhost mail14.jumboinc.com:

```
Error - unknown host mail14.jumboinc.com
```

Return Values

If checking the connection delay of the sales email config's mailhost (for example inbound.mail.jumboinc.com), the command returns:

```
Connection to inbound.mail.jumboinc.com took 15.0392208099365 seconds
```

Authorization

- Read: Organization Management
- Write: Read-only for administrators

Classification

Batch system testing

Notes

- Use the Latency Test if you want to see how well the network is responding. The test results are relative and must be compared to normal test results when your system is experiencing similar traffic. As a rule, the lower the latency the better. But increased network latency alone is not a sign of email trouble in the Message Security service.
- Use the **checkroute** command, Traceroute Test, to narrow the possible cause of slow latency.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `checkroute`, `testfirewall`, `testmail`, `testmx`

Related Fields

- Input: `orgname`
- Related: `is_email_config`

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "Test Tools & Mail Flow Troubleshooting."

checkroute

The `checkroute` command, or Traceroute Test, traces the network route from the Message Security server to the input mail server.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

`checkroute <email config org>, mailhost=<mail server | IP address>`

Example

```
checkroute salesemailconfig, mailhost=mailserver.jumboinc.com
```

Description

Traces the connection from the server to the input mail server, <mail server>. A common traceroute test traces the network hops between the Message Security service and your server.

- <email config org> -- Name of the email config containing the mailhost
Enclose <email config org> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.
- <mail server | IP address> -- The name of the mailhost to check

Errors

If a * character is listed in place of a time, the test failed. This failure may be due to some hops not accepting traceroutes.

Return Values

The results show each network hop per line. Each hop will be tested 3 times and these are shown in the results.

```
traceroute to mailserver.jumboinc.com
1 carl-39 (64.18.7.234) 0.335 ms 0.324 ms 0.367 ms
2 exoduscorp-rtr-f0-1 (10.1.252.158) 0.490 ms 0.354 ms 0.243 ms
3 172.31.0.9 (172.31.0.9) 1.241 ms 1.729 ms 1.243 ms
4 64.18.7.254 (64.18.7.254) 1.242 ms 1.232 ms 1.244 ms
5 inbound (64.18.7.231) 1.743 ms 1.729 ms 2.243 ms
traceroute complete
```

Authorization

- Read: Organization Management
- Write: Read-only for administrators

Classification

Batch system testing

Notes

- When a firewall blocks a traceroute test, this may take a few minutes.
- Some service providers prevent traceroutes.
- Traceroute tests to your email server are only helpful when paired with the traceroute results from your email server to the Message Security service.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related commands

Batch Commands: checklatency, testfirewall, testmail, testmx

Related Fields

- Input: orgname
- Related: is_email_config

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "Test Tools & Mail Flow Troubleshooting."

deletealias

The deletealias command removes a user's alias completely from the Message Security service.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

deletealias <alias>

Example

```
deletealias myalias@jumboinc.com
```

Description

Batch Interface Description for deletealias

Deletes the alias address, <alias>.

- <alias> -- The user alias being deleted.

Enclose <alias> in double quotes or preceded with a '\ symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

EZCommand Description for deletealias

See the Batch Interface Description for deletealias for general usage details.

When used as an EZCommand, the command must be URL-escaped in order to properly submitted.

Example:

```
deletealias myalias@jumboinc.com
```

changes to

```
deletealias%20myalias%40jumboinc.com
```

Errors

- Possible batch command error messages include:

```
'No such user 'username' (unknown administrator address supplied).'  
'String authorization failed.'  
'No commands to process.'  
'Command not recognized: command.'  
'You don't have permission to insert users into org name.'  
'No such organization 'org name'.'  
'No default user available for organization org name.'  
'No secret key in database.'
```

Note: This means "no secret key" found in the organization's EZCommand Shared Secret. The secret code must exist in the organization in which the administrator account resides.

- If the alias was not deleted successfully, possible batch command errors include:

```
'No arguments supplied.'  
'No such alias 'targetalias'.'  
'You don't have permission to delete aliases from username.'
```

Return Values

- Batch command interface return values:
 - If the `helpdesk@jumboinc.com` user alias was deleted, this string is returned:

```
' Deleted alias helpdesk@jumboinc.com from user
msmith@jumboinc.com.'
```
 - When used as an EZCommand, the HTTP response will contain a two-part return value: <status><message>
 - status -- 1 for success or 0 for failure
 - message -- Contains errors and additional details

Authorization

- Read: Email Aliases
- Write: Email Aliases

Classification

Batch user management; EZCommand-enabled

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: addalias, displayuser, listusers

Related Fields

Input: address

See Also

"Building a Batch File" on page 19

"About EZCommand" on page 22

deletedomain

The deletedomain command removes the domain from your organizational hierarchy.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
deletedomain <domain name | domain id>
```

Example

```
deletedomain jumboinc.com
```

Description

Deletes the domain record, <domain name>, from the Message Security service.

- <domain name> -- The domain being deleted.

Return Values

When using the Batch interface, if the `western.sales.jumboinc.com` domain was deleted, this string is returned:

```
'Deleted domain western.sales.jumboinc.com from organization Sales.'
```

Authorization

- Read: Edit Organization
- Write: Edit Organization

Classification

Batch Domain management

Notes

- Remove all users in this domain before removing the domain.
- Edit the domain's DNS MX entries to the Message Security service.
- To move a domain, see the **modifydomain** command.

Related Commands

Batch Commands: adddomain displaydomain, listdomains modifydomain, setorgsubstripping

Related Fields

Input: domainname, alias

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "Domains"

deleteorg

The deleteorg command removes an organization from the Message Security service.

Syntax

deleteorg <org name | iid>

Example

deleteorg "Jumbo's Western Region"

Description

Deletes the organization identified by the <org name>.

- <org name> -- The organization being deleted.

Enclose <org name> in double quotes or preceded with a '\> symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

Errors

If you have tried to delete an organization with existing user records, you will get this error message:

<Org name> has users which must be deleted before it can be.

Return Values

When using the Batch interface, if the Sales organization was deleted, this string is returned:

'Deleted organization Sales.'

Authorization

- Read: Delete Organizations
- Write: Delete Organizations

Classification

Batch org management

Notes

- The organization must not have any sub-organizations
- The organization must not have any users or domains
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: addorg, displayorg, getorgreport, listorgs, modifyorg, org_im_settings display, org_im_settings modify, setorgsubstripping

Related Fields

Input: orgname, iid

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “Organization Management”

deleteprovuser

The deleteprovuser command removes a provisional user that is known to be illegitimate. It won’t appear on your bill.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

deleteprovuser <user address>

Example

```
deleteprovuser john@jumboinc.com
```

Description

Removes the provisional user’s, <user address>, records from the Message Security service.

Note: Enclose <user address> in double quotes or preceded with a ‘` symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols

Authorization

- Read: Delete Users
- Write: Delete Users

Classification

Batch user management

Notes

- Used with SmartCreate, newly added users are unconfirmed provisional users. These users are promoted to a regular user after verified as associated with someone in your org by receiving 3 legitimate emails with a week. Once this criteria is met, the user is added to service. Otherwise the user is deleted.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `blockprovuser`, `displayprovuser`, `listprovusers`, `promoteprovuser`, `unblockprovuser`

Related Fields

Input: address

See Also

[“Building a Batch File” on page 19](#)

[“Editing Your Mail Handling Policies \(Non Account Bounce\)” on page 562](#)

[*The Message Security Administration Guide*, “Users and Quarantines”](#)

deleteuser

The `deleteuser` command removes users from the Message Security service.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
deleteuser <user address | u_id> [ , deactivate] [ , purge] [ , confirm ]
```

Example

```
deleteuser msmith@jumboinc.com
```

If the user being deleted is an administrator, use confirm:

```
deleteuser admin@jumboinc.com, confirm
```

Description

Batch Interface Description for deleteuser

Deletes a user record, <user address> from the Message Security service.

- <user address> -- The name of the user being deleted.

Enclose <user address> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

- deactivate -- The user record is deactivated until the day after the user’s quarantine period has expired. At this point, the user record is purged from the system.
 - To purge a deactivated user, the user must first be added to the system using the command “**adduser**” on page 144, and then purged from the system.
 - When a deactivated user is added to the system, a welcome message is not sent. The user must be purged and then added to the system for a welcome message to be sent.

This can either be done by using the **adduser** command followed by the **deleteuser** command using the purge parameter, or by waiting for the deactivated user’s quarantine period to expire and the automatic purging of the user record.

- When a deactivated user is added to the system, the user’s settings and quarantine are restored. A deactivated user can be added to any user organization in the account.
- A deactivated user can be added as an alias to another user. In the instance of an alias creation, the deactivated user’s record is purged from the system. For more information about user alias creation, see “**addalias**” on page 137.
- A deactivated user is not in the total number of users shown for an organization.
- purge -- The user record is deleted from the system.
- confirm -- A positional parameter which is required if the user being deleted is an administrator. The text `confirm` must be at the end of the command. There is no numeric equivalent.

EZCommand Description for deleteuser

See the Batch Interface Description for **deleteuser** for general usage details.

When used as an EZCommand, the command must be URL-escaped in order to properly submitted.

Example:

```
deleteuser msmith@jumboinc.com
```

changes to

```
deleteuser%20msmith%40jumboinc.com
```

Errors

- Possible batch command errors include:

```
'No such user 'username' (unknown administrator address supplied).'  
'String authorization failed.'  
'No commands to process.'  
'Command not recognized: command.'  
'You don't have permission to insert users into org name.'  
'No such organization 'org name'.'  
'No default user available for organization org name.'  
'No secret key in database'.'
```

Note: This means “no secret key” found in the organization’s EZCommand Shared Secret. The secret code must exist in the organization in which the administrator account resides.

- If deleting the user was not successful, possible batch command errors include:

```
'No arguments supplied.'  
'No user username.'  
'You don't have permission to delete username.'  
'Please don't go.'
```

“Please don’t go” means the administrator tried to delete her own account.

Return Values

- When using the Batch Interface, if `msmith@jumboinc.com` was deleted, this string is returned:

```
'Deleted user msmith@jumboinc.com.'
```

- When used as an EZCommand, the HTTP response will contain a two-part return value: <status><message>
 - status -- 1 for success or 0 for failure
 - message -- Contains errors and additional details

Authorization

- Read: Delete Users
- Write: Delete Users

Classification

Batch user management; EZCommand-enabled

Notes

- When using the batch commandline interface, remove an administrator's record before removing the administrator's user record. See the `confirm` parameter above.
- If removing a Default User, first remove the user from all associated organizations.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `adduser`, `displayuser`, `listusers`, `modifyuser`, `resetuser`, `suspenduser`

Related Fields

Input: `address`, `user_id`

See Also

"Building a Batch File" on page 19

"About EZCommand" on page 22

"Resending the Welcome Notification" on page 548

The Message Security Administration Guide, "Users and Quarantines"

displaydomain

The `displaydomain` command displays all of the selected domain's settings information.

Syntax

`displaydomain <domain name | domain id>`

Example

```
displaydomain jumboinc.com
```

Description

Displays the domain settings for the <domain name>

<domain name> -- The domain being displayed.

Return Values

For Batch command interface, these values are returned:

- If the hugeisp.com domain is associated with the sales organization, stripping is off, and hugeisp.com is a domain alias for the jumboinc.com domain, these comma delimited field-value strings are returned:

```
org sales,  
substrip 0,  
aliasedto jumboinc.com,  
domainid 900000811  
domainname hugeisp.com
```

- If the jumboinc.com domain is associated with the sales organization, stripping is off, and jumboinc.com has two aliases (hugeisp.com, jumboincwest.com), these comma delimited field-value strings are returned:

```
org sales,  
substrip 0,  
aliasedfrom "jumbo.com, jumboincwest.com",  
domainid 900000811  
domainname jumboinc.com
```

Authorization

- Read: Organization Management
- Write: Organization Management

Classification

Batch domain management

Related Commands

Batch Commands: adddomain, deletedomain, listdomains, modifydomain, setorgstripping

Related Fields

- Input: domainid, domainname
- Output: alias, aliasedfrom, aliasedto, org (orgname), substrip
- Related: domainid, domainname, iid, primary_did

See Also

“Building a Batch File” on page 19

“Message Center Settings and Password Examples” on page 536

The Message Security Administration Guide, “Domains”

displayorg

The displayorg command displays all the selected organization’s settings information.

Syntax

displayorg <org name | org's iid>

Example

```
displayorg "Jumbo's Western Region"
```

Description

Displays all of the settings information of either the <org name> string.

- <org name> -- The organization being displayed.

Enclose <org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Return Values

Below is a Batch command example of the returned comma delimited field-value string pairs with example values. This list has been alphabetized for reading convenience.

```

antivirus_sensitivity 0 (normal),
approved_senders empty,
archive 1 (on),
async_bounce NULL (),
at_notify_on NULL (),
authentication_data NULL,
authentication_type 1 (PMP),
autocreate_web 0 (off),
blatant_spam ERROR 571 Message Refused,
blocked_senders empty,
bounce_fragments NULL (),
company_name Jumbo Inc,
creator 200122328 (msmith@jumboinc.com),
create_method 2,
created_date 1145975006
default_message_limit NULL,
default_user 20012277 (pdefault@jumboinc.com),
disable_first_spam 0 (on),
disposition_virus h (blackhole)
message_encryption NULL (),
footer_on 0 (off),
iid 100001012,
im_enable NULL (),
im_external_enable NULL (),
im_proto_enable +all, +aim, +msn, +yahoo, +google,
is_email_config undef,
lang_locale NULL,
lastmod_date 11445962000,
max_message_size NULL (200M),
message_encryption NULL (),
message_encryption_criteria NULL,
ndr NULL (),
non_account_bounce 1 (on),
non_account_virus_scan NULL (),
nullsender_disposition NULL,
orgname sales,
out_at_notify_on NULL (),
outbound_max_message_size NULL (200M),
outbound_virus 0 (off),
outbound_virus_disposition 1 (bounce),
parent_org 100001011 (jumbo inc email config),
qsum_actionable basic delivery,
qsum_enable on,
qtine_redir_atq NULL (none),
qtine_redir_ndr NULL (none),
qtine_redir_spam NULL (none),
qtine_redir_virus NULL (none),
qtine_redir_out_atq NULL (none),
qtine_redir_out_virus NULL (none),
quarantine_links 1 (on),
quarsum_links 1 (on),
nullsender_disposition blackhole,
remotecmd_secret swordfish,
spam_notify_on 1 (on),
support_contact customeradmin@jumboinc.com,
tagonly_spam NULL (),
timezone America/Los Angeles ((GMT-08:00) Pacific Time (US & Canada));
Tijuana),
tls_notify_admin NULL (none),
tls_notify_on 0

```

```
virus_clean 1 (on),  
virus_notify 0 (Immediately),  
welcome_on 1 (on)  
zero_hour_notify_on 0 (off)  
zero_hour_scan 0 (off)
```

Authorization

- Read: Organization Management
- Write: Organization Management

Classification

Batch organization management

Notes

- Child organization settings are not displayed.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.
- The TLS, archiving, and encryption fields are only used with Message Security installations.

Related Commands

Batch Commands: addorg, deleteorg, getorgreport, listorgs, modifyorg, org_im_settings display, org_im_settings modify, setorgsubstripping

Related Fields

- Input: orgname, iid
- Output: antivirus_sensitivity, approved_senders (for orgs), archive, async_bounce, at_notify_on, authentication_data, authentication_type, blatant_spam, blatant_spam, blocked_senders (for orgs), bounce_fragments, company_name, create_method (for orgs), created_date, creator, default_message_limit, default_user, disable_first_spam, disposition_virus, message_encryption (for orgs), footer_on, iid, im_enable, im_external_enable, im_proto_enable, is_email_config, lang_locale (for orgs), lastmod_date (for orgs), max_message_size, ndr, non_account_bounce, non_account_virus_scan, nullsender_disposition, nullsender_headertag_validation, orgname, out_at_notify_on, outbound_max_message_size, outbound_virus, outbound_virus_disposition,

parent_org, qsum_actionable, qsum_enable, qtine_redir_atq, qtine_redir_ndr, qtine_redir_out_atq, qtine_redir_out_virus, qtine_redir_spam, qtine_redir_virus, quarantine_links, quarsum_links, remotecmd_secret, spam_notify_on, support_contact, tagonly_spam, timezone (for orgs), tls_notify_admin, tls_notify_on, virus_clean, virus_notify (for orgs), welcome_on

See Also

- “Building a Batch File” on page 19
 - “Message Center Settings and Password Examples” on page 536
 - “Resetting Users” on page 553
 - “Viewing Your Organization’s Sender Lists” on page 554
 - “Viewing Message Center Settings” on page 536
 - “Seeing if a User Has Received a Welcome Notification” on page 547
 - “Viewing Your Organization’s Sender Lists” on page 554
 - “Viewing Authentication and Password Settings” on page 540
 - “Viewing Quarantine Summary Notification Settings” on page 544
 - “Editing Message Center Access and Settings” on page 538
 - “Seeing if a User Has Received a Welcome Notification” on page 547
 - “Setting a Virus Notification Interval” on page 549
- The Message Security Administration Guide*, “Organization Management”

displayprovuser

The displayprovuser command shows the active list of provisional users.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

displayprovuser <email address>

Example

```
displayprovuser john@jumboinc.com
```

Description

Displays a provisional user address and the last time an email was received. The time is in UNIX seconds.

Enclose <user address> in double quotes or preceded with a '\> symbol if it contains a quote ('), double quote (""), backslash (\), apostrophe, commas, #, = symbols

Return Values

Using the Administration Console syntax:

```
ProvUser: john@jumboinc.com
Org: 100048729
TS1: 1141420639
TS3: 1141429660
```

The numbers following the return values are time stamps.

Authorization

- Read: Add Users
- Write: Read-only for administrators

Classification

Batch user management

Notes

- Used with SmartCreate, newly added users are unconfirmed provisional users. These users are promoted to regular user after verified as associated with someone in your org by receiving 3 legitimate emails with a week. Once this criteria is met, the user is added to service. Otherwise the user is deleted.
- When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: blockprovuser, deleteprovuser, listprovusers, promoteprovuser, unblockprovuser

Related Fields

- Input: address
- Output: iid, TS1, TS3

See Also

“Building a Batch File” on page 19

“Editing Your Mail Handling Policies (Non Account Bounce)” on page 562

The Message Security Administration Guide, “Users and Quarantines”

displayspool

The displayspool command shows the Spool Manager settings for your email config organization.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
displayspool <email config org>
```

Example

```
displayspool jumboemailconfig
```

Description

Displays Spool Manager settings for the email config organization, the <email config org >.

- < email config org name> -- The email config organization whose spool settings are being displayed.

Enclose <org name> in double quotes or preceded with a '\> symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

Errors

- When there is a failed connection during the spool delay period, mail is deferred with the SMTP error 451 Can't connect to yourdomain.com - psmtplib. According to SMTP protocol, mail will defer for 56 days before bouncing back to the sender.
- If the number of messages exceed your spool allocation, spooling stops, and incoming messages are returned with the error: 451 Can't connect to yourdomain.com - psmtplib. This is a 400-series error, so the sending server should defer and retry sending the message for 5 full days, according to the RFCs for SMTP.
- If calling **displayspool** against a non email config organization (ex: sales), you will get this error:

```
"Org 'sales' is not an email server configuration, ()"
```

Return Values

When using the Batch interface, if displaying the spool information for the jumboemailconfig organization, these comma delimited field-value strings are returned:

```
auto_unspool 0,
despool_max_connections 5,
duration 1145965599,
org jumboemailconfig,
quota 5242880, (In Administration Console shown in MB)
spool_delay 900,
spool_mech Suspend,
status Suspended,
used_pct 0,
used_size 0
```

Authorization

- Read: Spooling
- Write: Spooling

Classification

Batch spool management

Notes

- If within one minute three connection attempts to your mail server fail, Spool Manager starts the spool delay period which is 15 minutes by default.
 - During the spool delay period, Spool Manager will begin to spool your mail. If there's a successful connection during this period, the Spool Manager returns to monitoring connections to your mail server. The spooling will continue until the spool is full, until you suspend the spooling, or until spooling automatically unspools.
 - Spooling will not be triggered if there is not enough mail flow to your server. The minimum mail flow for spooling is about three messages per minute.
 - Messages that successfully passed the junk email filters, virus scanning, and mail policies are spooled. Junk mail and virus-infected messages are not spooled. They are quarantined. Blocked messages are not spooled.
- Note:** It is highly recommended that you set up alerts to notify you of spooling activity. Be sure your Spool Manager alerts are configured to send the notification to an account on your wireless device and not your email account as these will be spooled.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Command: modifyorg

Related Fields

- Input: orgname
- Output: auto_unspool, despoo_max_connections, duration, org (for spooling), quota, spool_delay, spool_mech, status, used_pct, used_size
- Related: is_email_config

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "Spool Manager" and "Administrator Alerts"

displayuser

The displayuser command shows all the user's settings information.

Syntax

```
displayuser <user address | user_id>
```

Example

```
displayuser msmith@jumboinc.com
```

Description

Displays information on user settings either by the <user address>.

- <user address> -- The user whose settings are being displayed.

Enclose <user address> in double quotes or preceded with a '\' symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols

Return Values

The Batch interface returns these comma delimited field-value strings. This list has been alphabetized for reading convenience.

```
active 1 (yes),
address msmith@jumboinc.com,
approved_recipients empty,
approved_senders empty,
blocked_senders empty,
create_method 0,
created_date 1145962000,
filter_adult 15 (aggressive),
filter_bulk 15 (aggressive),
filter_getrich 15 (aggressive),
filter_offers 15 (aggressive),
filter_racial 15 (aggressive),
initial_password flipbolt,
junkmail_filter 1 (on),
lang_locale NULL,
lastmod_date 1145962000,
message_encryption NULL (),
message_limit NULL,
message_limited 0 (no),
message_count 0,
notice_address NULL,
orgid 100001012' (sales),
password 5d000000,
```

```
timezone NULL,  
user_id 202846402,  
virus_notify NULL (),  
virus_state 0 (on),  
weblocked 0 (no),  
welcome_count 1,  
wireless_state 1 (off)
```

Authorization

- Read: User Settings
- Write: User Settings

Classification

Batch user management

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: adduser, deleteuser, listusers, modifyuser, resetuser, suspenduser

Related Fields

- Input: address, user_id
- Output: active, address, approved_senders (for users), approved_recipients, blocked_senders (for users), create_method (for users), created_date (for users), message_encrypt (for users), filter_adult, filter_bulk, filter_getrich, filter_offers, filter_racial, initial_password, junkmail_filter, lang_locale (for users), lastmod_date (for users), message_count, message_limit, message_limited, notice_address, orgid, password, timezone (for users), user_id, virus_notify (for users), virus_state, weblocked, welcome_count, wireless_state

See Also

"Building a Batch File" on page 19

“Message Center Settings and Password Examples” on page 536

“Viewing Your Organization’s Sender Lists” on page 554

“Viewing Message Center Settings” on page 536

“Viewing Authentication and Password Settings” on page 540

“Editing a PMP Password” on page 541

“Seeing if a User Has Received a Welcome Notification” on page 547

“Resending the Welcome Notification” on page 548

The Message Security Administration Guide, “Users and Quarantines”

domain_tls add

The domain_tls add command adds Postini Policy-Enforced TLS, used with Message Security installations, to organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
domain_tls add org=<email config orgtag | ID>,
```

```
hop=<ib_sender | ob_recipient>,
```

```
domain=<domain name>
```

Example

```
domain_tls add org=Salesemailconfig, hop=ib_sender,  
domain=jumboinc.com
```

Description

Adds Policy-Enforced TLS for orgs that need to identify domains that need inbound or outbound message traffic (ib_sender or ob_recipient) to be sent via a Transport Layer Security (TLS) connection. This command is run at the email config-level.

- orgtag -- Org name or ID of an existing email config organization enabled for Policy Enforced TLS
- hop -- Conversation segment between the Message Security service and a recipient or sender
 - ib_sender -- Inbound sender to the Message Security service
 - ob_recipient -- Outbound message traffic from the Message Security service to the recipient.
- domain -- The domain name requiring message traffic to be sent via a TLS connection.

Errors

You do not have the proper authorization to perform domain tls operations.

Return Values

The Administration Console return text for this example,

```
domain_tls add org=Salesemailconfig, hop=ib_sender,  
domain=jumboinc.com
```

would be:

```
Added tls domain jumboinc.com to Salesemailconfig
```

Authorization

- Read: Organization Management
- Write: Organization Management, Inbound Transport Security if using inbound or Outbound Transport Security if using outbound.

Classification

Batch domain and Policy-Enforced TLS

Related Commands

Batch Commands: domain_tls delete, domain_tls display, domain_tls modify

Related Fields

message_encryption (for orgs)

See Also

“Building a Batch File” on page 19

Postini Encryption Services Administration Guide, “Policy Enforced TLS”

domain_tls delete

The domain_tls delete command deletes the organization’s Policy-Enforced TLS settings which identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. Postini Policy-Enforced TLS is only used with Message Security installations.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
domain_tls delete org=<email config orgtag | ID>,
hop=<ib_sender | ob_recipient>,
domain=<domain name>
```

Example

```
domain_tls delete org=Salesemailconfig, hop=ib_sender,
domain=jumboinc.com
```

Description

Deletes an organization's Policy-Enforced TLS settings. This command is run at the email config-level.

- orgtag -- Org name or ID of an existing email config organization enabled for Policy-Enforced TLS
- hop -- Conversation segment between the Message Security service and a recipient or sender
 - ib_sender -- Inbound sender to the Message Security service
 - ob_recipient -- Outbound message traffic from the Message Security service to the recipient.
- domain -- The domain name requiring message traffic to be sent via a TLS connection

Errors

Possible error messages include:

You do not have the proper authorization to perform domain tls operations.

Return Values

The Administration Console return text for this example,

```
domain_tls delete org=Salesemalconfig, hop=ib_sender,  
domain=jumboinc.com
```

would be:

```
Deleted tls domain jumboinc.com from Salesemalconfig
```

Authorization

- Read: Organization Management
- Write: Organization Management, Inbound Transport Security if using inbound or Outbound Transport Security if using outbound.

Classification

Batch domain and Policy-Enforced TLS

Related Commands

Batch Commands: domain_tls add, domain_tls display, domain_tls modify

Related Fields

message_encryption (for orgs)

See Also

“Building a Batch File” on page 19

Postini Encryption Services Administration Guide, “Policy Enforced TLS”

domain_tls display

The domain_tls display command displays Policy-Enforced TLS settings for organizations which need to identify domain names that require inbound and outbound message traffic to be sent via a TLS connection. Postini Policy-Enforced TLS is only used with Message Security installations.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
domain_tls display org=<email config orgtag | ID>,  
hop=<ib_sender | ob_recipient>
```

Example

```
domain_tls display org=Salesemailconfig, hop=ib_sender
```

Description

Displays an organization's Transport Layer Security (TLS) settings. This command is run at the email config-level.

- orgtag -- Org name or ID of an existing email config organization enabled for Policy-Enforced TLS
- hop -- Conversation segment between the Message Security service and a recipient or sender
 - ib_sender -- Inbound sender to the Message Security service
 - ob_recipient -- Outbound message traffic from the Message Security service to the recipient.
- domain -- The domain name requiring message traffic to be sent via a TLS connection.

Errors

Possible error messages include:

You do not have the proper authorization to perform domain tls operations.

Return Values

The Administration Console return text for this example,

```
domain_tls display org=Salesemailconfig, hop=ib_sender
```

would be the organization and the time of the last failure alert in the user's local time settings. If return value includes never, no failure alerts have been set for the domain:

```
Inbound domain tls for organization Salesemailconfig.jumboinc.com  
domain, when added, last_failure_alert jumboinc.com, Tuesday, August  
21, 2007 11:19:04 AM PDT, never
```

If the domain had a failure alert, the return text would be:

```
Inbound domain tls for organization Salesemailconfig.jumboinc.com  
domain, when added, last_failure_alert jumboinc.com, Tuesday, August  
21, 2007 11:19:04 AM PDT, August 21, 2007 2:28:46 AM PDT
```

The outbound returns the domain name, the cert_validation setting, and the last modified date.

Authorization

- Read: Organization Management, Inbound Transport Security if using inbound or Outbound Transport Security if using outbound.
- Write: Organization Management

Classification

Batch domain and Policy-Enforced TLS

Related Commands

Batch Commands: domain_tls add, domain_tls delete, domain_tls modify

Related Fields

message_encryption (for orgs)

See Also

“Building a Batch File” on page 19

Postini Encryption Services Administration Guide, “Policy Enforced TLS”

domain_tls modify

The domain_tls modify command edits settings for the Postini Policy-Enforced TLS, which is only used with Message Security installations.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
domain_tls modify org=<email config orgtag | ID>,
hop=<ib_sender>, domain=<domain name> | _default,
<cert_validation=<encrypt | verify | trust | domain>
```

Example

```
domain_tls modify org=Salesemailconfig, hop=ib_sender,  
domain=_default, cert_validation=verify
```

Description

Edits Policy-Enforced TLS for organizations. This command is run at the email config-level.

- orgtag -- Org name or ID of an existing email config organization enabled for Policy-Enforced TLS
 - hop -- Conversation segment between the Message Security service and a recipient or sender
 - ib_sender -- Inbound sender to the Message Security service
- Note:** The ob_recipient hop which is the outbound message traffic from the Message Security service to the recipient, is not valid in this release.
- 'domain=<domain name>'-- The domain name requiring message traffic to be sent via a TLS connection
 - 'domain=_default' -- The default cert_validation value for this organization. This is used when adding new domains to an organization that do not have a default certification value.
 - cert_validation -- Certification type validation.

Default: Encryption Only

Errors

Possible error messages include:

You do not have the proper authorization to perform domain tls operations.

Authorization

- Read: Organization Management
- Write: Organization Management, Inbound Transport Security if using inbound or Outbound Transport Security if using outbound.

Classification

Batch domain and Policy-Enforced TLS

Related Commands

Batch Commands: domain_tls add, domain_tls delete, domain_tls display

Related Fields

Input: orgname, domainname

See Also

“Building a Batch File” on page 19

Postini Encryption Services Administration Guide, “Policy Enforced TLS”

encryption display_org

The encryption display_org command displays an organization’s encryption information. This command applies to Postini Message Encryption, which is only used with Message Security installations.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

encryption display_org, orgtag=<org name>

Example

```
encryption display_org, orgtag=Sales
```

Description

Displays the encryption information for an organization.

Enclose <org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols

Return Values

```
ext_encrypt_criteria  
out_tls_flags
```

```
ext_encrypt
route_id
out_tls_source_flags
out_tls_recipient_flags
in_tls_flags
```

Authorization

- Read: Message Encryption Management, Outbound Message Encryption
- Write: Message Encryption Management, Outbound Message Encryption

Classification

Batch organization management

Notes

The ext_encrypt_criteria and ext_encrypt are the message_encryption (for orgs), message_encryption_criteria fields.

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: encryption display_user, encryption list_users, encryption modify_org, encryption modify_user

Related Fields

Input: orgname

See Also

“Building a Batch File” on page 19

Postini Encryption Services Administration Guide

encryption display_user

The encryption display_user command displays user specific encryption information. This command applies to Postini Message Encryption, which is only used with Message Security installations.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
encryption display_user, address=<user address>
```

Example

```
encryption display_user, address=msmith@jumboinc.com
```

Description

Displays the encryption information for a specified user.

Enclose <user address> in double quotes or preceded with a '\ symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols

Return Values

```
ext_encrypt_criteria  
out_tls_flags  
route_id  
out_tls_source_flags  
out_tls_recipient_flags  
in_tls_flags
```

Authorization

- Read: Message Encryption Management, Outbound Message Encryption
- Write: Message Encryption Management, Outbound Message Encryption

Classification

Batch user management

Notes

- The ext_encrypt_criteria and ext_encrypt are the message_encryption (for orgs), message_encryption_criteria fields.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: encryption display_org, encryption list_users, encryption modify_org, encryption modify_user

Related Fields

Input: address

See Also

"Building a Batch File" on page 19

Postini Encryption Services Administration Guide

encryption list_users

The encryption list_users command lists all encryption users in this organization. This command applies to Postini Message Encryption, an optional product.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

encryption list_users, orgtag=<org name>, [ext_encrypt=<on | off | match>]

Example

```
encryption list_users, orgtag=Sales, ext_encrypt=on
```

Description

Lists all encryption users in this organization.

Enclose <user address> in double quotes or preceded with a '\' symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols

Return Values

Returns the user address which has the message encryption fields set. The user's organization, user address, ext_encrypt setting, and the ext_encrypt_criteria setting are returned. An Administration Console example of this command `encryption list_users, orgtag=Sales, ext_encrypt=on` which returns a user who has an message encryption field setting: `msmith@jumboinc.com`.

Authorization

- Read: Message Encryption Management, Outbound Message Encryption
- Write: Message Encryption Management, Outbound Message Encryption

Classification

Batch user management

Notes

- The ext_encrypt_criteria and ext_encrypt are the message_encryption (for orgs), message_encryption_criteria fields.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `encryption display_org`, `encryption display_user`, `encryption modify_org`, `encryption modify_user`

Related Fields

Input: orgname

See Also

“Building a Batch File” on page 19

Postini Encryption Services Administration Guide

encryption modify_org

The encryption modify_org command modifies external encryption settings for an organization. This command applies to Postini Message Encryption, an optional product.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
encryption modify_org, orgtag=<org name>,  
[service=<on | off | match | default>]  
[ ,criteria=header string]  
[ ,cascade=1]
```

Example

```
encryption modify_org, orgtag=Sales, service=on
```

Description

Modifies the encryption settings for an organization.

- <org name> -- The organization being modified.

Note: Enclose <org name> in double quotes or preceded with a ` symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

- 'service=on' -- Encryption is enabled
- 'service=off' -- Encryption is disabled
- 'service=match' -- System looks in the message header for string. If the string is found, the message is encrypted. The default is sensitivity: company-confidential.
- 'service=default' -- Sets the message encryption to match the string "Sensitivity: Company-Confidential"
- criteria -- Specifies the new criteria string to be used when the message encryption is set to 'match'. This is the message_encryption_criteria field.
- cascade -- If set to '1', changes will be cascaded down the organization hierarchy.

Note: Do not use numeric values for the service parameter values. For example, do not use service=0.

Authorization

- Read: Message Encryption Management, Outbound Message Encryption
- Write: Message Encryption Management, Outbound Message Encryption

Classification

Batch organization management

Notes

- For billing purposes, the usage is calculated by capturing, on the last day of the billing cycle, all users:
 - Who have encryption set at the user-level at 'on' or 'match'.
 - Who have encryption set to 'org default' and whose organization has encryption set to 'on' or 'match'.
 - A user's external encryption setting takes precedence to the organization associated with the user. This setting remains with the user if a user is moved to a different organization.

Billing only applies to organization and individual user external encryption settings. Content Manager encryption rules are not included.

- For best practice, we recommend using the encryption modify_org command rather than the modifyorg command used with the message_encryption (for orgs) field. The encryption commands are more efficient. The encryption family of commands offer additional encryption features within each command call.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: encryption display_org, encryption display_user, encryption list_users, encryption modify_user, modifyorg

Related Fields

- Input: orgname
- Output: message_encryption (for orgs)

See Also

"Building a Batch File" on page 19

Postini Encryption Services Administration Guide

encryption modify_user

The encryption modify_user command modifies external encryption settings for a user. This command applies to Postini Message Encryption, an optional product.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
encryption modify_user,  
address=<user address>,  
service=<on | off | match | default>
```

Example

```
encryption modify_user, address=msmith@jumboinc.com, service=on
```

Description

Modifies the encryption settings for a user.

- ‘service=on’ -- Encryption is enabled
- ‘service=off’ -- Encryption is disabled
- ‘service=match’ -- System looks in the message header for string. If the string is found, the message is encrypted. The default is sensitivity: company-confidential.
- ‘service=default’ -- Sets the message encryption behavior to match the user’s organization message encryption setting.

Enclose <user address> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols

Authorization

- Read: Message Encryption Management, Outbound Message Encryption
- Write: Message Encryption Management, Outbound Message Encryption

Classification

Batch user management

Notes

- For billing purposes, the usage is calculated by capturing, on the last day of the billing cycle, all users
 - Who have encryption set at the user-level at ‘on’ or ‘match’.
 - Who have encryption set to ‘org default’ and whose organization has encryption set to ‘on’ or ‘match’.
 - A user’s external encryption setting takes precedence to the organization associated with the user. This setting remains with the user if a user is moved to a different organization.

Billing only applies to organization and individual user external encryption settings. Content Manager encryption rules are not included.

- For best practice, we recommend using the encryption modify_user command rather than the modifyuser command used with the message_encrypt (for users) field. The encryption commands are more efficient. The encryption family of commands offer additional encryption features within each command call.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: encryption display_org, encryption display_user, encryption list_users, encryption modify_org

Related Fields

- Input: address
- Output: message_encrypt (for users)

See Also

"Building a Batch File" on page 19

Postini Encryption Services Administration Guide

getorgreport

The getorgreport command builds a traffic, virus, spam, or usage report for a selected organization.

Syntax

```
getorgreport <org name>, report=<report type> , date=<date>, [top=<number of reports>]
```

Example

- Batch command interface examples:

```
getorgreport sales, report=traffic_summary, date=20060916-20060901
```

```
getorgreport sales, report=spam_summary, date=20060331
getorgreport sales, report=usage_summary, date=20060331
getorgreport sales, report=spam_summary, date=20060331, top=10
```

Description

Build a report of type <report type> for organization, <org name> for a given day, <date>. This is done at the account org level.

- <org name> -- The organization referred to by the reports.

Enclose <org name> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols

- report -- This parameter lists the report type. Available report types include:
 - traffic_summary -- Traffic by Recipient report
 - virus_summary -- Virus by Account report
 - spam_summary -- Spam by Account report
 - usage_summary - Count of users on the given day
- date -- This parameter holds the date range for the report. Date is represented in the format:
 - traffic_summary -- YYYYMMDD[-YYYYMMDD]
 - virus_summary -- YYYYMMDD[-YYYYMMDD]
 - spam_summary -- YYYYMMDD[-YYYYMMDD]
- usage_summary -- YYYYMMDDtop -- This parameter shows how many report entries you want listed in the report summary. The example above demonstrates a top 10 listing for the spam report. This parameter is relevant for Traffic and Spam reports.

Default: top=20

Errors

- If using the Administration Console, verify the organization exists. Or verify the command punctuation (',') is correct:
- "No report matches".
- "Report currently unavailable"
- Verify you are using the correct date syntax for this report type, and you have included the parameter 'date=':
- "Please enter a date in format: YYYYMMDD."
- Check your mail server's mail flow:
- "The org test <your org name> does not have usage data rolled up. Please try an account level org."
- If the organization does not exist:

No organization <your org name>

Return Values

Note: See the Notes section below for the equivalent field labels shown on the Administration Console Batch Results page.

Traffic

Traffic Report returns these comma delimited fields for each user's report (recip) in the list.

```
acc_messages 7883,  
num_bytes 92323,  
num_bh_messages 0,  
num_f_messages 7883,  
num_messages 7883,  
num_q_messages 1,  
pct_bh_bytes 35.7,  
pct_bh_messages 0.0,  
pct_f_bytes 100.0,  
pct_f_messages 100.0,  
pct_q_bytes 0.0,  
pct_q_messages 0.0,  
recip msmith@jumboinc.com
```

Virus

Virus Report returns these comma delimited fields for each user's report in the list.

```
account Jumbo Inc,  
bytes 8622,  
clean_failures 0,  
cleanings 0,
```

```
inf_deliveries 0,  
num_viruses 6
```

Spam

Spam Report returns these comma delimited fields for each user's report in the list.

```
account Jumbo Inc,  
bad_isp 0,  
bad_sender 0,  
bulk 28,  
bytes 123320,  
commerce 4,  
deliveries 45,  
mmf 11,  
naughty 2,  
num_spams 45,  
racial 0,  
ssb 0
```

Usage

Usage Report returns these comma delimited fields for each customer's report in the list.

```
customerid 111111901,  
customername Jumbo Inc,  
messages 0,  
productid ee,  
sellerid 11111801  
stored_size 0,  
users 11
```

Authorization

- Read for Traffic, Virus, Spam reports: Special Permissions, Billing Reports, Billing Summary
- Read for Usage reports: Special Permissions, Billing Reports, Billing Summary, Usage Statements
- Write: View Reports
- Write: The Special Permissions, Billing Reports, Billing Summary, Usage Statements are Read-only for administrators

Classification

Batch organization management

Notes

- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.
- Confirm you have the correct Account-level access privileges before using this command.

The getorgreport summaries in the Administration Console Batch Results page return the report fields in easy to read labels. Below are the report field names followed by the Batch page field labels.

Traffic

Traffic report fields -- Batch page field labels:

```
acc_messages -- Acct Msgs
num_bh_messages -- Blocked Acct Msgs
num_bytes -- Bytes
num_f_messages -- Forward Acct Msgs
num_messages -- Messages
num_q_messages -- Quarantined Acct Msgs
pct_bh_bytes -- Blocked Acct Msgs, % of Bytes
pct_bh_messages -- Blocked Acct Msgs, % of Msgs
pct_f_bytes -- Forward Acct Msgs, % of Bytes
pct_f_messages -- Forward Acct Msgs, % of Msgs
pct_q_bytes -- Quarantined Acct Msgs, % of Bytes
pct_q_messages -- Quarantined Acct Msgs, % of Msgs
recip -- Recipient
```

Virus

Virus report fields -- Batch page field labels:

```
account -- Account
bytes -- Virus Bytes
cleanings -- Virus Cleaned
clean_failures -- Virus Cleaning Failures
inf_deliveries -- Infected Deliveries from Quarantine
num_viruses -- Viruses Detected
```

Spam

Spam report fields -- Batch page field labels:

```
account -- Account
bad_isp -- Blocked Server
bad_sender -- Blocked Sender
bytes -- Spam Bytes
commerce -- Special Offer
mmf -- Get Rich
ssb -- Blatant Spam Blocking
num_spams -- Spam
naughty -- Sexually Explicit
```

```
racial -- Racially Insensitive  
deliveries -- Delivered from Quarantine  
bulk -- Bulk Mail
```

Usage

Usage report fields -- Batch page field labels

```
customerid -- customerid  
customername -- customer name  
messages -- values  
productid -- productid  
sellerid -- sellerid  
stored_size -- values  
users -- values (can be users, stored_size, messages)
```

Related Commands

Batch Commands: addorg, deleteorg, displayorg, listorgs, modifyorg, org_im_settings display, org_im_settings modify, setorgsubstripping

Related Fields

- Input: orgname
- Traffic Report Output: acc_messages, num_bh_messages, num_bytes, num_f_messages, num_messages, num_q_messages, pct_bh_bytes, pct_bh_messages, pct_f_bytes, pct_f_messages, pct_q_bytes, pct_q_messages, recip
- Virus Report Output: account, bytes, cleanings, clean_failures, inf_deliveries, num_viruses
- Spam Report Output: account, bad_isp, bad_sender, bulk, bytes, commerce, deliveries, mmf, naughty, num_spams, racial, ssb
- Usage Report Output: customerid, customername, messages, productid, sellerid, users

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “Reports”

help

The help command lists the syntax, an example, and quick tips for a command in the Administration Console.

Syntax

```
help <command>
```

Example

```
help displayorg
```

Description

Displays syntax, example, and quick tips for a command.

Errors

Always test your command syntax before using the command in a final production configuration. Some help command output may include arguments that you do not have access to, depending upon your administrative authority level. Using these arguments can return errors if you do not have authority to call these arguments.

Return Values

An example of the 'help displayorg' return value:

```
Displayorg
```

```
Syntax: displayorg <orgname|iid>
```

```
Displays information on <orgname>.
```

```
Enclose <orgname> in double quotes if it contains an apostrophe.
```

Authorization

- Read: Same privileges as the command listed
- Write: Read-only for administrators

Classification

Batch help utility

See Also

"Batch Processing Steps" on page 16

iplock add_range

The iplock add_range command allows emails from specific domains with specific IP addresses to be delivered to an organization and its sub-organizations.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
iplock add_range org=<email config org name>, domain=<domain name>, range=<IP address>[/<CIDR subnet>]
```

Note: When adding an IP range using the *iplock add_range* command, new ranges are not enabled by default (the default mode is off). To turn the IP Lock rule on, you must set the command for mode=on. Run the following command to enable your IP range:

```
iplock modify org=<orgtag>, domain=<domain>, mode=on
```

Examples

Single Domain and IP Address/CIDR Subnet

```
iplock add_range org=sales_email_config, domain=jumboinc.com, range=64.18.0.0
```

```
iplock add_range org=sales_email_config, domain=jumboinc.com, range=64.18.0.0/16
```

Description

Allows emails from specific domains with specific IP addresses to be delivered to an organization and its sub-organizations. The sub-org's settings will be overwritten when parent org IP settings change. Peer organizations or organizations higher in the hierarchy are not overwritten.

If junk email messages are reaching your users because the sender is falsifying a domain name in your Approved Senders list, and if this spoofed domain is vital to your business and cannot be removed from the approved senders list, use this batch command to set up an IP lock on this domain.

Note: To create these IP locks you can create a batch file which should be maintained and kept up to date with all valid IP's for the allowed domain. All messages sent to you from this domain with IP addresses not in the allowed IP lock list will be bounced with a SMTP error: 550 IP Authorization check failed - psmtip.

- <email config org name> -- The associated email config organization for this IP lock. These configurations affect the email config organization and all sub-organizations. The sub-org's settings will be overwritten when parent org IP settings change.

Enclose <email config org name> in double quotes or preceded with a '\ symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

- <domain name> -- The name of the sender's domain whose messages are locked to this organization. This domain can be the message's envelope MAIL FROM address or the message's header From: address.
- <IP address> -- The Internet Protocol (IP) address used by the locked domain.
- <IP address/CIDR subnet> -- In addition to an IP address, a subnetwork can be listed using Classless Internet Domain Routing (CIDR) notation. The major CIDR blocks are:

/24 allows for a full class C

/16 allows for a full class B

/8 allows for a full class A

For more information about CIDR notation, see RFC 1518, 1519, and 4632 at the *Internet Engineering Task Force (IETF) RFC* page. In addition, the Internet has several Subnet calculators which are useful determining your Subnet Block. For a good selection, search either for Subnet calculator or CIDR calculator.

Note: This command does not support the subnet mask notation.

WARNING: Before applying this command:

- If you already have a list of locked domains, copy them out prior to making any changes. Always make a backup before editing your list.
- Always validate to confirm your script is correct before applying any changes.

One way to confirm your script is running correctly is to check the iplock display command's output.

The command does not validate the domain or IP addresses. This is done at runtime.

- Check your support contact address to see if it uses a domain on the IP lock list. All alerts that are set at the email config organization, such as the Connection Manager alerts, bounce if being sent from any support contact address that is the same as the domain it is being delivered to. To avoid this, add the Message Security service's IP blocks to your IP lock list. This issue happens since the support contact IP address does not match the Message Security service's IP address which is the actual sender of the alert. The Message Security service IP ranges are:

Systems 5, 6, 7, 8, 20: 64.18.0.0/20

System 9: 74.125.148.0/22

Systems 20, 200, 201: 207.126.144.0/20

Errors

- If any <IP addresses> are configured with a domain, then all traffic from other IP addresses claiming to be from the <domain name> will be blocked with the SMTP error: 550 IP Authorization check failed - psmtp.
- If the range syntax is not correct, the system returns the error, range: Please enter a valid value for the ip range. For example, an error is returned for any range with the domain name, range=jumboinc.com:64.18.0.0.

Return Values

- Single domain and IP addresses

Command: iplock add_range org=_email_config , domain=jumboinc.com, range=64.18.0.0/16

Returns: Added jumboinc.com as allowed for 64.18.0.0/16

iplock display command returns: jumboinc.com -> 64.18.0.0/16

Authorization

- Read: Junk Email Settings
- Write: Junk Email Settings

Classification

Batch organization IP management

Notes

- With the iplock set of commands, you:
 - Apply a domain's IP lock at an email config organization level.
 - Add a single domain or IP range. To enter multiple range entries, either build a batch file or call the iplock add_range command successively.
 - Can selectively remove individual IP locks from a domain
- The ip blocked messages are counted in the 'Blocked Sender' spam reports.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock delete, iplock delete_range, iplock display, iplock set_disposition

Related Fields

Input: domainname, orgname

Related: is_email_config

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “IP Ranges and Security”, and “*Avoid Spoofing*”

iplock delete

The iplock delete command removes all domains with IP limitations configured in the specified email configuration organization.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
iplock delete org=<email config org name>
```

Example

```
iplock delete org=sales_email_config
```

Description

Removes all IP locks for all domains that are configured in an email config organization, <email config org name>. To selectively remove individual IP locks, see iplock delete_range.

- <email config org name> -- The name of the organization where this configuration will be configured. These configurations affect the email config organization and all sub-orgs. The sub-org's settings will be overwritten when parent org IP settings change. Peer organizations or organizations higher in the hierarchy are not overwritten.

Enclose <email config org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

- <domain name> -- The name of the sender's domain whose messages are locked to this organization. This domain can be the message's envelope MAIL FROM address or the message's header From: address.
- <IP address>[CIDR subnet]-- The NetBlock with the IP address and the optional subnet. The Internet Protocol (IP) address used by the IP locked domain. In addition to an IP address, a subnetwork can be listed using Classless Internet Domain Routing (CIDR) notation. This NetBlock is necessary for command to be processed, however it is not used. This command clears all NetBlocks configured in the organization.

WARNING: The <IP address> is necessary for the command to be processed, however, all entries of this domain are deleted. Any sub-org's domains are deleted when parent org IP settings change. Peer organizations or organizations higher in the hierarchy are not overwritten.

Authorization

- Read: Application Management, Junk Email Settings
- Write: Application Management, Junk Email Settings

Classification

Batch Org IP management

Notes

- If an email config organization is converted to a simple organization, the IP locks for any domain associated with the email config is deleted. The information is not retained.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, iplock delete_range, iplock display, iplock set_disposition

Related Fields

- Input: orgname, domainname
- Related: is_email_config

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "IP Ranges and Security", and "Avoid Spoofing"

iplock delete_range

The iplock delete_range command removes either one IP limitation or all IP limitations for one domain configured in the specified email config organization.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
iplock delete_range org=<email config org name>, domain=<domain name>, range=<<IP address [/CIDR subnet]> | all>
```

Example

If the domain has multiple IP limitations (63.18.0.0/16, 64.18.0.0/16), this example removes both IP limitations from this domain:

```
iplock delete_range org=sales_email_config, domain=jumboinc.com, range=all
```

To delete a specific IP limitation for the domain, this example removes only the limitation for 64.18.0.0/16.

```
iplock delete_range org=sales_email_config, domain=jumboinc.com, range=64.18.0.0/16
```

Description

Removes one IP lock or all IP locks for <domain name>, that are configured in an email config organization, <email config org name>. To remove all IP locks associated with all of an email config organization's domains, see iplock delete.

- <email config org name> -- The name of the email config organization where this configuration will be configured. These configurations affect the email config organization and all sub-orgs. The sub-org's settings will be overwritten when parent org IP settings change. Peer organizations or organizations higher in the hierarchy are not overwritten.

Enclose <org name> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

- <domain name> -- The name of the sender's domain whose messages are locked to this organization. This domain can be the message's envelope MAIL FROM address or the message's header From: address.
- <IP address>[CIDR subnet]-- The NetBlock with the IP address and the optional subnet. The Internet Protocol (IP) address used by the IP locked domain. In addition to an IP address, a subnetwork can be listed using Classless Internet Domain Routing (CIDR) notation. This NetBlock is necessary for command to be processed, however it is not used. This command clears all NetBlocks configured in the organization.

WARNING: The <IP address> is necessary for the command to be processed, however, all entries of this domain are deleted. Any sub-org's domains are deleted when parent org IP settings change. Peer organizations or organizations higher in the hierarchy are not overwritten.

Return Values

Locked IP address deleted

Removed jumboinc.com from allowed list for 64.18.0.0

All locked IP addresses for a domain have been deleted

Removed jumboinc.com from allowed list for all

Authorization

- Read: Application Management, Junk Email Settings
- Write: Application Management, Junk Email Settings

Classification

Batch Org IP management

Notes

- The iplock delete_range command clears the one or all IP locks for a specific domain. The iplock delete_range command deletes all IP locks for all domains associated with an email config organization.
- If an email config organization is converted to a simple organization, the IP locks for any domain associated with the email config is deleted. The information is not retained.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, iplock delete, iplock display, iplock set_disposition

Related Fields

- Input: orgname, domainname
- Related: is_email_config

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "IP Ranges and Security", and "Avoid Spoofing"

iplock display

The iplock display command lists all allowed sending domains and associated IPs configured in an email config organization.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

iplock display org=<email config org name>

Example

```
iplock display org=sales_email_config
```

Description

The iplock display batch command lists all domain and associated IP addresses locked to an organization.

- <email config org name> -- The name of the email config organization where this configuration will be configured.

Enclose <org name> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("'), backslash (\), apostrophe, commas, #, = symbols.

Return Values

Domain has two locked IP addresses

```
jumboinc.com -> 64.18.0.0/16  
jumboinc.com -> 207.126.144.0/24
```

No Locked IP addresses for this domain

```
No ip / domain mappings present.
```

Organization is not an email config organization

```
iplock display is not allowed to non-email-config org
```

Authorization

- Read: Application Management, Junk Email Settings
- Write: Read-only for administrators

Classification

Batch IP management

Notes

- If an email config organization is converted to a user organization, the IP locks for any domain associated with the email config is deleted. The information is not retained.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, iplock delete, iplock delete_range, iplock set_disposition

Related Fields

- Input: orgname
- Related: is_email_config

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "IP Ranges and Security", and "Avoid Spoofing", and "Avoid Spoofing"

iplock set_disposition

The iplock set_disposition command configures the IP lock's response behavior when a message does not match the IP range.

Note: This command is not available in this version. The default disposition is to 'reject' the message if it does not match a domain's IP lock. The message is bounced with a 500 error.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
iplock set_disposition org=<email config org name>, domain=<domain name>,  
disposition=<reject | ignore | quarantine>
```

Example

The default behavior is to reject with a 550 error any message that does not match the IP range:

```
iplock set_disposition org=sales_email_config, domain=jumboinc.com,  
disposition=reject
```

Description

Sets the response behavior for any messages that do not match the IP lock range for <domain name>.

- <email config org name> -- The name of the email config organization where this configuration is configured. These configurations affect the email config organization and all sub-orgs. The sub-org's settings will be overwritten when parent org IP settings change. Peer organizations or organizations higher in the hierarchy are not overwritten.

Enclose <org name> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("'), backslash (\), apostrophe, commas, #, = symbols.

- <domain name> -- The name of the sender's domain whose messages are locked to this organization. This domain can be the message's envelope MAIL FROM address or the message's header From: address.
- disposition=reject -- If the message does not match the locked IP range for this domain, an 'ERROR 550 IP Authorization check failed' error message is bounced back to the sender. This is the default setting.
- disposition=ignore -- If the message does not match the locked IP range for this domain, the message is ignored, the information is logged, but no error message is returned.
- disposition=quarantine -- If the message does not match the locked IP range for this domain, the message is quarantined. These messages are counted in the report generated from the bad_sender report field.

Authorization

- Read: Application Management, Junk Email Settings
- Write: Application Management, Junk Email Settings

Classification

Batch Org IP management

Notes

- The iplock set_disposition command is not available in this version. The default behavior is to ‘reject’ a message that does not match a locked IP range for a specific domain.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, iplock delete, iplock delete_range, iplock display

Related Fields

- Input: orgname, domainname
- Related: is_email_config

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “IP Ranges and Security”, and “*Avoid Spoofing*”

listdomains

The listdomains command returns a list of domains in an organization. The list can be all domains or it can be sorted and filtered.

Syntax

```
listdomains <domain name qstring | ALL> , targetOrg=<org name>  
[.orgtagqs=<orgtag qstring> ] [.primaryqs=<primary domain qstring> ]  
[.aliases=<0 | 1> ] [.childorgs=<0/No | 1/Yes> ] [.sort=<sortspec> ]  
[.fields=<fieldlist> ] [.start=<startindex> ] [.end=<endindex> ]
```

Example

- Batch command interface examples:

- List all domains starting with the `sales` org, and sort the results by org name in ASCII ascending order:

```
listdomains ALL, targetOrg=sales, childorgs=1, sort=ORTAG:a
```

It is important to set the targetOrg value if your authorization is limited to the targetOrg or below. Otherwise the system will return an authorization error.

- List the domains ending in ‘com’, include the aliases, and traverse the child organizations:

```
listdomains com$, targetOrg=sales, aliases=1, childorgs=1
```

- List the domains by domain name, org id, and creation date:

```
listdomains ALL, targetOrg=Sales, childorgs=1,  
fields=DOMAINNAME|IID|created_ts
```

- Only list the creation time stamp for the domains in the Sales organization and below:

```
listdomains ALL, targetOrg=Sales, childorgs=1,  
fields=created_ts
```

Description

Displays domain name and domainid of a set of domains, filtering and sorting as requested.

- The list is limited to 15,000 domains.
- Enclose <org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Batch parameter options for listdomains include:

domain name qstring

The domain name you are searching for. This is the target text matched to the search results using the qstring rules explained below.

qstring

The qstring rules are:

- If the target text starts with '=', the result must be an exact match. For example, =jumboinc.com returns exact matches.
- If the target text starts with '%', the result can be a substring match. For example, %jumbo returns all domain names containing jumbo.
- If the target text ends with '\$', the result ends with this match. For example, .com\$ returns all domain names ending in .com.
- If the target text has no qstring marker, the result will begin with the matched text. For example, jumbo returns all domain names beginning with jumbo.

Note: The qstring filtering is not case sensitive.

ALL

The ALL parameter returns all domains. The list is sorted and filtered if additional options are present. This parameter is case sensitive.

targetOrg

The targetOrg is the top-level org IID or org name where the search begins. Note the capital 'O' in the spelling of targetOrg.

- Enclose <org name> in double quotes or preceded with a '\' symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols. In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Note: The search is much faster if this parameter is specified.

Default: Authority root for current admin.

orgtagsgs qstring

The orgtagsgs is the org name used in filtering the search for domains. The domain search must match this orgname using the qstring rules explained above.

primaryqs qstring

The primaryqs is the primary domain name used in filtering the search for domains. The domain search must match this primary domain name using the qstring rules explained above.

aliases

The aliases parameter values are:

'aliases=0' -- Do not include domain aliases in the search results.

'aliases=1' -- Include domain aliases

Default: aliases=1

childorgs

Use this parameter if you need to list sub organizations. This is especially true when using the targetOrg option.

0/No -- Do not include sub organizations in the search results

1/Yes -- Include sub organizations

Default: childorgs=1

sort

Pairs of sortable fields and sort order separated by either a ':' or '|'.

Sortable fields include:

- DOMAINNAME
- PRIMARY_DID
- ORGTAG
- IID
- PRIMARY_DOM
- CREATED_TS
- DOMAINID

Sort order include:

- a = ASCII ascending
- d = ASCII descending
- na = numeric ascending
- nd = numeric descending

Default: sort=ORGTAG:a

fields

The fields parameter is a list of field data displayed in the search results. These are separated by ‘ | ’.

- All of the sortable fields can be used. See the sort parameter option.

domain_id

start

The start parameter is the starting index of the paginated sorted results returned in the search.

Default: start=0

end

The end parameter is the ending index of the paginated sorted results returned in the search.

Default: end=last

Return Values

Batch command interface return values:

- Default return values of the jumboinc.com domain information using listdomains ALL, targetOrg=Sales, these comma delimited field-value strings are returned in the batch command interface:

```
domainid 900000811,  
domainname jumboinc.com
```

Return values using Administration Console syntax:

```
jumboinc.com 900000811  
1 of a total of 1 matching records found.
```

- Return values are dependent upon the command's parameter options. For example, using listdomains ALL, targetOrg=Sales, childOrgs=1, fields=created_ts will return only the Sales organization's domains creation time stamp (shown in the Administration Console syntax):

```
1115397891  
1 of a total of 1 matching records found.
```

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Note: The qstring filtering requires at least one All Standard Privileges authorization.

Classification

Batch domain management

Notes

- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.
- Note spelling of the 'orgtagqs' parameter.

Related Commands

Batch Commands: adddomain, deletedomain, displaydomain, modifydomain, setorgsubstripping

Related Fields

- Input: created_ts (for domains), domainid, domainname, orgname, orgtag, primary_did
- Output: created_ts (for domains), domainid, domainname

See Also

"Building a Batch File" on page 19

"Message Center Settings and Password Examples" on page 536

The Message Security Administration Guide, "Domains"

listorgs

The listorgs command returns a list of organizations. The list can be all organizations or it can be sorted and filtered.

Syntax

```
listorgs <orgtag gstring | ALL>  
[ , targetOrg=<org name> ] [ , childorgs=<0/No | 1/Yes> ]  
[ , sort=<sortspec> ] [ , fields=<fieldlist> ] [ , start=<startindex> ]  
[ , end=<endindex> ]
```

Example

Batch command interface examples:

- To list all orgs under the sales organization, and sort these by the org's ID in numeric descending order:

```
listorgs ALL, targetOrg=sales, sort=IID:nd
```

- To list all orgs that contain 'POP' in the organization's name:

```
listorgs %POP, targetOrg=sales
```

- To list all organizations listing these IM field values, and show from line 25 to 49:

```
listorgs ALL, targetOrg=sales,  
fields=im_enable|im_external_enable|im_proto_enale,start=25,end=49
```

- To list all organizations starting with Sales, and list the localized language and timezone:

```
listorgs ALL, targetOrg=Sales, childorgs=1,  
fields=lang_locale|timezone
```

- To list all organizations starting with Sales, and list the creator, support contact, default user field values:

```
listorgs ALL, targetOrg=Sales, childorgs=1,  
fields=creator|support_contact|default_user
```

- To list the language for all orgs under Sales:

```
listorgs ALL, targetOrg=Sales, childorgs=1, fields=lang_locale
```

Description

Displays the iid and org name of a set of orgs, filtering and sorting as requested.

- The list is limited to 15,000 organizations.
- It is important to set the targetOrg value when using this command. Otherwise the system will return an authorization error if your org listing is outside of your administrative authority.

Batch parameter options for listorgs include:

orgtag qstring

The ‘orgtag qstring’ is the organization you are searching for. This is the target text matched to the search results using the qstring rules explained below.

qstring

The qstring parameter values are:

- If the target text starts with ‘=’, the result must be an exact match. For example, =sales returns exact matches.
- If the target text starts with ‘%’, the result can be a substring match. For example, %POP returns all organization names containing POP.
- If the target text ends with ‘\$’, the results ends with this match. For example, inc\$ returns all organization names ending in inc.
- If the target text has no qstring marker, the result will begin with the matched text. For example, Sales returns all organization names beginning with Sales.

Note: The qstring filtering is not case sensitive.

ALL

The ALL parameter returns all organization names. The list is sorted and filtered if additional options are present. This parameter is case sensitive.

targetOrg

The targetOrg is the top-level org IID or org name where the search begins. The search is much faster if this parameter is specified. And, note the capital ‘O’ in the spelling of targetOrg.

Enclose <org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Default: Authority root for current admin

childorgs

Use this parameter to list sub organizations using the targetOrg option.

0/No -- Do not include sub organizations in the search results

1/Yes -- Include sub organizations

Default: childorgs=1

sort

Pairs of sortable fields and sort order separated by either a ‘:’ or ‘|’.

Sortable fields include:

- ORGTAG
- IID

Sort order include:

- a = ASCII ascending
- d = ASCII descending
- na = numeric ascending
- nd = numeric descending

Default: sort=IID:na

fields

List of field data to display in search results. These are separated by ' | '.

- All of the sortable fields can be used. See the sort parameter option.
- archive, at_notify_on, bounce_fragments, creator, default_user, disable_first_spam, footer_on, im_enable, im_external_enable, im_proto_enable, lang_locale, non_account_virus_scan, out_at_notify_on, spam_notify_on, support_contact, timezone, virus_clean, welcome_on

Default: fields=IID|ORGTAG

start

The start parameter is the starting index of the paginated sorted result pairs to return in the search.

Default: start=0

end

Ending index of the paginated sorted result pairs to return in the search.

end=last

Return Values

- When using the Batch Interface, the default return values for the sales organization using `listOrgs ALL, targetOrg=Sales`, these comma delimited field-value strings are returned in the Batch command interface:

```
orgname sales,  
iid 100001011
```

Return values using Administration Console syntax:

```
100001011 sales  
1 of a total of 1 matching records found.
```

- Return values are dependent upon the command's parameter options. For example, using `listorgs ALL, targetOrg=Sales, childorgs=1, fields=lang_locale` will return only the Sales organization's and sub organization's localized language values. (shown in the Administration Console syntax):

```
es.iso-8859-1  
ja_jp.iso-2022-jp  
en_us.iso-8859-1  
fr.utf8  
de.utf8  
en_us.utf8  
6 of a total of 6 matching records found.
```

If you wanted the organization's name in addition to the language value using `listorgs ALL, targetOrg=Sales, childorgs=1, fields=orgtag|lang_locale` (shown in the Administration Console syntax):

```
Sales es.iso-8859-1  
TokyoSales ja_jp.iso-2022-jp  
CaliforniaSales en_us.iso-8859-1  
ParisSales fr.utf8  
BerlinSales de.utf8  
ChicagoSales en_us.utf8  
6 of a total of 6 matching records found.
```

Authorization

- Read: Organization Management
- Write: Organization Management

Note: The qstring filtering requires at least one All Standard Privileges authorization.

Classification

Batch org management

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: addorg, deleteorg, displayorg, getorgreport, modifyorg, org_im_settings display, org_im_settings modify, setorgsubstripping

Related Fields

- Input: archive, at_notify_on, bounce_fragments, creator, default_user, disable_first_spam, footer_on, iid, im_enable, im_external_enable, im_proto_enable, lang_locale (for orgs), non_account_virus_scan, orgname, orgtag, out_at_notify_on, spam_notify_on, support_contact, timezone (for orgs), virus_clean, welcome_on
- Output: archive, at_notify_on, bounce_fragments, creator, default_user, disable_first_spam, footer_on, iid, im_enable, im_external_enable, im_proto_enable, lang_locale (for orgs), non_account_virus_scan, orgname, orgtag, out_at_notify_on, spam_notify_on, support_contact, timezone (for orgs), virus_clean, welcome_on

See Also

“Building a Batch File” on page 19

“Message Center Settings and Password Examples” on page 536

The Message Security Administration Guide, “Organization Management”

listprovusers

The listprovusers command returns a list provisional users. The list can be all provisional users or it can be sorted and filtered.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
listprovusers <org name>
[, subset=ALL | BLOCK | UNBLOCK] [, addressqs=<match spec>]
[, childorgs=<0/No | 1/Yes>] [, sort=<sortspec> ] [, fields=<fieldlist> ]
[, start=<startindex> ] [, end=<endindex> ]
```

Example

```
listprovusers My Company, subset=ALL, sort=TS1:d,  
fields=ADDRESS|TS1|TS3
```

Description

Displays information about a set of provisional users, filtering and sorting as requested.

- <org name> -- The organization associated with the provisional users.

Note: Enclose <org name> in double quotes or preceded with a '\ symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

The batch parameter options for listprovusers include:

subset

The subset parameter options include:

- ALL -- All provisional users. This parameter is case sensitive.
- BLOCK -- Users permanently blocked from being added to the Message Security service.
- UNBLOCK -- Unconfirmed provisional users who are not permanently blocked from becoming regular users.

Default: subset=ALL

addressqs

The addressqs parameter is the provisional user email address you are searching for. This is the target text matched for the search results using the match specifications.

The match specifications include:

- If the target text starts with '=', the result must be an exact match. For example, =msmith@jumboinc.com returns exact matches.
- If the target text starts with '%', the result can be a substring match. For example, %smith returns all provisional user address containing smith.
- If the target text ends with '\$', the result ends with this match. For example, .com\$ returns all provisional user addresses ending in .com.
- If the target text has no match specifications, the result will begin with the matched text. For example, jumbo returns all provisional user addresses beginning with jumbo.

Note: The addressqs filtering is not case sensitive.

Note: Enclose <user address> in double quotes or preceded with a '\' symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols. In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

childorgs

The childorgs parameter searches sub organizations.

- 0/No -- Do not include sub organizations in the search results.
- 1/Yes -- Include sub organizations

Default: childorgs=1

sort

The sort parameter consists of pairs of sortable fields and sort order separated by either a ':' or '|'.

Sortable fields include:

- TS1 -- Timestamp when message was received. The time is in UNIX seconds.
- TS3 -- Timestamp when the user received the 3rd email and was promoted. The time is in UNIX seconds.
- ADDRESS -- Provisional user email address

Sort order include:

- a = ASCII ascending
- d = ASCII descending

Default: sort=TS1:d

fields

The fields parameter is a list of fields to display in results, separated by ‘ | ’.

Note: This is limited to sortable fields. See the sort option.

Default: fields=ADDRESS|TS1

start

The start parameter is the starting index of the pagination for sorted result pairs returned in the search.

Default: start=0

end

The end parameter is the ending index of the pagination sorted result set returned in the search.

end=last

Return Values

If the Sales organization had one provisional user, joe@jumboinc.com, the command returns (using the Administration Console syntax):

```
Provisional users under Sales
joe@jumboinc.com 1145975006
1 of a total of 1 matching records found.
```

Note: The number following the user address is a time stamp.

Authorization

- Read: User Settings
- Write: User Settings

Note: The addressqs filtering requires at least one All Standard Privileges authorization.

Classification

Batch user management

Notes

- If your account has the SmartCreate feature enabled, users in your domains whose address ends in `@yourdomain`, will be added automatically to the Message Security service as unconfirmed provisional users. These users are promoted to regular users after being verified as associated with someone in your org by receiving 3 legitimate emails with a week. Once this criteria is met, the user is added to the service. Otherwise the user is deleted and you are not billed for it.
- The provisional user list is limited to 15,000 users.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `blockprovuser`, `deleteprovuser`, `displayprovuser`, `promoteprovuser`, `unblockprovuser`

Related Fields

Input: `orgname`, `address`, `TS1`, `TS3`

See Also

[“Building a Batch File” on page 19](#)

[“Viewing Your Organization’s Sender Lists” on page 554](#)

[“Editing Your Mail Handling Policies \(Non Account Bounce\)” on page 562](#)

The Message Security Administration Guide, “Users and Quarantines”

listusers

The `listusers` command returns a list of users. The list can be all users or it can be sorted and filtered.

Syntax

```
listusers <user address qstring | 'ALL', targetOrg=<org name>
```

```
[, orgtagqs=<orgtag qstring>] [, primaryqs=<primary address qstring>]
```

```
[, aliases=<0 | 1>] [, childorgs=<0/No | 1/Yes>]
```

```
[, sort=<sortspec>] [, fields=<fieldlist>]  
[, start=<startindex>] [, end=<endindex>]  
[, type_of_user=<im | all>]
```

Example

- To list all of the aliases for a single user, use the example below. The return values are a comma separated list of aliases for jim@jumboinc.com:

```
listusers ALL, primaryqs=jim@jumboinc.com, targetOrg=100046262,  
childorgs=1, aliases=1
```

- To list all primary user addresses and associated aliases in an org hierarchy, use the example below. The return values are in a list composed of primary user addresses (PRIMARY_ADD is [null], ADDRESS is the primary address), and of primary user address and that user's aliases (PRIMARY_ADD is the primary user address, ADDRESS is that user's alias):

```
listusers ALL, targetOrg=[accountorg], childorgs=1,  
fields=PRIMARY_ADD|ADDRESS, aliases=1, sort=primary_add:nd
```

- To list a user address from an alias. The return values are the alias address and the primary user address. In this case the return value is alias4mary@jumboinc.com mary@jumboinc.com:

```
listusers =alias4mary@jumboinc.com, targetOrg=200046262,  
childorgs=1, aliases=1, fields=ADDRESS|PRIMARY_ADD
```

- To list all users starting the search at the sales organization, and sorting the list by ascending user addresses:

```
listusers ALL, targetOrg=sales, sort=ADDRESS:a
```

- To list users whose user address includes 'alias':

```
listusers %alias, targetOrg=sales
```

- To list only the users' organization IDs:

```
listusers ALL, targetOrg=Sales, childorgs=1, fields=IID
```

Description

Displays information about a set of users, filtered and sorted as requested.

- The list is limited to 15,000 users.
- It is important to set the targetOrg value if your authorization is limited to the targetOrg or below. Otherwise the system will return an authorization error.

Batch parameter for listusers include:

address qstring

An address qstring parameter is the partial or full user's email address. This is the target text to match with the search results using the qstring rules explained below.

qstring

The qstring includes:

- If target text starts with '=', the result must be an exact match. For example, =msmith@jumboinc.com returns exact matches.
- If the target text starts with '%', the result can be a substring match. For example, %smith returns all users' addresses containing smith.
- If the target text ends with '\$', the result ends with this match. For example, .com\$ returns all users' addresses ending in .com.
- If the target text has no qstring marker, the result will start with the matched text. For example, msm returns all user addresses beginning with msm.

Note: The qstring filtering is not case sensitive.

ALL

The ALL parameter returns all user addresses. The list is sorted and filtered if additional options are present. This parameter is case sensitive.

targetOrg

The targetOrg is the top-level org IID or org name where the search begins. This is much faster if specified. Note the capital 'O' in the spelling of targetOrg.

Default: Authority root of current admin

orgtagqs qstring

The orgtagqs parameter is the orgname used in filtering the search for users. The user search must match this orgname using the qstring rules explained above.

primaryqs qstring

The primaryqs parameter is the primary user address used in filtering the search for users. The user search must match this primary user address using the qstring rules explained above.

aliases

The aliases parameter includes:

- aliases=0 -- Don't include user aliases in the search results.
- aliases=1 -- Include user aliases

childorgs

Use this parameter if you need to list sub organizations. This is especially true when using the targetOrg option.

- 0/No -- Do not include sub organizations in the search results
- 1/Yes -- Include sub organizations

Default: childorgs=1

sort

The sort parameter is composed of pairs of sortable fields and sort order separated by either a ‘:’ or ‘|’.

Sortable fields include:

- ADDRESS
- ORGTag
- PRIMARY (primary u_id)
- PRIMARY_ADD (primary address)
- IID
- UID

Sort order include:

- a = ASCII ascending
- d = ASCII descending
- na = numeric ascending
- nd = numeric descending

Default: sort=ADDRESS:a

fields

The fields parameter is a list of fields to display in results, separated by ‘|’.

- The sortable fields can be used. See the sort parameter option.
- active, address, create_method, created_ts, primary_add, timezone, u_id

To list all users starting with the Sales organization, and including whether the user is active, how the user was created and the date of creation:

```
listusers ALL, targetOrg=Sales, childorgs=1,  
fields=active|create_method|created_ts
```

Default: fields=ADDRESS|ORGTAG

start

The start parameter is the starting index of the paginated sorted result pairs to return in the search.

Default: start=0

end

The end parameter is the ending index of the paginated sorted result pairs to return in the search.

Default: end=last

type_of_user

The type_of_user parameter is the user type being listed.

- im -- List of IM users only
- all -- List of all types of users

Errors

- When using the Batch interface, if you want to return sub-organizations, the childorg needs to be on (`childorg=1`). Otherwise a possible error message is
"0 of a total of 0 matching records found."
- Note spelling of 'orgtagqs'.

Return Values

Batch command interface return values:

- Default return values for the sales organization using `listusers ALL, targetOrg=Sales`, these comma delimited field-value strings are returned in the Batch interface:

```
orgtag sales,  
address msmith@jumboinc.com
```

- Return values using Administration Console syntax:

```
msmith@jumboinc.com sales  
1 of a total of 1 matching records found.
```

- Return values are dependent upon the command's parameter options. For example, using `listusers ALL, targetOrg=Sales, childorgs=1, fields=IID` will return only the org ID values for all users in the Sales organization and sub organizations. (shown in the Administration Console syntax):

```
100046267  
100052426  
100045290  
3 of a total of 3 matching records found.
```

If you wanted the user's name in addition to the org's ID using `listusers ALL, targetOrg=Sales, childorgs=1, fields=ADDRESS|IID` (shown in the Administration Console syntax):

```
jim@jumboinc.com 100046267  
carlos@jumboinc.com 100052426  
asako@jumboinc.com 100045290  
3 of a total of 3 matching records found.
```

Authorization

- Read: User Settings
- Write: User Settings

Note: The qstring filtering requires at least one All Standard Privileges authorization.

Classification

Batch user management

Notes

- Enclose <user address> in double quotes or preceded with a '\ symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.
- When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: adduser, deleteuser, displayuser, modifyuser, resetuser, suspenduser

Related Fields

- Input: active, address, create_method (for users), created_ts (for users), orgname, orgtag, primary_add, timezone (for users), u_id
- Output: active, address, create_method (for users), created_ts (for users), orgname, orgtag, primary_add, timezone (for users), u_id

See Also

“Building a Batch File” on page 19

“Message Center Settings and Password Examples” on page 536

“Viewing Your Organization’s Sender Lists” on page 554

“Resetting Users” on page 553

“Listing User Aliases and Primary Addresses” on page 566

The Message Security Administration Guide, “Users and Quarantines”

modifydomain

The modifydomain command can move a domain, set subdomain stripping, and modify domain aliases.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

modifydomain <domain name>,

[neworg=<org name> | substrip=<yes | no> | alias=<alias name| -alias name>]
[catchall=< user address | NONE>]

Example

Batch Interface examples:

- To move `jumboinc.com` to another org:

```
modifydomain jumboinc.com, neworg=Jumbo Sales Org
```

- To turn off subdomain substripping for `jumboinc.com`:

```
modifydomain jumboinc.com, substrip=no
```

- To set a domain alias for `jumboinc.com`:

```
modifydomain jumboinc.com, alias=jumboalias.com
```

- To delete `jumboalias.com` domain alias and add another:

```
modifydomain jumboinc.com, alias='-jumboalias.com, jumbo.com'
```

- To turn subdomain substripping on, delete an alias, and add a new domain alias:

```
modifydomain jumboinc.com, substrip=1, alias="-jumbo.com,  
jumboalias.com"
```

Note the double quotes for the comma delimited alias values.

- To set `catch@jumboinc.com` as the domain's catchall mailbox:

```
modifydomain jumboinc.com, catchall=catch@jumboinc.com
```

Description

Modifies the domain record, <domain name>. Used to move domains, set domain substripping, and add/remove aliases. These fields can be viewed by the **displaydomain** command

- <domain name> -- The domain you are modifying.
- neworg -- The domain is moved to this organization.

Enclose <org name> in double quotes or preceded with a '\' symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.
- 'substrip=no' -- Turns off domain substripping.
- 'substrip=yes' -- Turns on domain substripping.
- alias -- Adds a domain alias. To remove an alias, use a '-' symbol before the alias name. Enclose comma-separated aliases in single or double quotes.
- catchall -- The user address of the Catchall User which is the initial single user of a domain acting as a placeholder before you have set up your registered users. A secondary role of the Catchall User is to filter inbound unregistered email for viruses. To turn this parameter off, use NONE.

For robust production code, use the **non_account_virus_scan** field to filter inbound unregistered email for viruses rather than the Catchall User legacy feature. The catchall parameter is a legacy feature available to some accounts. If your organization is not configured for catchall email, you will get a system error. For more information, please contact Support.

Note: The catchall parameter automatically disables **non_account_bounce**

Return Values

If the `western.sales.jumboinc.com` domain was moved to a new organization, this string is returned:

```
'Moved domain western.sales.jumboinc.com from Sales to  
WestCoastSales.'
```

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Classification

Batch domain management

Notes

When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: adddomain, deletedomain, displaydomain, listdomains, setorgsubstripping

Related Fields

Input: address, catchall, domainname, orgname

See Also

"Building a Batch File" on page 19 *The Message Security Administration Guide*, "Domains"

modifyorg

The modifyorg command modifies an organization's settings.

Syntax

```
modifyorg <org name> [,field=<value>, ...]
```

Example

```
modifyorg sales, support_contact=user_support@jumboinc.com,  
max_message_size=250  
modifyorg sales, im_enable=on
```

Description

Modifies an organization record.

- <org name> -- The organization being modified.
Enclose <org name> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.
- <field>=<value> -- Any org-level field that you have privileges to edit. If you include a read-only field, the system will return an error.
Enclose <value> in double quotes if it contains a comma delimited list. For example, approved_senders="+joe@jumboinc.com, +mary@hugeisp.com".

Return Values

Batch command interface return values:

If the Sales organization's approved_senders field was modified, this string is returned:

```
'Modified Sales: Set approved_senders to +msmith@jumboinc.com'
```

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Classification

Batch org management, and IM management (im_enable flag)

Notes

- Current organization values can be viewed with the **displayorg** command.
- The authentication data field can be configured by **modifyorg** by using the **authentication_data** field.

Whenever the shared secret is changed in the scripts, it should also be changed in the **authentication_data** field for the org which contains the users being authenticated.

- If an email config organization is converted to a simple organization, the IP locks for any domain associated with the email config is deleted. The information is not retained. To display an email config organization's IP locks for a domain, see the iplock display command.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: addorg, deleteorg, displayorg, encryption modify_org, listorgs, org_im_settings display, org_im_settings modify, setorgsubstripping

Related Fields

Input: antivirus_sensitivity, approved_senders (for orgs), archive, async_bounce, at_notify_on, authentication_data, blatant_spam, blatant_spam, blocked_senders (for orgs), company_name, creator, default_user, disable_first_spam, disposition_virus, message_encryption (for orgs), footer_on, iid, im_enable, im_external_enable, im_proto_enable, is_email_config, lang_locale (for orgs), lastmod_date (for orgs), max_message_size, ndr, non_account_bounce, nullsender_disposition, nullsender_headertag_validation, orgname, out_at_notify_on, outbound_max_message_size, outbound_virus, outbound_virus_disposition, parent_org, qsum_actionable, qsum_enable, qtine_redir_atq, qtine_redir_ndr, qtine_redir_out_atq, qtine_redir_out_virus, qtine_redir_spam, qtine_redir_virus, quarantine_links, quarsum_links, remotecmd_secret, spam_notify_on, support_contact, tagonly_spam, timezone (for orgs), tls_notify_admin, tls_notify_on, virus_clean, virus_clean, virus_notify (for orgs), welcome_on

See Also

“Building a Batch File” on page 19

“Editing Your Mail Handling Policies (Non Account Bounce)” on page 562

“Viewing Message Center Settings” on page 536

“Seeing if a User Has Received a Welcome Notification” on page 547

“Adding Users and Domains to Sender Lists” on page 555

“Viewing Message Center Settings” on page 536

“Editing Quarantine Summary Notifications” on page 546

“Viewing Message Center Settings” on page 536

“Viewing and Editing Message Encryption Settings” on page 565

“Setting a Virus Notification Interval” on page 549

The Message Security Administration Guide, “Organization Management”

modifyuser

The modifyuser command modifies a user’s settings.

Syntax

```
modifyuser <user address> [, <field>=<value>, ...]
```

Example

```
modifyuser msmith@jumboinc.com
modifyuser msmith@jumboinc.com, junkmail_filter=0
modifyuser msmith@jumboinc.com, virus_state=0, virus_notify=9
modifyuser msmith@jumboinc.com, filter_bulk=14, filter_adult=12,
filter_getrich=12, filter_offers=12, filter_racial=12
modifyuser msmith@jumboinc.com, approved_senders="+yahoogroups.com,
+groups.yahoo.com"
```

Note: Enclose field lists in double quotes if they contain commas. For example, `approved_senders="joe@jumboinc.com, mary@hugeisp.com"`.

Description

Batch Interface Description for modifyuser

Modifies a user record. Field values can be viewed with the displayuser command.

- `<user address>` -- The user email address being modified.

Enclose `<user address>` in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘‘), double quote (“”), backslash (\), apostrophe, commas, #, = symbols.

- `<field>=<value>` -- The user record settings being modified.

Note: Only fields with administrator modification authorization can be used with the modifyuser command.

EZCommand Description for modifyuser

See the Batch Interface Description for modifyuser for general usage details.

- When used as an EZCommand, the command must be URL-escaped in order to properly submitted.

Example:

```
modifyuser msmith@jumboinc.com, junkmail_filter=0
```

changes to

```
modifyuser%20msmith%40jumboinc.com%20junkmail_filter=0
```

Errors

- Possible error messages include:

```
'No such user 'username' (unknown administrator address supplied).'  
'String authorization failed.'  
'No commands to process.'  
'Command not recognized: command.'  
'You don't have permission to insert users into org name.'  
'No such organization 'org name'.'  
'No default user available for organization org name.'  
'No secret key in database.'
```

Note: This means “no secret key” found in the organization’s EZCommand Shared Secret. The secret code must exist in the organization in which the administrator account resides.

- If the user modification was not successful, possible errors include:

```
'Modified username: set field to value [set field to value]...'  
'Please pick an address to modify.'  
'No such user: username.'  
'Unknown field: fieldname.'  
'You don't have authorization to set field on table username.'  
'Please specify a value for field.'
```

- If changing a user’s address name to a deactivated user’s address, the system returns an error. In this example, changing msmith@jumboinc.com to the deactivated user, jill@jumboinc.com returns this error:

```
jill@jumboinc.com is already in use as an address.
```

Note: If you include a read-only field with this command, the system will return an error.

Return Values

Batch command interface return values:

- If modifying msmith@jumboinc.com by changing the adult and getrich filters, this string is returned:

'Modified msmith@jumboinc.com: Set filter_getrich to moderate. Set filter_adult to 13.'

- When used as an EZCommand, the HTTP response will contain a two-part return value: <status><message>
 - status -- 1 for success or 0 for failure
 - message -- Contains errors and additional details

Authorization

- Read: User Settings
- Write: User Settings

Classification

Batch user management; EZCommand-enabled

Notes

- Avoid updating a Default User. This is because changes affect only new users—not an org's existing users. If you update spam filters in an org's Default User and want existing users in the org to share those same levels, you must update each existing user's filters.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Note: For modifying a PMP password, do not use a single quote ('), a double quote ("), a comma (,), or a backslash (/) as part of the password text.

Related Commands

- Batch Commands: adduser, deleteuser, displayuser, listusers, resetuser, suspenduser
- User Password Commands: password force_update, password reset, password_policy display, password_policy update

Related Fields

Input: active, address, approved_senders (for users), approved_recipients, blocked_senders (for users), message_encrypt (for users), filter_adult, filter_bulk, filter_getrich, filter_offers, filter_racial, filter_racial, initial_password, junkmail_filter, lang_locale (for users), message_count, message_limit, message_limited, notice_address, orgid, password, timezone (for users), timezone (for users), user_id, virus_notify (for users), virus_state, webblocked, welcome_count, wireless_state

See Also

“Building a Batch File” on page 19

“About EZCommand” on page 22

“Message Center Settings and Password Examples” on page 536

“Viewing Message Center Settings” on page 536

“Viewing Message Center Settings” on page 536

“Viewing Message Center Settings” on page 536

“Editing a PMP Password” on page 541

The Message Security Administration Guide, “Users and Quarantines”

notification display

The notification display command displays an organization’s notification information.

Syntax

notification display

type=<all | attachment_manager_inbound | attachment_manager_outbound | early_detection_quarantine | first_spam | password_reset | quarantine_summary | spam | suspension | virus | welcome_user>,

org=<target Org>

Example

```
notification display type=virus, org=sales
```

Description

Displays an organization's notification attributes depending on the notification type

Notification type descriptions:

- all -- Only used for displaying. Will display all notification settings for the target organization.
- attachment_manager_inbound -- Notification sent when an attachment arrives on inbound mail. This is only used with Message Security installations.
- attachment_manager_outbound -- Notification sent when an attachment is sent on outbound mail. This is only used with Message Security installations.
- early_detection_quarantine -- Notification sent when early detection places a potential threat under quarantine.
- first_spam -- Notification sent when the first spam message gets quarantined in a new user's Message Center
- password_reset -- Allows modification of password reset notification text
- quarantine_summary -- Controls the quarantine summary report
- spam -- Shows the spam notification state and link status.
- suspension -- Allows modification of suspension notification text
- virus -- This notification is sent when a virus is detected.
- welcome_user -- Controls the welcome notice users receive within 24 hours of account creation.

Note: If the organization does not have the notification's feature configured, the notification information is not returned.

- org -- The notification's organization

Return Values

In return values, the 'text' parameter shows:

- text=<delete | default> -- The organization's notification message is the default.
- text=link:<the org which shares the notification text> -- The organization shares its notification with another org. Shared notifications can be modified by either organization.
- text=unlink -- Removes the link to the shared organization. When unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org.deletefor

Batch parameter options for notification display include:

notification display type=all

```
attachment_manager_inbound notification settings:  
state=off  
text=default  
  
attachment_manager_outbound notification settings:  
state=off  
text=default  
  
early_detection_quarantine notification settings:  
state=off  
text=default  
  
first_spam notification settings:  
cc=none  
state=on  
text=default  
  
password_reset notification settings:  
text=default  
  
quarantine_summary notification settings:  
delivery_hour=9 pm  
inbox_delivery=on  
state=on  
subject_links=on  
text=default  
  
spam notification settings:  
cc=none  
frequency=Daily  
state=on  
text=default  
  
suspension notification settings:  
text=default  
  
virus notification settings:  
cc=none  
state=Immediately  
text=default  
  
welcome_user notification settings:  
cc=none  
state=on  
text=default
```

notification display type=attachment_manager_inbound

```
state=off  
text=default
```

notification display type=attachment_manager_outbound

```
state=off  
text=default
```

notification display type=early_detection_quarantine

state=off
text=default

notification display type=first_spam

cc=none
state=on
text=default

notification display type=password_reset

text=default

notification display type=quarantine_summary

delivery_hour=9 pm
inbox_delivery=on
state=on
subject_links=on
text=default

notification display type=spam

cc=none
frequency=Daily
state=on
text=default

notification display type=suspension

text=default

notification display type=virus

cc=none
state=Immediately
text=default

notification display type=welcome_user

cc=none
state=on
text=default

Authorization

- Read: Notification Messages, Edit Organizations (as a general rule)
- Write: Notification Messages, Edit Organizations (as a general rule)

Note: The authorizations are dependent upon the type of notification.

Classification

Batch organization management

Related Commands

Batch Command: notification modify

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “Quarantine Summary and Notifications”

notification modify

The notification modify command creates, modifies, and deletes notifications associated with an organization.

Syntax

```
notification modify type=attachment_manager_inbound, org=<org name> [ ,  
<state=<user | quarantine redirect | both | off> | [ , text=link:<the org name which  
shares the notification text> | unlink | default ]
```

```
notification modify type=attachment_manager_outbound, org=<org name> [ ,  
state= user | quarantine redirect | both | off ] | [ , text=link:<the org name which  
shares the notification text> | unlink | default ]
```

```
notification modify type=early_detection_quarantine, org=<org name> [ , state=<  
on | off > | [ , text=link:<the org name which shares the notification text> | unlink |  
default ]
```

```
notification modify type=first_spam, org=<org name> [ , state=< on/1 | off/0> ] | [ ,  
text=link:<the org which shares the notification text> | unlink | default ] | [ ,  
cc=<user address> ]
```

```

notification modify type=password_reset, org=<org name> [ , text=link:<the org
which shares the notification text> | unlink | default ]

notification modify type=quarantine_summary, org=<org name> [ , state=<on |
off> ] | [ , inbox_delivery=<on | off> ] | [ , delivery_hour=<4 thru 21 which is an hour
between 4 a.m. and 9 p.m> ] | [ , subject_links=<on | off> ] | [ ,text=default ]

notification modify type=spam, org=<org name> [ , state=<on | off> ] | [ ,
text=link:<the org name which shares the notification text> | unlink | default ] | [
, cc=<user address> ] | [ , frequency=< 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 > ]

notification modify type=suspension, org=<org name> [ , <text=link:<the org which
shares the notification text> | unlink | default ]]

notification modify type=virus, org=<org name> [ , state=<immediately | one per
day | organization default | off> ] | [ , text=link:<the org which shares the
notification text> | unlink | default ] | [ , cc=<user address> ]

notification modify type=welcome_user, org=<org name> [ , state=<on | off> ] | [ ,
text=link:<the org name which shares the notification text> | unlink | default ] | [
, cc=<user address> ]

```

Example

```

notification modify type=attachment_manager_inbound, org=sales,
state=user, text=default

notification modify type=attachment_manager_outbound, org=sales,
state=user, text=link:engineering_org

notification modify type=early_detection_quarantine, org=sales,
state=on, text=default

notification modify type=first_spam, org=sales, state=on, text=unlink,
cc=<msmith@jumboinc.com

notification modify type=password_reset, org=sales, text=default

notification modify type=quarantine_summary, org=sales, state=on,
inbox_delivery=off, delivery_hour=6, subject_links=on, text=default

notification modify type=spam, org=sales, state=on, text=default,
cc=msmith@jumboinc.com, frequency=3

notification modify type=suspension, org=sales, text=default

notification modify type=virus, org=sales, state=immediately,
text=default, cc=msmith@jumboinc.com

notification modify type=welcome_user, org=sales, state=on,
text=default, cc=msmith@jumboinc.com

```

Description

Modifies an organization's notification information depending upon the notification type.

Notification type descriptions:

- attachment_manager_inbound -- Notification sent when an attachment arrives on inbound mail. This is only used with Message Security installations.
 - state=< user | quarantine redirect | both | off> -- Sends attachment manager notifications directly to the user, the quarantine redirect address, both the user and the redirect, or off. This is optional.
 - text=<delete | default> | link:<the org which shares the notification text> | unlink -- The text parameter resets the organization's notification message to the default, shares the notification with another organization which can be modified by either org, unlink shared notifications. When unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org. This is optional.
- attachment_manager_outbound -- Notification sent when an attachment is sent on outbound mail. This is only used with Message Security installations.
 - state=< user | quarantine redirect | both | off> -- Sends attachment manager notifications directly to the user, the quarantine redirect address, both the user and the redirect, or off. This is optional.
 - text=<delete | default> | link:<the org which shares the notification text> | unlink -- The text parameter resets the organization's notification message to the default, shares the notification with another organization which can be modified by either org, unlink shared notifications. When unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org. This is optional.
- early_detection_quarantine -- Notification sent when early detection places a potential threat under quarantine.
 - state=< on | off> -- An on/off switch for early detection notifications. This corresponds to the zero_hour_notify_on field shown in the displayorg output. This is optional.
 - text=<delete | default> | link:<the org which shares the notification text> | unlink -- The text parameter resets the organization's notification message to the default, shares the notification with another organization which can be modified by either org, unlink shared notifications. When unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org. This is optional.

This corresponds to the zero_hour_notify_text field shown in the displayorg output.

Note: If an organization does not have the notification's feature, an "Invalid notification type." error is returned.

- first_spam -- Notification sent when the first spam message gets quarantined in a new user's Message Center
 - state=< on/1 | off/0> -- An on/off switch for first spam notifications. This is optional.
 - text=<delete | default> | link:<the org which shares the notification text> | unlink -- The text parameter resets the organization's notification message to the default, shares the notification with another organization which can be modified by either org, unlink shared notifications. When unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org. This is optional.
 - cc=< user address > -- The address of the user who will be cc'ed when the notification is sent. This address must be a valid user under the same email config. This is optional.
 - password_reset -- Allows modification of password reset notification text. This is optional.
 - text=<delete | default> | link:<the org which shares the notification text> | unlink -- The text parameter resets the organization's notification message to the default, shares the notification with another organization which can be modified by either org, unlink shared notifications. When unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org. This is optional.
- quarantine_summary -- Controls the quarantine summary report
 - state=< on | off> -- An on/off switch for quarantine summary notifications. This is optional.
 - inbox_delivery=< on | off > -- Controls whether the quarantine summary allows sending quarantine mail to your inbox directly from the summary. This is optional.
 - delivery_hour=<4 thru 21 which is an hour between 4 a.m. and 9 p.m.> -- Controls the time of day when the summary will be sent. This is optional.
 - subject_links=< on | off > -- Controls whether summary has subject links to allow the user to view the messages. This is optional.
 - text=default -- Sets the organization's notification message to the default. This is optional.
- spam -- Enables the spam notification, sets links to the text to another organization's notification, adjusts the frequency of updates, and edits the cc address. This setting is only appropriate when quarantine summaries are disabled. When enabled, the quarantine summaries replace the spam notifications.
 - state=< on | off> -- An on/off switch for spam notifications. This is optional.
 - text=<delete | default> | link:<the org which shares the notification text> | unlink -- The text parameter resets the organization's notification message to the default, shares the notification with another organization which can be modified by either org, unlink shared notifications. When

unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org. This is optional.

- cc=< user address > -- The address of the user who will be cc'ed when the notification is sent. This address must be a valid user under the same email config. This is optional.
- frequency=< 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 > -- Number of days between spam notification updates. For frequency=1, this means daily notification updates. This is optional.
- suspension -- Allows modification of suspension notification text
 - text=<delete | default> | link:<the org which shares the notification text> | unlink -- The text parameter resets the organization's notification message to the default, shares the notification with another organization which can be modified by either org, unlink shared notifications. When unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org. This is optional.
- virus -- This notification is sent when a virus is detected.
 - state=< immediately | one per day | organization default | off> -- Controls whether virus notification is sent immediately, once a day, as defined by the org default, or off. This is optional.
 - text=<delete | default> | link:<the org which shares the notification text> | unlink -- The text parameter resets the organization's notification message to the default, shares the notification with another organization which can be modified by either org, unlink shared notifications. When unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org. This is optional.
 - cc= <user address > -- The address of the user who will be cc'ed when the notification is sent. This address must be a valid user under the same email config. This is optional.
- welcome_user -- Controls the welcome notice users receive within 24 hours of account creation.
- state=< on | off> -- An on/off switch for spam notifications. This is optional.
- text=<delete | default> | link:<the org which shares the notification text> | unlink -- The text parameter resets the organization's notification message to the default, shares the notification with another organization which can be modified by either org, unlink shared notifications. When unlinking shared notifications, the designated org keeps a copy of the notification, but it can not be updated by the other sharing org. This is optional.
- cc= <user address > -- The address of the user who will be cc'ed when the notification is sent. This address must be a valid user under the same email config. This is optional.

Authorization

- Read: Notification Messages, Edit Organizations (as a general rule)
- Write: Notification Messages, Edit Organizations (as a general rule)

Note: The authorizations are dependent upon the type of notification.

Classification

Batch organization management

Related Commands

Batch Commands: notification display

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “Quarantine Summaries and Notifications”

org_im_settings display

The org_im_settings display command displays all of the IM settings for an organization. This command applies to Postini IM Security, an optional product.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

`org_im_settings display orgtag=<org name>`

Example

```
org_im_settings display orgtag=sales
```

Description

Displays an im settings record for a given org:

- orgtag -- Name of the organization whose IM settings are being displayed.

Enclose <org name> in double quotes or preceded with a \' symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

Errors

Possible errors include:

"You don't have Instant Messenger feature."

"Please enter an orgtag"

"You have entered an invalid organization or one that you do not have permission over."

Return Values

From the Administration Console, the command returns:

```
im_enable: 1
im_proto_enable: +all
im_external_enable: 1
file_transfer_receive: internal_only
file_transfer_send: off
disposition custom journal: off
disposition standard journal: off
disposition archive: off
disposition email:
```

Authorization

- Read: IM Management
- Write: IM Management

Classification

Batch IM organization management

Notes

When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, im display, im list, im listforuser, listusers, modifyorg, user_im_settings add, user_im_settings delete, user_im_settings display, user_im_settings modify, org_im_settings modify

Related Fields

- Input: orgname, orgtag
- Output: custom_journal, file_transfer_receive, file_transfer_send, standard_journal, archive, im_enable, im_external_enable, im_proto_enable

See Also

[“Building a Batch File” on page 19](#)

[“Editing Message Archiving Settings” on page 564](#)

org_im_settings modify

The org_im_settings modify command modifies an organization's IM settings. This command applies to Postini IM Security, an optional product.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
org_im_settings modify orgtag=<org name>
[ , disposition=<null | off | archive | standard_journal | custom_journal>]
[ , disposition_email=<user address>]
[ , file_transfer_receive=< off | internal_only | include_external | null> ]
[ , file_transfer_send=< off | internal_only | include_external | null> ]
```

Example

```
org_im_settings modify orgtag=sales,
disposition="archive,standard_journal"
```

Description

Modifies an the organization im settings record for a given orgtag:

- orgtag -- The organization name
Enclose <org name> or <user address> in double quotes or preceded with a \' symbol if it contains a quote ('), double quote ("'), backslash (\), apostrophe, commas, #, = symbols.
- disposition -- The setting for the organization's IM archiving strategy.
- disposition_email -- The IM user's email address

Errors

Possible errors include:

"You don't have Instant Messenger feature."
"You have entered an invalid organization or one that you do not have permission over."
"You don't have permission ot perform this command."
"The proto_enable value must begin with +all or -all."
"Invalid protocol entered."
"Invalid external_enabled value."
"Journal email option is required."
"Invalid syntax for custom email address."

Return Values

"Org im settings record modified."

Authorization

- Read: IM Management
- Write: IM Management

Classification

Batch IM organization management

Notes

- The file transfer controls affect Yahoo!, AIM, and MSN. At this time, Google Talk transfers are blocked by default.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, im display, im list, im listforuser, listusers, modifyorg, user_im_settings add, user_im_settings delete, user_im_settings display, user_im_settings modify, org_im_settings display

Related Fields

- Input: address, file_transfer_receive, file_transfer_send
- Related: archive, custom_journal, orgname, standard_journal

See Also

"Building a Batch File" on page 19

"Editing Message Archiving Settings" on page 564

password force_update

The password force_update command forces a user or all users in an organization to change their passwords the next time the user logs into the system. This command is used with an organization using the PMP password policy configuration.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

password force_update user=<user address>

password force_update org=<org name> [, cascade= <yes | no>]

Example

- To force an individual user to change a password:

```
password force_update user=msmith@jumboinc.com
```

- To force all users in an organization to change their passwords:

```
password force_update org=Sales
```

- To force all users in an organization to change their passwords and include all users in sub-organizations:

```
password force_update org=Sales, cascade=yes
```

Description

Forces either a user or all users in an organization to change passwords. These can not be done at the same time.

- ‘cascade=yes’ -- All users in the sub-organizations are forced to change passwords. Use caution with this option. This will force password updates to all sub organizations regardless of individual user requirements.
- ‘cascade=no’ -- Only the initial organization user passwords will be updated. The sub-organizations are not reset.

Default: cascade = no

Note: Enclose <org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Errors

Return Values

Authorization

- Read: User Settings, Password, Change Admin Password (if the user is an administrator), Edit Organizations
- Write: User Settings, Password, Change Admin Password (if the user is an administrator), Edit Organizations

Classification

Batch organization management, and user management

Notes

When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: password reset, password_policy display, password_policy update

Related Fields

Input: address, orgname

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "User Authentication"

password reset

The password reset command resets a user's password. This command is used with an organization using the PMP password policy configuration.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
password reset user=<user address> [, password=<text>] [, notify=<yes | no>]
```

Example

- To reset an individual user's password to a randomly derived password using the organization's password policies:

```
password reset user=msmith@jumboinc.com
```

- To reset an individual user's PMP password to a specific password using the user's organization's password policies, and to send the user a notification of the password update:

```
password reset user=msmith@jumboinc.com, password=a8f2KTT*#,  
notify=yes
```

Description

Resets a PMP user's password.

- If a user and a clear text password are specified, this password is set following the user's organizational PMP password policies. If the password does not match the password policies, it is rejected and the user tries again.
- If a user is specified without a specific password, a randomly derived password will be generated using the organization's password policies.
- password -- A clear text password for a PMP user.

Note: A PMP password using the password policy configuration will not work with a single quote ('), a double quote ("'), a comma (,), or a backslash (/).

- 'notify=yes' -- The user or all users in an organization will be notified that the passwords have been updated.
- 'notify=no' -- No notification is sent to a user.

Default: notify=no

Errors

Possible error messages include:

Please specify a user.

Authorization

- Read: User Settings, Password, Change Admin Password (if the user is an administrator)
- Write: User Settings, Password, Change Admin Password (if the user is an administrator)

Classification

Batch organization management, and user management

Related Commands

Batch Commands: password force_update, password_policy display, password_policy update

Related Fields

Input: address

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “User Authentication”

password_policy display

The password_policy display command displays the password policy for an organization. This command is used with an organization using the PMP password policy configuration.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
password_policy display <org=<org name>> | <iid=<org ID>>
```

Example

```
password_policy display org=Sales
```

Description

Displays the password policy for an organization.

If a PMP password using the password policy configuration does not exist for this organization, the default settings are displayed. The default settings for a new user getting a PMP password policy configuration is different from the initial default settings of a current PMP user who has been moved to the PMP password policy configuration. See the Return Values section for details.

Enclose <org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Errors

Possible error messages include:

This org does not have the appropriate feature authorization.

If you have the wrong authorization privileges:

You do not have the proper authorization to perform password_policy display.

Return Values

In the Administration Console, this information is returned for the Sales organization.

- New user with the PMP password policy configuration default settings:

Organization: Sales
Contain at least 6 characters
Not exceed 32 characters
Not be a dictionary word
Not be your email address
Contain 3 of the 4 character types: English uppercase letters, English lowercase letters, numbers, and symbols (such as !, #, \$, %)

- Current PMP user (who has been moved to the PMP password policy configuration) default settings:

Organization: Sales
Contain at least 1 character
Not exceed 100 characters

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Classification

Batch organization management

Notes

When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: password force_update, password reset, password_policy update

Related Fields

Input: orgname

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “User Authentication”

password_policy update

The password_policy update command creates a password policy for a new organization or updates the password policy for an existing organization. This command is used with an organization using the PMP password policy configuration.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
password_policy update <org=<org name>> | <iid=<org ID>>  
[, min_length=<1 - 10 | null>]  
[, required_complexity=<no | yes | null>]  
[, max_login_attempts=<1 - 10 | null>]  
[, lockout_period=<1 - 999 number of minutes | null>]  
[, max_password_age=<1 - 999 number of days | null>]  
[, password_history=<0 | 1 - 24 | null>]  
[, cascade= <no | yes | null>]
```

Example

- The basic setting recommendation is for min_length=6 and required_complexity=yes. The remaining parameters should match your company's password policy.

```
password_policy update org=Sales, min_length=6,  
required_complexity=yes, lockout_period=60
```

Description

Updates the password policy for an existing organization, including sub-organizations if cascade is enabled. If a PMP password policy configuration does not exist for this organization, one is created with the default settings.

- <org name> -- The email config organization being updated.
- min_length -- The minimum number of characters in the password. The values can range from 1 to 10.

Default: min_length=6 (for new users of PMP password policy configuration)

Default: min_length=1 (for current PMP users who have migrated to the PMP password policy configuration)

- required_complexity=no or required_complexity=null -- The PMP password policy's complexity rules are not enabled. When a password is changed, it will not be compared against the complexity rules.

Default: required_complexity=no (for current PMP users who have migrated to the PMP password policy configuration)

- 'required_complexity=yes' -- The PMP password policy's complexity rules are enabled. If the new password does not match these rules, the new password will be rejected. This is the recommended setting. For more information on complexity rules see the Notes below.

Default: required_complexity=yes (for new users to the PMP password policy configuration)

- max_login_attempts -- The maximum number of allowed login attempts. The values can range from 1 - 10. If the value is null, no limit is placed on the number of login attempts. The login attempts are checked every 10 minutes. The recommended setting is to match your company's password policy.

Default: login_attempts=null

- lockout_period -- The lockout duration, in minutes. The lockout is triggered once the invalid log in threshold is reached. The values can be 1 - 999. After this period, a user is allowed to resume attempting to log in to the login window. If the value is null, an administrator will have to reset this value before the user can successfully attempt another login. The recommended setting is to match your company's password policy.

Default: lockout_period=10

- password_history -- The number of stored recently used passwords. The values can be 1 - 24. If 0, a new password is always accepted. New passwords can not match passwords in the password history

Default: password_history=0

- max_password_age -- The number of days this password will be valid. After this date, the password must be changed. On the final maximum day, the time of day the password expires is the same time of day used when the password was created. The numeric values can be 1 - 999. If null, the password never expires.

Default: max_password_age=null

- ‘cascade=no’ -- Sub organization passwords will not be updated with new changes.
- ‘cascade=yes’ -- Sub organization passwords will be updated. Use caution with this option. This will propagate the updates to all sub organizations regardless of individual users requirements.

Note: Enclose <org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Classification

Batch organization management

Notes

The rules of complexity are:

- Not be a dictionary word
- Not be the user’s email address (user name, domain, or whole address)
- Three of these four criteria must be met before a password is accepted. An example is a8f2KTT*#. The password candidate must include one or more:
 - Lower case English letters (A thru Z)
 - Upper case English letters (a thru z)
 - Numbers (0 thru 9)
 - Symbols, for example !#\$%

Note: A PMP password policy configuration will not work with a single quote (‘), a double quote (“), a comma (,), or a backslash (\).

- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: password force_update, password reset, password_policy display

Related Fields

Input: orgname

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “User Authentication”

promoteprovuser

The promoteprovuser command adds a provisional user to the Message Security service and removes the provisional user record. This command is used with SmartCreate.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

promoteprovuser <user address>

Example

```
promoteprovuser provuser@jumboinc.com
```

Description

Adds the provisional user to the Message Security service as a regular user, and removes the provisional user record.

Enclose <user address> in double quotes or preceded with a ‘` symbol if it contains a quote (‘), double quote (“”), backslash (\), apostrophe, commas, #, = symbols.

Authorization

- Read: Add Users
- Write: Add Users

Classification

Batch user management

Notes

- Used with SmartCreate, newly added users are unconfirmed provisional users and are promoted to a regular user after verified as associated with someone in your org by receiving 3 legitimate emails with a week. Once this criteria is met, the user is added to service. Otherwise the user is deleted.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `blockprovuser`, `deleteprovuser`, `displayprovuser`, `listprovusers`, `unblockprovuser`

Related Fields

Input: address

See Also

[“Building a Batch File” on page 19](#)

[“Editing Your Mail Handling Policies \(Non Account Bounce\)” on page 562](#)

[*The Message Security Administration Guide*, “Users and Quarantines”](#)

resetuser

The `resetuser` command resets most of a user's policy settings to the settings of the organization's Default User. This command can be used with any user, and is commonly used to reset a suspended user.

Syntax

```
resetuser <user address>
```

Example

```
resetuser msmith@jumboinc.com
```

Description

Resets most user fields for <user address> to the settings of the default user for the organization <user address> is in. This will clear most customizations made since the user was created. Below are the fields that do not change when a user is reset.

Note: Enclose <user address> in double quotes or preceded with a \' symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

The fields that do not change include:

address, creator, create_method (for users), created_ts (for users), iid, initial_password, user_id, orgid, welcome_count

Return Values

If `msmith@jumboinc.com` has been suspended, the reset command returns:

```
Reset user msmith@jumboinc.com.
```

Authorization

Write: Help Desk

Classification

Batch user management

Notes

When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: modifyuser, suspenduser

Related Fields

Input: address

See Also

“Building a Batch File” on page 19

“Resetting Users” on page 553

The Message Security Administration Guide, “Users and Quarantines”

setorgsubstripping

The setorgsubstripping command enables domain stripping for all domains in an organization.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

setorgsubstripping <org name | iid>,<1 | 0>

Example

```
setorgsubstripping sales,1
```

Description

Turns off/on stripping for users of all domains under an org and all domains under that org's sub organizations:

- <org name> -- The name of the organization associated with the domains to be stripped. Enclose <org name> in double quotes or preceded with a ‘` symbol if it contains a quote (‘), double quote (“”), backslash (\), apostrophe, commas, #, = symbols.
- ‘1’ -- Sub domain stripping is enabled
- ‘0’ -- Sub domain stripping is not available for this organization

Errors

"Please supply a valid sub-stripping value (0 or 1)" -- Do not use 'on' or 'off' with this command.

Return Values

If the `sales` organization domain substripping was enabled, the command would return:

```
Set sub-strip state of sales to 1.
```

Authorization

- Read: Edit Organizations
- Write: Edit Organization

Classification

Batch domain management

Notes

- Org Substripping enables subdomain stripping for all domains in a particular organization. For example, the `jumboinc.com` domain has subdomain stripping enabled. For the user `msmith@jumboinc.com`, messages to `msmith@corp.jumboinc.com` and `msmith@dev.jumboinc.com` would be filtered as configured for `msmith@jumboinc.com`.
- Use this command for stripping subdomains in an organization. For individual organizations and domains, use the '**substrip**' field with the **adddomain** command when creating the domain. Or, when editing an existing domain, use the '**substrip**' field with the **modifydomain** command.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `adddomain`, `modifydomain`

Related Fields

- Input: orgname, iid
- Related: substrip

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “Domains”

showallowedips

The showallowedips command lists all allowed sending domains and associated IPs configured in an organization.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Note: The iplock display command has replaced the showallowedips command. For more information, see iplock display.

Syntax

```
showallowedips <org name>
```

Example

```
showallowedips sales
```

Description

The showallowedips batch command lists all domain and associated IP addresses locked to an organization.

- <org name> -- The name of the organization where this configuration will be configured.

Enclose <org name> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Return Values

No Locked Domain:IP addresses

No ip / domain mappings present.

Locked Domain:IP addresses

domain.com -> 64.19.7.234/16

Authorization

- Read: Application Management, Junk Email Settings
- Write: Read-only for administrators

Classification

Batch IP management

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: adddomain, deletedomain, deletealias

Related Fields

- Input: orgname
- Related: is_email_config

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "IP Ranges and Security", and "Avoid Spoofing", and "Avoid Spoofing"

suspenduser

The suspenduser command suspends a user by disabling all filtering and the user's access to the Message Center.

Syntax

```
suspenduser <user address> [ , notify] [ , hardSuspend] [ , deliver]
```

Example

```
suspenduser msmith@jumboinc.com, hardSuspend  
suspenduser msmith@jumboinc.com, notify, hardSuspend, deliver  
suspenduser msmith@jumboinc.com
```

Description

Batch Interface Description for suspenduser

Suspends <user address>. All filtering is turned off/on. The user's access to the Message Center is disabled.

- <user address> -- The user whose filtering is being suspended.

Note: Enclose <user address> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("'), backslash (\), apostrophe, commas, #, = symbols.

- notify -- User receives Suspension notification explaining the suspension.

This is a positional parameter, and is optional. If used, the parameter must be at the end of the command. There is no numeric equivalent.

- hardsuspend -- User is flagged as not allowed to log into the Message Center. If the user has User Access modify privileges for Junk Email Settings or Virus Settings, you must select this option to prevent them from logging into the Message Center and re-enabling filtering.

This is a positional parameter and is optional. If used, the parameter must be at the end of the command.

- deliver -- Delivers all quarantined mail to the user's inbox before suspending the user. Virus infected email is not cleaned.

This is a positional parameter and is optional. If used, the parameter must be at the end of the command. There is no numeric equivalent.

EZCommand Description for suspenduser

See the Batch Interface Description for suspenduser for general usage details.

When used as an EZCommand, the command must be URL-escaped in order to properly submitted. For example:

```
suspenduser msmith@jumboinc.com, notify
```

changes to

```
suspenduser%20msmith%40jumboinc.com%20notify
```

Errors

Batch command interface errors:

- Possible errors include:

```
'No such user 'username' (unknown administrator address supplied).'  
'String authorization failed.'  
'No commands to process.'  
'Command not recognized: command.'  
'You don't have permission to insert users into org name.'  
'No such organization 'org name'.'  
'No default user available for organization org name.'  
'No secret key in database.'
```

- If suspending the user was not successful, possible errors are:

```
'No arguments supplied.'  
'No user 'username'.  
'You don't have permission to suspend user name.'
```

Return Values

Batch command interface return values:

- If `msmith@jumboinc.com` was suspended, this string is returned:

```
'Suspended user msmith@jumboinc.com.'
```

If a particular delivery was included, a `<delivery_status>` would be included after the user's name in the return value.

- When used as an EZCommand, the HTTP response will contain a two-part return value: `<status><message>`

status -- 1 for success or 0 for failure

message -- Contains errors and additional details

Authorization

Write: Help Desk

Classification

Batch user management; EZCommand-enabled

Notes

- Fully suspended users (users suspended using the batch command `suspenduser msmith@jumboinc.com, hardsuspend`) are not counted as accounts in the billing statements.
- To unsuspend users in the core batch environment, use the **resetuser** command. See the Task Example, “Resetting Users” on page 553, for more information.
- In addition when using a batch file, comments begin with a ‘#’ hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `adduser`, `deleteuser`, `displayuser`, `listusers`, `modifyuser`, `resetuser`

Related Fields

Input: address

See Also

“Building a Batch File” on page 19

“About EZCommand” on page 22

“Resetting Users” on page 553

The Message Security Administration Guide, “Users and Quarantines”

testfirewall

The testfirewall command tests whether your firewall allows email traffic from IP addresses outside of the Message Security service IP range.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
testfirewall <user address>
```

Example

```
testfirewall jumbomailserver@jumboinc.com
```

Description

Determines if connections to the mail server are not blocked by the firewall.

- <user address> -- Address of the user to be used as the test message recipient.

Enclose <user address> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("'), backslash (\`), apostrophe, commas, #, = symbols.

Return Values

- If your server is blocking connections from outside IP addresses, you will see a message saying the test passed.

```
Checking firewall from 12.158.34.71...passed (did not accept connection)
```

- If your server is accepting connections from outside of the IP addresses, you will see a message saying the connection was accepted. The test failed.

```
Checking firewall from 12.158.34.71...failed (accepted connection)
```

Authorization

- Read: Organization Management
- Write: Organization Management

Classification

Batch test management

Notes

- Malicious senders may attempt to send traffic directly to port 25 on your server, and bypass filtering and security. We recommend you configure your email server or firewall to accept traffic only from the Message Security service.
- When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

WARNING: You must be sure to add all of your domains to the Message Security service before locking down your firewall to accept only email traffic from the service IP range. Otherwise, email sent to unregistered domains may bounce.

Related Commands

Batch Commands: checklatency, checkroute, testmail, testmx

Related Fields

Input: address

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "Test Tools & Mail Flow Troubleshooting"

testmail

The testmail command verifies whether your email server can receive a message. This is the SMTP Message Test.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
testmail <user address>, mailtype=<1 | 0>
```

Example

```
testmail msmith@jumboinc.com, mailtype=1
```

Description

Sends a test email to the input email address. <user address>. The test generates an actual message. You should use an email address that is an account on your email server and is registered with the Message Security service.

- <user address> -- Address of the user to be used as the message recipient.
- 'mailtype = 0' -- Tests mail connectivity through the Message Security service to your mail server.
- 'mailtype=1' -- Tests mail generated by the Message Security service such as alerts, quarantine summaries, and quarantined messages. Used to send directly to the user's mail host.

Enclose <user address> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote (""), backslash (\), apostrophe, commas, #, = symbols.

Errors

When the SMTP Message test fails, you will see a summary similar to the successful test results. The last line of the summary points out where the transaction failed. For example:

```
Establish connection...
Sending HELO
```

HELO failed.

- SMTP Connection failed -- See *The Message Security Administration Guide*, "Troubleshooting Incoming Email Delivery" for full steps.
- HELO failed -- This usually indicates an issue with your mail server. Look at your mail server logs for the exact SMTP error it returned. This information will help you resolve this issue.
- MAIL FROM failed -- This indicates that your mail server will not accept the sender or timed out during this phase of the test. Look in your mail server logs for the exact SMTP error it returned. This information will help you resolve this issue.
- RCPT TO failed -- This usually indicates that your mail server rejected the recipient or timed out during this phase of the test. Does the recipient have an email box on the server? Look in your mail server logs for the exact SMTP error it returned.
- Sending message data failed -- This indicates that your mail server rejected the body of the email message or timed out during this phase of the test. Look at your mail server logs for the exact SMTP error it returned.

Return Values

- Successful test mail flow through the data center (mailtype=0) displays the following test summary:

```
Sending test mail to msmith@jumboinc.com:  
Establish connection...  
Sending HELO  
Sending MAIL FROM  
Sending RECPY TO  
Sending data  
End of data dot  
Success  
The email data center can deliver email to this email server from an  
external email server.
```

- Successful test of an email generated by the data center (mailtype=1):

```
Sending test email to msmith@jumboinc.com:  
Establish connection...  
Sending HELO  
Sending MAIL FROM  
Sending RECPY TO  
Sending data  
End of data dot  
Success  
The email data center can deliver email to this email server from an  
external email server.
```

- Successful test of an email from the Message Security service directly to your mail host:

```
Sending test email to msmith@jumboinc.com:  
Establish connection...  
Sending HELO  
Sending MAIL FROM
```

```
Sending RECPT TO  
Sending data  
End of data dot  
Success  
The email data center can deliver email to this email server.
```

In all 3 cases the recipient, `msmith@jumboinc.com`, will receive a test email message.

Authorization

- Read: User Settings
- Write: Read-only for administrators

Classification

Batch test management

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `checklatency`, `checkroute`, `testfirewall`, `testmx`

Related Fields

Input: address

See Also

"Building a Batch File" on page 19

The Message Security Administration Guide, "Test Tools & Mail Flow Troubleshooting"

testmx

The `testmx` command tests your MX records. This is the MX Record Test.

Syntax

testmx <domain name>

Example

testmx mailserver.jumboinc.com

Description

Checks the mail exchange record of the input domain, <domain name>.

- <domain name>= Name of the domain whose DNS MX entries you wish to test

Errors

Test Fails

- If the MX Record test fails for the selected domain, emails may not be filtered or even bounce. You will see the results of the test followed by the relevant parts of your DNS MX entries as seen by the DNS servers used by the Message Security service. For example:

```
testmx to jumboinc.com: No MX record found containing  
'sla2.psmtp.com'  
jumboinc.com IN MX 100 jumboinc.com.sla1.psmtp.com  
jumboinc.com IN MX 200 jumboinc.com.sla2.psmtp.com  
jumboinc.com IN MX 300 jumboinc.com.slb1.psmtp.com  
jumboinc.com IN MX 400 jumboinc.com.slb2.psmtp.com
```

- For ‘No MX record found containing ‘sNaM.psmtp.com’ or ‘No MX record found containing ‘sNbM.psmtp.com’ -- Add the appropriate entry. There should be one MX entry for each:

```
jumboinc.com IN MX 100 jumboinc.com.sNa1.psmtp.com  
jumboinc.com IN MX 200 jumboinc.com.sNa2.psmtp.com  
jumboinc.com IN MX 300 jumboinc.com.sNb1.psmtp.com  
jumboinc.com IN MX 400 jumboinc.com.sNb2.psmtp.com
```

Additional Errors

- Multiple MX records found containing ‘sNaM.psmtp.com’

or

Multiple MX records found containing 'sNbM.psmtp.com' -- Remove the duplicate entry listed.

- Unable to resolve 'jumboinc.com' -- Create a DNS MX entries for the domain on the authority DNS server. Currently no entries can be found. This may be a symptom of trouble with your authority DNS server.
- Non-psmtp MX record found: 'jumboinc.com' -- Either your DNS MX entries for the domain have not propagated to the Message Security service's DNS servers or you need to change the ID for your DNS MX entries to indicate to other servers that they need to ask your DNS server for new entries.
- Unable to retrieve MX records for 'jumboinc.com' -- This likely indicates trouble with one or all of your authority DNS servers.
- Priority of psmtp MX records must be higher than Customer MX records -- Change your DNS MX entries for the domain so that the Message Security service entries are higher than the entries which route to your mail server.

Return Values

Successful MX Record test showing mail from the selected domain is routing correctly to the Message Security service:

```
jumboinc.com: MX records OK.  
jumboinc.com IN MX 100 jumboinc.com.sla1.psmtp.com  
jumboinc.com IN MX 200 jumboinc.com.sla2.psmtp.com  
jumboinc.com IN MX 300 jumboinc.com.slb1.psmtp.com  
jumboinc.com IN MX 400 jumboinc.com.slb2.psmtp.com
```

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Read-only for administrators

Classification

Batch test management

Notes

Related Commands

Batch Commands: checklatency, checkroute, testfirewall, testmail

Related Fields

Input: domainname

See Also

“Building a Batch File” on page 19

The Message Security Administration Guide, “Test Tools & Mail Flow Troubleshooting”

unlockprovuser

The unlockprovuser command unblocks provisional users who have been blocked from becoming regular users. Provisional users are created with SmartCreate.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

unlockprovuser <user address>

Example

```
unlockprovuser msmit@jumboinc.com
```

Description

Re-activates a blocked provisional user.

Enclose <user address> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Authorization

- Read: Add Users
- Write: Add Users

Classification

Batch user management

Notes

- Used with SmartCreate, newly added users are unconfirmed provisional users. These users are promoted to regular user after verified as associated with someone in your org by receiving 3 legitimate emails within a week. Or the user can be blocked or unblocked from being added to the Message Security service. Once the email criteria is met, the user is added to service. Otherwise the user is deleted.
- When using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: `blockprovuser`, `deleteprovuser`, `displayprovuser`, `listprovusers`, `promoteprovuser`

Related Fields

Input: address

See Also

"Building a Batch File" on page 19

Task Examples: "Editing Your Mail Handling Policies (Non Account Bounce)" on page 562

The Message Security Administration Guide, "Users and Quarantines"

user_im_settings add

The `user_im_settings add` command adds an IM settings record for a given user email address. Postini IM Security is an optional product.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
user_im_settings add address=<user address>,
external_enable=<on | off>,
proto_enable=<+ | ->all | aim | msn | yahoo | google>
```

Example

```
user_im_settings add address=msmith@jumboinc.com, external_enable=on,
proto_enable=+all
```

Description

Adds an user im settings record for a given user address.

- address -- Address of user email

Note: Enclose <user address> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote (""), backslash (\), apostrophe, commas, #, = symbols.
- external_enable=on -- Enables IM users to communicate outside of your organization
- external_enable=off -- Disables IM communication outside of your organization
- proto_enable=<+ | -> -- adds or removes a protocol

Errors

Possible errors include:

"You don't have Instant Messenger feature."
"Please enter the address to add the user im settings record."
"Cannot find the user with address"
"You don't have permission to perform this command."
"User Im Settings record already exists for this user."
"The proto-enable value must begin with +all or -all."
"Invalid protocol entered."
"Invalid external_enable value."

Return Values

"User im settings record added."

Authorization

- Read: IM Management
- Write: IM Management

Classification

Batch IM user management

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, im delete, im display, im list, im listforuser, listusers, modifyorg, user_im_settings delete, user_im_settings display, user_im_settings modify, org_im_settings display, org_im_settings modify

Related Fields

Input: address, im_external_enable, im_proto_enable

See Also

"Building a Batch File" on page 19

user_im_settings delete

The user_im_settings delete command deletes an IM settings record for a given user email address. Postini IM Security is an optional product.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

user_im_settings delete address=<user address>

Example

```
user_im_settings delete address=msmith@jumboinc.com
```

Description

Deletes an user im settings record for a given user address.

- address -- Email address of the user.

Enclose <user address> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

Errors

Possible errors include:

"You don't have Instant Messenger feature."
"Please enter the address to delete the user im settings record."
"Cannot find the user with address"
"You don't have permission to perform this command."
"User im settings record not deleted because im names exist for this user."

Return Values

"User im settings record deleted."

Authorization

- Read: IM Management
- Write: IM Management

Classification

Batch IM user management

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, im delete, im display, im list, im listforuser, listusers, modifyorg, user_im_settings add, user_im_settings display, user_im_settings modify, org_im_settings display, org_im_settings modify

Related Fields

Input: address

See Also

“Building a Batch File” on page 19

user_im_settings display

The user_im_settings display command displays IM settings for a given user email address. Postini IM Security is an optional product.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

`user_im_settings display address=<user address>`

Example

```
user_im_settings display address=msmith@jumboinc.com
```

Description

Displays user's im settings for a given address.

- address -- Email address of the user

Enclose <user address> in double quotes or preceded with a ‘\’ symbol if it contains a quote (‘), double quote (“), backslash (\), apostrophe, commas, #, = symbols.

Errors

Possible errors include:

"You don't have Instant Messenger feature."
"Please enter the address to display the user im settings record."
"Cannot find the user with address"
"You don't have permission to perform this command."
"No Such User."

Return Values

u_id
address
external_enable
proto_enable
file transfer receive
file transfer send

Authorization

- Read: IM Management
- Write: IM Management

Classification

Batch IM user management

Notes

In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, im delete, im display, im list, im listforuser, listusers, modifyorg, user_im_settings add, user_im_settings delete, user_im_settings modify, org_im_settings display, org_im_settings modify

Related Fields

- Input: address
- Output: address, file_transfer_receive, file_transfer_send, im_external_enable, im_proto_enable, u_id

See Also

“Building a Batch File” on page 19

user_im_settings modify

The user_im_settings modify command modifies IM settings for a given user email address. Postini IM Security is an optional product.

This command is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
user_im_settings modify address=<user address>,
external_enable=<on | off>,
proto_enable=< + | - >all | aim | msn | yahoo | google>
[, file_transfer_receive=< off | internal_only | include_external >]
[, file_transfer_send=< off | internal_only | include_external >]
```

Example

```
user_im settings modify address=msmith@jumboinc.com,
external_enable=on, proto_enable=+all,
file_transfer_receive=internal_only, file_transfer_send=off
```

Description

Modifies an user im settings record for a given user address.

- address -- Email address of user

Note: Enclose <user address> in double quotes or preceded with a '\` symbol if it contains a quote ('), double quote ("), backslash (\), apostrophe, commas, #, = symbols.

- external_enabled=on -- Enables IM users to communicate outside of your organization
- external_enabled=off -- Disables IM communication outside of your organization
- proto_enabled -- Either adds or removes a protocol
- file_transfer_receive -- Enables receiving IM file transfers internally within the organization or to everyone.
- file_transfer_send -- Enables sending IM file transfers internally within the organization or to everyone.

Errors

Possible errors include:

```
"You don't have Instant Messenger feature."  
"Please enter the address to modify the user im settings record."  
"You don't have permission to perform this command."  
"The proto_enable value must begin with +all or -all."  
"Invalid protocol entered."  
"No User Im Settings record already exists for this user."  
"Invalid external_enable value."
```

Return Values

```
"User im settings record modified."
```

Authorization

- Read: IM Management
- Write: IM Management

Classification

Batch IM user management

Notes

- New IM record values are inherited from the user's org im settings.
- In addition when using a batch file, comments begin with a '#' hash symbol. If not on a separate line, the hash symbol could be interpreted as part of a user or organization name.

Related Commands

Batch Commands: iplock add_range, im delete, im display, im list, im listforuser, listusers, modifyorg, user_im_settings add, user_im_settings delete, user_im_settings display, org_im_settings display, org_im_settings modify

Related Fields

Input: address, file_transfer_receive, file_transfer_send, im_external_enable, im_proto_enable

See Also

"Building a Batch File" on page 19

Chapter 6

Batch Organization Fields

About Batch Organization Fields

The batch organization fields hold org-level data which a command can either create, delete, display, list, or modify. This information is diverse. It can be names, email addresses, numbers, dispositions, on/off switches, boolean true/false values.

Organization Field Reference Page Syntax Notations

Each field's syntax section uses notation and punctuation to show you where to put your specific information, and what information is required or optional:

The reference pages use the Administration Console syntax and have an example for each field:

- The field name is required. In the Administration Console, commas are required.
- Information between '< >' symbols means you need to add your specific information here. (for example: <field>=<value> becomes approved_senders=+mary@hugeisp.com)
- Information between '[]' square brackets mean this type of information is optional.
- A choice of values are separated by '|'. (for example: async_bounce= <on | off | NULL > means you have a choice of async_bounce=on,async_bounce=off, or async_bounce=NULL.)
- Some fields have '+' or '-' notations. Read the field description and examples carefully to understand what these notations mean for that particular field.
- It is important to confirm you have authorization to display or edit a field (Read/Write authorization). The Authorization section shows each field's requirements.
- The Related Commands section shows which commands take the field as input or as output. Input means the field is used in the command's arguments. Output means the command returns this field-value pair when the command is successfully executed.

See “Batch Command and Field Quick Summary” on page 27, and “Batch Field Quick Summary” on page 111 for additional information.

antivirus_sensitivity

The antivirus_sensitivity field is a flag indicating the strength of virus blocking allowed for this organization.

Syntax

```
antivirus_sensitivity=<normal | aggressive>
```

Examples

- When the field is returned as output:

```
antivirus_sensitivity 0 (normal)
```

- To change the setting:

```
modifyorg sales, antivirus_sensitivity=16
```

Description

Flag indicating whether virus cleaning is allowed for this organization.

- normal /0/NUL-- Virus sensitivity is at the normal strength for this organization. The normal strength value can be the string `normal`, 0, or NULL. We recommend using the string `normal` since it is easier to read. This is the default.
- aggressive/16 -- Virus sensitivity is at the aggressive strength for this organization. The aggressive strength value can be the string `aggressive` or 16. We recommend using the string `aggressive` since it is easier to read.

Field Type

Org-level

Authorization

- Read: Virus
- Write: Virus

Related Commands

- Input: `modifyorg`
- Output: `displayorg`

Related Fields

`disposition_virus`, `timezone` (for orgs), `virus_notify` (for orgs)

See Also

“Viewing Your Organization’s Sender Lists” on page 554

“Adding Users and Domains to Sender Lists” on page 555

The Message Security Administration Guide, “Virus Blocking”

approved_senders (for orgs)

The approved_senders field holds an email address or domain to be added or removed from the organization-level Approved Senders list.

Syntax

```
approved_senders=<[+] | -email address>, ... | <[+] | -domain name>, ... |<empty>
```

Examples

- When field is returned as output:

```
approved_senders jim@hugeisp.com
```

- Adding a sender to the org's Approved Senders list, either is correct:

```
modifyorg sales, approved_senders=+jim@hugeisp.com  
modifyorg sales, approved_senders=jim@hugeisp.com
```

- Removing a sender from a org's Approved Senders list:

```
modifyorg sales, approved_senders=-jim@hugeisp.com
```

- Adding a domain and removing a domain from the org's Approved Senders list, either is correct:

```
modifyorg sales, approved_senders="+jumboinc.com,-hugeisp.com"  
modifyorg sales, approved_senders="jumboinc.com,-hugeisp.com"
```

- See [approved_senders \(for users\)](#) for examples of adding senders to the user's Message Center Approved Senders list.

Description

Addresses and domains can be added or removed from the org-level Approved Senders list:

- Each address or domain needs its own operator (+ or -). The + symbol is optional. The - symbol is required.
- empty -- The field is not active.
- Lists of addresses or domains are comma delimited, and must be enclosed in quotes.

Example:

```
approved_senders="+jumboinc.com,-hugeisp.com"
```

Field Type

Org-level

Authorization

- Read: Junk Email
- Write: Junk Email

Notes

- Mail from senders on this list will bypass the Junk Email filters.
- Entries apply to all users in the organization, but are not visible to the organization's users allowing the administrator to customize the lists between organizations.
- If virus blocking is enabled for the recipient, message will not be delivered even though on the Approved Senders list. See the organization-level **disposition_virus** field for more information.
- At the organization-level, the Blocked Senders list overrides the Approved Senders list. At the user-level, the Approved Senders list overrides the Blocked Senders list. The user-level Approved Senders list overrides the organization-level Blocked Senders list.
- Adding or deleting a domain applies to subdomains. For example, approving the domain jumboinc.com also approves the subdomain sales.jumboinc.com.
- Org-level sender lists do not validate the sending email server against the domain
- IP addresses can not be added to the Approved Senders list. See the addallowedip command for more details.
- Approved and Blocked Senders lists have a size limit of 4000 characters which approximately equates to 100 to 130 addresses and domains per list.

Related Commands

- Input: addorg, modifyorg, modifyuser (approved_senders for users)
- Output: displayorg
- Related: adddomain

Related Fields

approved_recipients (users), approved_senders (for users), blocked_senders (for orgs), blocked_senders (for users)

See Also

- “Viewing Your Organization’s Sender Lists” on page 554
- “Adding Users and Domains to Sender Lists” on page 555
- “Viewing Message Center Settings” on page 536
- The Message Security Administration Guide*, “Approved and Blocked Sender Lists”

archive

The archive field lists whether archiving is on or off for an organization. This field applies to Postini Message Archiving, which is only used with Message Security installations.

Syntax

archive=<on/1 | off/0 | NULL ()>

Examples

When field is returned as output:

```
archive 1 (on)
```

Description

Lists archiving state

- on/1 -- Archiving is on for this organization.
- off/0 -- Archiving is off for this organization.
- NULL () -- This field is not active.

Default: archive=off

Field Type

Org-level

Authorization

- Read: Edit organizations
- Write: Edit organizations

Notes

The archive field is the same value as the **archive_enable** field which is used by the archive_settings commands.

Related Commands

- Output: displayorg, modifyorg, org_im_settings display
- Related: archive_settings display, archive_settings modify

Related Fields

archive_enable, custom_journal, retention_months, standard_journal

See Also

“Editing Message Archiving Settings” on page 564

Postini Message Archiving Administration Guide

archive_enable

The archive_enable field enables archiving to be on or off for an organization. This field applies to Postini Message Archiving, which is only used with Message Security installations.

Syntax

archive_enable=<on | off | NULL>

Examples

- When the field is returned as output, example as empty:

```
archive_enable NULL
```

- To change the setting:

```
archive_settings modify org=Jumbo ABC, archive_enable=on,  
mail_flow=on, journaling=on
```

Description

Lists archiving state

- on -- Archiving is on for this organization.
- off -- Archiving is off for this organization.
- NULL -- This field is not active.

Default: off

Field Type

Org-level

Authorization

- Read: Edit organizations
- Write: Edit organizations

Notes

- When archiving is enabled, mail_flow and journaling must be on.
- The archive_enable field is the same value as the **archive** field used by the displayorg, modifyorg, and org_im_settings display commands.

Related Commands

- Input: archive_settings modify
- Output: archive_settings display

Related Fields

archive, mail_flow, journaling, retention_months

See Also

[Editing Message Archiving Settings](#)

[Postini Message Archiving Administration Guide](#)

async_bounce

The `async_bounce` field lists whether the Connection Manager's Asynchronous Bouncing control is activated for inbound traffic. This control is for email servers that issue “unknown user” bounce messages asynchronously and require added security.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
async_bounce=on | off | NULL ()
```

Examples

- When the field is returned as output:

```
async_bounce NULL()
```

- To turn the feature on:

```
modifyorg sales, async_bounce=on
```

Description

Used for email servers such as Microsoft Exchange and qmail that accept inbound mail before validating and possibly sending a bounced “unknown user” reply.

- on -- By activating this feature, the Message Security service will compare directory information with incoming recipients to measure erroneous delivery attempts.
- off -- Turns this feature off for the org.
- NULL ()-- This field is not active.

Field Type

Org-level

Authorization

- Read: Auto Connection Manager
- Write: Auto Connection Manager

Notes

When activating this service, it is important to keep your user list up to date to avoid Directory Harvest Attacks (DHA) false positives.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

blatant_spam, non_account_bounce, ndr

See Also

“Viewing Your Organization’s Sender Lists” on page 554

The Message Security Administration Guide, “Connection Manager”

at_notify_on

The at_notify_on field shows the recipient notification status for messages quarantined by the Inbound Attachment Manager.

Syntax

at_notify_on=< 0 | 1 | 2 | 3 | NULL ()>

Examples

- When the field is returned as output:

```
at_notify_on NULL()
```

- To turn the recipient notification on:

```
modifyorg sales, at_notify_on=1
```

Description

Notification sent to recipient of Inbound Attachment Manager notifications:

- 0 (Off) -- Notification is turned off for the org
- 1 (Send to Redirect) - If your spam filters are configured to deliver all user spam to a single administrator's quarantine, the notification is sent to this administrator. This is also known as a redirect to the Attachment Manager Quarantine Redirect address.
- 2 (Send to User) -- Notification sent to the user
- 3 (Send to Both) -- Notification sent to both the user and the redirect address
- NULL() -- This field is not active.

Note: The field values are case sensitive. The values can have double quotes. ("Send to Redirect")

Field Type

Org-level

Authorization

- Read: Notification Messages
- Write: Notification Messages

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

max_message_size, out_at_notify_on (Outbound field),
outbound_max_message_size, qsum_actionable, qsum_enable, qtine_redir_atq,
qtine_redir_out_atq, qtine_redir_ndr

See Also

The Message Security Administration Guide, “Quarantine Summary & Notifications”

authentication_data

The authentication_data field holds the text used for non-PMP authentication of users and administrators when logging into the Message Center or Administration Console.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
authentication_data= <XAuth string | NULL>
authentication_data=<POP mail server | NULL>
authentication_data=<POP mail server, < @ | +domain extension>
authentication_data=<POP mail server, <@ | +USERDOMAIN>
```

Examples

- When the field is returned as output:

```
authentication_data NULL
```

- To change an organization's POP authentication to a POP server configured to authenticate the POP server machine name or IP address:

```
modifyorg sales, authentication_data="mypass"
```

- To change an organization's POP authentication to a POP server configured to authenticate the POP server machine name and the user's domain name, using two possible domain syntax:

```
modifyorg sales, authentication_data="mypass, @jumboinc.com"
modifyorg sales, authentication_data="mypass, +jumboinc.com"
```

- To change an organization's POP authentication to a POP server configured to authenticate the POP server machine name and several user domain names, using two possible domain syntax:

```
modifyorg sales, authentication_data="mypass, @USERDOMAIN"
modifyorg sales, authentication_data="mypass, +USERDOMAIN"
```

- Add an org with POP authentication:

```
addorg sales, parent=Jumbo Inc, authentication_data="mypass,
@jumboinc.com"
```

Description

String holding the text that is used to validate users in a non-PMP authenticated organization which are either POP or XAuth. To enable XAuth, a request must be submitted through a support ticket.

- XAuth Authentication -- <a non-hashed authstring>

Example of Syntax:

```
authentication_data=<shared secret><user@domain.com>
```

- When used with an EZCommand solution, the authstring is URL escaped. See “EZCommand Reference” on page 24. POP Authentication has three cases:
 - <mail server> -- Used when the POP server is configured only to authenticate the POP server’s machine name or IP address.
 - <mail server>,<@ | +domain extension> -- Used when the POP server is configured to authenticate the POP server and a user’s domain. The domain can have either ‘@’ or ‘+’ symbols.
 - <mail server>,<@ | +USERDOMAIN> -- Used when the POP server is configured to authenticate the POP server and several user domains. This is for organizations with multiple domains and need to pass each domain to the POP server. The USERDOMAIN variable can be have either ‘@’ or ‘+’ symbols.

Example:

```
authentication_data="@jumboinc.com"
```

- NULL -- This field is not active.
- Lists are comma delimited, and must be enclosed in double quotes.

Example:

```
authentication_data="@hugeisp.com,@jumboinc.com"
```

WARNING: POP authentication will fail when the USERDOMAIN syntax is used when the domain your POP server authenticates does not match the domain of the user address.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

POP authentication is the only authentication method compatible with the **blatant_spam** field.

Related Commands

- Output: displayorg
- Input: addorg, modifyorg

Related Fields

authentication_type, blatant_spam, initial_password (for users), password, remotecmd_secret

See Also

“Viewing Your Organization’s Sender Lists” on page 554

“Viewing Authentication and Password Settings” on page 540

The Message Security Administration Guide, “User Authentication”

authentication_type

The authentication_type field holds the type of authentication protocol used by an organization.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

authentication_type = < 1 | 4 | 5 >

Examples

When the field is returned as output:

```
authentication_type 1 (PMP)
```

Description

Defines the type of authentication used by an organization:

- 1 = Privately Managed Passwords, (PMP)
- 4 = POP Authentication, (POP)
- 5 = SHA1 Cross-Authentication, (XAuth)

Note: To change your authentication type, please contact your support representative.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Read-only for administrators

Notes

This field is useful with the **authentication_data** field. The authentication_type field helps determine what type of password string should be used in the authentication_data field.

Related Commands

Output: displayorg

Related Fields

authentication_data, initial_password (for users), password

See Also

“Viewing Your Organization’s Sender Lists” on page 554

“Viewing Authentication and Password Settings” on page 540

The Message Security Administration Guide, “User Authentication”

autocreate_web

The autocreate_web field determines whether users can be automatically created when the organization is using POP authentication. This is the Web Autocreate feature. After an organization's Authentication Method is set to POP and the Authentication Data is configured, an administrator can either enable user autocreation or not. For this autocreation method, a user is added automatically to the Message Security service when first logging in to the Message Center.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
autocreate_web=<off/0> | <on/1>
```

Examples

- When calling the field:

```
modifyorg sales, autocreate_web=off
```

- When the field is returned:

```
autocreate_web 0 (off)
```

Description

Users are created on successful authentication to the Message Center:

- off -- Turns this feature off for the org.
- on -- Unrecognized users in these domains are added automatically to the Message Security service when they first log in to the Message Center.

Note: The numeric equivalents to 'on' and 'off' are useful for debugging purposes. For robust production code, use the text value, 'on' or 'off'.

Field Type

Org-level

Authorization

- Read -- Edit Organizations
- Write -- Edit Organizations

Notes

- Applies only if the organization has associated domains.
- Web Autocreate works only for orgs that use POP Authentication.
- Web Autocreate does not work if the org is an email server config.
- Users are added to the organization associated with the domain.
- After enabling, send a message to users requesting that they log in to the Message Center to activate their own spam filtering account.

Related Commands

Input: modifyorg

Related Fields

async_bounce, authentication_data

See Also

“Viewing Your Organization’s Sender Lists” on page 554

The Message Security Administration Guide, “Organization Management”

blatant_spam

The blatant_spam field lists the activation status for Blatant Spam Blocking which bounces or blackholes (deletes) obvious spam before it reaches your email servers.

Syntax

blatant_spam=<OFF | blackhole | ERROR 571 Message Refused | NULL>

Examples

- When the field is returned as output:

```
blatant_spam blackhole
```

- To change the setting:

```
modifyorg sales, blatant_spam=blackhole
```

Description

Turns OFF, deletes <blackhole>, or bounces <ERROR 571 Message Refused> the most obvious spam before it reaches the email servers:

- OFF or NULL-- Turns this feature off for the org
- blackhole -- Deletes obvious spam without sending a return error
- ERROR 571 Message Refused -- Bounces obvious spam back to the sender with the error message

Field Type

Org-level

Authorization

- Read -- Junk Email
- Write -- Junk Email

Notes

- Messages from approved senders or containing approved content bypass all spam filtering including Blatant Spam Blocking.
- Depending upon your service package, Blatant Spam Blocking might always be set to blackhole disposition.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

spam_notify_on, tagonly_spam

See Also

The Message Security Administration Guide, “Spam Filters”

blocked_senders (for orgs)

The blocked_senders field lists an email address or a domain to be added or removed from the organization-level Blocked Senders list. All messages from these senders or domains will be quarantined.

Syntax

```
blocked_senders=< [+] | -emailaddress> | < [+] | -domain name | empty>,...
```

Examples

- When returning the field as output, and the value is empty:

```
blocked_senders empty
```

- Adding a sender to the org's Blocked Senders list, either is correct:

```
modifyorg sales, blocked_senders=+jim@hugeisp.com  
modifyorg sales, blocked_senders=jim@hugeisp.com
```

- Removing a sender from the org's Blocked Senders list:

```
modifyorg sales, blocked_senders=-jim@hugeisp.com
```

- Adding a domain and removing a domain from a Blocked Senders list, either is correct:

```
modifyorg sales, blocked_senders="+jumboinc.com,-hugeisp.com"  
modifyorg sales, blocked_senders="jumboinc.com,-hugeisp.com"
```

Note: See blocked_senders (for user Blocked Sender lists) for examples of blocking senders from the user's Message Center Blocked Senders list.

Description

Addresses and domains can be added or removed from the Blocked Senders list:

- Each address or domain needs its own operator (+ or -). The + symbol is optional. The - symbol is required.
- empty -- This field is not active.
- Lists of addresses or domains are comma delimited, and must be enclosed in quotes.

Field Type

Org-level

Authorization

- Read: Junk Email
- Write: Junk Email

Notes

- Entries apply to all users in the organization, but are not visible to the organization's users allowing the administrator to customize the lists between organizations.
- At the organization-level, the Blocked Senders list overrides the Approved Senders list. At the user-level, the Approved Senders list overrides the Blocked Senders list. The user-level Approved Senders list overrides the organization-level Blocked Senders list.
- Adding or deleting a domain from the list applies to subdomains. For example, approving the domain jumboinc.com also approves the subdomain sales.jumboinc.com.
- If an organization has Industry Heuristics turned on, messages with industry content will still be quarantined if the sender or domain is in organization's Blocked Senders list.
- IP addresses can not be added to the Blocked Senders list. See the addallowedip command for more details.
- Blocked Senders lists have a size limit of 4000 characters which approximately equates to 100 to 130 addresses and domains per list.
- Top Level Domain (TLD) can not be blocked using an organization-level Blocked Senders list (.com, .edu, .uk).

Related Commands

- Output: displayorg
- Input: modifyorg
- Related: adddomain, modifyuser

Related Fields

approved_senders (for users), blocked_senders (for users), approved_recipients

See Also

"Viewing Your Organization's Sender Lists" on page 554

“Adding Users and Domains to Sender Lists” on page 555

“Viewing Message Center Settings” on page 536

The Message Security Administration Guide, “Approved and Blocked Sender Lists”

bounce_fragments

The bounce_fragments field enables partial message fragments to be received or bounced.

Syntax

```
bounce_fragments=<on | off | NULL ()>
```

Examples

- When the field is returned as output:

```
bounce_fragments NULL ()
```

- To modify the company name:

```
modifyorg sales, bounce_fragments=on
```

Description

Enables partial message fragments to be quarantined or bounced:

- on -- Message fragments are bounced with a 571 error.
- off -- Message fragments are quarantined

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Related Commands

- Output: displayorg
- Input: addorg, modifyorg

See Also

The Message Security Administration Guide, “Organization Management”

company_name

The company_name field holds the company or entity name that is used in email notifications.

Syntax

company_name=<text>

Examples

- When the field is returned as output:

```
company_name "Jumbo Inc"
```

- To modify the company name:

```
modifyorg sales, company_name=Jumbo Inc
```

Description

Company or entity name that is used in the email notifications.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Related Commands

- Output: displayorg
- Input: modifyorg

See Also

“Viewing Authentication and Password Settings” on page 540

“Seeing if a User Has Received a Welcome Notification” on page 547

The Message Security Administration Guide, “Organization Management”

create_method (for orgs)

The create_method field shows how an organization was created.

Syntax

create_method = 2 | 3

Examples

```
create_method = 2
```

Description

Describes how an organization was created:

- 2 -- Created in the Administration Console
- 3 -- Created by the **addorg** batch command

Field Type

Org-level

Authorization

- Read: Org Management
- Write: Read-only for administrators

Notes

- This field only applies to deployments of Perimeter Manager Enterprise Edition, Release 5.0 and later. This includes Message Security for Enterprises.
- Organizations created during a Directory Sync synchronization are created by the addorg command, and the organizations' create_method field value is 3. Directory Sync is an optional feature.

Related Commands

- Output: displayorg
- Related: displayuser

Related Fields

created_date, created_date (for users), created_ts (for users)

See Also

The Message Security Administration Guide, “Organization Management”

created_date

The created_date field holds the creation time stamp for an organization.

Syntax

created_date=<date>

Examples

```
created_date 1145962000
```

Description

Creation time stamp for the organization represented in UNIX seconds.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Read-only for administrators.

Notes

This field only applies to deployments of Perimeter Manager Enterprise Edition, Release 5.0 and later. This includes Message Security for Enterprises

Related Commands

Output: displayorg

Related Fields

create_method (for orgs), create_method (for users), created_date (for users), created_ts (for users)

See Also

The Message Security Administration Guide, “Organization Management”

creator

The creator field lists the ID and name of the administrator who created the organization.

Syntax

creator=<user address | NULL (none)>

Examples

- When the field is returned as output:

Description

The creator field lists the user ID and address of the administrator who created the organization.

- NULL (none) -- This field is not active.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Read-only for administrators

Related Commands

Output: displayorg

See Also

The Message Security Administration Guide, “Organization Management”

custom_journal

The custom_journal field is an on/off switch for IM conversations sent to the IM administrator’s email address. This field applies to Postini IM Security, an optional product.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

custom_journal= < on | off >

Examples

- When the field is returned as output:

```
custom_journal on
```

- To change the setting:

```
org_im_settings modify orgtag=sales,  
disposition="archive,cuztom_journal"
```

Description

On and Off switch for IM conversations sent to IM administrator's email.

- on -- Enables IM conversations to be sent to admin's email address
- off -- Disables IM conversations to be sent to admin's email address
- Enclose a disposition list in double quotes if it contains commas.

Field Type

Org IM management

Authorization

- Read: IM Management
- Write: IM Management

Notes

An organization's IM conversations are journaled by being sent as email to participants and/or text of the conversation is sent directly to the Message Archiving for storage:

- Standard journaling -- IM conversation text is sent as an email message to all conversation participants who are in this user's organization. This is equivalent to the 'Standard Email' feature in the Administration Console.
- Custom journaling -- IM conversations are sent as an email message to an administrator's email address. This is equivalent to the 'This email address' feature in the Administration Console.
- Message Archiving -- IM conversations are sent directly to Message Archiving for storage. Available for Message Archiving customers only.

Related Commands

- Input: org_im_settings modify
- Output: org_im_settings display

Related Fields

archive, standard_journal

See Also

“Editing Message Archiving Settings” on page 564

Postini Message Archiving Administration Guide

default_message_limit

The default_message_limit field holds the maximum number of messages each registered user or alias in an organization can receive per day.

Syntax

default_message_limit=<0 - 99999999 | NULL>

Examples

- When the field is returned as output:

```
default_limit NULL
```

- To change the default message limit:

```
modifyorg sales1, default_message_limit=1000
```

Description

Default limit to number of messages per day for users in this organization.

- NULL -- No limit is imposed.

Field Type

Org-level

Authorization

- Read: Traffic Limits
- Write: Traffic Limits

Notes

- When exceeded, incoming messages are bounced, returning a 554 Mailbox limit exceeded error message to the sender.
- Setting a message limit is useful for protecting mail servers against malicious attacks.
- All messages are counted against this limit, including legitimate and quarantined messages.
- The count is approximate, so it's suggested only for values over 100.
- This limit can also be applied to the individual users. Whichever limit is lower (the org limit or the user limit) applies for the user. If a user's limit is blank and a value is set for the org, the org value applies to the user.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

message_limit (for users)

See Also

“Viewing Message Center Settings” on page 536

The Message Security Administration Guide, “Organization Management”

default_user

The default_user field lists the name of the organization's Default User template used when creating a new user in this org.

Syntax

```
default_user=<pdefault@<domain> | postinidefault@<domain> |  
<name>@<domain>
```

Examples

- When assigning the field:

```
modifyorg sales, pdefault@jumboinc.com
```

- When the field is returned as output (using Administration Console syntax):

```
default_user 200122277 (pdefault@jumboinc.com)
```

Description

The existing user template with user-level settings applied to a new user for this organization.

- pdefault@<your domain> -- The initial Default User residing at the top-level Account org. This user is not billed.
- postinidefault@<your domain> -- Another reserved name for a Default User. This user is not billed.
- <name>@<your domain> -- If a user's address is designated in the default_user field, this user is no longer a standard user, but rather a Default User template. This Default User is not billed.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

- Every org containing users must have a Default User.
- You can create additional Default Users, give them unique settings, and assign them to separate orgs. New users in these orgs get the unique settings.

Related Commands

- Output: displayorg
- Input: modifyorg

See Also

“Message Center Settings and Password Examples” on page 536

“Viewing Message Center Settings” on page 536

“Resetting Users” on page 553

The Message Security Administration Guide, “Users and Quarantines”

disable_first_spam

The disable_first_spam field is an organization-level activation switch for a new user’s notification telling the user the first spam message has been quarantined in the user’s Message Center.

Syntax

disable_first_spam=<0/on | 1/off | NULL ()>

Examples

- When the field is returned as output:

```
disable_first_spam 0 (on)
```

- To change the disable setting:

```
modifyorg sales, disable_first_spam=1
```

Description

Switch for first spam notification.

- 1/off -- The first spam notification will be sent to users in this organization. This is the default setting.
- 0/on-- The first spam notification will not be sent to users in this organization.
- NULL () -- This field is not active.

Default: disable_first_spam=1

Field Type

Org-level

Authorization

- Read -- Notification Messages
- Write -- Notification Messages

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

welcome_on

See Also

“Viewing Authentication and Password Settings” on page 540

“Seeing if a User Has Received a Welcome Notification” on page 547

“Resending the Welcome Notification” on page 548

The Message Security Administration Guide, “Quarantine Summary & Notifications”

disposition_virus

The disposition_virus field holds the disposition status of an email containing a virus. The disposition can be either redirected, deleted, quarantined, or tagged as a virus in the message email headers.

Syntax

```
disposition_virus=<redirect | quarantine | blackhole | tagonly | NULL ()>
```

Examples

- When the field is returned as output, for example empty:

```
disposition_virus h (blackhole)
```

- To change the disposition:

```
modifyorg sales, disposition_virus=blackhole
```

Description

Determines disposition of emails containing detected viruses:

- redirect -- Message is redirected and quarantined in an administrator's quarantine (the quarantine redirect address).
- quarantine -- Message is quarantined in user's Message Center quarantine.
- blackhole -- Message is deleted.
- tagonly -- The message is sent, with the virus payload, to the recipient, with a special X-pstnvirus header.
- NULL () -- This field is not active.

Field Type

Org-level

Authorization

- Read -- Virus
- Write -- Virus

Notes

When a virus is detected, the Message Security service inserts the `X-pstnvirus` header to show what virus was caught. The format of the header when a virus is detected by McAfee is:

`X-pstnvirus: McAfee_Virus_Name`

For further details on one of these viruses, you can search for `McAfee_Virus_Name` at the McAfee Virus Information Library site:

<http://vil.nai.com>

The format of the header for the Authentium Antivirus engine (an optional feature for service packages) which scans inbound messages:

`X-pstnvirus: AUTH-Authentium_Virus_Name`

The text `AUTH-` is not part of the virus name. The text indicates that the virus was not detected by the McAfee engine, and was caught by Authentium. For further details on a virus caught by Authentium Antivirus, you can search for `Authentium_Virus_Name` on the

<http://www.authentium.com/support/AVMatrix/portal.aspx>

Following are examples of the same virus if detected by McAfee or Authentium:

`X-pstnvirus: W32/Mydoom.bb@MM`

`X-pstnvirus: AUTH-W32/Mydoom.AY@mm`

Messages with the `X-pstnvirus` header will be delivered to your users only in the following cases:

- Virus disposition is set to Message Header Tagging for the organization that contains the user. In this case, all viruses will be tagged with the header and delivered to your mail server.
- The administrator (or user, if allowed) delivers the infected or cleaned virus to the user.

The `X-pstnvirus` header is omitted only when virus protection is not enabled for a user, or there is no Message Security service user associated with the recipient's address.

Related Commands

- Output: `displayorg`
- Input: `modifyorg`
- Related: `modifydomain`

Related Fields

antivirus_sensitivity, non_account_virus_scan, timezone (for orgs), virus_clean, virus_notify (for orgs)

See Also

[“Viewing Your Organization’s Sender Lists” on page 554](#)

[“Adding Users and Domains to Sender Lists” on page 555](#)

The Message Security Administration Guide, “Virus Blocking”

file_transfer_receive

The file_transfer_receive field enables receiving IM file transfers internally within the organization or to everyone. This field applies to Postini IM Security, an optional product.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
file_transfer_receive=< off | internal_only | include_external >
```

Examples

- When the field is returned as output:

```
file_transfer_receive off
```

- When modifying an organization’s IM record:

```
org_im_settings modify orgtag=sales,  
file_transfer_receive=internal_only
```

Description

- Enables IM file transfers internally and externally. The file transfer controls affect Yahoo!, AIM, and MSN. At this time, Google Talk transfers are blocked by default:
- off -- The file transfer feature is not enabled
- internal_only -- File transfers to users in the organization only
- include_external -- File transfers to any user

Default: file_transfer_receive=off

Field Type

Org-level

Authorization

- Read: IM Management
- Write: IM Management

Related Commands

- Input: org_im_settings modify
- Output: org_im_settings display

Related Fields

file_transfer_send

See Also

file_transfer_send

The file_transfer_send field enables sending IM file transfers internally within the organization or to everyone. This field applies to Postini IM Security, an optional product.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
file_transfer_send=< off | internal_only | include_external >
```

Examples

- When the field is returned as output:

```
file_transfer_send off
```

- When modifying an organization's IM record:

```
org_im_settings modify orgtag=sales, file_transfer_send=internal_only
```

Description

- Enables sending IM file transfers internally and externally. The file transfer controls affect Yahoo!, AIM, and MSN. At this time, Google Talk transfers are blocked by default:
- off -- The file transfer feature is not enabled
- internal_only -- Can send file transfers to users in the organization only
- include_external -- Can send file transfers to any user

Default: file_transfer_send=off

Field Type

Org-level

Authorization

- Read: IM Management
- Write: IM Management

Related Commands

- Input: org_im_settings modify
- Output: org_im_settings display

Related Fields

file_transfer_receive

See Also

footer_on

The footer_on field holds the activation status for an organization-level outbound Compliance Footer which describes an email policy or legal compliance. This is only used with Message Security installations.

Syntax

footer_on=<on | off>

Examples

- When assigning the field:

```
modifyorg sales, footer_on=on
```

- When the field is returned as output:

```
footer_on 0 (off)
```

Description

Switch for outbound compliance footer.

- on -- Footer will be applied to all outbound messages.
- off -- This feature is not available for the organization.

Field Type

Org-level

Authorization

- Read: Outbound Applications Manager
- Write: Outbound Applications Manager

Related Commands

- Output: displayorg
- Input: modifyorg

See Also

The Message Security Administration Guide, “Configuring Outbound Servers”

iid

The iid field lists the unique sequential database assigned key for this organization.

Syntax

iid=<database key number>

Examples

When the field is returned as output:

```
iid 100050344
```

Description

Sequential database assigned key.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Read-only for administrators

Notes

An organization can be referenced by several different fields:

- orgname -- The organization's string name
- orgtag -- The organization's string name in the database
- iid -- The organization's unique sequential database assigned key
- orgid -- The user-level foreign key for the organization's iid field.
- org -- In both the domain and spool context, this is the associated organization to the domain or to the spooling event.

Related Commands

- Input: adddomain, deleteorg, displayorg, modifyorg, setorgsubstripping
- Output: displayorg, displayprovuser, im display, listdomains, listorgs, listusers

Related Fields

iid, org (for domains), orgname, orgtag, parent_org

See Also

The Message Security Administration Guide, “Organization Management”

im_enable

The im_enable field is an organization-level switch enabling Postini IM Security, which is an optional product.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

im_enable=<off/0 | on/1 | NULL ()>

Examples

- When the field is returned as output:

```
im_enable 1 (on)
```

- To change the setting:

```
modifyorg= sales, im_enable=on
```

Description

Enables IM Security:

- off -- Disables IM usage for an organization.
- on -- IM management is enabled.
- NULL () -- This field is not active.

Note: The numeric equivalents to ‘on’ and ‘off’ are useful for debugging purposes. For robust production code, use the text value, ‘on’ or ‘off’.

Field Type

Org-level

Authorization

- Read: IM Management
- Write: IM Management

Related Commands

- Input: modifyorg, org_im_settings modify
- Output: displayorg, org_im_settings display

Related Fields

im_external_enable, im_proto_enable

See Also

“Editing Message Archiving Settings” on page 564

im_external_enable

The `im_external_enable` field is an organization-level IM Security switch which enables IM users to communicate with external users. Postini IM Security is an optional product.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
im_external_enable=<off/0 | on/1 | NULL ()>
```

Examples

- When the field is returned as output:

```
im_external_enable 1 (on)
```

- To change the setting:

```
modifyorg sales, im_external_enable=on
```

- Adding the ‘on’ flag to the `im_external_enable` field via the `external_enable` parameter:

```
user_im_settings add address=msmith@jumboinc.com, external_enable=on,  
proto_enable=+all
```

Description

Enables Instant Messaging (IM) users in an org to communicate with external users:

- 0/off -- Your IM users can not communicate with contacts outside of your organization. Instant messaging is restricted to user's within your company.
- 1/on -- Enables IM users to communicate outside of your organization.
- NULL () -- This field is not active.

Note: The numeric equivalents to ‘on’ and ‘off’ are useful for debugging purposes. For robust production code, use the text value, ‘on’ or ‘off’.

Field Type

Org-level

Authorization

- Read: IM Management
- Write: IM Management

Notes

External messages are any IM communication with user's outside of the account-level organization.

Related Commands

- Input: user_im_settings add, user_im_settings modify
- Output: displayorg, org_im_settings display, user_im_settings display
- Related: iplock add_range, im delete, im list, im listforuser, listusers

Related Fields

im_external_enable, im_proto_enable

See Also

"Editing Message Archiving Settings" on page 564

"Message Center Settings and Password Examples" on page 536

im_proto_enable

The im_proto_enable field lists what IM protocols are allowed for the organization. This field applies to Postini IM Security, an optional product.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

im_proto_enable=<+ | -protocol>,... | NULL

Examples

- When the field is returned as output:

```
im_proto_enable +all, +msn, +aim, +yahoo, +google
```

- Adding a protocol and removing another:

```
modifyorg sales, im_proto_enable=+yahoo,-AIM
```

- Adding all protocols to the im_proto_enable field via the proto_enable parameter:

```
user_im_settings add address=msmith@jumboinc.com,  
external_enable=on, proto_enable=+all
```

Description

Specifies what IM protocols are allowed:

- +<protocol> -- Adds the protocol to the list.
- -<protocol> -- Removes the protocol from the list.
- NULL -- This field is not active.

Field Type

Org-level

Authorization

- Read: IM Management
- Write: IM Management

Notes

- The supported protocols include MSN, GOOGLE, Yahoo!, AIM, and 'all' meaning all of the supported protocols. The + or -all value must be explicitly defined in the **im_proto_enable** field.
- By allowing or disallowing MSN, you are also allowing or disallowing the user of Windows Messenger.

Related Commands

- Input: user_im_settings add, user_im_settings modify
- Output: displayorg, org_im_settings display, user_im_settings display

Related Fields

im_enable, im_external_enable

See Also

“Editing Message Archiving Settings” on page 564

is_email_config

The is_email_config field states whether a configuration is the email config organization or not.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

is_email_config=<no | yes | undef>

Examples

- When the field is returned as output, example as an empty field:

```
is_email_config undef
```

- To change the setting:

```
modifyorg jumboemailconfig, is_email_config=yes
```

Description

Email Config org type is specified for inbound server configuration:

- no -- The organization is not the Email Config organization. It is either your Account organization or a user organization.
- yes -- This organization is an Email Config organization.
- undef -- This field is not active. It is empty.

Notes

If an email config organization which has blocked IP ranges for a domain is converted to a user organization, the blocked IP ranges are deleted. The information is not kept. To see an email config organization's IP locks, see the iplock display command.

Field Type

Org-level

Authorization

- Read: Edit Organization
- Write: Edit Organization

Related Commands

- Output: displayorg
- Input: modifyorg
- Related: checklatency, checkroute, iplock add_range, iplock delete, iplock delete_range, iplock display, iplock set_disposition

See Also

"Message Center Settings and Password Examples" on page 536

The Message Security Administration Guide, "Organization Management"

journaling

The journaling field enables message archive journaling for an organization. This field applies to Postini Message Archiving, which is only used with Message Security installations.

Syntax

journaling = <on | off>

Examples

```
archive_settings modify org=Jumbo ABC, archive_enable=on,  
mail_flow=on, journaling=on
```

Description

Enables archiving of journaled messages:

- on -- Journaling is enabled
- off -- Journaling is not enabled

Note: The **archive_enable** field must be enabled for **mail_flow** and **journaling** to be modified.

Field Type

Org-level

Authorization

- Read: Edit organizations
- Write: Edit organizations

Related Commands

- Input: archive_settings modify
- Output: archive_settings display

Related Fields

archive, archive_enable, mail_flow, retention_months

See Also

[“Editing Message Archiving Settings” on page 564](#)

[Postini Message Archiving Administration Guide](#)

lang_locale (for orgs)

The lang_locale field enables organization-level language localization in the Quarantine Summary's static text, the default top text, character sets, and date format.

Syntax

```
lang_locale=<language code string | NULL>
```

Examples

- When the field is returned as output, example as empty:

```
lang_locale NULL
```

- English (U.S.) UTF-8 with date format: Quarantine Summary 9/14/2006 5:00 P.M.

```
modifyorg sales, lang_locale=en_us.utf8
```

- Spanish (Spain) ISO 8859-1 with date format: Resumen de Cuarentena 14/09/2006 17:00

```
modifyorg sales, lang_locale=es.iso.8859-1
```

Note: See the lang_locale (for users) for more information.

Description

Language code and date format used by Quarantine Summary.

- NULL -- This field is not active.

See the *The Message Security Administration Guide*, “Quarantine Summary & Notifications” chapter for the latest list of supported language codes and date formats.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Related Commands

- Output: displayorg
- Input: modifyorg

See Also

“Viewing Message Center Settings” on page 536

“Editing Quarantine Summary Notifications” on page 546

The Message Security Administration Guide, “Quarantine Summary & Notifications”

lastmod_date (for orgs)

The lastmod_date field holds the date the organization was last modified.

Syntax

lastmod_date=<time stamp>

Examples

When the field is returned as output:

```
lastmod_date 1145962000
```

Description

Timestamp of last record modification for the organization. This is in UNIX seconds.

Field Type

Org-level

Authorization

- Read: Edit Organization
- Write: Read-only for administrators

Related Commands

Output: displayorg

See Also

The Message Security Administration Guide, “Organization Management”

mail_flow

The mail_flow field turns on or off the inbound and outbound archiving. This field applies to Postini Message Archiving, which is only used with Message Security installations.

Syntax

mail_flow=<on | off>

Examples

```
archive_settings modify org=Jumbo ABC, archive_enable=on,  
mail_flow=on, journaling=on
```

Description

Turns inbound and outbound archiving on and off:

- on -- Inbound and outbound archiving is enabled
- off -- Inbound and outbound archiving is not enabled

Note: The **archive_enable** field must be enabled for **mail_flow** and **journaling** to be modified.

Field Type

Org-level

Authorization

- Read: Edit organizations
- Write: Edit organizations

Related Commands

- Input: archive_settings modify
- Output: archive_settings display

Related Fields

archive, archive_enable, journaling, retention_months

See Also

“Editing Message Archiving Settings” on page 564

Postini Message Archiving Administration Guide

max_message_size

The max_message_size field holds the organization-level maximum size of inbound attachments-per-message that users can receive.

Syntax

max_message_size=<1 - 300 (MB) | NULL (200M)>

Examples

- When the field is returned as output:

```
max_message_size 200M
```

- To change the setting:

```
modifyorg sales, max_message_size=250
```

Description

Maximum size of inbound messages in megabytes, allowed for this organization.

- NULL (200M) -- This field is not active.

Default: max_message_size=200 M

- When an attached message exceeds this limit it is bounced. And a SMTP error 552 Message too large - psmtp message is returned to the sender.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

- The max_message_size filter, although configured through the Attachment Manager is not disabled by turning off the Attachment Manager.
- See outbound_max_message_size field for the maximum size of attachments-per-message that users can send.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

at_notify_on, outbound_max_message_size, qsum_actionable, qsum_enable, qtine_redir_atq, qtine_redir_out_atq, qtine_redir_ndr

See Also

[“Viewing Message Center Settings” on page 536](#)

[“Viewing Message Center Settings” on page 536](#)

[The Message Security Administration Guide, “Organization Management”](#)

message_encryption (for orgs)

The message_encryption field enables outbound organization-level messages to be encrypted and sent to a secure portal. This field applies to Postini Message Encryption, which is only used with Message Security installations.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
message_encryption=<on | off | match | NULL ()>
```

Examples

- When the field is returned as output:

```
message_encryption on
```

- To change the setting:

```
modifyorg sales, message_encryption=on
```

Note: See message_encryption (for a user’s outbound encrypted messages) for additional examples.

Description

Enable external encryption:

- on -- Messages are always encrypted with Message Security.
- off -- Messages not encrypted with Message Security, but may have Transport Layer Security (TLS).
- match -- System looks in the message header for string. If the string is found, the message is encrypted with Message Security. The default is sensitivity: company-confidential.
- NULL () -- This field is not active.

Default: message_encryption=off

Field Type

Org-level

Authorization

- Read: Outbound Message Encryption
- Write: Outbound Message Encryption

Notes

Entries apply to all users in the organization

Related Commands

- Output: displayorg
- Input: modifyorg
- Related: displayuser (Output), domain_tls add, domain_tls delete, domain_tls display, encryption display_org

Related Fields

message_encrypt (for users), message_encryption_criteria

See Also

“Viewing and Editing Message Encryption Settings” on page 565

Postini Encryption Services Administration Guide, “How Connection Security Works”

message_encryption_criteria

The message_encryption_criteria field holds a header or subject string identifying outbound organization-level messages that need to be encrypted. This field applies to Postini Message Encryption, which is only used with Message Security installations.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

message_encryption_criteria=<string> | NULL

Examples

- When the field is returned as output:

```
message_encryption_criteria Encrypt this message
```

- To change the setting:

```
modifyorg sales, message_encryption_criteria=This message is encrypted
```

Description

Holds a header string used to identify outbound messages that need to be encrypted.

- <string> -- Message text.
- NULL -- This field is not active.

Default: message_encryption_criteria=NULL

Field Type

Org-level

Authorization

- Read: Outbound Message Encryption
- Write: Outbound Message Encryption

Related Commands

- Output: displayorg
- Input: modifyorg
- Related: encryption display_org, encryption modify_org

Related Fields

message_encryption (for orgs)

See Also

“Viewing and Editing Message Encryption Settings” on page 565

Postini Encryption Services Administration Guide, “How Connection Security Works”

ndr

The `ndr` field holds outbound mail configuration (block or blackhole) for undeliverable bounce messages generated by the organization’s mail server. This is the control for Undeliverable Bounce Message handling. This is only used with Message Security installations.

Syntax

```
ndr=<off | blackhole | quarantine | NULL ()>
```

Examples

- When the field is returned as output:

```
ndr off
```

- To change the setting:

```
modifyorg sales, ndr=quarantine
```

Description

Outbound mail configuration to block or blackhole undeliverable bounce messages generated by your mail server:

- off -- Undeliverable bounce messages are deferred up to five days before bouncing.
- blackhole -- Undeliverable messages are accepted as if successfully delivered and then silently discarded.
- quarantine -- Undeliverable messages are quarantined to the administrator’s quarantine.
- NULL () -- This field is not active.
- Default: off

Note: Make sure the quarantine administrator account is set up before using the quarantine or Blackhole values with this field.

Field Type

Org-level

Authorization

- Read: Outbound Server Management
- Write: Outbound Server Management

Notes

Some mail servers silently discard these messages when they are not deliverable. Others, such as Microsoft Exchange and qmail, accept all mail traffic and then create a new outgoing mail message in the event there is no recipient account. If the sending address is forged or unavailable, undeliverable bounce messages may become caught in your system. Since the Message Security service is acting as a proxy, your sending email server will not realize it can discard these messages.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

async_bounce, non_account_bounce, qtine_redir_ndr, nullsender_disposition

See Also

“Viewing Your Organization’s Sender Lists” on page 554

The Message Security Administration Guide, “Configuring Outbound Servers”

non_account_bounce

The non_account_bounce field is a switch for Non-Account Bouncing. When on, messages are bounced if not addressed to a registered user or alias.

Syntax

```
non_account_bounce=<on/1 | off/0 | NULL ()>
```

Examples

- When the field is returned as output:

```
non_account_bounce 1 (on)
```

- To change the setting:

```
modifyorg sales, non_account_bounce=on
```

Description

Mail is bounced if the recipient is not found in the database. The SMTP error message 550 No such user - psmtplib is returned to the sender.

- on -- Mail is bounced if not addressed to a registered user or alias.
- off -- This feature is not available.
- NULL -- This field is not active.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

- By activating this feature, the Message Security service will compare directory information with incoming recipients to measure erroneous delivery attempts. When activating this service, it is imperative that you keep your directory up to date.
- This setting is used for organizations that contain domains. Non-Account Bouncing applies to all domains in an organization.
- Non-Account Bouncing takes precedence over **non_account_virus_scan**. Don't enable Non-Account Bouncing for an org if you want to enable **non_account_virus_scan**, or SmartCreate which handle unknown recipients differently.
- No reports or statistics of bounced messages are logged.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

async_bounce, ndr, disposition_virus, non_account_virus_scan

See Also

[Viewing Your Organization's Sender Lists](#)

[The Message Security Administration Guide, "Organization Management"](#)

non_account_virus_scan

The non_account_virus_scan field enables virus scanning for non-account messages.

Syntax

non_account_virus_scan=<on/1 | off/0 | NULL ()>

Examples

```
modifyorg sales, non_account_virus_scan = on
```

Description

Enables an inbound message for unregistered users to be filtered for viruses.
There is no notification associated with this disposition:

- on -- Deletes virus-infected messages sent to unregistered users, before they reach your mail server. This takes priority over **disposition_virus**.

Default: non_account_virus_scan=on for accounts created in version 6.7 and above.

- off -- Message sent to unregistered users are not scanned for viruses.

Note: Management of this functionality must be done at the account-level or email config-level.

Note: The non_account_virus_scan field does not apply if **non_account_bounce** is enabled. **non_account_bounce** takes precedence over non_account_virus_scan.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

- If you have Message Archiving, unregistered user messages with viruses bounced or blackholed viruses are not archived.
- Unregistered blackholed messages are not included in an organization's Traffic report
- In the case of non_account_virus_scan not being 'on', if a SmartCreate provisional user's messages have viruses and the organization's **disposition_virus**=quarantine, the message is deferred.
- If non_account_virus_scan is 'on', then the provisional's user messages with viruses will be blackholed or deleted.

Related Commands

- Output: displayorg
- Input: addorg, modifyorg

Related Fields

disposition_virus, non_account_bounce

See Also

“Viewing Authentication and Password Settings” on page 540

“Seeing if a User Has Received a Welcome Notification” on page 547

The Message Security Administration Guide, “Virus Blocking”

nullsender_disposition

The nullsender_disposition field holds a Non-Delivery Report/Receipt (NDR) message disposition, allowing organizations to filter inbound valid and spam NDRs. This functionality is available for the Message Filtering, Message Security, and Message Discovery products.

Syntax

nullsender_disposition=<quarantine | blackhole | <“errstr”> | ERROR <“errstr”> | NULL >

Examples

When the field is given as input:

```
addorg Sales, parent="Jumbo, San Carlos",
nullsender_disposition=quarantine
modifyorg Sales, nullsender_disposition=blackhole
modifyorg Sales, nullsender_disposition="511 Refused - no sender"
addorg Sales, parent="Jumbo, San Carlos",
nullsender_disposition="ERROR 499 Deferred - no sender"
```

When field is returned as output:

```
nullsender_disposition quarantine
```

Description

This field holds the disposition for a valid or spam NDR inbound message based on the null sender address in the envelope's FROM field. The NDR filter does not block NDRs with a sender address. An example of a valid NDR message is, after sending mail to someone's who is out of the office, your mail server receives an auto-reply vacation report. If your domain has been used in the FROM field of a spammer's mail (spoofed), your mail server receives a NDR report if the mail was sent to a non-existing recipient.

The NDR filtering dispositions include:

- quarantine -- Insert the message into the recipient's quarantine. These messages appear in the user's Message Center or Quarantine Summary with the a blank in the filter column.
- blackhole - Silently discard the message.
- <“errstr”> -- Bounce the SMTP request with the error code + custom error string. The error string must be a syntactically correct RFC 821 response string. This is the same as the ERROR <“errstr”> but, in some instances, more convenient.

The field accepts 4xx and 5xx error codes. The messages with 4xx error codes will be continuously rejected. The practical error codes are the 5xx codes. The messages with 5xx codes are permanently rejected.

- ERROR <“errstr”> -- Bounce a SMTP request with the error string response. The error string must be a syntactically correct RFC 821 response string. The addorg and modifyorg commands return an error for ill-formatted syntax.

The error string is returned to the address in the Return-Path or the SMTP envelope sender address FROM: field.

- NULL -- This field is not active.

Default: NULL

Field Type

Org-level

Authorization

- Read: Edit organizations
- Write: Edit organizations

Notes

- The nullsender_disposition field's value takes precedence over Approved/Blocked Senders, Content Manager or Attachment Manager rules. The NDR filter runs before the junk filters. Virus blocking processes NDR messages as usual.
- The nullsender_disposition field's quarantined and blocked totals appear in the Traffic reports by domain and by recipient.
- When initially using this field, set the disposition to quarantine. And, during the period of an NDR storm, change the disposition to blackhole.
- In the case of the nullsender_disposition field, there is no redirect of quarantine messages to an administrator's address. The qtine_redir_ndr field is associated with the ndr field only.
- The nullsender_disposition functionality is used when an NDR message returns with a null sender value. Some mail servers do not generate NDRs with a null sender value. For example, Microsoft Exchange, configured for asynchronous bouncing, generates NDR messages with null sender values. Other mail servers, such as Postfix, these may not accept email for invalid addresses. These generate valid NDR messages without a null sender.
- To reduce the amount of invalid NDRs resulting from spam, use a combination of the nullsender_disposition field, turn on Non-Account Bouncing, and create custom content filters if your service includes the Content Manager.

Related Commands

- Input: addorg, modifyorg
- Output: displayorg

Related Fields

- ndr (for Message Security product only)

See Also

The Message Security Administration Guide, “Content Manager”

nullsender_headertag_validation

The nullsender_headertag_validation field holds the number of hours a NDR or “bounce” message will be accepted by the system for any outbound message sent with a header containing a digital signature. This functionality is available for the Message Filtering, Message Security, and Message Discovery products.

Syntax

```
nullsender_headertag_validation=< 1 - 336 | 0 | NULL >
```

Examples

When the field is given as input:

```
modifyorg Sales, nullsender_headertag_validation=120
```

When field is returned as output:

```
nullsender_headertag_validation 120
```

Description

When valid messages are sent out, digital signatures are added to the message's Received Header. The nullsender_headertag_validation field holds the number of hours this digital signature is valid if the sent message is returned with a NDR or bounce message.

All mail with a null sender lacking this signature or is received after the signature expires, is subject to the nullsender_disposition field's setting.

- 0, NULL -- The feature is disabled.
- 1- 336 -- Number of hours the NDR message is kept as a response for a sent outbound message.

Default: 120 hours (5 days)

Field Type

Org-level

Authorization

- Read: Edit organizations, Outbound Server Management
- Write: Edit organizations, Outbound Server Management

Notes

This field is equivalent to the Administration Console's organization's Inbound Spam Filters Null Sender Header Tag Validation hours field.

Related Commands

- Input: modifyorg
- Output: displayorg

Related Fields

- ndr (for Message Security product only), nullsender_disposition

See Also

The Message Security Administration Guide, “*Content Manager*”

orgname

The orgname field lists the name of the current organization.

Syntax

orgname=<text string>

Examples

- When the field is returned as output:

```
orgname sales
```

- Change an organization's name:

```
modifyorg sales, orgname=Hugeisp
```

- An orgname with a comma needs double quotes:

```
orgname="JumboInc Email Organization, San Carlos"
```

- An orgname with an apostrophe needs double quotes:

```
orgname="JumboInc's Western Org"
```

Description

A unique name used to reference an organization within the Administration Console:

- Enclose the organization's name in double quotes if it contains an apostrophe or commas.

The unique identifying number (**iid**) of the organization can sometimes be substituted for orgname. The IID is useful for debugging purposes. For robust production code, use the **orgname** field value.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

- Value must be unique, not matching orgname or any other organization or other customers on the same system.
- orgnames can have white spaces. Depending upon your system environment, orgnames should not have forward slashes.
- The Batch interface allows apostrophes, commas, #, =, " " symbols in user or organization names. These must be either in double quotes or proceeded by a '\` symbol.
- An organization can be referenced by several fields:
 - org -- The organization name in the **displayspool** output
 - orgname -- The organization's string name
 - orgtag -- The organization's string name in the database
 - iid -- The organization's unique sequential database assigned key
 - orgid (for users) -- The organization's iid or orgname for the organization containing the user.

Related Commands

- Output: displayorg
- Input: adddomain, addorg, adduser, archive_settings display, archive_settings modify, checklatency, checkroute, deleteorg, displayorg, displayspool, domain_tls add, domain_tls delete, domain_tls display, domain_tls modify, encryption display_org, encryption modify_org, getorgreport, iplock add_range, iplock delete, iplock delete_range, iplock display, iplock set_disposition, listdomains, listorgs, listprovusers, listusers, modifydomain, modifyorg, notification display, notification modify, org_im_settings display, org_im_settings modify, password force_update, password_policy display, password_policy update, setorgsubstripping

Related Fields

iid, The Message Security Administration Guide, “Organization Management” org (for domains), orgid, orgtag, parent_org

See Also

The Message Security Administration Guide, “Organization Management”

orgtag

The orgtag field lists the name of the current organization. It is equivalent to the orgname field.

Syntax

orgtag=<text string>

Examples

The field as output of a command:

```
orgtag sales
```

Description

orgtag is the organization’s string name in the database. It is equivalent to the orgname field.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

The batch interface allows apostrophes, commas, #, =, " " symbols in user or organization names. These must be either in double quotes or proceeded by a \' symbol.

Related Commands

- Input: encryption display_org, encryption modify_org, listdomains, listorgs, listusers, notification display, notification modify, org_im_settings display
- Output: im list, listusers

Related Fields

iid, org (for domains)
The Message Security Administration Guide, “Organization Management”, orgname, parent_org

See Also

The Message Security Administration Guide, “Organization Management”

out_at_notify_on

The out_at_notify_on field holds the notification recipient for messages quarantined for Outbound Attachment Manager rules. This is only used with Message Security installations.

Syntax

out_at_notify_on=< 0 | 1 | 2 | 3 | NULL ()>

Examples

- The field as output of a command:

```
out_at_notify_on 0
```

- To change the setting:

```
modifyorg sales, out_at_notify_on=1
```

Description

Notification sent to recipient of Outbound Attachment Manager notifications:

- 0 (Off) -- Notification is turned off for this organization
- 1 (Send to Redirect) -- If your spam filters are configured to deliver all user spam to a single administrator's quarantine, the notification is sent to this administrator. This is also known as a redirect to the Attachment Manager Quarantine Redirect address.
- 2 (Send to User)-- Notification sent to the user
- 3 (Send to Both) -- Notification sent to both the user and the redirect administrator's address.
- NULL() -- This field is not active.

Field Type

Org-level

Authorization

- Read: Notification Messages
- Write: Notification Messages

Notes

Organization-level approved senders can optionally bypass attachment filters

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

at_notify_on (Inbound), max_message_size, outbound_max_message_size, qsum_actionable, qsum_enable, qtine_redir_atq, qtine_redir_out_atq, qtine_redir_ndr

See Also

“Viewing Authentication and Password Settings” on page 540

“Seeing if a User Has Received a Welcome Notification” on page 547

The Message Security Administration Guide, “Quarantine Summary and Notifications”

outbound_max_message_size

The outbound_max_message_size field holds the maximum size of attachments-per-message that users in the organization can send. This is only used with Message Security installations.

Syntax

outbound_max_message_size=<1 - 300 (MB) | NULL (200M)>

Examples

- The field as output of a command:

```
outbound_max_message_size 200M
```

- To change the setting:

```
modifyorg sales, outbound_max_message_size=200
```

Description

Maximum size of message megabytes, allowed for this organization.

- NULL (200M) -- This field is not active.

Default: outbound_max_message_size=200 MB

Field Type

Org-level

Authorization

- Read: Outbound Applications Management
- Write: Outbound Applications Management

Notes

Messages that exceed this limit are bounced, returning a SMTP error 552 Message too large - psmtplib message to the sender.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

max_message_size (inbound)

See Also

[“Viewing Message Center Settings” on page 536](#)

[“Viewing Message Center Settings” on page 536](#)

[The Message Security Administration Guide, “Organization Management”](#)

outbound_virus

The outbound_virus field holds the activation status for outbound virus scanning. This is only used with Message Security installations.

Syntax

outbound_virus = <on/1 | off/0>

Examples

- When returned from displayorg:

```
outbound_virus 1 (on)
```

- When assigned:

```
modifyorg sales, outbound_virus=1
```

Description

Switch for outbound virus scanning.

- on -- Virus scanning is enabled for outbound messages
- off -- This feature is not available for this organization

Note: The numeric equivalents to ‘on’ and ‘off’ are useful for debugging purposes. For robust production code, use the text value, ‘on’ or ‘off’.

Field Type

Org-level

Authorization

- Read: Outbound Applications Management
- Write: Outbound Applications Management

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

disposition_virus, out_at_notify_on, outbound_virus_disposition

See Also

The Message Security Administration Guide, “Virus Blocking”

outbound_virus_disposition

The outbound_virus_disposition field lists the disposition (bounce or redirect) of an outbound email containing a virus. This is only used with Message Security installations.

Syntax

```
outbound_virus_disposition=< 1 | 2 >
```

Examples

- When assigning the field:

```
modifyorg sales, outbound_virus_disposition=2
```

- When the field is returned as output:

```
outbound_virus_disposition 1 (bounce)  
outbound_virus_disposition 2 (quarantine)
```

Description

Viruses detected in outbound email can either be:

- 1 -- Bounced
- 2 -- Redirected to outbound virus quarantine (**qtine_redir_out_virus** address). If the **qtine_redir_out_virus** field is NULL, the outbound mail is bounced.

Default: outbound_virus_disposition = 1

Field Type

Org-level

Authorization

- Read: Outbound Applications Management
- Write: Outbound Applications Management

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

disposition_virus, out_at_notify_on, outbound_virus

See Also

The Message Security Administration Guide, “Virus Blocking”

parent_org

The parent_org field lists the organization that is one level up in the org hierarchy.

Syntax

parent_org=<text string>

Examples

- When moving an org to a new parent:

```
modifyorg sales, parent_org=Hugeisp  
modifyorg sales, parent_org="JumboInc's Western Org"
```

- When the field is returned as output:

```
parent_org 100001011 (Hugeisp)
```

Description

A valid orgname:

- Entering a new parent reassigns the current org to a new parent, moving it to a new location in the hierarchy.
- The parent organization's name can be the unique identifying number (IID) of the organization
- Enclose <parent org> in double quotes or preceded with a '\ symbol if it contains an apostrophe or commas, #, =, " , ' symbols.

Note: The parent_org, as an organization, has an associated iid value, a unique identifying organization number. The iid can be substituted for the parent_org in some instances and is useful for debugging purposes. But for robust, finished production code, use the parent_org fields' value.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

- Do not create a hierarchical loop.
- If this organization is a mail host config, it cannot be moved above or below another mail host config.

Related Commands

- Input: addorg
- Output: displayorg

Related Fields

iid, org (for domains)The Message Security Administration Guide, “Organization Management”, orgname, orgtag

See Also

The Message Security Administration Guide, “Organization Management”

qsum_actionable

The qsum_actionable field determines if Quarantine Summary links are available.

Syntax

`qsum_actionable=<“not actionable” | “basic delivery”>`

Examples

- When the field is returned as output:

```
qsum_actionable not actionable
```

- To change the setting:

```
modifyorg sales, qsum_actionable="not actionable"
```

Description

Lists whether links available in Quarantine Summary notifications.

- “not actionable” -- No delivery link in Quarantine Summary
- “basic delivery” -- Messages are linked in the Quarantine Summary.

Field Type

Org-level

Authorization

- Read: Notification Messages
- Write: Notification Messages

Notes

The qsum_enable fields must be ‘on’ for this field to work.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

at_notify_on (Inbound), max_message_size, out_at_notify_on, outbound_max_message_size, qsum_enable, qtine_redir_atq, qtine_redir_out_atq, qtine_redir_ndr

See Also

“Viewing Message Center Settings” on page 536

“Editing Quarantine Summary Notifications” on page 546

The Message Security Administration Guide, “Quarantine Summary and Notifications”

qsum_enable

The qsum_enable field is a switch that sends the Quarantine Summary notifications.

Syntax

qsum_enable=< on | off >

Examples

- When the field is returned as output:

qsum_enable on

- To change the setting:

modifyorg sales, qsum_enable=on

Description

Switch for send quarantine summary notifications.

- on -- Getting Quarantine Summary notifications enabled
- off -- Will not get Quarantine Summary notifications

Field Type

Org-level

Authorization

- Read: Notification Messages
- Write: Notification Messages

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

at_notify_on (Inbound), max_message_size, out_at_notify_on, outbound_max_message_size, qsum_actionable, qtine_redir_atq, qtine_redir_out_atq, qtine_redir_ndr

See Also

“Viewing Message Center Settings” on page 536

“Editing Quarantine Summary Notifications” on page 546

The Message Security Administration Guide, “Quarantine Summary and Notifications”

qtine_redir_atq

The qtine_redir_atq field holds Attachment Manager Quarantine Redirect administrator address for inbound attachments.

Syntax

```
qtine_redir_atq=< valid user address | NULL (none) >
```

Examples

- When the field is returned as output, example as empty:

```
qtine_redir_atq NULL (none)
```

- To change the setting:

```
modifyorg sales, qtine_redir_atq=msmith@jumboinc.com
```

Description

If your spam filters are configured to deliver all user spam to a single administrator's quarantine, the notification is sent to this administrator <valid user address>. This is also known as a redirect to the Attachment Manager Quarantine Redirect address.

- NULL (none) -- This field is not active.

Field Type

Org-level

Authorization

- Read: Attachment Manager
- Write: Attachment Manager

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

at_notify_on (Inbound), max_message_size, out_at_notify_on, outbound_max_message_size, qsum_actionable, qsum_enable, qtine_redir_ndr, qtine_redir_out_atq

See Also

The Message Security Administration Guide, “Quarantine Summary and Notifications”

qtine_redir_ndr

The qtine_redir_ndr field holds the user email address for the quarantined outbound Undeliverable Bounce Messages. When an outbound message is quarantined as an undeliverable Bounce message, the message is stored in this Message Center. This is only used with Message Security installations.

Syntax

qtine_redir_ndr=<valid user address | NULL (none)>

Examples

- When the field is returned as output, example as empty:

```
qtine_redir_ndr NULL (none)
```

- To change the setting:

```
modifyorg sales, qtine_redir_ndr=ndruser@jumboinc.com
```

Description

Undeliverable outbound bounced email for this organization is quarantined to this user.

- NULL (none) -- This field is not active.

Field Type

Org-level

Authorization

- Read: Outbound Server Management
- Write: Outbound Server Management

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

at_notify_on (Inbound), max_message_size, out_at_notify_on, outbound_max_message_size, qsum_actionable, qsum_enable, qtine_redir_atq, qtine_redir_out_atq

See Also

“Viewing Message Center Settings” on page 536

“Editing Quarantine Summary Notifications” on page 546

The Message Security Administration Guide, “Quarantine Summary and Notifications”

qtine_redir_out_atq

The qtine_redir_out_atq field holds the user address for the Attachment Manager quarantined email for this organization. When an outbound message is quarantined by Attachment Manager, the message is stored in this Message Center. This is only used with Message Security installations.

Syntax

qtine_redir_out_atq=<valid user address | NULL (none)>

Examples

- When the field is returned as output:

```
qtine_redir_out_atq support@jumboinc.com
```

- To change the setting:

```
modifyorg sales, qtine_redir_out_atq=support@jumboinc.com
```

Description

Attachment Manager email for this organization is quarantined to this user.

Field Type

Org-level

Authorization

- Read: Outbound Applications Management
- Write: Outbound Applications Management

Related Commands

- Input: modifyorg
- Output: displayorg

Related Fields

at_notify_on (Inbound), max_message_size, out_at_notify_on, outbound_max_message_size, qsum_actionable, qsum_enable, qtine_redir_atq, qtine_redir_ndr

See Also

“Viewing Message Center Settings” on page 536

“Editing Quarantine Summary Notifications” on page 546

The Message Security Administration Guide, “Quarantine Summary and Notifications”

qtine_redir_out_virus

The qtine_redir_out_virus field holds the email address for the user receiving outbound virus email quarantine for an organization. When an outbound message is quarantined as a virus, the message is stored in this Message Center. This is only used with Message Security installations.

Syntax

qtine_redir_out_virus=<valid user address | NULL (none)>

Examples

- When the field is returned as output:

```
qtine_redir_out_virus support@jumboinc.com
```

- To change the setting:

```
modifyorg sales, qtine_redir_out_virus=support@jumboinc.com
```

Description

Outbound virus email for this organization is quarantined to this user.

- NULL (none) -- This field is not active.

Field Type

Org-level

Authorization

- Read: Outbound Applications Management
- Write: Outbound Applications Management

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

qtine_redir_out_atq

See Also

“Viewing Message Center Settings” on page 536

“Editing Quarantine Summary Notifications” on page 546

The Message Security Administration Guide, “Quarantine Summary and Notifications”

qtine_redir_spam

The qtine_redir_spam field holds email address for the user receiving inbound spam email quarantine for an organization. When an outbound message is quarantined as spam, the message is stored in this Message Center. This is only used with Message Security installations.

Syntax

```
qtine_redir_spam=<valid user address | NULL (none)>
```

Examples

- When the field is returned as output:

```
qtine_redir_spam support@hugeisp.com
```

- To change the setting:

```
modifyorg sales, qtine_redir_spam=support@hugeisp.com
```

Description

Spam email for this organization is quarantined to this user.

- NULL (none) -- This field is not active.

Field Type

Org-level

Authorization

- Read: Junk Email
- Write: Junk Email

Related Commands

- Output: displayorg
- Input: modifyorg

See Also

“Viewing Message Center Settings” on page 536

“Editing Quarantine Summary Notifications” on page 546

The Message Security Administration Guide, “Quarantine Summary and Notifications”

qtine_redir_virus

The qtine_redir_virus holds the email address for the user receiving inbound virus email quarantine for an organization. When an outbound message is quarantined as a virus, the message is stored in this Message Center. This is only used with Message Security installations.

Syntax

qtine_redir_virus=<valid user address | NULL (none)>

Examples

When the field is returned as output:

```
qtine_redir_virus support@hugeisp.com  
modifyorg sales, qtine_redir_virus=support@hugeisp.com
```

Description

Virus email for this organization is quarantined to this user.

- NULL (none) -- This field is not active.

Field Type

Org-level

Authorization

- Read: Virus
- Write: Virus

Related Commands

- Output: displayorg
- Input: modifyorg

See Also

The Message Security Administration Guide, “Quarantine Summary and Notifications”

quarantine_links

The quarantine_links field is a switch to enable quarantine message links to be available in the Message Center.

Syntax

```
quarantine_links=< off/0 | on/1 >
```

Examples

- When assigning the field:

```
modifyorg sales, quarantine_links=0
```

- When the field is returned:

```
quarantine_links 1 (on)
```

Description

Enables quarantine message links to be on or off.

- off -- Enables the Message Center links
- on -- Blocks the Message Center links

Note: The numeric equivalents to ‘on’ and ‘off’ are useful for debugging purposes. For robust production code, use the text value, ‘on’ or ‘off’.

Field Type

Org-level

Authorization

- Read: Junk Email
- Write: Junk Email

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

`quarsum_links`

See Also

“Editing Message Center Access and Settings” on page 538

“Viewing Authentication and Password Settings” on page 540

The Message Security Administration Guide, “Quarantine Summary and Notifications”

quarsum_links

The `quarsum_links` field is a switch enabling Quarantine Summary message links to be available.

Syntax

`quarsum_links=< 0/off | on/1 | NULL () >`

Examples

- When the field is returned as output:

`quarsum_links 0 (off)`

- To change the setting:

`modifyorg sales, quarsum_links=0`

Description

Enable quarantine summary message link.

- off -- Disables the Quarantine Summary links
- on -- Enables the Quarantine Summary links
- NULL () -- This field is not active.

Note: The numeric equivalents to ‘on’ and ‘off’ are useful for debugging purposes. For robust production code, use the text value, ‘on’ or ‘off’.

Field Type

Org-level

Authorization

- Read: Notification Messages
- Write: Notification Messages

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

quarantine_links

See Also

“Viewing Message Center Settings” on page 536

“Editing Quarantine Summary Notifications” on page 546

“Editing Message Archiving Settings” on page 564

The Message Security Administration Guide, “Quarantine Summary and Notifications”

remotecmd_secret

The remotecmd_secret field holds the shared secret for digitally signing EZCommand URLs.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
remotecmd_secret=<string | NULL>
```

Examples

- When the field is returned as output:

```
remotecmd_secret swordfish
```

- To change the setting:

```
modifyorg sales, remotecmd_secret=swordfish
```

Description

Shared secret for digitally signing EZCommand URLs.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

[authentication_data](#)

See Also

The Message Security Administration Guide, “Batch Processing and EZCommands

retention_months

The retention_months field holds the number of months archived messages are retained for an organization. This field applies to Postini Message Archiving, which is only used with Message Security installations.

Syntax

`retention_months <number of months integer>`

Examples

In the Administration Console, the field is returned as output with a different label:

```
Archive Retention Months: 3
```

Description

Lists the number of months an organization’s archived messages are retained.

When an organization is created, this field inherits its initial value from your account’s maximum archive retention setting.

Note: To change the organization’s archive retention period, please contact your support representative.

Field Type

Org-level

Authorization

- Read: Edit organizations-Advanced Applications-Message Archiving
- Write: Read-only for administrators

Related Commands

Output: archive_settings display

Related Fields

archive, mail_flow, journaling

See Also

[Postini Message Archiving Administration Guide](#)

spam_notify_on

The spam_notify_on field is a switch enabling the sending of spam quarantine notifications.

Syntax

spam_notify_on=<on/1 | off/0 | NULL ()

Examples

- When the field is returned as output:

```
spam_notify 1 (on)
```

- To change the setting:

```
modifyorg sales, spam_notify_on=on
```

Description

Sends spam quarantined notifications:

- on -- Spam quarantine notifications can be sent
- NULL ()-- This field is not active.
- off -- Spam quarantine notifications are disabled

Field Type

Org-level

Authorization

- Read: Notification Messages
- Write: Notification Message

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

blatant_spam, tagonly_spam

See Also

“Viewing Authentication and Password Settings” on page 540

“Seeing if a User Has Received a Welcome Notification” on page 547

The Message Security Administration Guide, “Quarantine Summary and Notifications”

standard_journal

The standard_journal field is an on/off switch enabling IM conversations to be sent to all participants in the user’s organization. This field applies to Postini IM Security, an optional product.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
standard_journal= < on | off >
```

Examples

- When the field is returned as output:

```
standard_journal on
```

- To change the setting:

```
org_im_settings modify orgtag=sales,  
disposition="archive,standard_journal"
```

Description

Enables IM standard journaling:

- on -- Enables IM conversations to be sent to all participants
- off -- Disables IM conversations to be sent to all participants

Field Type

Org IM management

Authorization

- Read: IM Management
- Write: IM Management

Notes

An organization's IM conversations are journaled by being sent as email to participants and/or text of the conversation is sent directly to the Message Archiving for storage:

- Standard journaling -- IM conversation text is sent as an email message to all conversation participants who are in this user's organization. This is equivalent to the 'Standard Email' feature in the Administration Console.
- Custom journaling -- IM conversations are sent as an email message to an administrator's email address. This is equivalent to the 'This email address' feature in the Administration Console.
- Message Archiving -- IM conversations are sent directly to Message Archiving for storage. Available for Postini Message Archiving customers only.

Related Commands

- Input: org_im_settings modify
- Output: org_im_settings display

Related Fields

archive, custom_journal

See Also

"Editing Message Archiving Settings" on page 564

Postini Message Archiving Administration Guide

support_contact

The support_contact field holds the address of the support contact for the organization. This address is used for all help links, and is the sender for notifications.

Syntax

support_contact=<support user address>

Examples

- When the field is returned as output:

```
support_contact support@hugeisp.com
```

- To change the setting:

```
modifyorg sales, support_contact=support@hugeisp.com
```

Description

Address of support contact for the organization:

- Address must look like a real email address. This address does not have to be registered with the Message Security service.
- Domain or user must be identified in the Message Security service system and removable to the same mailhost as this organization.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

- This is an important contact in case of emergencies.
- This is the support email link in the Quarantine Summary notification.
- For Directory Sync, notifications will be sent to this address whenever a synchronization occurs. In the case of Directory Sync, the name used for the support contact is DirSync Manager.

Related Commands

- Output: displayorg
- Input: modifyorg

See Also

“Viewing Authentication and Password Settings” on page 540

“Seeing if a User Has Received a Welcome Notification” on page 547

The Message Security Administration Guide, “Organization Management.”

tagonly_spam

The tagonly_spam field enables adding header tags to a spam email instead of forwarding the email to quarantine.

Syntax

```
tagonly_spam=< off/0 | on/1 | NULL () >
```

Examples

- When the field is returned as output:

```
tagonly_spam off
```

- To change the setting:

```
modifyorg sales, tagonly_spam=off
```

Description

Add header tags to spam email instead of quarantining.

- off -- Header tags are not enabled. The email is quarantined.
- on -- Header tags are enabled and the email is not quarantined.
- NULL () -- This field is not active.

Note: The numeric equivalents to ‘on’ and ‘off’ are useful for debugging purposes. For robust production code, use the text value, ‘on’ or ‘off’.

Field Type

Org-level

Authorization

- Read: Junk Email
- Write: Junk Email

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

blatant_spam, spam_notify_on

See Also

The Message Security Administration Guide, “Quarantine Summary and Notifications”

timezone (for orgs)

The timezone field holds the user’s timezone, a UNIX TZ string used in Message Center II.

Syntax

timezone = <UNIX TZ string>

Examples

When the field is returned as output:

```
timezone America/Los_Angeles ((GMT-8:00) Pacific Time (US & Canada);  
Tijuana)
```

Description

Holds the UNIX TZ string used in Message Center II.

Default: timezone = NULL

Field Type

Org-level

Authorization

- Read: Application Management, Account Settings, Regional Settings
- Write: Application Management, Account Settings, Regional Settings

Related Commands

- Output: displayorg
- Related: displayuser

Related Fields

timezone (for users)

See Also

The Message Security Administration Guide, “The Message Center”

tls_notify_admin

The `tls_notify_admin` field lists the administrator who receives the email config organization’s Policy Enforced TLS alerts. This field applies to Postini Policy-Enforced TLS, which is only used with Message Security installations.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

`tls_notify_admin = <admin user address | NULL>`

Examples

- To change the setting:

```
modifyorg Sales tls_notify_admin = msmith@jumboinc.com
```

- To enable a TLS alert:

```
modifyorg Sales tls_notify_admin = msmith@jumboinc.com,  
tls_notify_on=600
```

Description

Lists the email config organization's administrator address which will receive the TLS alerts. The user receiving these alerts must be an administrator for the email config organization.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

This field is applicable to email config organizations only.

Related Commands

- Input: modifyorg
- Output: displayorg

Related Fields

tls_notify_on

See Also

Postini Encryption Services Administration Guide, “Policy Enforced TLS”

tls_notify_on

The `tls_notify_on` field enables Policy-Enforced TLS alerts for an email config organization. It also acts as a throttle for the alert notifications by designating how much time elapses before additional notifications. This field applies to Postini Policy-Enforced TLS, which is only used with Message Security installations.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

`tls_notify_on = <0 | 1 - 86400>`

Examples

To change the setting:

```
modifyorg Sales tls_notify_on = 600
```

Description

Enables the TLS alerts for an email config organization. This is also a throttle determining how many seconds transpire before another alert is sent.

- 0 -- TLS alerts are off.
- 1 - 86400 -- TLS alerts are enabled. The value is the number of seconds that must elapse before additional alerts are sent concerning this domain's failed TLS handshake to this organization.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

This field is applicable to email config organizations only.

Related Commands

- Input: modifyorg
- Output: displayorg

Related Fields

tls_notify_admin

See Also

Postini Encryption Services Administration Guide, “Policy Enforced TLS”

virus_clean

The virus_clean field is a flag indicating whether a virus cleaning is allowed for this organization.

Syntax

virus_clean=<off/0 | on/1>

Examples

- When the field is returned as output:

```
virus_clean 1 (on)
```

- To change the setting:

```
modifyorg sales, virus_clean=1
```

Description

Flag indicating whether virus cleaning is allowed for this organization.

- off -- Virus cleaning is not enabled for this organization
- on -- Messages can have virus cleaning and be delivered if successful

Note: The numeric equivalents to ‘on’ and ‘off’ are useful for debugging purposes. For robust production code, use the text value, ‘on’ or ‘off’.

Field Type

Org-level

Authorization

- Read: Virus
- Write: Virus

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

antivirus_sensitivity, disposition_virus, timezone (for orgs), virus_notify (for orgs)

See Also

“Viewing Your Organization’s Sender Lists” on page 554

“Adding Users and Domains to Sender Lists” on page 555

The Message Security Administration Guide, “Virus Blocking”

virus_notify (for orgs)

The virus_notify field specifies how frequently virus notification email will be generated for the organization.

Syntax

virus_notify=<0 | 1 | 9 | NULL ()>

Examples

When the field is returned as output:

```
virus_notify 0 (Immediately)
```

To change the setting:

```
modifyorg JumboInc virus_notify=9
```

Description

Lists how frequently virus notification email will be generated:

- 0 -- Immediately
- 1 -- No more than one notice per day
- 9 -- Disable notifications for this organization
- NULL () -- This field is not active. The default is the user-level virus_notify setting.

Field Type

Org-level

Authorization

- Read: Notification Messages
- Write: Notification Messages

Notes

The user-level virus_notify field takes precedent over the org-level virus_notify field.

Related Commands

- Input: modifyorg
- Related: displayuser (as output)

Related Fields

antivirus_sensitivity, disposition_virus, timezone (for orgs), virus_clean, virus_notify (for users)

See Also

“Viewing Authentication and Password Settings” on page 540

“Seeing if a User Has Received a Welcome Notification” on page 547

“Setting a Virus Notification Interval” on page 549

The Message Security Administration Guide, “Virus Blocking”

welcome_on

The welcome_on field allows the system to send out welcome notifications. It shows whether a message should receive a welcome message at some point within the next 24 hours.

Syntax

```
welcome_on=on/1 | off/0
```

Examples

- When the field is returned as output:

```
welcome_on 1 (on)
```

- To change the setting:

```
modifyorg sales, welcome_on=on
```

Description

This field should not be modified.

- on -- A welcome message can be sent. Usually this is within the next 24 hours.
- off -- Sending a welcome message has been disabled.

Note: The numeric equivalents to ‘on’ and ‘off’ are useful for debugging purposes. For robust production code, use the text value, ‘on’ or ‘off’.

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

The **adduser** command's **welcome** parameter enables the welcome message to be sent immediately.

Related Commands

- Output: displayorg
- Input: modifyorg
- Related: adduser

Related Fields

disable_first_spam

See Also

“Viewing Authentication and Password Settings” on page 540

“Seeing if a User Has Received a Welcome Notification” on page 547

“Seeing if a User Has Received a Welcome Notification” on page 547

The Message Security Administration Guide, “Organization Management”

zero_hour_notify_on

The zero_hour_notify_on field enables a virus notification email sent to the message's recipient.

Syntax

zero_hour_notify_on=on/1 | off/0

Examples

- When the field is returned as output:

```
zero_hour_notify_on 1 (on)
```

- To change the setting:

```
modifyorg sales, zero_hour_notify_on=on
```

Description

- on -- Enables sending a message recipient when Early Detection Quarantine quarantines a message. This message is sent immediately.
- off -- Disables sending a message when a message is quarantined by Early Detection Quarantine.

Default: zero_hour_notify_on=off

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

- This field can be viewed before the Early Detection Quarantine waiver is signed. Once the Early Detection Quarantine waiver is signed in the Administration Console, this field can be edited.
- To modify in the Administration Console Orgs Notification page, Notifications (+ Read + Modify) is required.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

[“zero_hour_scan” on page 409](#)

See Also

zero_hour_scan

The zero_hour_scan field enables or disables the Early Detection Quarantine feature.

Syntax

`zero_hour_scan=< 1 | 0 >`

Examples

- When the field is returned as output:

`zero_hour_scan 1 (on)`

- To change the setting:

`modifyorg sales, zero_hour_scan=1`

Description

- 1 -- Enables Early Detection Quarantine.
- 0 -- Disables Early Detection Quarantine.

Default: zero_hour_scan=0

Field Type

Org-level

Authorization

- Read: Edit Organizations
- Write: Edit Organizations

Notes

This field can be viewed before the Early Detection Quarantine waiver is signed. Once the Early Detection Quarantine waiver is signed in the Administration Console, this field can be edited. Otherwise, the system returns an error.

Related Commands

- Output: displayorg
- Input: modifyorg

Related Fields

[“zero_hour_notify_on” on page 407](#)

See Also

Chapter 7

Batch User Fields

About Batch User Fields

The batch user fields hold user-level data which a command can either create, delete, display, list, or modify. This information is diverse. It can be names, email addresses, numbers, dispositions, on/off switches, boolean true/false values.

User Field Reference Page Syntax Notations

Each field's syntax section uses notation and punctuation to show you where to put your specific information, and what information is required or optional:

The reference pages use the Administration Console syntax and have an example for each field:

- The field name is required. In the Administration Console batch page, commas are required.
- Information between '< >' symbols means you need to add your specific information here. (for example: <field>=<value> becomes approved_senders=+mary@hugeisp.com)
- Information between '[]' square brackets mean this type of information is optional.
- A choice of values are separated by '|'. (for example: lang_locale= <language code string | NULL > means you have a choice of lang_locale=en_us.utf8, or lang_locale=NULL)
- Some fields have '+' or '-' notations. Read the field description and examples carefully to understand what these notations mean for that particular field.
- It is important to confirm you have authorization to display or edit a field (Read/Write authorization). The Authorization section shows each field's requirements.
- The Related Commands section shows which commands take the field as input or as output. Input means the field is used in the command's arguments. Output means the command returns this field-value pair when the command is successfully executed.

See “Batch Command and Field Quick Summary” on page 27, and “Batch Field Quick Summary” on page 111 for additional information.

active

The active field indicates whether the user has ever logged into the Message Center.

Syntax

```
active=< no/0 | yes/1 >
```

Examples

When returned by the displayuser command:

```
active 1 (yes)
```

Description

Switch shows whether user has logged into the Message Center.

- no -- The user has not logged into the Message Center
- yes -- The user has logged into the Message Center

Note: The numeric equivalents to ‘no’ and ‘yes’ are useful for debugging purposes. For robust production code, use the text value, ‘no’ or ‘yes’.

Field Type

User-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Related Commands

- Input: listusers
- Output: displayuser, listusers

See Also

“Viewing Message Center Settings” on page 536

“Seeing if a User Has Received a Welcome Notification” on page 547

“Resending the Welcome Notification” on page 548

The Message Security Administration Guide, “User’s and Quarantines”

address

The address field holds the email address of the user or the user’s alias.

Syntax

address=<legal email address>

Examples

- When the field is returned as output:

```
address kkerns@jumboinc.com
```

- Adding a Instant Message (IM) screen name:

```
im add im_name=MSN:kristie_kerns@hotmail.com,  
address=kkerns@jumboinc.com
```

- Changing a user’s address:

```
modifyuser msmith@jumboinc.com, address=msmith@hugeisp.com
```

Description

Email address of user or user’s alias.

Field Type

User-level

Authorization

- Read: Change Address
- Write: Change Address

Notes

The Batch interface allows apostrophes, commas, #, =, " ", ' ' symbols in user or organization names. These must be either in double quotes or proceeded by a \' symbol.

Related Commands

- Input: addalias, deletealias, deleteprovuser, deleteuser, displayprovuser, displayuser, encryption display_user, encryption modify_user, iplock add_range, im listforuser, listusers, modifydomain, modifyuser, org_im_settings modify, password force_update, password reset, promoteprovuser, resetuser, suspenduser, testfirewall, testmail, unblockprovuser, user_im_settings add, user_im_settings delete, user_im_settings display, user_im_settings modify
- Output: displayprovuser, displayuser, im list, listprovusers, listusers

Related Fields

primary_add

See Also

The Message Security Administration Guide, “User’s and Quarantines”

approved_recipients

The approved_recipients field holds an email address or domain to be added or removed from the Approved Recipients list which is also known as the Approved Mailing list located in the user’s Message Center.

Syntax

approved_recipients=< [+] | -user address>< [+] | -domain name>,... | ‘empty’

Examples

- When the field is returned as output, example as empty:

```
approved_recipients empty
```

- Adding a mailing list to the Approved Mailing list, either is correct:

```
modifyuser msmith@jumboinc.com,  
approved_recipients=+newupdates@hugeisp.com  
modifyuser msmith@jumboinc.com,  
approved_recipients=newupdates@hugeisp.com
```

- Removing a mailing list from a user's Approved Mailing list:

```
modifyuser msmith@jumboinc.com, approved_recipients=-  
newupdates@hugeisp.com
```

- Adding a domain and removing a domain from the Approved Mailing list, either is correct:

```
modifyuser msmith@jumboinc.com,  
approved_recipients="+jumboinc.com,-hugeisp.com"  
modifyuser msmith@jumboinc.com, approved_recipients="jumboinc.com,-  
hugeisp.com"
```

- Clearing the Approved Mailing list:

```
modifyorg sales, approved_recipients=NULL
```

Description

Approved recipient address list:

- (empty) -- This field is not active. It is empty.
- Lists can be comma delimited
- Each address or domain needs its own operator (+ or -). The + symbol is optional. The - symbol is required.

Field Type

User-level

Authorization

- Read: Sender Lists
- Write: Sender Lists

Notes

- Adding or deleting a domain applies to subdomains.
- Approved Recipient lists have a size limit of 4000 characters which approximately equates to 100 to 130 addresses and domains per list.

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

Related Fields

approved_senders (for orgs), blocked_senders (for users), blocked_senders (for orgs), approved_senders (for users)

See Also

“Viewing Message Center Settings” on page 536

The Message Security Administration Guide, “Approved and Blocked Sender Lists”

approved_senders (for users)

The approved_senders field holds an email address or domain to be added or removed from the user-level Approved Senders list in the user’s Message Center.

Syntax

approved_senders=<[+] | -user address>, ... | <[+] | -domainname>, ... | <empty>

Examples

- When the field is returned as output:

```
approved-sender empty
```

- Adding a sender to the user’s Approved Senders list, either is correct:

```
modifyuser msmith@jumbocinc.com, approved_senders=+jim@hugeisp.com  
modifyuser msmith@jumbocinc.com, approved_senders=jim@hugeisp.com
```

- Removing a sender from a user’s Approved Senders list:

```
modifyuser msmith@jumbocinc.com, approved_senders=jim@hugeisp.com
```

- Adding a domain and removing a domain from the Approved Senders list, either is correct:

```
modifyuser msmith@jumbocinc.com, approved_senders="+jumboinc.com,-hugeisp.com"
```

```
modifyuser msmith@jumbocinc.com, approved_senders="jumboinc.com,-hugeisp.com"
```

Note: See “approved_senders (for orgs)” on page 306 (for an org’s Approved Sender lists) for additional examples.

Description

Addresses and domains can be added or removed from the user’s Approved Senders list:

- Each address or domain needs its own operator (+ or -). The + symbol is optional. The - symbol is required.
- empty -- This field is not active. It is empty.
- Lists of addresses or domains are comma delimited, and must be enclosed in quotes.
- If on rare occasions an address has spaces, escape these spaces with backslashes.

Field Type

User-level

Authorization

- Read: Sender Lists
- Write: Sender Lists

Notes

- Mail from senders on this list will bypass the Junk Email filters.
- If virus blocking is enabled for the recipient, the message will not be delivered even though on the Approved Senders list.
- At the organization-level, the Blocked Senders list overrides the Approved Senders list. At the user-level, the Approved Senders list overrides the Blocked Senders list. The user-level Approved Senders list overrides the organization-level Blocked Senders list.
- Adding or deleting a domain applies to subdomains. For example, approving the domain jumboinc.com also approves the subdomain sales.jumboinc.com.
- User-level sender lists do not validate the sending email server against the domain
- Approved Senders lists have a size limit of 4000 characters which approximately equates to 100 to 130 addresses and domains per list.
- You can not have the same address in the approved_senders list and the blocked senders list. Unexpected results may happen.

Related Commands

- Input: adduser, modifyuser
- Output: displayuser
- Related: displayorg, modifyorg

Related Fields

approved_senders (for orgs), blocked_senders (for users), blocked_senders (for orgs), approved_recipients

See Also

“Viewing Message Center Settings” on page 536

“Viewing Message Center Settings” on page 536

The Message Security Administration Guide, “Approved and Blocked Sender Lists”

blocked_senders (for users)

The blocked_senders field lists an email address or a domain to be added or removed from the user-level Blocked Senders list. All messages from these senders or domains will be quarantined in the user's Message Center.

Syntax

```
blocked_senders=<[+] | -emailaddress> | <[+] | -domain name> | <empty>,...
```

Examples

- When the field is returned as output:

```
blocked-senders empty
```

- Adding a sender to the user's Blocked Senders list, either is correct:

```
modifyuser msmith@jumboinc.com, blocked_senders=+jim@hugeisp.com  
modifyuser msmith@jumboinc.com, blocked_senders=jim@hugeisp.com
```

- Removing a sender from the user's Blocked Senders list:

```
modifyuser msmith@jumboinc.com, blocked_senders=-jim@hugeisp.com
```

- Adding a domain and removing a domain from a user's Blocked Senders list, either is correct:

```
modifyuser msmith@jumboinc.com, blocked_senders="+jumboinc.com,-  
hugeisp.com"  
modifyuser msmith@jumboinc.com, blocked_senders="jumboinc.com,-  
hugeisp.com"
```

Note: See "blocked_senders (for orgs)" on page 321 (for an org's Blocked Sender lists) for additional examples.

Description

Addresses and domains can be added or removed from the Blocked Senders list:

- Each address or domain needs its own operator (+ or -). The + symbol is optional. The - symbol is required.
- empty -- This field is not active. It is empty.
- Lists of addresses or domains are comma delimited, and must be enclosed in quotes.
- If on rare occasions an address has spaces, escape these spaces with backslashes.

Field Type

User-level

Authorization

- Read: Senders Lists
- Write: Senders Lists

Notes

- Adding or deleting a domain from the list applies to subdomains. For example, approving the domain jumboinc.com also approves the subdomain sales.jumboinc.com.
- If an organization has Industry Heuristics turned on, messages with industry content will still be quarantined if the sender or domain is in user's Blocked Senders list.
- IP addresses can not be added to the user's Blocked Senders list. See the addallowedip command for more details.
- Blocked Senders lists have a size limit of 4000 characters which approximately equates to 100 to 130 addresses and domains per list.
- Top Level Domain (TLD) can not be blocked using an organization-level Blocked Senders list (.com, .edu, .uk).
- At the organization-level, the Blocked Senders list overrides the Approved Senders list. At the user-level, the Approved Senders list overrides the Blocked Senders list. The user-level Approved Senders list overrides the organization-level Blocked Senders list.

Related Commands

- Input: adduser, modifyuser
- Output: displayuser
- Related: displayorg, modifyorg, adddomain

Related Fields

approved_senders (for users), approved_senders (for orgs), blocked_senders (for users), blocked_senders (for orgs), approved_recipients

See Also

“Viewing Authentication and Password Settings” on page 540

“Viewing Message Center Settings” on page 536

The Message Security Administration Guide, “Approved and Blocked Sender Lists”

create_method (for users)

The create_method field shows how a user is created.

Syntax

create_method = < 0 | 1 | 2 | 3 | 5>

Examples

create_method=0

Description

Shows how a user was created.

- 0 -- Created using SMTP Autocreate, a deprecated feature
- 1 -- Created using Auto Web creation
- 2 -- Created using the Administration Console
- 3 -- Created using **adduser** batch command
- 5 -- Created using SmartCreate

Field Type

Users-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Notes

Organizations created during a Directory Sync synchronization are created by the addorg command, and the organizations' create_method field value is 3. Directory Sync is an optional feature.

Related Commands

- Input: listusers
- Output: displayuser, listusers

Related Fields

created_date (for users), created_ts (for users), create_method (for orgs)creator, support_contact

See Also

The Message Security Administration Guide, “User’s and Quarantines”

created_date (for users)

The created_date field shows when the user was created in UNIX seconds.

Syntax

created_date = <date in UNIX seconds >

Examples

```
created_date = 1145962000
```

Description

User creation date in UNIX seconds.

Field Type

User-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Notes

This field only applies to deployments of Perimeter Manager Enterprise Edition, Release 2.5 and later. This includes Message Security for Enterprises.

Related Commands

Output: displayuser

Related Fields

create_method (for users), created_date (for users), created_ts (for users), creator, support_contact

See Also

The Message Security Administration Guide, “User’s and Quarantines”

created_ts (for users)

The created_ts field holds the date the im_map record was created. This field applies to Postini IM Security, an optional product.

Syntax

created_ts= <user creation date>

Examples

- As output which is in UNIX seconds:

```
created_ts 1145962000
```

- The Administration Console output:

```
created_ts: 2006/04/14 00:36:28 GMT
```

Description

The date the im_map record was created. This date is displayed in the Administration Console in Greenwich Mean Time. For example:

```
created_ts: 2006/04/14 00:36:28 GMT
```

Field Type

User-level

Authorization

- Read: IM Management
- Write: Read-only for administrators

Related Commands

- Input: listusers
- Output: im display, listusers
- Related: listdomains

Related Fields

create_method (for users), created_date (for users), create_method (for orgs), creator, support_contact

See Also

filter_adult

The filter_adult field holds the sexual content filter settings for the user.

Syntax

filter_adult=<numeric | text string>

Examples

When assigning the field:

```
modifyuser msmith@jumboinc.com, filter_adult=11  
modifyuser msmith@jumboinc.com, filter_adult=moderate
```

When the field is returned:

```
filter_adult 15 (aggressive)
```

Description

Filter level of sexual content

- 11/off (1)
- 12/lenient (2)
- 13/moderate (3) (medium, in Message Center II)
- 14/moderately-aggressive (4) (aggressive, in Message Center II)
- 15/aggressive (5) (very aggressive, in Message Center II)

Field Type

User-level

Authorization

- Read: Spam Filter (Message Center Classic); Sexually Explicit (Message Center II)
- Write: Spam Filter (Message Center Classic); Sexually Explicit (Message Center II)

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

Related Fields

filter_bulk, filter_getrich, filter_offers, filter_racial, junkmail_filter

See Also

“Editing Message Center Access and Settings” on page 538

“Viewing Authentication and Password Settings” on page 540

The Message Security Administration Guide, “Users and Quarantines”

filter_bulk

The filter_bulk field holds the general spam filter setting for the user. This filter handles the bulk of the spam being blocked.

Syntax

```
filter_bulk=<number | text>
```

Examples

When the field is assigned:

```
modifyuser msmith@jumboinc.com, filter_bulk=11  
modifyuser msmith@jumboinc.com, filter_bulk=aggressive
```

When the field is returned:

```
filter_bulk 15 (aggressive)
```

Description

Level of general spam filtering:

- 11/lenient (1)
- 12/moderately-lenient (2) (very lenient, in Message Center II)
- 13/moderate (3) (medium, in Message Center II)
- 14/moderately-aggressive (4) (aggressive, in Message Center II)
- 15/aggressive (5) (very aggressive, in Message Center II)

Note: To turn off the spam filtering, see the field “junkmail_filter” on page 434

Field Type

User-level

Authorization

- Read: Spam Filters
- Write: Spam Filters

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

Related Fields

filter_adult, filter_getrich, filter_offers, filter_racial, junkmail_filter, *The Message Security Administration Guide*, “Approved and Blocked Sender Lists” (for orgs)

See Also

“Viewing Message Center Settings” on page 536

The Message Security Administration Guide, “Users and Quarantines”

filter_getrich

The filter_getrich field holds the Get Rich Quick category filter setting for the user.

Syntax

filter_getrich=<number | text>

Examples

When the field is assigned:

```
modifyuser msmith@jumboinc.com, filter_getrich=15  
modifyuser msmith@jumboinc.com, filter_getrich=lenient
```

When the field is returned:

```
filter_getrich 15 (aggressive)
```

Description

Level of get-rich-quick content:

- 11/off (1)
- 12/lenient (2)
- 13/moderate (3) (medium, in Message Center II)
- 14/moderately-aggressive (4) (aggressive, in Message Center II)
- 15/aggressive (5) (very aggressive, in Message Center II)

Field Type

User-level

Authorization

- Read: Spam Filters
- Write: Spam Filters

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

Related Fields

`filter_adult`, `filter_bulk`, `filter_offers`, `filter_racial`, `junkmail_filter`

See Also

[“Viewing Message Center Settings” on page 536](#)

[*The Message Security Administration Guide*, “Users and Quarantines”](#)

filter_offers

The `filter_offers` field holds the Special Offers category filter setting for the user.

Syntax

```
filter_offers=<number | text>
```

Examples

When the field is assigned:

```
modifyuser msmith@jumboinc.com, filter_offers=11  
modifyuser msmith@jumboinc.com, filter_offers=moderate
```

When the field is returned:

```
filter_offer 15 (aggressive)
```

Description

Level of special offer content:

- 11/off (1)
- 12/lenient (2)
- 13/moderate (3) (medium, in Message Center II)
- 14/moderately-aggressive (4) (aggressive, in Message Center II)
- 15/aggressive (5) (very aggressive, in Message Center II)

Field Type

User-level

Authorization

- Read: Spam Filters
- Write: Spam Filters

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

Related Fields

filter_adult, filter_bulk, filter_getrich, filter_racial, junkmail_filter

See Also

“Viewing Authentication and Password Settings” on page 540

The Message Security Administration Guide, “Users and Quarantines”

filter_racial

The filter_racial field holds Racially Insensitive category filter setting for the user.

Syntax

filter_racial=<number | text>

Examples

When the field is assigned:

```
modifyuser msmith@jumboinc.com, filter_racial=12  
modifyuser msmith@jumboinc.com, filter_racial=moderate
```

When the field is returned:

```
filter_racial 15 (aggressive)
```

Description

Level of racially insensitive content:

- 11/off (1)
- 12/lenient (2)
- 13/moderate (3) (medium, in Message Center II)
- 14/moderately-aggressive (4) (aggressive, in Message Center II)
- 15/aggressive (5) (very aggressive, in Message Center II)

Field Type

User-level

Authorization

- Read: Spam Filters
- Write: Spam Filters

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

Related Fields

filter_adult, filter_bulk, filter_getrich, filter_offers, filter_racial, junkmail_filter

See Also

“Viewing Message Center Settings” on page 536

The Message Security Administration Guide, “Users and Quarantines”

im_name

The im_name field holds the IM user's screen name. This field applies to Postini IM Security, an optional product.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

im_name=<protocol : IM screen name>

Examples

- When the field is returned as output:

```
im_name MSN:kristie_kerns@hotmail.com
```

- Adding an IM user:

```
im add im_name=MSN:kristie_kerns@hotmail.com,  
address=kkerns@jumboinc.com
```

Description

The IM user's screen name.

Field Type

User-level

Authorization

- Read: User Settings, IM Management
- Write: User Settings, IM Management

Related Commands

- Input: iplock add_range, im delete, im display, im listforuser
- Output: im display, im list, im listforuser

See Also

initial_password

The initial_password field holds the PMP password assigned to this user when the user was first added to the service.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

initial_password=<8 printable characters | NULL>

Examples

When a field is returned as output, example as empty:

```
initial_password NULL
```

Description

System generated temporary password for new users in orgs with PMP authentication. This password expires after 30 days.

- NULL -- This field is not active.

Field Type

User-level

Authorization

- Read: Change Passwords
- Write: Read-only for administrators

Notes

- Users are prompted to change the password when first logging into the Message Center/or Administration Console.
- Requires user org uses PMP authentication.

Related Commands

- Output: displayuser
- Related: adduser

Related Fields

authentication_data, authentication_type, password, remotecmd_secret

See Also

“Viewing Authentication and Password Settings” on page 540

The Message Security Administration Guide, , “Users and Quarantines”

junkmail_filter

The junkmail_filter field is an on/off switch for Spam Filtering.

Syntax

```
junkmail_filter=<off/0 | on/1>
```

Examples

- When the field is assigned:

```
modifyuser msmith@jumbocinc.com, junkmail_filter=on
```

- When the field is returned:

```
junkmail_filter 1 (on)
```

Description

Spam filtering control:

- off -- Junk email filtering is disabled
- on -- Junk email filtering is enabled

Note: The numeric equivalents to 'on' and 'off' are useful for debugging purposes. For robust production code, use the text value, 'on' or 'off'.

Field Type

User-level

Authorization

- Read: Junk Email Settings
- Write: Junk Email Settings

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

Related Fields

filter_adult, filter_bulk, filter_getrich, filter_offers, filter_racial

See Also

“Editing Message Center Access and Settings” on page 538

“Viewing Authentication and Password Settings” on page 540

The Message Security Administration Guide, “Spam Filters”

lang_locale (for users)

The lang_locale field enables user-level language localization in Message Center’s static text, the default top text, character sets, and date format.

Syntax

lang_locale=<language code string | NULL>

Examples

- When the field is returned as output, example as empty:

```
lang_locale NULL
```

- English (U.S.) UTF-8

```
modifyuser msmith@jumboinc.com, lang_locale=en_us.utf8
```

- Spanish (Spain) ISO 8859-1

```
modifyuser msmith@jumboinc.com, lang_locale=es.iso
```

Note: See the lang_locale (for orgs) for additional information.

Description

Language code used by Message Center.

- NULL -- This field is not active.

See the “Language and Timezone” on page 569 for a list of supported language codes.

Field Type

User-level

Authorization

- Read: Regional Settings
- Write: Regional Settings

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

See Also

“Viewing Authentication and Password Settings” on page 540

The Message Security Administration Guide, “Quarantine Summary & Notifications”

lastmod_date (for users)

The lastmod_date field shows the last time the user record was modified.

Syntax

lastmod_date=<time stamp>

Examples

When the field is returned as output:

```
lastmod_date 1145962000
```

Description

Timestamp of last record modification for the user's record. This is in UNIX seconds.

Field Type

User-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Related Commands

Output: displayuser

Related Fields

created_date (for users), created_ts (for users), lastmod_date (for orgs)

See Also

The Message Security Administration Guide, “Reports”

message_count

The message_count field holds the approximate number of messages received by this user within one day.

Syntax

message_count=<0 - 99999999>

Examples

When the field is returned from displayuser:

```
message_count 16
```

Description

Number of messages received today from the Message Security service.

The count goes up in increments of 8 for system performance optimization.

Field Type

User-level

Authorization

- Read: Traffic Limits
- Write: Read-only for administrators

Related Commands

Output: displayuser

See Also

“Viewing Message Center Settings” on page 536

The Message Security Administration Guide, “Users and Quarantines”

message_encrypt (for users)

The message_encryption field enables outbound user messages to be encrypted and sent to a secure portal. This field applies to Postini Message Encryption, which is only used with Message Security installations.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

message_encryption=<on | off | match | NULL ()>

Examples

- When the field is returned as output:

```
message_encryption NULL ()
```

- To change the setting:

```
modifyuser msmith@jumboinc.com, message_encryption=on
```

Note: See `message_encryption` (for an org's outbound encrypted messages) for additional examples.

Description

Enable external encryption:

- `on` -- Messages are always encrypted with Message Security.
- `off` -- Messages not encrypted with Message Security, but may have Transport Layer Security (TLS).
- `match` -- System looks in the message header for "string. If the string is found, the message is encrypted with Message Security. The default is `sensitivity: company-confidential`.
- `NULL ()` -- This field is not active.

Field Type

User-level

Authorization

- Read: Outbound External Encryption
- Write: Outbound External Encryption

Notes

Entries apply only to this user

Related Commands

- Input: `adduser`, `modifyuser`
- Output: `displayuser`
- Related: `displayorg`, `modifyorg`, `encryption modify_user`

Related Fields

`message_encryption` (for orgs)

See Also

Postini Encryption Services Administration Guide, “How Connection Security Works”

message_limit

The message_limit field holds the maximum number of messages allowed per day for this user.

Syntax

```
message_limit=<0 - 99999999> | NULL>
```

Examples

- When the field is returned as output:

```
message_limit 1000
```

- To change the setting:

```
modifyuser msmith@jumboinc.com, message_limit= 1000
```

Description

Number of message per day allowable:

- NULL -- No limit is set.

Note: If the number of messages exceed the limit, subsequent messages are deferred with a 400 error code asking the sending MTA to send again later.

Field Type

User-level

Authorization

- Read: Traffic Limits
- Write: Traffic Limits

Notes

- This limit can also be set for individual users or for the organization as a whole. Whichever limit is lower—the org limit or a user's limit—applies for the user. If a user's limit is blank and a value is set for the org, the org value applies to the user.
- When exceeded, incoming messages are bounced, returning a 554 Mailbox limit exceeded message to the sender.
- Setting a message limit is useful for protecting mail servers against malicious attacks, such as email bombs.
- All messages are counted against this limit, including legitimate and quarantined messages. The count is approximate, so it's suggested only for values over 100.

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

Related Fields

default_message_limit (for org), message_limited

See Also

“Viewing Message Center Settings” on page 536

The Message Security Administration Guide, “Users and Quarantines”

message_limited

The message_limited field is yes/no switch showing the user has reached the daily message limit.

Syntax

message_limited=<no/0 | yes/1>

Examples

When the field is returned from the displayuser command:

```
message_limited 0 (no)
```

Description

Shows the user has reached the message limit.

- no -- Message limit has not been reached
- yes -- Message limit has been reached

The numeric equivalents to ‘no’ and ‘yes’ are useful for debugging purposes. For robust production code, use the text value, ‘no’ or ‘yes’.

Field Type

User-level

Authorization

- Read: Traffic Limits
- Write: Read-only for administrators

Related Commands

Output: `displayuser`

See Also

[“Viewing Message Center Settings” on page 536](#)

[*The Message Security Administration Guide*, “Users and Quarantines”](#)

notice_address

The notice_address field holds the address where notifications for this user are sent.

Syntax

`notice_address=<legal email address | NULL>`

Examples

- When the field is returned as output:

```
notice_address msmith@jumboinc.com
```

- Adding a new user:

```
adduser jim@jumboinc.com, notice_address=support@jumboinc.com
```

- Clearing the notice_address field:

```
modifyuser msmith@jumboinc.com, notice_address=NULL
```

Description

Address to which system generated notices are sent.

- NULL -- This field is not active.

Field Type

User-level

Authorization

- Read: Change Address
- Write: Change Address

Notes

- For the Default User, enter an address here only if you intend for a single administrator to receive notifications for users in orgs using this Default User (not typical). Otherwise, leave this field blank when setting up a Default User account.
- Notifications include quarantine summary, notifications, and password changes.

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

See Also

“Editing Message Center Access and Settings” on page 538

The Message Security Administration Guide, “Users and Quarantines”

orgid

The orgid field holds a unique ID for the organization containing the user.

Syntax

orgid=<iid | orgtag>

Examples

- When the field is assigned:

```
orgid=org1
```

- When the field is returned:

```
orgid 100001012 (sales)
```

Description

The user level’s foreign key for the organization’s iid field.

Note: An organization has a text name and an associated iid value, a unique identifying organization number. The iid can be substituted for the orgid in some instances and is useful for debugging purposes. But for robust, finished production code, use the orgtag or orgname fields’ value.

- This organization must exist, and the admin must have the “User Settings” privileges at both the old and new organization.
- Enclose the organization’s name in double quotes if it contains an apostrophe or commas.

Field Type

User-level

Authorization

- Read: User Settings
- Write: User Settings

Notes

- The Batch interface allows apostrophes, commas, #, =, " " symbols in user or organization names. These must be either in double quotes or proceeded by a \' symbol.
- An organization can be referenced by several fields:
 - org - The organization name in the **displayspool** output
 - orgname -- The organization's string name (org-level)
 - orgtag -- The organization's string name in the database (org-level)
 - iid -- The organization's unique sequential database assigned key (org-level)
 - orgid -- The organization's iid or orgname for the organization containing the user.(user-level)

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

Related Fields

uid, u_id, user_id

See Also

The Message Security Administration Guide, “Users and Quarantines”

password

The password field holds the encrypted PMP user password.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

password=<printable characters>

Examples

- When the field is returned as output (encrypted):

password 3pds9999

- To change the setting (which is plain text):

modifyuser msmith@jumboinc.com, password=swordfish

Description

This holds the encrypted PMP user password. This allows assigning a new user a new password. The user will need this password to access the user's Message Center II and/or Administration Console if the user is an administrator.

Display shows the encrypted version. Input takes the plain version (modifyuser, password reset).

Default: minimum password length for an existing user who has migrated to the PMP password policy configuration is 1; minimum password length for new user of the PMP password policy configuration is 6 characters

Default: maximum password length is 32 characters

A PMP password must match the rules of complexity:

- Not be a dictionary word
- Not be the user's email address (user name, domain, or whole address)
- Three of these four criteria must be met before a password is accepted. An example is a8f2KTT*#. The password candidate must include one or more:
 - Lower case English letters (A thru Z)
 - Upper case English letters (a thru z)
 - Numbers (0 thru 9)
 - Symbols, for example !#\$%

Note: A PMP password will not work with a single quote ('), a double quote ("), a comma (,), or a backslash (/).

Field Type

User-level

Authorization

- Read: Change Passwords
- Write: Change Passwords

Related Commands

- Input: adduser, modifyuser, password reset
- Output: displayuser
- Related: resetuser

Related Fields

authentication_data, authentication_type, initial_password, remotecmd_secret

See Also

“Viewing Authentication and Password Settings” on page 540

“Editing a PMP Password” on page 541

The Message Security Administration Guide, “User Authentication”

primary

The primary field holds the primary user’s unique identifying ID.

Syntax

primary = <user ID>

Examples

```
primary 202846402
```

Description

The primary user ID (not a user alias)

Field Type

User-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Related Commands

Output: listusers

See Also

The Message Security Administration Guide, “Users and Quarantines”

primary_add

The primary_add field holds the primary user address.

Syntax

primary_add = < user name >

Examples

primary_add msmith@jumboinc.com

Description

The primary user address (not a user alias)

Field Type

User-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Notes

The Batch interface allows apostrophes, commas, #, =, " ", ‘ ’ symbols in user or organization names. These must be either in double quotes or proceeded by a \' symbol.

Related Commands

- Input: listusers
- Output: listusers

Related Fields

address, primary

See Also

The Message Security Administration Guide, “Users and Quarantines”

timezone (for users)

The timezone field holds the user’s timezone, a UNIX TZ string. This is used in Message Center, and for Message Center Classic scheduling of “quiet times,” when messages should not be forwarded to the user’s mobile device.

Syntax

timezone=<UNIX TZ string | NULL>

Examples

When the field is returned as output:

```
timezone MST7
```

Description

UNIX TZ timezone for Message Center, and for Message Center Classic user wireless email settings which applies only if Wireless Forwarding is enabled for the user.

- NULL -- This field is not active.

WARNING: Don't change this setting in the Administration Console. It should be managed by the users themselves, at the user's Message Center.

WARNING: This is not the Org setting for if users in this org receive a regularly scheduled Quarantined Summary notification, the notification is sent based on this time zone.

Default: timezone = NULL

Field Type

User-level

Authorization

- Read: User Settings
- Write: User Settings

Related Commands

- Input: adduser, listusers, modifyuser (see warning above)
- Output: displayuser, listusers

Related Fields

timezone (for orgs)

See Also

"Viewing Authentication and Password Settings" on page 540

The Message Security Administration Guide, "The Message Center"

TS1

The TS1 field holds the most recent timestamp for a good email message to a provisional user.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

TS1= < time in UNIX seconds >

Examples

TS1 1145962000

Description

Timestamp of the most recent good email message was received for a provisional user.

Field Type

Provisional user management

Authorization

- Read: Add Users
- Write: Read-only for administrators

Notes

Used with SmartCreate, newly added users are unconfirmed provisional users. These users are promoted to regular user after verified as associated with someone in your org by receiving 3 legitimate emails within a week. Or the user can be blocked or unblocked from being added to the Message Security service. Once the email criteria is met, the user is added to service. Otherwise the user is deleted.

Related Commands

- Input: listprovusers
- Output: displayprovuser
- Related: blockprovuser, deleteprovuser, promoteprovuser, unblockprovuser

Related Fields

address, TS3

See Also

The Message Security Administration Guide, “Users and Quarantines”

TS3

The TS3 field holds the timestamp for the oldest email message to a provisional user.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

TS3 = < time in UNIX seconds>

Examples

```
TS1 1145962000
```

Description

Timestamp of oldest email for a provisional user. The timestamp is in UNIX seconds.

If TS3=0, the user is blocked. See the **blockprovuser** command for more details.

Field Type

Provisional user management

Authorization

- Read: Add Users
- Write: Read-only for administrators

Notes

Used with SmartCreate, newly added users are unconfirmed provisional users. These users are promoted to regular user after verified as associated with someone in your org by receiving 3 legitimate emails within a week. Or the user can be blocked or unblocked from being added to the Message Security service. Once the email criteria is met, the user is added to service. Otherwise the user is deleted.

Related Commands

- Input: listprovusers
- Output: displayprovuser
- Related: blockprovuser, deleteprovuser, promoteprovuser, unblockprovuser

Related Fields

address, TS3

See Also

The Message Security Administration Guide, “Users and Quarantines”

uid

The uid field holds the user's unique ID.

Syntax

uid = < user ID >

Examples

uid 202846402

Description

The user's unique ID.

Field Type

User-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Related Commands

Output: listusers

Related Fields

orgid, u_id, user_id

See Also

The Message Security Administration Guide, “Users and Quarantines”

u_id

The u_id field holds a unique ID for this user.

Syntax

u_id=<user ID>

Examples

When the field is returned as output:

u_id 202846402

Description

Unique user ID. This is the same as the **uid** and **user_id** fields.

Field Type

User-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Related Commands

- Input: listusers
- Output: im display, listusers, user_im_settings display

Related Fields

orgid, uid, user_id

See Also

The Message Security Administration Guide, “Users and Quarantines”

user_id

The user_id field holds a unique ID for this user, and is useful when escalating an issue to Customer Care.

Syntax

user_id=<user ID>

Examples

When the field is returned:

```
user_id 2001122283
```

Description

Unique key for each user. A user's primary email address can be changed, but its ID always remains the same. This is the same as the **uid** and **u_id** fields.

Field Type

User-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Related Commands

Output: displayuser

Related Fields

orgid, uid, u_id

See Also

The Message Security Administration Guide, “Users and Quarantines”

virus_notify (for users)

The virus_notify field holds frequency of a user's virus notifications.

Syntax

```
virus_notify=<0 | 1 | 9 | NULL ()>
```

Examples

- When the field is returned as output:

```
virus_notify NULL ()
```

- To change the setting:

```
modifyuser msmith@jumboinc.com, virus_notify=1
```

Description

How frequently virus notification email will be generated:

- 0 -- Immediately
- 1 -- No more than one notice per day
- 9 -- Disable notifications
- NULL () -- This field is not active. Uses organization setting as the default.

Field Type

User-level

Authorization

- Read: Virus Settings
- Write: Virus Settings

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

See Also

“Setting a Virus Notification Interval” on page 549

The Message Security Administration Guide, “Virus Filters”

virus_state

The virus_state field is an on/off/unavailable switch for virus scanning functionality.

Syntax

```
virus_state=< 0/on | 1/off | 2/unavailable >
```

Examples

- When assigning the field:

```
modifyuser msmit@jumboinc.com, virus_state=on
```

- When the field is returned:

```
virus_state 0 (on)
```

Description

Virus scanning switch for on, off, not allowed.

- 0/on -- Virus scanning is enabled
- 1/off -- Virus scanning is disabled
- 2/unavailable -- Virus scanning is off and cannot be changed

Field Type

User-level

Authorization

- Read: Virus Settings
- Write: Virus Settings

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

See Also

The Message Security Administration Guide, “Virus Filters”

weblocked

The weblocked field is an on/off switch giving Message Center Access for the user.

Syntax

weblocked=<0/no | 1/yes>

Examples

- When assigning the field:

```
modifyuser msmit@jumboinc.com, weblocked=1
```

- When the field is returned:

```
weblocked 0 (no)
```

Description

Controls web access:

- 0/no -- The Message Center Access is enabled. The user can log in.
- 1/yes -- The Message Center Access is disabled. The user can not log in.

Field Type

User-level

Authorization

Write: Suspend User

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

See Also

“Editing Message Center Access and Settings” on page 538

The Message Security Administration Guide, “Users and Quarantines”

welcome_count

The welcome_count field holds whether a welcome message have been sent.

Syntax

welcome_count=<1 | 0>

Examples

When the field is returned as output:

```
welcome_count 1
```

Description

Records if a welcome message has been sent:

- 1 -- Welcome message has been sent
- 0 -- Welcome message has not been sent to new user

Field Type

User-level

Authorization

- Read: User Settings
- Write: Read-only for administrators

Related Commands

Output: displayuser

See Also

“Viewing Authentication and Password Settings” on page 540

“Seeing if a User Has Received a Welcome Notification” on page 547

The Message Security Administration Guide, “Customizing Notifications”

wireless_state

The wireless_state field is an on/off/unavailable switch for Wireless Forwarding which allows the user to forward messages to a text-enabled phone, PDA, or other mobile device.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

```
wireless_state=<0/on | 1/off | 2/unavailable>
```

Examples

- When assigning the field:

```
modifyuser msmith@jumboinc.com, wireless_state=0
```

- When the field is returned:

```
wireless_state 1 (off)
```

Description

Wireless email switch:

- 0/on -- When checked, users can enable Wireless Forwarding at the Message Center.
- 1/off -- This feature is not available to this user.
- 2/unavailable -- Temporarily unavailable for a user, but does not remove the user's permission.

Field Type

User-level

Authorization

Write: Wireless Settings

Notes

- Available only to North American users and applies only to Message Center Classic.
- To make Wireless Forwarding temporarily unavailable for a user without removing this permission, set Wireless Forwarding in the user's General Settings to "Not allowed."

Related Commands

- Input: adduser, modifyuser
- Output: displayuser

See Also

"Editing Message Center Access and Settings" on page 538

The Message Security Administration Guide, "Customizing Notifications"

Chapter 8

Batch Domain Fields

About Batch Domain Fields

The batch domain fields hold domain-level data which a command can either create, delete, display, list, or modify. This information is diverse. It can be names, email addresses, numbers, dispositions, on/off switches, boolean true/false values.

Domain Field Reference Page Syntax Notations

Each field's syntax uses notation and punctuation to show you where to put your specific information, and what information is required or optional:

The reference pages use the Administration Console syntax and have an example for each field:

- The field name is required. In the Administration Console, commas are required.
- Information between '< >' symbols means you need to add your specific information here. (For example: <field>=<value> becomes domainname=@hugeisp.com)
- Information between '[]' square brackets mean this type of information is optional.
- A choice of values are separated by '|'. (for example: substrip= <on | off> means you have a choice of substrip=on, or substrip=off)
- It is important to confirm you have authorization to display or edit a field (Read/Write authorization). The Authorization section shows each field's requirements.
- The Related Commands section shows which commands take the field as input or as output. Input means the field is used in the command's arguments. Output means the command returns this field-value pair when the command is successfully executed.

See "Batch Command and Field Quick Summary" on page 27, and "Batch Field Quick Summary" on page 111 for additional information.

alias

The alias field holds the domain's aliases.

Syntax

alias = <alias>, ...

Examples

```
modifydomain jumboinc.com, alias=jumboalias.com
```

Description

Lists a domain's aliases.

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Edit Organizations, Manage Domains

Related Commands

Related: modifydomain

Related Fields

aliasfrom, aliasedto

See Also

The Message Security Administration Guide, “Domains”

aliasedfrom

The aliasedfrom field lists a domain's aliases.

Syntax

aliasedfrom < domain's alias >, ...

Examples

aliasedfrom jumbo.com

aliasedfrom "jumbo.com, jumboincwest.com"

Description

Lists a domain's aliases.

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Read-only for administrators

Related Commands

Output: displaydomain

See Also

The Message Security Administration Guide, “Domains”

aliasedto

The aliasedto field lists the domain associated with this alias.

Syntax

aliasedto <primary domain name>

Examples

aliasedto jumboinc.com

Description

Lists the domain associated with this alias.

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Read-only for administrators

Related Commands

Output: displaydomain

See Also

The Message Security Administration Guide, “Domains”

catchall

This is a legacy feature, and available if your account has been configured for a catchall account. This feature has been superseded by Non Account Virus Blocking, which automatically deletes viruses for unregistered accounts. See the organization field, **non_account_virus_scan**, to enable this feature.

The catchall field holds the user account assigned as the Catchall User for the initial domain.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

catchall = <user address | NONE>

Examples

```
catchall catchalluser@jumboinc.com
```

Description

User account assigned as the Catchall User for the initial domain.

- user address -- Catchall User mail address
- NONE -- This feature is not available for this organization.

The catchall parameter automatically disables **non_account_bounce**

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Read-only for administrators

Notes

- This is a legacy feature available to some accounts. This feature is only available if your account has been configured for a catchall account. If your organization is not configured for catchall email, you will get a system error. The catchall feature is not available in the Postini Web Services API. For more information, please contact Support.
- For robust production code, use the **non_account_virus_scan** field, which filters inbound email for viruses, even for unregistered users.
- Do not create an alias for a domain with a Catchall User. The Catchall User should be configured with the primary domain name. The catchall configuration acts as a user alias and takes precedence over a domain alias. The domain alias will not function if a Catchall User is configured with it.

Related Commands

Input: modifydomain

Related Fields

non_account_virus_scan

See Also

The Message Security Administration Guide, “Domains”

created_ts (for domains)

The created_ts (for domains) field holds the domain's creation timestamp.

Syntax

created_ts <timestamp in UNIX seconds>

Examples

created_ts 1145962000

Description

Contains the domains creation timestamp.

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Read-only for administrators

Related Commands

- Input: listdomains
- Output: listdomains

Related Fields

created_ts (for users)

See Also

The Message Security Administration Guide, “Reports”

domainid

The domainid field holds the domain’s unique ID.

Syntax

domainid = < domain ID >

Examples

domainid 100001012

Description

Holds the domain’s unique ID.

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Read-only for administrators

Related Commands

- Input: deletedomain, displaydomain, listdomains
- Output: listdomains

Related Fields

domainname, primary_did

See Also

The Message Security Administration Guide, “Domains”

domainname

The domainname field holds the name of the domain.

Syntax

domainname=< domain name >

Examples

- When the field is returned as output:

domainname jumboinc.com

- To delete the domain with the domainname ‘jumboinc.com’:

deletedomain jumboinc.com

Description

Name of the domain

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Edit Organizations, Manage Domains

Related Commands

- Input: adddomain, deletedomain, displaydomain, domain_tls add, domain_tls delete, domain_tls modify, iplock add_range, iplock delete, iplock delete_range, iplock display, iplock set_disposition, listdomains, modifydomain, testmx
- Output: displaydomain, listdomains

Related Fields

domainid, iid, org (for domains), primary_did, substrip

See Also

The Message Security Administration Guide, “Domains”

org (for domains)

The org field holds the organization associated with the domain.

Syntax

org = <org name>

Examples

When the field is returned as output:

```
org sales
```

Description

The organization associated with this domain.

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Read-only for administrators

Related Commands

Output: `displaydomain`

See Also

The Message Security Administration Guide, “Domains”

primary_did

The primary_did field holds the primary domain ID.

Syntax

`primary_did = <domain ID>`

Examples

```
primary_did 100001012
```

Description

A primary domain's ID (not an alias).

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Read-only for administrators

Related Commands

Output: listdomains

See Also

The Message Security Administration Guide, “Domains”

primary_dom

The primary_dom field holds the primary domain name associated with a domain alias.

Syntax

primary_dom = < primary domain name >

Examples

primary_dom jumboinc.com

Description

The primary domain's name associated with a domain alias.

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Read-only for administrators

Related Commands

Output: listdomains

See Also

The Message Security Administration Guide, “Domains”

substrip

The substrip field enables subdomain stripping for the domain.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

substrip=< on/1 | off/0 >

Examples

substrip=on

Description

Enables Subdomain Stripping for a domain. The sub domains become aliases for the primary domain.

- on -- Domain stripping is enabled
- off -- Domain stripping is disabled

Note: The substrip field is the same as the **sub_strip** field.

Default: substrip = off

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Edit Organizations, Manage Domains

Related Commands

- Input: adddomain, modifydomain
- Output: displaydomain, setorgsubstripping

See Also

The Message Security Administration Guide, “Domains”

sub_strip

The sub_strip field enables subdomain substripping for the domain.

This field is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Syntax

sub_strip=< on/1 | off/0 >

Examples

sub_strip=on

Description

Enables subdomain substripping for a domain. The sub domains become aliases for the primary domain.

- on -- Domain substripping is enabled
- off -- Domain substripping is disabled

Note: The sub_strip field is the same as the **substrip** field.

Default: sub_strip = off

Field Type

Domain

Authorization

- Read: Edit Organizations, Manage Domains
- Write: Edit Organizations, Manage Domains

Related Commands

- Input: adddomain, modifydomain
- Output: displaydomain, setorgsubstripping

See Also

The Message Security Administration Guide, “Domains”

Chapter 9

Batch Report Fields

About Batch Report Fields

The batch report fields hold the return data displayed by the getorgreport command. The reports return information about your organization's traffic, spam, virus, and billing/usage activity.

Report Field Reference Page Syntax Notations

Each field's syntax section uses notation to show you what type of information is returned:

The reference pages use the Administration Console syntax and have an example for each field:

- Information between '< >' symbols shows the specific type of information this field will contain.
- It is important to confirm you have authorization to display a report field (Read/Write authorization). The Authorization section shows each field's requirements.

See "Batch Command and Field Quick Summary" on page 27, and "Batch Field Quick Summary" on page 111 for additional information.

acc_messages

The acc_messages field holds the number of email messages sent to accounts or aliases registered in the Message Security service for the Traffic Report.

Syntax

acc_messages = <string of total number of message>

Examples

When the field is returned as output:

```
acc_message 2
```

For a traffic summary report in the Administration Console, acc_messages is the same as Acct Msgs.

Description

The number of email messages sent to accounts or aliases registered in the Message Security service in inbound Traffic Report.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators
- Review the **getorgreport** command authorizations before running the Traffic Report summary.

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

num_bh_messages, num_bytes, num_f_messages, num_messages,
num_q_messages, pct_bh_bytes, pct_bh_messages, pct_f_bytes,
pct_f_messages, pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports

account

The account field holds the user account for spam and virus messages in the org-level Spam and Virus Reports.

Syntax

account = <account name>

Examples

When the field is returned as output:

```
account Sales
```

Description

Virus and Spam Report account name.

Field Type

Org Virus and Spam Reports

Authorization

- Read: View Reports
- Write: Read-only for administrators
- Review the **getorgreport** command authorizations before running the Spam or Virus Report summary.

Related Commands

Output: getorgreport (Org Virus and Spam Summary Reports)

Related Fields

- spam: bad_isp, bad_sender, bulk, bytes, commerce, deliveries, mmf, naughty, num_spams, racial, ssb
- virus: bytes, cleanings, clean_failures, inf_deliveries, num_viruses

See Also

The Message Security Administration Guide, “Reports”

bad_isp

The bad_isp field holds the total number of quarantined messages due to a Blocked Senders listed domain. Used in the Spam Report.

Syntax

bad_isp= <total number string>

Examples

When the field is returned as output:

```
bad_isp 3
```

Description

Messages quarantined because the domain was listed in the Blocked Senders list, not a specific address.

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Note: Review the **getorgreport** command authorizations before running the Spam Report summary.

Related Commands

Output: getorgreport

Related Fields

account, bad_sender, bulk, bytes, commerce, deliveries, mmf, naughty, num_spams, racial, ssb

See Also

The Message Security Administration Guide, “Reports”

bad_sender

The bad_sender field holds the total number of quarantined messages due to the sender being listed on the Blocked Senders list either at the org or user level. Used in the Spam Report.

Syntax

bad_sender= <total number string>

Examples

When the field is returned as output:

```
bad_sender 3
```

Description

Messages quarantined because the sender was listed in the Blocked Senders list either at org or user levels.

Notes

Mail messages that do not match a domain's IP block and have a quarantine disposition, are included in the bad_sender field's total.

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Spam Report summary.

Related Commands

Output: getorgreport

Related Fields

account, bad_isp, bulk, bytes, commerce, deliveries, mmf, naughty, num_spams, racial, ssb

See Also

The Message Security Administration Guide, “Reports”

bulk

The bulk field holds the total number of messages quarantined by the general category for junk email filtering for the Spam Report

Syntax

bulk= <total number string>

Examples

When the field is returned as output:

```
bulk 3
```

Description

General category for junk email filtering (may include characteristics of the other specific filter categories).

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Spam Report summary.

Related Commands

Output: **getorgreport** (Org Spam Summary Report)

Related Fields

account, bad_isp, bad_sender, bytes, commerce, deliveries, mmf, naughty, num_spams, racial, ssb

See Also

The Message Security Administration Guide, “Reports”

bytes

The bytes field holds the total number of quarantined spam or virus messages in bytes for the Spam or Virus Report.

Syntax

bytes= <total number string>

Examples

When the field is returned as output:

```
bytes 3
```

Description

Spam and Virus Bytes. Total size of quarantined spam or virus messages.

Field Type

Org Spam and Virus Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Spam or Virus Report summary.

Related Commands

Output: getorgreport (Org Spam and Virus Summary Reports)

Related Fields

- virus: account, cleanings, clean_failures, inf_deliveries, num_viruses
- spam: account, bad_isp, bad_sender, bulk, commerce, deliveries, mmf, naughty, num_spams, racial, ssb

See Also

The Message Security Administration Guide, “Reports”

cleanings

The cleanings field holds the number of viruses cleaned for the Virus Report.

Syntax

cleanings= <total number string>

Examples

When the field is returned as output:

```
cleanings 3
```

Description

Total number of viruses cleaned.

Field Type

Org Virus Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Virus Report summary.

Related Commands

Output: getorgreport (Org Virus Summary Report)

Related Fields

account, bytes, clean_failures, inf_deliveries, num_viruses

See Also

The Message Security Administration Guide, “Reports”

clean_failures

The clean_failures field holds the number of viruses cleaning failures for the Virus Report.

Syntax

clean_failures= <total number string>

Examples

When the field is returned as output:

```
clean_failures 3
```

Description

Total number of viruses cleaning failures.

Field Type

Org Virus Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Virus Report summary.

Related Commands

Output: getorgreport (Org Virus Summary Report)

Related Fields

account, bytes, cleanings, inf_deliveries, num_viruses

See Also

The Message Security Administration Guide, “Reports”

commerce

The commerce field holds the number of filtered special offers for the Spam Report.

Syntax

commerce= <total number string>

Examples

When the field is returned as output:

```
commerce 3
```

Description

Total number of filtered special offers.

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Spam Report summary.

Related Commands

Output: getorgreport (Org Spam Summary Report)

Related Fields

account, bad_isp, bad_sender, bulk, bytes, deliveries, mmf, naughty, num_spams, racial, ssb

See Also

The Message Security Administration Guide, “Reports”

customerid

The customerid field holds unique identifying number for an Message Security service account customer. Used in the Usage Report.

Syntax

customerid=<unique id>

Examples

As part of the settings output of the getorgreport command:

```
customerid 11111101
```

Description

Unique customer ID.

Field Type

Org Report Management

Authorization

- Read: Account-level permissions
- Write: Read-only for administrators

Note: Review the **getorgreport** command authorizations before running the Usage Report summary.

Related Commands

Output: getorgreport

Related Fields

customername, messages, productid, sellerid, stored_size, users

See Also

The Message Security Administration Guide, “Reports”

customername

The customername field holds the name of the customer. Used in the Usage Report.

Syntax

customername=<customer name>

Examples

As part of the usage_summary report output of the getorgreport command:

```
customername Jumbo Inc
```

Description

Usage summary report field for customer's name.

Field Type

Org Report Management

Authorization

- Read: Account-level permissions
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Usage Report summary.

Related Commands

Output: getorgreport

Related Fields

customerid, messages, productid, sellerid, stored_size, users

See Also

The Message Security Administration Guide, “Reports”

deliveries

The deliveries field holds the number of spam messages delivered from Quarantine to the user’s mailbox for the Spam Report.

Syntax

deliveries= <total number string>

Examples

When the field is returned as output:

```
deliveries 3
```

Description

Total number of spam messages delivered from Quarantine to the user's mailbox.

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Spam Report summary.

Related Commands

Output: getorgreport Org Spam Summary Report)

Related Fields

account, bad_isp, bad_sender, bulk, bytes, commerce, mmf, naughty, num_spams, racial, ssb

See Also

The Message Security Administration Guide, “Reports”

inf_deliveries

The inf_deliveries field holds the total number of infected deliveries from quarantine virus messages for the Virus Report.

Syntax

inf_deliveries = <total number string>

Examples

When the field is returned as output:

```
inf_deliveries 3
```

Description

Total number of infected deliveries from quarantine spam messages.

Field Type

Org Virus Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Virus Report summary.

Related Commands

Output: getorgreport

Related Fields

account, bytes, cleanings, clean_failures, num_viruses

See Also

The Message Security Administration Guide, “Reports”

messages

The messages field holds the total number of messages for the Usage Report.

Syntax

messages=<number of messages in report>

Examples

When the field is returned as output:

```
messages 11
```

Description

Number of messages in Usage Report output

Field Type

Org Report Management

Authorization

- Read: Account-level permissions
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Usage Report summary.

Related Commands

Output: getorgreport

Related Fields

customerid, customername, productid, sellerid, stored_size, users

See Also

The Message Security Administration Guide, “Reports”

mmf

The mmf field holds the total number of Get Rich messages for the Spam Report.

Syntax

mmf= <total number string>

Examples

When the field is returned as output:

```
mmf 3
```

Description

Total number of Get Rich messages in the Spam Report.

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Spam Report summary.

Related Commands

Output: getorgreport (Org Spam Summary Report)

Related Fields

account, bad_isp, bad_sender, bulk, bytes, commerce, deliveries, naughty, num_spams, racial, ssb

See Also

The Message Security Administration Guide, “Reports”

naughty

The naughty field holds the total number of messages triggering the Sexually Explicit junk email filter for the Spam Report.

Syntax

naughty= <total number string>

Examples

When the field is returned as output

```
naughty 3
```

Description

Total number of messages triggering the Sexually Explicit junk email filter.

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Spam Report summary.

Related Commands

Output: **getorgreport** (Org Spam Summary Report)

Related Fields

account, bad_isp, bad_sender, bulk, bytes, commerce, deliveries, mmf, num_spams, racial, ssb

See Also

The Message Security Administration Guide, “Reports”

num_bh_messages

The num_bh_messages field holds the total size of blackholed messages for the Traffic Report.

Syntax

num_bh_messages= <total number string>

Examples

When the field is returned as output:

```
num_bh_messages 3
```

For a traffic summary report in the Administration Console, num_bh_messages is the same as Blocked Acct Msgs.

Description

Total number of blackholed messages.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Review the **getorgreport** command authorizations before running the Traffic Report summary.

Related Commands

Output: getorgreport

Related Fields

acc_messages, num_bytes, num_f_messages, num_messages,
num_q_messages, pct_bh_bytes, pct_bh_messages, pct_f_bytes,
pct_f_messages, pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

num_bytes

The num_bytes field holds the total size of messages in bytes for the Traffic Report.

Syntax

num_bytes= <total number string>

Examples

When the field is returned as output:

```
num_bytes 3
```

For a traffic summary report in the Administration Console, num_bytes is the same as Bytes.

Description

Total number of messages in bytes.

Field Type

Org Traffic Report

Authorization

Read: View Reports

Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_f_messages, num_messages,
num_q_messages, pct_bh_bytes, pct_bh_messages, pct_f_bytes,
pct_f_messages, pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

num_f_messages

The num_f_messages field holds the total number of messages delivered directly to your mail server for all addresses in the server’s domain for the Traffic Report. This is Forward Acct Messages.

Syntax

num_f_messages= <total number string>

Examples

When the field is returned as output:

```
num_f_messages 3
```

For a traffic summary report in the Administration Console, num_f_messages is the same as Forward Acct Msgs.

Description

Total number of messages delivered directly to your mail server for all addresses in the server's domain.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_messages,
num_q_messages, pct_bh_bytes, pct_bh_messages, pct_f_bytes,
pct_f_messages, pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

num_messages

The num_messages field holds the total number of messages passed through the Message Security service for the Traffic Report.

Syntax

num_messages= <total number string>

Examples

When the field is returned as output:

```
num_messages 3
```

For a traffic summary report in the Administration Console, num_messages is the same as Messages.

Description

Total number of messages passed through the Message Security service.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_f_messages,
num_q_messages, pct_bh_bytes, pct_bh_messages, pct_f_bytes,
pct_f_messages, pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

num_q_messages

The num_q_messages field holds the total number of quarantined messages for the Traffic Report.

Syntax

num_q_messages= <total number string>

Examples

When the field is returned as output:

```
num_q_messages 3
```

For a traffic summary report in the Administration Console, num_q_messages is the same as Quarantined Acct Msgs.

Description

Total number of quarantined messages.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_f_messages,
num_messages, pct_bh_bytes, pct_bh_messages, pct_f_bytes, pct_f_messages,
pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

num_spams

The num_spams field holds the number of quarantined spam for the Spam Report.

Syntax

num_spams= <total number string>

Examples

When the field is returned as output:

```
num_spams 3
```

Description

Total number of quarantined spam.

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Spam Summary Report)

Related Fields

account, bad_isp, bad_sender, bulk, bytes, commerce, deliveries, mmf, naughty, racial, ssb

See Also

The Message Security Administration Guide, “Reports”

num_viruses

The num_viruses field holds the total number of quarantined viruses for the Virus Report.

Syntax

num_viruses = <total number string>

Examples

When the field is returned as output:

```
num_viruses 3
```

Description

Total number of quarantined viruses.

Field Type

Org Virus Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Virus Summary Report)

Related Fields

account, bytes, cleanings, clean_failures, inf_deliveries

See Also

The Message Security Administration Guide, “Reports”

pct_bh_bytes

The pct_bh_bytes field holds the total percent of blackholed messages in bytes for the Traffic Report.

Syntax

pct_bh_bytes= <total number string>

Examples

When the field is returned as output:

```
pct_bh_bytes 3.0
```

For a traffic summary report in the Administration Console, pct_bh_bytes is the same as Blocked Acct Msgs, % of Bytes.

Description

Total number of percent of blackholed messages in bytes.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_f_messages,
num_messages, num_q_messages, pct_bh_messages, pct_f_bytes,
pct_f_messages, pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

pct_bh_messages

The pct_bh_messages field holds the total percent of blackholed messages for the Traffic Report.

Syntax

pct_bh_messages= <total number string>

Examples

When the field is returned as output:

```
pct_bh_messages 3.0
```

For a traffic summary report in the Administration Console, pct_bh_messages is the same as Blocked Acct Msgs, % of Messages.

Description

Total number of percent of blackholed messages.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_f_messages,
num_messages, num_q_messages, pct_bh_bytes, pct_f_bytes, pct_f_messages,
pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

pct_f_bytes

The pct_f_bytes field holds the total percent of bytes delivered to your mail server for the account in bytes for the Traffic Report.

Syntax

pct_f_bytes= <total number string>

Examples

When the field is returned as output:

```
pct_f_bytes 3.0
```

For a traffic summary report in the Administration Console, pct_f_bytes is the same as Forwarded Acct Msgs, % of Bytes.

Description

Total number of percent of forwarded messages in bytes whether blackholed or bounced.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_f_messages,
num_messages, num_q_messages, pct_bh_bytes, pct_bh_messages,
pct_f_messages, pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

pct_f_messages

The pct_f_messages field holds the total percent of messages delivered to your mail server for the account for the Traffic Report.

Syntax

pct_f_messages= <total number string>

Examples

When the field is returned as output:

```
pct_f_messages 3.0
```

For a traffic summary report in the Administration Console, pct_f_messages is the same as Forwarded Acct Msgs, % of Msgs.

Description

Total number of percent of forwarded messages.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_f_messages,
num_messages, num_q_messages, pct_bh_bytes, pct_bh_messages,
pct_f_bytes, pct_q_bytes, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

pct_q_bytes

The pct_q_bytes field holds the total percent of quarantined messages in bytes for the Traffic Report.

Syntax

pct_q_bytes= <total number string>

Examples

When the field is returned as output:

```
pct_q_bytes 3.0
```

For a traffic summary report in the Administration Console, pct_q_bytes is the same as Quarantined Acct Msgs, % of Bytes.

Description

Total number of percent of quarantined messages in bytes.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_f_messages,
num_messages, num_q_messages, pct_bh_bytes, pct_bh_messages,
pct_f_bytes, pct_f_messages, pct_q_messages, recip

See Also

The Message Security Administration Guide, “Reports”

pct_q_messages

The pct_q_messages field holds the total percent of quarantined messages for the Traffic Report.

Syntax

pct_q_messages= <total number string>

Examples

When the field is returned as output:

pct_q_messages 3.0

For a traffic summary report in the Administration Console, pct_q_messages is the same as Quarantined Acct Msgs, % of Msgs.

Description

Total number of percent of quarantined messages.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_f_messages,
num_messages, num_q_messages, pct_bh_bytes, pct_bh_messages,
pct_f_bytes, pct_f_messages, pct_q_bytes, recip

See Also

The Message Security Administration Guide, “Reports”

productid

The productid field holds the Message Security service product name for the Usage Report.

Syntax

productid=<name of product>

Examples

As part of the settings output of the getorgreport command:

```
productid ee
```

Description

Product name used in the Usage Report.

Field Type

Org Report Management

Authorization

- Read: Account_level permissions
- Write: Read-only for administrators

Related Commands

Output: getorgreport

Related Fields

customerid, customername, messages, sellerid, stored_size, users

See Also

The Message Security Administration Guide, “Reports”

racial

The racial field holds the number of messages triggering the Racially Insensitive junk email filter for the Spam Report.

Syntax

racial= <total number string>

Examples

When the field is returned as output:

```
racial 3
```

Description

Total number of messages triggering the Racially Insensitive junk email filter.

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Spam Summary Report)

Related Fields

account, bad_isp, bad_sender, bulk, bytes, commerce, deliveries, mmf, naughty, num_spams, ssb

See Also

The Message Security Administration Guide, “Reports”

recip

The recip field holds the email address of the recipient account for the Traffic Report.

Syntax

recip= <email address>

Examples

When the field is returned as output:

```
recip msmith@jumboinc.com
```

For a traffic summary report in the Administration Console, recip is the same as Recipient.

Description

Email address of the recipient account.

Field Type

Org Traffic Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Traffic Summary Report)

Related Fields

acc_messages, num_bh_messages, num_bytes, num_f_messages,
num_messages, num_q_messages, pct_bh_bytes, pct_bh_messages,
pct_f_bytes, pct_f_messages, pct_q_bytes, pct_q_messages

See Also

The Message Security Administration Guide, “Reports”

sellerid

The sellerid field holds the unique identifying number of the Message Security service seller for the Usage Report

Syntax

sellerid=<seller's id>

Examples

As part of the settings output of the getorgreport command:

```
sellerid 11111801
```

Description

Holds the unique identifying number of the Message Security service seller for the Usage Report.

Field Type

Org Usage Report Management

Authorization

- Read: Account-level permissions
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Usage Summary Report)

Related Fields

customerid, customername, messages, productid, stored_size, users

See Also

The Message Security Administration Guide, “Reports”

ssb

The ssb field holds the number of messages impacted by the Blatant Spam Blocking for the Spam Report.

Syntax

ssb= <total number string>

Examples

When the field is returned as output:

```
ssb 3
```

Description

Total number of messages impacted by the Blatant Spam Blocking filter.

Field Type

Org Spam Report

Authorization

- Read: View Reports
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Spam Summary Report)

Related Fields

account, bad_isp, bad_sender, bulk, bytes, commerce, deliveries, mmf, naughty, num_spams, racial

See Also

The Message Security Administration Guide, “Reports”

stored_size

The stored_size field holds the total number of stored message bytes in the archive for the last month for the Usage Report. This field applies to Postini Message Archiving, an optional product.

Syntax

stored_size=< number of messages in bytes >

Examples

As part of the settings output of the getorgreport command:

```
stored_size 0
```

Description

Holds the total number of stored messages in bytes in the archive for the last month. The total is rounded to the nearest gigabyte.

Field Type

Org Report Management

Authorization

- Read: Account-level permissions
- Write: Read-only for administrators

Related Commands

Output: getorgreport

Related Fields

customerid, customername, messages, productid, sellerid, users

See Also

The Message Security Administration Guide, “Reports”

users

The users field holds the total number of users in the Usage Report.

Syntax

users=<number of users>

Examples

As part of the settings output of the getorgreport command:

```
users 11
```

Description

Number of primary users listed in a Usage Report for an organization. The total does not include user aliases.

Field Type

Org Report Management

Authorization

- Read: Account-level permissions
- Write: Read-only for administrators

Related Commands

Output: getorgreport (Org Usage Summary Report)

Related Fields

customerid, customername, messages, productid, sellerid, stored_size

See Also

The Message Security Administration Guide, “Reports”

Chapter 10

Batch Spool Fields

About Batch Spool Fields

The batch spool fields hold the return data displayed by the displayspool command. These fields are associated with your email config organization.

These fields are applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Spool Field Reference Page Syntax Notations

Each field's syntax section uses a notation to show you what type of information is returned:

The reference pages use the Administration Console syntax and have an example for each field:

- Information between '< >' symbols shows the specific type of information this field will contain.
- A range of possible values are separated by '|'. (for example: `spool_delay=<900 | 1800 | 3600>` means you have a choice of `spool_delay=900`, `spool_delay=1800`, or `spool_delay=3600`)
- It is important to confirm you have authorization to display the displayspool output (Read/Write authorization). The Authorization section shows each field's requirements.

See “Batch Command and Field Quick Summary” on page 27, and “Batch Field Quick Summary” on page 111 for additional information.

auto_unspool

The auto_unspool field is the on/off switch for automatically delivering spooled messages.

Syntax

```
auto_unspool=<off/0 | on/1>
```

Examples

When the field is returned as output:

```
auto_unspool 0
```

Description

Switch for delivering spooled messages automatically:

- on -- Automatic unspooling is enabled. While you have spooled mail, Spool Manager will poll your server one time per minute until it has been available for 3 subsequent minutes. Then, it will automatically stop spooling and unspool your spooled mail.
- off -- Automatic unspooling is disabled. Manual unspooling is enabled

Note: The numeric equivalents to on and off are useful for debugging purposes. For robust production code, use the text value, on or off.

Field Type

Org Spool management

Authorization

- Read: Spooling
- Write: Read-only for administrators

Related Commands

Output: displayspool

Related Fields

despool_max_connections, duration, org (for spooling), quota, spool_delay, spool_mech, status, used_pct, used_size

See Also

The Message Security Administration Guide, “Spool Manager”

despool_max_connections

The despool_max_connections field holds the maximum number of dedicated connections which will deliver your spooled mail when an outage is complete. This is the Unspooling Connection Rate.

Syntax

despool_max_connections=<number of dedicated connections string>

Examples

When the field is returned as output:

```
despool_max_connections 5
```

Description

Number of dedicated connections which will deliver your spooled mail when an outage is complete.

Field Type

Org Spool management

Authorization

- Read: Account-level Spooling
- Write: Read-only for Account organization administrators

Notes

- This rate should deliver messages at a volume that your mail servers can safely manage. We recommend allocating no more than 15% of the sum of your connection limits.
- The despool_max_connections field is the same as the Unspooling Rate field in the Administration Console batch return value.

Related Commands

Output: displayspool

Related Fields

auto_unspool, duration, org (for spooling), quota, spool_delay, spool_mech, status, used_pct, used_size

See Also

The Message Security Administration Guide, “Spool Manager”

duration

The duration field holds the amount of time since spooling was last activated, or the amount of time that spooling has been activated.

Syntax

duration=<duration time in UNIX seconds >

Examples

When the field is returned as output:

```
duration 1800
```

Description

Amount of time since spooling was last activated, or the amount of time that spooling has been activated.

Field Type

Org Spool management

Authorization

- Read: Spooling
- Write: Read-only for administrators

Related Commands

Output: displayspool

Related Fields

auto_unspool, despool_max_connections, org (for spooling), quota, spool_delay, spool_mech, status, used_pct, used_size

See Also

The Message Security Administration Guide, “Spool Manager”

org (for spooling)

The org field holds the name of the email config organization managed by Spool Manager.

Syntax

org=<email config name>

Examples

When the field is returned as output:

```
org jumboemailconfig
```

Description

Name of the email config organization associated with spooling.

Field Type

Org Spool management

Authorization

- Read: Spooling
- Write: Read-only for administrators

Notes

The Batch interface allows apostrophes, commas, #, =, " ", ' ' symbols in user or organization names. These must be either in double quotes or preceded by a '\' symbol.

Related Commands

Output: displayspool

Related Fields

auto_unspool, despool_max_connections, duration, quota, spool_delay, spool_mech, status, used_pct, used_size

See Also

The Message Security Administration Guide, “Spool Manager”

quota

The quota field holds the assigned space available for spooling for this email config managed by Spool Manager.

Syntax

quota=<assigned space in bytes>

Examples

As part of the settings output of the displayspool command:

```
quota 5242880
```

Description

Assigned space available for spooling for this email config in bytes. It is displayed in the Administration Console as MB.

Field Type

Org Spool management

Authorization

- Read: Account-level Spooling
- Write: Read-only for Account organization administrators

Notes

- Allocation is altered by amending your service contract.
- The quota field is the same as the Allocated Spool field in the Administration Console batch return value.

Related Commands

Output: displayspool

Related Fields

auto_unspool, despool_max_connections, duration, org (for spooling),
spool_delay, spool_mech, status, used_pct, used_size

See Also

The Message Security Administration Guide, “Spool Manager”

spool_delay

The spool_delay field, in conjunction with connection failures, determines how many seconds before spooling starts

Syntax

```
spool_delay=<900 | 1800 | 3600>
```

Examples

When the field is returned as output:

```
spool_delay 900
```

Description

In seconds, determines how many minutes before spooling starts:

- Spooling delay choices are 15 (900 seconds), 30 (1800), 60 (3600) minutes.

Field Type

Org Spool management

Authorization

- Read: Spooling
- Write: Read-only for administrators

Notes

The spool_delay field is the same as the Spooling Delay field in the Administration Console batch return value.

Related Commands

Output: displayspool

Related Fields

auto_unspool, despool_max_connections, duration, org (for spooling), quota, spool_mech, status, used_pct, used_size

See Also

The Message Security Administration Guide, “Spool Manager”

spool_mech

The spool_mech field holds the initiation mechanism that starts spooling.

Syntax

spool_mech=<“Automatic” | “Start Manually” | “Suspend” | “Spool Delay”>

Examples

As part of the settings output of the displayspool command:

```
spool_mech Suspend
```

Description

Spool initiation states:

- Automatic -- The Spool Manager starts spooling automatically when there is an outage. Spool Manager must be set to automatic for the automatic initiation to occur.
- “Start Manually” -- You may start spooling messages while upgrading server software, hardware, network, or any other process that might interrupt delivery of email messages. Spooling begins once you click the Submit button in the Administration Console, and continues until you select set the Spooling Mechanism to Suspend.

Note: Spool Manager does not issue alerts for manually initiated spooling.

- Suspend -- Spooling is turned off. Spooling will not occur even if your email server is down.
- “Spool Delay” -- Delay of spooling in seconds

Field Type

Org Spool management

Authorization

- Read: Spooling
- Write: Read-only for administrators

Notes

The spool_mech field is the same as the Spooling Mechanism field in the Administration Console batch return value.

Related Commands

Output: displayspool

Related Fields

auto_unspool, despool_max_connections, duration, org (for spooling), quota, spool_delay, status, used_pct, used_size

See Also

The Message Security Administration Guide, “Spool Manager”

status

The status field holds email config organization's status managed by Spool Manager.

Syntax

status=<“Not Provisioned” | Suspended | “Standing By” | Spooling | Unspooling>

Examples

As part of the settings output of the displayspool command:

```
status Suspended
```

Description

Email config organization's spooling status:

- “Not Provisioned” -- Customers have not purchased spooling services.
- Suspended -- Spooling is disabled and will not engage even if there's a server or network outage.
- “Standing By” -- Spooling is activated and monitoring the number of failed connections.
- Spooling -- Spooling process is in progress.
- Unspooling -- Spool Manager is in the process of delivering messages from spool storage. Once unspooling is complete, the status returns to Standing By.

Field Type

Org Spool management

Authorization

- Read: Spooling
- Write: Read-only for administrators

Related Commands

Output: displayspool

Related Fields

auto_unspool, despool_max_connections, duration, org (for spooling), quota, spool_delay, spool_mech, used_pct, used_size

See Also

The Message Security Administration Guide, “Spool Manager”

used_pct

The used_pct field is the percentage of the assigned spooling space that has been used.

Syntax

used_pct= < total number string>

Examples

As part of the settings output of the displayspool command:

used_pct 3.0

Description

The percentage of assigned spooling space that has been used.

Field Type

Org Spool management

Authorization

- Read: Spooling
- Write: Read-only for administrators

Notes

The used_pct field is the same as the Spool Percent Used field in the Administration Console batch return value.

Related Commands

Output: displayspool

Related Fields

auto_unspool, despool_max_connections, duration, org (for spooling), quota, spool_delay, spool_mech, status, used_size

See Also

The Message Security Administration Guide, “Spool Manager”

used_size

The used_size field shows the used amount of allocated spool storage for an email config managed by Spool Manager.

Syntax

used_size= < total amount in bytes >

Examples

As part of the settings output of the displayspool command:

```
used_size 0
```

Description

Shows the total of used allocated spool storage in bytes.

Spool Manager does not issue alerts for manually initiated spooling.

Field Type

Org Spool management

Authorization

- Read: Account-level Spooling
- Write: Read-only for Account organization administrators

Notes

The used_size field is the same as the Spool Used field in the Administration Console batch return value.

Related Commands

Output: displayspool

Related Fields

auto_unspool, despool_max_connections, duration, org (for spooling), quota, spool_delay, spool_mech, status, used_pct

See Also

The Message Security Administration Guide, “Spool Manager”

Chapter 11

Examples of Common Tasks

About Common Task Examples

This chapter presents examples of common organization, Message Center, and notification using the batch command interface. Also included are tasks for Postini Message Archiving, Postini Message Encryption, and Postini IM Security, which are optional products. Many of the larger tasks are divided into smaller related task examples with one evaluating different field locations, relationships, and values, and the other showing how to edit the data using a collection of batch commands.

These tasks assume familiarity with the:

- Administration Console's organization, user, and domain concepts and configurations
- Command line interfaces, in general

Task Example Syntax

Using the Administration Console syntax, code lines beginning with '#' symbols are interpreted by the batch command interface as comments. These pass through the interface processes without change. Code lines without the '#' symbol are batch commands which create, modify, and delete data throughout your account's organizational hierarchy.

The example below shows a set of commented lines, the displayorg batch command, and a commented data field and related value, a field-value pair. In the example, one of the field-value pairs returned by the displayorg command is the **is_email_config** field which distinguishes email config organizations from account or user organizations. This type of specific field information is important to understand when working with the batch command interface.

```
#Is JumboEmailConfig really an email config org?  
#The answer is in is_email_config field-value pair returned by the  
#displayorg command.  
  
displayorg JumboEmailConfig
```

```
#is_email_config yes
```

Each task code sample is documented explaining these inter-relationships and has links to a reference pages for additional examples and information.

Message Center Settings and Password Examples

Viewing Message Center Settings

This example shows how to determine:

- If the user has ever used the Message Center
- The user's Sender lists, spam filters, timezone, and local language

See also "Editing Message Center Access and Settings" on page 538, "Viewing Authentication and Password Settings" on page 540, and "Seeing if a User Has Received a Welcome Notification" on page 547.

Note: This example uses the Administration Console batch command syntax.

Find a User's Current Message Center Settings

1. **Use the displayuser command to display the user's Message Center settings:**

```
displayuser msmith@jumboinc.com
```

2. **Determine if the user has ever logged into the Message Center by finding the active field in the displayuser command's output.**

```
active '1 (yes)'
```

3. **From the same displayuser output, find the user's approved_recipients, approved_senders, and blocked_senders lists.**

```
approved_recipients mydomain.com
```

```
approved-senders jim@hugeisp.com
```

```
blocked-senders "msmith@jumboinc.com, joe@jumboinc.com,  
matt@hugeisp.com"
```

The **approved_recipients** field holds an email address or domain to be added or removed from the Approved Recipients list which is also known as the Approved Mailing list located in the user's Message Center.

The **approved_senders (for users)** field holds an email address or domain to be added or removed from the user-level Approved Senders list in the user's Message Center.

The Approved Senders list overrides the organization-level Approved Senders and Blocked Senders lists.

Note: If virus blocking is enabled for the recipient, the message will not be delivered even though the recipient is on the Approved Senders list.

The **blocked_senders (for users)** field lists an email address or a domain to be added or removed from the user-level Blocked Senders list. All messages from these senders or domains will be quarantined in the user's Message Center.

Note: Approved/Blocked Senders and Recipient lists have a size limit of 4000 characters which approximately equates to 100 to 130 addresses and domains per list.

4. From the same displayuser output, find the user's spam filter settings.

```
junkmail_filter '1 (on)'  
filter_adult '15 (aggressive)'  
filter_bulk '15 (aggressive)'  
filter_getrich '15 (aggressive)'  
filter_offer '15 (aggressive)'  
filter_racial '15 (aggressive)'
```

The **junkmail_filter** field is an on/off switch for Spam Filtering

The **filter_adult** field holds the sexual content filter settings for the user.

The **filter_bulk** field holds the general spam filter setting for the user. This filter handles the bulk of the spam being blocked.

The **filter_getrich** field holds the Get Rich Quick category filter setting for the user.

The **filter_offers** field holds the Special Offers category filter setting for the user.

The **filter_racial** field holds Racially Insensitive category filter setting for the user.

5. In the displayuser output, the timezone (for users) field holds the time zone selected by the user.

```
timezone=MST7
```

The timezone field is shown in the Quarantine Summary and the Message Center.

WARNING: Don't change this setting in the Administration Console. It should be managed by the users themselves, at the user's Message Center.

6. **Also found in the displayuser output, the lang_locale (for users) field enables user-level language localization in Message Center's static text, the default top text, character sets, and date format.**

```
lang_local en_us.utf8
```

This affects Quarantine Summary and (if set to a supported language) Message Center. See "Language and Timezone" on page 569 for supported languages and character encodings, and the field values.

Editing Message Center Access and Settings

This example shows how to edit the Message Center settings at the org-level and includes:

- Locating the org's Default User
- Enabling Message Center access for all users in the organization
- Setting permissions to let users modify their own spam filters, turn filters on or off, manage personal sender lists, and add user aliases.

See also "Viewing Authentication and Password Settings" on page 540, and "Seeing if a User Has Received a Welcome Notification" on page 547.

Note: This example uses the Administration Console batch command syntax.

Edit an Organization's Default User Settings Used for Each New User's Message Center

1. **Use the displayorg command to locate your org's Default User template.**

```
displayorg Sales
```

The output of this command lists several settings. Find the **default_user**.

```
default_user pdefault@jumboinc.com
```

Note: The naming convention for a Default User is <pdefault@<domain>, postinidefault@<domain>, <name>@<domain>.

2. **Using the displayuser command, determine the Default User's Message Center access setting.**

```
displayuser pdefault@jumboinc.com
```

The displayuser output lists several user settings. Find the weblocked setting which, in this example, Message Center access is blocked.

```
weblocked '1 (yes)'
```

The **weblocked** field is an on/off switch giving Message Center Access for the any user including the Default User. The '0 (no)' means the access not blocked. It is enabled and users can log into their Message Centers.

3. **Using the modifyuser command, enable the Message Center access using the Default User template.**

```
modifyuser pdefaultSales@jumboinc.com, weblocked=0
```

It is important to enable Message Center access at the Default User-level — whether or not you want users to have it. This ensures that new users added to an org can have Message Center access.

4. **Using the displayuser command, find the address where notifications are sent to the Default User. And, if needed, edit this notification address.**

```
displayuser pdefaultuser@jumboinc.com
```

The displayuser command's output includes several user settings. Find the **notice_address** field which holds the address where notifications for this user are sent. This example shows an unassigned notice address which is the common case.

```
notice_address
```

Giving this Default User field a value is a special case. Enter an address only if you intend for a single administrator to receive notifications for users in orgs using this Default User (not typical). Otherwise, leave this field blank when setting up a Default User account.

```
notice_address support@jumboinc.com
```

5. **Using the displayuser command, find all of the present Default User spam filter settings listed below. Then, using the modifyuser command, edit the Default User's spam filter settings for your organization.**

```
displayuser pdefaultuser@jumboinc.com
```

```
modifyuser pdefaultuser@jumboinc.com, junkmail_filter=on,  
filter_bulk=moderate, filter_adult=moderately-aggressive,  
filter_bulk=moderate, filter_getrich=moderate, filter_offer  
=moderate, filter_racial=moderate
```

The **junkmail_filter** field is an on/off switch for Spam Filtering

The **filter_adult** field holds the sexual content filter settings for the user.

The **filter_bulk** field holds the general spam filter setting for the user. This filter handles the bulk of the spam being blocked.

The **filter_getrich** field holds the Get Rich Quick category filter setting for the user.

The **filter_offers** field holds the Special Offers category filter setting for the user.

The **filter_racial** field holds Racially Insensitive category filter setting for the user.

WARNING: Ignore other User Access permissions for a Default User, as they don't apply. New users receive these settings instead from the org's User Access, not from the Default User.

Viewing Authentication and Password Settings

This example shows how to find an organization's authentication and password settings. This includes finding:

- Types of authentication and authentication data
- Passwords

This example is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

See the task example, “Editing a PMP Password” on page 541 for more information. This example uses the Administration Console batch command syntax.

Note: This example uses the Administration Console batch command syntax.

Find an Org's Message Center Authentication Type and Passwords

1. Using the **displayorg** command, determine your organization's Message Center authentication password (XAuth, POP, PMP) used for all of the org's users.

```
displayorg Sales
```

The **displayorg** command's output lists several settings. Find the **authentication_type** field which holds the type of authentication used in an organization. In this example, the type is POP authentication.

```
authentication_type=4 for POP authentication
```

Since POP authentication is a non-PMP authentication type, find the **authentication_data** field which holds the text string used for non-PMP authentication of users and administrators when logging into the Message Center or Administration Console.

```
authentication_data "apopserver,@jumboinc.com"
```

If the authentication type is XAuth, find the XAuth authentication secret:

```
authentication_data swordfish
```

2. If the organization's authentication is PMP, use the **displayuser** command to find the user-level PMP passwords.

```
displayuser msmith@jumboinc.com
```

If the user is a new user and has never logged into the Message Center or Administration Console, find the user-level **initial_password** field. This field holds the PMP password assigned to this user when the user was first added to the service. This password is not encrypted.

```
initial_password fr0g#T2
```

Note: Users are prompted to change the initial password when first logging into the Message Center/or Administration Console.

If the user has already updated the initial password and used the Message Center or Administration Console, find the **password** field which holds the user's encrypted PMP password.

```
password 5d00000
```

Editing a PMP Password

This example shows how to change a user's PMP password.

This example is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

This example uses the Administration Console batch command syntax.

Change a User's PMP Password

1. See “Viewing Authentication and Password Settings” on page 540 to determine if the:
 - Organization uses PMP authentication
 - User has logged into the Message Center or Administration Console
2. Using the **displayuser** command, find the user-level **password** field which holds the encrypted PMP user password.

```
displayuser msmith@jumboinc.com
```

The displayuser command's output lists the password field:

```
password 5d00000
```

3. Use the modifyuser command to change the user's PMP password.

```
modifyuser msmith@jumboinc.com, password= 1passWrd
```

Note: To change the passwords for several users, using this example's syntax, follow the steps explained in "Building a Batch File" on page 19.

Notification Examples

Viewing Message Center General Notification Settings

This example shows how to view the Message Center notifications include contact information, new account notifications, and filter notifications.

See also, "Seeing if a User Has Received a Welcome Notification" on page 547" for more information.

Note: This example uses the Administration Console batch command syntax.

Determine an Organization's User Notification Settings

1. Using the displayorg command, find the organization's company name, and support contact.

```
displayorg Sales
```

From the displayorg command's output, find the **company_name** field which holds the company or entity name that is used in email notifications:

```
company_name Jumbo Inc.
```

The **support_contact** field which holds the address of the support contact for the organization. This is the sender for org notifications and it is important that this setting has a value.

```
support_contact helpdesk@jumboinc.com
```

2. Using the same displayorg command output, find the organization's notification settings.

The **disable_first_spam** field which is an activation switch for a new user's notification telling the user the first spam message has been quarantined in the user's Message Center.

```
disable_first_spam 1
```

The **welcome_on** field shows whether a welcome message can be sent. It should not be edited.

```
#welcome_on on
```

Note: The user-level **welcome_count** field shows whether a welcome message has been sent to a specific user. Use the **displayuser** command to view this field's setting.

```
at_notify_on "Send to User"  
at_notify_on "Send to Both"
```

The **at_notify_on** field shows the recipient notification status for messages quarantined by the Inbound Attachment Manager. Of the possible values, the notification can be sent to the User or to the redirect address and the User.

```
#out_at_notify_on "Send to User"  
#out_at_notify_on "Send to Both"
```

The **out_at_notify_on** field holds the notification recipient for messages quarantined for Outbound Attachment Manager rules. (Message Security only)

```
#spam_notify_on on
```

The **spam_notify_on** field is a switch enabling the sending of spam quarantine notifications.

```
#virus_notify 1
```

The **virus_notify (for orgs)** field specifies how frequently virus notification email will be generated for the organization.

Editing Message Center General Notification Settings

This example shows how to edit the Message Center notifications include contact information, new account notifications, and filter notifications.

See the example, “Viewing Authentication and Password Settings” on page 540” for more information.

This example uses the Administration Console batch command syntax.

Edit the Organization’s Notifications

1. See “Viewing Message Center General Notification Settings” on page 542 to find the organization’s:
 - Notification contacts
 - Notification settings
2. At the org-level, change your organization’s Message Center user notification contacts using the **modifyorg** command.

```
modifyorg Sales, company_name=Jumbo Inc,  
support_contact=helpdesk@jumboinc.com
```

The **company_name** field holds the company or entity name that is used in email notifications.

The **support_contact** field holds the address of the support contact for the organization. This is the sender for org notifications.

3. Using the modifyorg command, change the initial Message Center spam notifications.

```
modifyorg Sales, disable_first_spam=0
```

The **disable_first_spam** field is an activation switch for a new user's notification telling the user the first spam message has been quarantined in the user's Message Center. When 'off' the user is notified.

4. Using the modifyorg command, change your organization's Message Center filter notification settings:

```
modifyorg Sales, at_notify_on="Send to Redirect",  
out_at_notify_on="Send to Redirect", spam_notify_on=on,  
virus_notify=1
```

The **at_notify_on** field shows the recipient notification status for messages quarantined by the Inbound Attachment Manager. Of the possible values, the notification can be sent to the User or to the redirect address and the User.

The **out_at_notify_on** field holds the notification recipient for messages quarantined for Outbound Attachment Manager rules. (Message Security only)

The **spam_notify_on** field is a switch enabling the sending of spam quarantine notifications.

The **virus_notify (for orgs)** field specifies how frequently virus notification email will be generated for the organization.

Viewing Quarantine Summary Notification Settings

This example shows how to view:

- Quarantine Summary settings
- General Quarantine Summary notifications
- Quarantine Summary redirect notifications

See the ““Editing Quarantine Summary Notifications” on page 546” for more information.

This example uses the Administration Console batch command syntax.

Determine the Quarantine Summary Notification Settings

1. Using the displayorg command, determine if the Quarantine Summary links are enabled.

```
displayorg Sales
```

The **quarantine_links** field is a switch to enable quarantine message links to be available in the Message Center.

```
quarantine_links '1 (on)'
```

The **quarsum_links** field is a switch enabling Quarantine Summary message links to be available.

```
quarsum_links 1
```

2. Using the displayorg command, determine the general Quarantine Summary notification settings.

```
displayorg Sales
```

The **qsum_actionable** field holds the action available in Quarantine Summary notifications.

```
qsum_actionable "basic delivery"
```

The **qsum_enable** field is a switch that sends the Quarantine Summary notifications. It must be ‘on’ for the **qsum_actionable** field to work.

```
qsum_enable on
```

The **lang_locale (for orgs)** field enables org-level language localization in the Quarantine Summary. See “Language and Timezone” on page 569 for supported languages and character encodings, and the field values.

```
lang_locale en_us.utf8
```

3. Using the displayorg command, determine your organization’s Message Center Quarantine redirected notification settings.

```
displayorg Sales
```

The **qtine_redir_ndr** field holds the user email address for the quarantined outbound Undeliverable Bounce Messages. When an outbound message is quarantined as an undeliverable Bounce message, the message is stored in this Message Center. (Message Security only)

```
qtine_redir_ndr outboundadmin@jumboinc.com
```

The **qtine_redir_out_atq** field holds the user address for the Attachment Manager quarantined email for this organization. When an outbound message is quarantined by Attachment Manager, the message is stored in this Message Center. (Message Security only)

```
qtine_redir_out_atq out_admin@jumboinc.com
```

The **qtine_redir_out_virus** field holds the email address for the user receiving outbound virus email quarantine for an organization. When an outbound message is quarantined as a virus, the message is stored in this Message Center. (Message Security only)

```
qtine_redir_out_virus admin@jumboinc.com
```

The **qtine_redir_spam** field holds email address for the user receiving inbound spam email quarantine for an organization. When an outbound message is quarantined as spam, the message is stored in this Message Center.

```
qtine_redir_spam spam_admin@jumboinc.com
```

The **qtine_redir_virus** field holds the email address for the user receiving inbound virus email quarantine for an organization. When an inbound message is quarantined as a virus, the message is stored in this Message Center.

```
qtine_redir_virus admin@jumboinc.com
```

Editing Quarantine Summary Notifications

This example shows how to edit the:

- Quarantine Summary settings
- General Quarantine Summary notifications
- Quarantine Summary redirect notifications

See the example, “Viewing Quarantine Summary Notification Settings” on page 544 for more information.

Note: This example uses the Administration Console batch command syntax.

Edit the Quarantine Summary Notification Settings

1. See “Viewing Quarantine Summary Notification Settings” on page 544 to find your Quarantine Summary Notification settings.

2. Using the **modifyorg** command, enable the Quarantine Summary links.

```
modifyorg Sales, quarantine_links=on, quarsum_links=on
```

The **quarantine_links** field is a switch to enable quarantine message links to be available in the Message Center.

The **quarsum_links** field is a switch enabling Quarantine Summary message links to be available.

3. Using the **modifyorg** command, edit the general Quarantine Summary notification settings.

```
modifyorg Sales, qsum_actionable= "basic delivery", qsum_enable=on, lang_locale= en_us.utf8
```

The **qsum_actionable** field holds the action available in Quarantine Summary notifications.

The **qsum_enable** field is a switch that sends the Quarantine Summary notifications. It must be ‘on’ for the **qsum_actionable** field to work.

The lang_locale (for orgs) field enables org-level language localization in the Quarantine Summary.

4. Using the modifyorg command, edit the Message Center Quarantine redirected notification settings.

```
modifyorg Sales, qtine_redir_ndr= outboundadmin@jumboinc.com,  
qtine_redir_out_atq = out_admin@jumboinc.com, qtine_redir_out_virus  
= admin@jumboinc.com, qtine_redir_spam = spam_admin@jumboinc.com,  
qtine_redir_virus = admin@jumboinc.com
```

The **qtine_redir_ndr** field holds the user email address for the quarantined outbound Undeliverable Bounce Messages. When an outbound message is quarantined as an undeliverable Bounce message, the message is stored in this Message Center. (Message Security only)

The **qtine_redir_out_atq** field holds the user address for the Attachment Manager quarantined email for this organization. When an outbound message is quarantined by Attachment Manager, the message is stored in this Message Center. (Message Security only)

The **qtine_redir_out_virus** field holds the email address for the user receiving inbound virus email quarantine for an organization. When an inbound message is quarantined as a virus, the message is stored in this Message Center. (Message Security only)

The **qtine_redir_spam** field holds email address for the user receiving inbound spam email quarantine for an organization. When an outbound message is quarantined as spam, the message is stored in this Message Center.

The **qtine_redir_virus** field holds the email address for the user receiving inbound virus email quarantine for an organization. When an inbound message is quarantined as a virus, the message is stored in this Message Center.

Seeing if a User Has Received a Welcome Notification

This example shows how to determine if a has received a welcome notification.

See also, “Resending the Welcome Notification” on page 548 for additional information.

Note: This example uses the Administration Console batch command syntax.

Find the Welcome Notification Setting

1. **Using the displayuser command, determine if a user qualifies for a welcome notification. The user must not be active and the user has not yet been welcomed.**

```
displayuser msmith@jumboinc.com
```

The **active** field indicates whether the user has ever logged into the Message Center. If the user is active, a welcome notification is not sent.

```
active '1 (yes)'
```

The **welcome_count** field indicates if a welcome message has been sent.

```
#The user has not been sent a welcome message (0/none sent)
welcome_count 0
```

2. **Using the displayorg command, determine if the org's welcome message function is enabled.**

```
displayorg Sales
```

If the **welcome_on** field is enabled for this user's org, then the next time the system runs the process (overnight), it looks for users in that org that meet both conditions, and for any that it finds, it sends the notification.

```
welcome_on '1 (on)'
```

Resending the Welcome Notification

The Welcome notification can not be resent. Once the notification has been sent, the Welcomed flag is set to True and can not be reset. There are a few options for working around this:

- Do nothing, and rely on the My First Spam notification.
- Check whether user has ever logged into the Message Center and had messages quarantined.

See “[Seeing if a User Has Received a Welcome Notification](#)” on page 547 for more information.

Note: This example uses the Administration Console batch command syntax.

Options Once a Welcome Notification is Sent

1. **Do nothing and rely on the My First Spam Notification.**

The user will receive the My First Spam notification when the first junk email message is quarantined. This notification is similar to the Welcome notification and includes the user's initial password. But determine if the My First Spam notification is enabled.

2. **Using the displayorg command, determine if the My First Spam notification has been sent.**

```
displayorg Sales
```

The **disable_first_spam** field is an activation switch for a new user's notification telling the user the first spam message has been quarantined in the user's Message Center. When 'off' the user is notified.

```
disable_first_spam 1
```

3. **Using the displayuser command, determine if the user has ever logged in to the Message Center.**

```
displayuser msmith@jumboinc.com
```

The **active** field indicates whether the user has ever logged into the Message Center.

```
active: '0 (no)'
```

In the Administration Console, check the user's quarantine, and if the user also has not had any messages quarantined, you can safely delete and immediately recreate the user.

4. **Using the adduser command, create a new user record and send the Welcome notification immediately.**

```
adduser msmith@jumboinc.com, org= Sales, welcome=1
```

The **adduser <user address>, welcome= <1 or 0>** parameter, if enabled, sends an immediate welcome message (welcome=1) when a user is created.

Setting a Virus Notification Interval

This example shows how to set a virus notification interval for an organization and for a user.

Note: This example uses the Administration Console batch command syntax.

Enable the Virus Notificaion Interval

1. **Using the displayorg command, determine the virus notification interval for an organization and set a new value.**

```
displayorg Sales
```

The **virus_notify (for orgs)** field holds frequency of a user's virus notifications.

The possible values:

0=immediately

1=nomore than one notice per day

9=disable notification

NULL=(user only) use org-level setting

```
virus_notify 9
```

2. Using the modifyorg command, set a new notification interval.

```
modifyorg Sales, virus_notify=1
```

3. Using the modifyuser command, set a virus notification interval for a user.

```
modifyuser msmith@jumboinc.com, virus_notify=0
```

The **virus_notify (for users)** field holds frequency of a user's virus notifications.

Org Settings Examples

Listing the Organizational Hierarchy

This example describes how to list an organization with one domain, one email configuration, and one or more user organizations. It shows:

- List and display your organizations
- List and display your domains
- List your users and display a user's record

See also, *The Message Security Administration Guide*, “Organization Hierarchy and Design”

Note: This example uses the Administration Console batch command syntax.

List All of Your Organizational Hierarchy

1. Using the listorgs command, list all of your organization hierarchy including the account, email config, and all user organizations

```
listorgs ALL, childorgs=1
```

The **listorgs** command returns a list of your Account, Email Config, and User organizations showing each org's unique ID number and the organization's name (iid, orgtag).

If you get an error “You don't have permission to listorgs for the organization...”, try starting your list with an org you have authorization for using the **targetOrg** parameter.

```
listorgs ALL, targetOrg=Sales, childorgs=1
```

2. Using the **displayorg** command, display your account organization.

```
displayorg JumboAccount
```

The **displayorg** command returns all of the settings for an organization.

The account organization (account org) is used primarily for billing. Do not add users or domains to the account org.

The initial naming convention for account organizations is ‘<your company name> Account’.

3. Using the **displayorg** command, display your email config organization.

```
displayorg JumboEmailConfig
```

An email server configuration (email config) manages several email server tasks. In the batch environment, this organization manages spooling and IP address management. Note in the org's settings, the **is_email_config** field is set to 'yes', confirming this is an email config org.

```
is_email_config yes
```

4. Using the **displayorg** command, display a user organization and find the Default User for that organization.

```
displayorg Sales
```

User organizations reside below the email config configured for the organization's domains. A User org is where users and domains are added to the hierarchy. Note in the org's settings, the **default_user** field lists user template of all new user settings for that organization.

```
default_user pdefault@jumboinc.com
```

List Your Domains and a Domain's Settings

1. Using the **listdomains** command, list all of your domains.

```
listdomains ALL, childorgs=1
```

The **listdomains** command returns a list of your domains showing each domain's unique domain ID number and domain name (domainid, domainname).

2. Using the **listdomains** command, list the domains only and without domain aliases.

```
listdomains ALL, aliases=0, childorgs=1
```

With the parameter **aliases=0**, the list will be domains only and no domain aliases.

3. If you do not have permission to list all the domains in your account, start the listing with the targetOrg parameter.

```
listdomains ALL, targetOrg=Sales, childorgs=1
```

If you get an error “You don't have permission to listdomains for the organization...”, try starting your list with an org you have authorization for using the targetOrg parameter.

4. Once you can list your domains, select a domain to display the settings.

```
listdomains ALL, targetOrg=Sales, childorgs=1, aliases=0
```

The **listdomains** command returns a list of your domains showing each domain's unique domain ID number and domain name (domainid, domainname).

With the parameter **aliases=0**, the list will be domains only and no domain aliases.

5. Using the displaydomain command, display a domain's settings.

```
displaydomain jumboinc.com
```

The **displaydomain** command returns all of the settings for a domain. The example code uses a pseudo domain name, jumboinc.com.

List All Users and Display Settings

1. Using the listusers command, list all of your users.

```
listusers ALL, childorg=1
```

The **listusers** command returns a list of your users including the user's email address and the user's organization name (address, orgtag).

2. List all of your users without the user aliases and starting the list with an organization you have permissions to access.

```
listusers ALL, targetOrg=Sales, aliases=0, childorgs=1
```

With the parameter **aliases=0**, the list will be users' primary email addresses only and none of the users' aliases.

3. Using the displayorg command, display the Default User settings and a regular user's settings.

```
displayorg Sales
```

To locate a Default User either use the **default_user** field with the **displayorg** command or see if the **listusers** command's output returns a user with the Default User naming convention, pdefault@<domain>, postinidefault@<domain>, <name>@<domain>.

```
default_user pdefault@jumboinc.com
```

The Default User settings template is applied to all new users to this organization unless you modify the new user's settings with the **adduser** or **modifyuser** commands.

4. Using the **displayuser** command, display the Default User's settings.

```
displayuser pdefault@jumboinc.com
```

The **displayuser** command returns all of the settings for a user. The example code uses pseudo user addresses for the Default User and a regular user.

5. Using the **displayuser** command, display a user's settings.

```
displayuser msmith@jumboinc.com
```

The **displayuser** command returns all of the settings for a user. The example code uses pseudo user addresses for the Default User and a regular user.

A regular user's settings contains all of specific services, filter settings, administrators, and other policies.

Resetting Users

This example describes how a suspended user is reset. A suspended user's mailflow is not being filtered by the Message Security service. When reset, this user's mail is re-established in the filtering processes. Most of the reset user's settings come from the Default User's settings. It shows:

- Locate and read the Default User settings
- Reset the suspended user

Note: This example uses the Administration Console batch command syntax.

Reset a User

1. Using the **listusers** command, locate the Default User in your organizations.

```
listuser ALL, targetOrg=sales, childOrgs=1
```

Use **listusers** if you do not know which parent organization has your default user. Usually the Default User's name has 'pdefault' or 'postinidefault' in it.

```
displayorg sales
```

If you know the organization associated with your default user, use **displayorg** to view the **default_user** field.

```
default_user pdefault@jumboinc.com
```

2. Using the displayuser command, display the Default User settings.

```
displayuser pdefault@jumboinc.com
```

3. Using the resetuser command, reset a suspended user.

```
resetuser msmith@jumboinc.com
```

The user will be reset with the Default User settings except for these fields:
address, creator, create_method (for users), iid, initial_password, user_id, orgid, welcome_count

4. Using the displayuser command, display the user's settings.

```
displayuser msmith@jumboinc.com
```

Viewing Your Organization's Sender Lists

This example describes how to view an organization's sender lists. At the org-level the Senders lists are composed of the Approved Senders list and the Blocked Senders list.

See the “Adding Users and Domains to Sender Lists” on page 555 and “Viewing Message Center Settings” on page 536 for more information.

Note: This example uses the Administration Console batch command syntax.

Determine an Organization's Sender Lists

1. Using the displayorg command, determine your organization's Sender list settings.

```
displayorg Sales
```

In the displayorg command's output, find the **approved_senders (for orgs)** field which holds an email address or domain in the Approved Senders list.

```
approved_senders jm@jumboinc.com,hugeisp.com
```

The org -level Approved Senders list overrides the org-level Blocked Senders list, but not the user-level Blocked Senders.

If virus blocking is enabled for the recipient, message will not be delivered even though on the Approved Senders list. The **disposition_virus** field holds the status of an email containing a virus. The **virus_clean** field is a flag indicating whether a virus cleaning is allowed for this organization.

```
disposition_virus blackhole
```

```
virus_clean 1
```

In the displayorg command's output, find the **blocked_senders (for orgs)** field which holds lists an email address or a domain for the Blocked Senders list. All messages from these senders or domains are quarantined.

```
blocked_senders jm@jumboinc.com,hugeisp.com
```

If an organization has Industry Heuristics turned on, messages with industry content will still be quarantined if the sender or domain is in organization's Blocked Senders list.

The org-level sender lists are not visible to the user-level sender lists. This allows you to customize lists between organizations.

Note: These lists have a size limit of 4000 characters which approximately equates to 100 to 130 addresses and domains per list.

Adding Users and Domains to Sender Lists

This example describes how add users and domains to an organization's sender lists.

This example is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

The example uses:

- The **approved_senders (for orgs)** field holds an email address or domain in the Approved Senders list.

The org -level Approved Senders List overrides the org-level Blocked Senders list, but not the user-level Blocked Senders.

- The **blocked_senders (for orgs)** field holds lists an email address or a domain for the Blocked Senders List. All messages from these senders or domains are quarantined.

If an organization has Industry Heuristics turned on, messages with industry content will still be quarantined if the sender or domain is in organization's Blocked Senders list.

The org-level Sender lists are not visible to the user-level lists. This allows you to customize lists between organizations.

Note: These lists have a size limit of 4000 characters which approximately equates to 100 to 130 addresses and domains per list.

See the “Viewing Your Organization's Sender Lists” on page 554 and “Viewing Message Center Settings” on page 536 for more information.

Note: This example uses the Administration Console batch command syntax.

Remove One User from an Approved Senders List

1. **Using the modifyorg command, remove one user from the org-level Approved Senders list.**

```
modifyorg sales, approved_senders= -jim@hugeisp.com
```

2. **Using the modifyuser command, remove one user from the user-level Approved Senders list.**

```
modifyuser msmith@jumboinc.com, approved_senders= -jim@hugeisp.com
```

3. **Using the modifyuser command, remove one user from the user-level Approved Recipients list.**

```
modifyuser msmith@jumboinc.com, approved_recipients= -newupdates@hugeisp.com
```

Remove One User from a Blocked Senders List

1. **Using the modifyorg command, remove one blocked sender from an org-level Senders list. and from a user-level list.**

```
modifyorg sales, blocked_senders= -jim@hugeisp.com
```

2. **Using the modifyuser command, remove one blocked sender from a user-level Senders list.**

```
modifyuser msmith@jumboinc.com, blocked_senders= -jim@hugeisp.com
```

Remove All Approved Senders from an Approved Senders List.

1. **Using the modifyorg command, remove all users from an org-level Approved Senders list.**

```
modifyorg msmith@jumboinc.com, approved_senders=NULL
```

2. **Using the modifyuser command, remove all users from a user-level Approved Senders list.**

```
modifyuser msmith@jumboinc.com, approved_senders=NULL
```

3. **Using the modifyuser command, remove all mailing lists from a user-level Approved Recipients list.**

```
modifyuser msmith@jumboinc.com, approved_recipients=NULL
```

Remove All Blocked Senders from a Senders List

1. **Using the modifyorg command, remove all users from an org-level Blocked Senders list.**

```
modifyuser msmith@jumboinc.com, blocked_senders=NULL
```

2. **Using the modifyuser command, remove all users from a user-level Blocked Senders list**

```
modifyuser msmith@jumboinc.com, blocked_senders=NULL
```

Remove All Users from a Senders List Except for One User

- 1. Using the modifyorg command, replace the org-level Approved Senders list and the Blocked Senders list with one user.**

```
modifyorg msmith@jumboinc.com, approved_senders=jim@hugeisp.com  
modifyorg msmith@jumboinc.com, blocked_senders=jim@hugeisp.com
```

- 2. Using the modifyuser command, replace the user-level Approved Senders and Blocked Senders lists with one user.**

```
modifyuser msmith@jumboinc.com, approved_senders=mary@jumboinc.com  
modifyuser msmith@jumboinc.com, blocked_senders=jim@hugeisp.com
```

- 3. Using the modifyuser command, replace the user-level Approved Recipients list with mailing list**

```
modifyuser msmith@jumboinc.com, approved_recipients=hugeisp.com
```

Add and Remove a Domain from an Approved Senders List

- 1. Using the modifyorg command, add a new domain to the Approved Senders list.**

```
modifyorg Sales, approved_senders=+jumboinc.com
```

- 2. Add a new domain and remove a new domain to the Approved Senders list.**

```
modifyorg Sales, approved_senders="+jumboinc.com, -hugeisp.com"
```

- 3. Add a new user to the Blocked Senders List.**

```
modifyorg Sales, blocked_senders=+jim@hugeisp.com
```

- 4. Add and remove users from the Blocked Senders List.**

```
modifyorg Sales, blocked_senders="+jim@hugeisp.com, -  
mary@jumboinc.com"
```

- 5. Replace the whole Blocked Senders List with one user.**

```
modifyorg Sales, blocked_senders=jim@hugeisp.com
```

Add New Domains to the Blocked Senders Lists

- 1. Add a new domain and remove a domain from the Blocked Senders List.**

```
modifyorg Sales, blocked_senders="+jumboinc.com, -hugeisp.com"
```

- 2. Replace the whole Blocked Senders list with one user.**

```
modifyorg Sales, blocked_senders=jumboinc.com
```

Viewing Message Limit Policies

Message limit policies are for the maximum size of attachments, the maximum number of messages per day, and for the total each user has received.

- Setting a message limit is useful for protecting mail servers against malicious attacks, such as email bombs. All messages are counted against this limit, including legitimate and quarantined messages. The count is approximate, so it's suggested only for values over 100.

See “Viewing Message Center Settings” on page 536 for additional information

Note: This example uses the Administration Console batch command syntax.

Message Limitations for an Organization

1. **Using the displayorg command, determine your message limitations for this organization.**

```
displayorg Sales
```

The **max_message_size** field holds the maximum size of inbound attachments-per-message that users in the organization can receive.

```
max_message_size 200M
```

The **outbound_max_message_size** field holds the maximum size of attachments-per-message that users in the organization can send. (Message Security only)

```
outbound_max_message_size 200M
```

The **default_message_limit** field holds the maximum number of messages each registered user or alias in an organization can receive per day.

Leave this field blank to impose no limit.

```
default_message_limit 1000
```

Message Limitations for a User

1. **Using the displayuser command, determine your message limitations for a user.**

```
displayuser msmith@jumboinc.com
```

The user-level **message_limit** field holds the maximum number of messages allowed per day for a specific user.

```
message_limit 1000
```

This limit can also be set for individual users. Whichever limit is lower—the org limit or a user's limit—applies for the user. If a user's limit is blank and a value is set for the org, the org value applies to the user. For best practices, manage the message limits at the organizational level.

The user-level **message_count** field holds the approximate number of messages received by this user in one day. And the user-level **message_limited** field shows whether this user has reached the daily message limit.

```
message_count 16
```

```
message_limited 0 (no)
```

Editing Your Message Limit Policies

You can change message limit settings at your org-level and user-levels.

See “Viewing Message Center Settings” on page 536 for additional information.

Note: This example uses the Administration Console batch command syntax.

Edit Organization Message Limit Settings

1. Using the **modifyorg** command, edit the organization's message limits.

```
modifyorg Sales, max_message_size=250,  
outbound_max_message_size=250, default_message_limit=1000
```

The **max_message_size** field holds the maximum size of inbound attachments-per-message that users in the organization can receive.

Default: max_message_size => 200M

The **outbound_max_message_size** field holds the maximum size of attachments-per-message that users can send. (Message Security only)

Default: outbound_max_message_size => 200M

The **default_message_limit** field holds the maximum number of messages each registered user or alias in an organization can receive per day.

Leave the **default_message_limit** field blank to impose no limit.

All messages are counted against this limit, including legitimate and quarantined messages. The count is approximate, so it's suggested only for values over 100.

Edit User Message Limit Settings

1. Using the modifyuser command, edit the user's message limit.

```
modifyuser msmitth@jumboinc.com, message_limit=1000
```

The user-level **message_limit** field holds the maximum number of messages allowed per day for a specific user.

This limit can also be set for individual users. Whichever limit is lower—the org limit or a user's limit—applies for the user. If a user's limit is blank and a value is set for the org, the org value applies to the user. For best practices, manage the message limits at the organizational level.

In addition, the user-level message limitations has two read-only fields. The user-level **message_count** field holds the approximate number of messages received by this user in one day. And the user-level **message_limited** field shows whether this user has reached the daily message limit.

```
message_count 16
```

```
message_limited 0 (no)
```

Viewing Mail Handling Policies (Non Account Bouncing)

If your organization is associated with a domain, determine your org's policy for handling mail to unrecognized user addresses:

- Non Account Bouncing
- Web Autocreate and POP authentication
- SmartCreate and Provisional Users
- Connection Manager Asynchronous Bounce
- Outbound Bounce Messages (Message Security only)

Note: The organization's settings show the status of several mail handling policy fields. Only one of these fields should be enabled.

Note: Web Autocreate, SmartCreate, Connection Manager Asynchronous Bouce are applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

To view this organizational hierarchy follow the steps outlined in the task example, “Message Center Settings and Password Examples” on page 536”. See the “Editing Your Mail Handling Policies (Non Account Bounce)” on page 562 task examples for more information.

Note: This example uses the Administration Console batch command syntax.

View the Bounce, Auto Create, and Content Manager Policies

1. Using the displayorg command, view the Non Account Bounce setting.

```
displayorg Sales
```

When **non_account_bounce** is on, messages are bounced if they are not addressed to a registered user or alias.

```
non_account_bounce on
```

2. Using the displayorg command, view the Web Autocreate policy setting.

```
displayorg Sales
```

When **blatant_spam** is on, unrecognized users are automatically added when the user first logs into the Message Center:

```
autocreate_web=on
```

This field is used only for organizations with POP authentication. Check the **authentication_type** field to see the type of POP configuration, and check the **authentication_data** field has a POP login password.

```
authentication_type=4, for POP authentication
```

```
authentication_data="mypopserver,@jumbo.com"
```

3. Using SmartCreate to add unrecognized user addresses.

SmartCreate automatically adds unrecognized user addresses with a domain associated with your orgs. The **listprovusers** command lists these unconfirmed *provisional users*. These users are promoted to a regular user after being verified as associated with someone in your org by receiving 3 legitimate emails within a week.

```
listprovusers Sales, subset=ALL, childorgs=1
```

Rather than relying on a SMTP “250” response from the server to validate recipients, SmartCreate validates by identifying that the messages themselves are legitimate (that is, not spam). Use this with any type of email server, including Microsoft Exchange.

4. Using the displayorg command, view the mail handling policies for the Connection Manager inbound mail.

```
displayorg Sales
```

The **async_bounce** field enables the Connection Manager's control for inbound traffic. This control is for email servers, such as Microsoft Exchange and qmail, that issue "unknown user" asynchronous bounce messages and require added security from the Message Security service.

```
async_bounce on
```

By enabling this field, the Message Security service will compare directory information with incoming recipients to measure erroneous delivery attempts.

5. **Using the displayorg command, view the mail handling policies for the Connection Manager outbound mail. (Message Security product only)**

```
displayorg Sales
```

The **ndr** field holds the outbound mail policy for undeliverable bounce messages generated by your organization's mail server.

```
ndr=off  
ndr=blackhole  
ndr=quarantine  
ndr=NULL()
```

Use this field if you are using a server that bounces undeliverable messages by email instead of SMTP code. This includes qmail, Microsoft Exchange (by default), and some Lotus Domino mail servers.

Editing Your Mail Handling Policies (Non Account Bounce)

Once you have determined your organization's mail handling policies, you can change those policies.

Note: Non Account Bounce, SmartCreate, and Web Autocreate are not compatible. Only enable one policy.

See "Viewing Your Organization's Sender Lists" on page 554 for more information.

Note: This example uses the Administration Console batch command syntax.

Edit Bounce, Auto Create, and Content Manager Settings

1. **Using the modifyorg command, to edit an org's mail handling policies.**

```
modifyorg Sales, non_account_bounce=on,autocreate_web=off,  
async_bounce=on, ndr=blackhole
```

2. **Using the listprovusers and the displayprovuser commands to edit the SmartCreate provisional users.**

```
#To list ALL provisional users
```

```
listprovusers Sales, subset=ALL, childorgs=1
```

```
#List all blocked provisional users and sort #the list by the first  
timestamp (TS1) in #descending order.
```

```
listprovusers Sales, subset BLOCKED, childorgs=1, sort=TS1:d
```

The **listprovusers** command to list all or list a filtered list of your organization's provisional users.

The **displayprovuser** command to list the last time a provisional user has received an email.

```
displayprovuser msmith@jumboinc.com
```

These users are promoted to a regular user after being verified as associated with someone in your org by receiving 3 legitimate emails within a week.

3. Using the provisional user commands to edit these types of users.

```
blockprovuser msmith@jumboinc.com
```

The **blockprovuser** command blocks this user from ever being promoted to the Message Security service.

```
unblockprovuser msmith@jumboinc.com
```

The **unblockprovuser** command unblocks a provisional user making it possible for this user to be promoted.

```
promoteprovuser msmith@jumboinc.com
```

The **promoteprovuser** command adds the provisional user to the Message Security service as a regular user.

```
deleteprovuser msmith@jumboinc.com
```

The **deleteprovuser** command deletes a provisional user.

Quarantine Summary Example

Editing the Localized Language Setting

This example shows how to set the language for the Quarantine Summary.

Note: This example uses the Administration Console batch command syntax.

1. Using the **displayorg** command, view the present settings for the Quarantine Summary language.

```
displayorg Sales
```

The **lang_locale (for orgs)** field sets the Quarantine Summary language.

```
lang_locale en.utf8
```

2. Using the **modifyorg** command, change the language setting.

```
modifyorg Sales, lang_locale=es.iso-8859-1
```

Static text in the Quarantine Summary, along with the default top text, will display in the chosen language. See “Language and Timezone” on page 569 for supported languages and character encodings, and the field values.

Message Archiving Example

Editing Message Archiving Settings

These commands apply to Postini Message Archiving, an optional product, only used with Message Security installations. Contact your account representative for further information.

Summary:

- Determine your organization's archive settings
- Modify these settings
- Disable the Message Center subject links

If your company policy requires internal archiving of all messages -- for instance, as an SEC requirements policy to archive all messages viewed by employees, allowing users to open messages in the Message Center can significantly increase the number of messages you must archive. To prevent this from happening, disable the Subject links. Then to open a quarantined message, users must first forward the message to their Inbox. Delivered message can be tracked as usual by your own archiving methods.

Note: This example uses the Administration Console batch command syntax.

1. **Using the displayorg command, determine if archiving is enabled for this org.**

```
displayorg Sales
```

The **archive** field lists whether archiving is enabled for this organization.

```
archive on
```

2. **Using the archive_settings display command, determine the archive settings.**

```
archive_settings display Sales
```

The **archive_settings display** command displays the archives' settings for an organization.

```
#Executed Without Incident
#Message Archiving Settings for Sales:
#Archive Enable on
#Mail Flow on
#Journaling off
#Archive Retention Months:12
```

3. Using the archive_settings modify command, change the archive settings for an organization.

```
archive_settings modify org=Jumbo ABC, archive_enable=on,  
mail_flow=on, journaling=on
```

The **archive_settings modify** command edits the archives' settings for an organization. Enables or disables archiving.

The **archive_enable** field enables archiving to be on for an organization.

The **journaling** field enables message archive journaling for an organization.

The **mail_flow** field turns on or off the inbound and outbound archiving.

4. Using the modifyorg command, disable the Message Center's Quarantine Summary subject link for your organization.

```
modifyorg Sales, quarantine_links=0  
modifyorg Sales, quarsum_links=0
```

The **quarantine_links** field is a switch to enable quarantine message links to be available in the Message Center.

The **quarsum_links** field is a switch enabling Quarantine Summary message links to be available.

Message Encryption Example

This example is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Viewing and Editing Message Encryption Settings

These commands apply to Postini Message Encryption, an optional product, only used with Message Security installations.

Message Encryption outbound encryption can be enabled for an organization and for an individual user. This example is for an organization.

Note: This example uses the Administration Console batch command syntax.

1. Using the displayorg command, determine the org's Message Encryption setting.

```
displayorg Western Jumbo Sales, message_encryption=match
```

The **message_encryption (for orgs)** field enables outbound organization-level messages to be encrypted and sent to a secure portal

2. Using the modifyorg command, edit the Message Encryption setting.

```
modifyorg Western Jumbo Sales, message_encryption=on
```

IM Security Example

This example is applicable to the Google Message Security, Google Message Discovery, and Google Message Filtering products only.

Viewing and Editing an Org's IM Settings

These commands apply to Postini IM Security, an optional product.

The IM Security settings can be viewed and edited at the org-level and at the individual user-level. This example is for the org-level settings.

Note: This example uses the Administration Console batch command syntax.

1. **Using the `org_im_settings display` command, determine the org's IM settings.**

```
org_im_settings display Western Jumbo Sales
```

The `org_im_settings display` command displays all of the IM settings for an organization.

```
#im_enable 1
#im_proto_enable +all
#im_external_enable 1
#disposition custom journal off
#disposition standard journal off
#disposition archive off
#disposition email msmith@jumboinc.com
```

2. **Using the `org_im_settings modify` command, edit the org's IM settings.**

```
org_im_settings modify orgtag=Western Jumbo Sales,
disposition="archive,standard_journal",
disposition_email=helpwest@jumboinc.com
```

User Settings Examples

Listing User Aliases and Primary Addresses

Three common user lists are

- Getting all aliases for one user
- Listing all primary user addresses and associated aliases for an org hierarchy.
- Getting a primary user address from a user's alias.

Note: This example uses the Administration Console batch command syntax.

1. **Using the `listusers` command, list all of the aliases for a single user.**

```
listusers ALL, primaryqs=jim@jumboinc.com, targetOrg=100046262,  
childorgs=1, aliases=1
```

The return values are a comma separated list of aliases for
jim@jumboinc.com

2. List all primary user addresses and associated aliases in an org hierarchy.

```
listusers ALL, targetOrg=[accountorg], childorgs=1,  
fields=PRIMARY_ADD|ADDRESS, aliases=1, sort=primary_add:nd
```

The return values are in a list composed of primary user addresses
(PRIMARY_ADD which is [null], and ADDRESS for the primary address), and
of primary user address and that user's aliases (PRIMARY_ADD is the
primary user address, ADDRESS is that user's alias)

3. List a user address from an alias.

```
listusers =alias4mary@jumboinc.com, targetOrg=200046262,  
childorgs=1, aliases=1, fields=ADDRESS|PRIMARY_ADD
```

The return values are the alias address and the primary user address. In this
case the return value is:

```
alias4mary@jumboinc.com mary@jumboinc.com
```

Appendix A

Additional Reference Information

Language and Timezone

The language for quarantine summary message can be set through the lang_locale field. See “lang_locale (for users)” on page 435 and “lang_locale (for orgs)” on page 350 for more information.

Following are the available languages:

Language	Batch Code	Character Encoding
English	en_us.utf8	English (U.S.) UTF-8
	en_us.iso-8859-1	English (U.S.) ISO 8859-1
	en_uk.utf8	English (U.K.) UTF-8
	en_uk.iso-8859-1	English (U.K.) ISO 8859-1
Deutsche/ German	de.utf8	German UTF-8
	de.iso-8859-1	German ISO 8859-1
Español/ Spanish	es.utf8	Spanish (Spain) UTF-8
	es.iso-8859-1	Spanish (Spain) ISO 8859-1
	es_mx.utf8	Spanish (Mexico) UTF-8
	es_mx.iso-8859-1	Spanish (Mexico) ISO 8859-1
Français/ French	fr.utf8	French UTF-8
	fr.iso-8859-1	French ISO 8859-1
Greek	gr.utf8	Greek UTF-8
Italiano/Italian	it.utf8	Italian UTF-8
	it.iso-8859-1	Italian ISO 8859-1

Language	Batch Code	Character Encoding
Japanese	ja_jp.utf8	Japanese UTF-8
	ja_jp.euc-jp	Japanese EUC-JP
	ja_jp.shift-jis	Japanese SHIFT-JIS
Korean	ko_kr.utf8	Korean UTF-8
	ko_kr.euc-kr	Korean EUC-KR
Netherlands/ Dutch	nl.utf8	Dutch UTF-8
	nl.iso-8859-1	Dutch ISO 8859-1
Polish	pl.utf8	Polish UTF-8
Portuguese	pt.utf8	Portuguese UTF-8
	pt.iso-8859-1	Portuguese ISO 8859-1
Russian	ru.utf8	Russian UTF-8
Chinese	zh_cn.utf8	Chinese (Simplified) UTF-8
	zh_cn.gb2312	Chinese (Simplified) GB2312
	zh_tw.utf8	Chinese (Traditional) UTF-8
	zh_tw.big5	Chinese (Traditional) Big5
	zh_tw.big5-hkscs	Chinese (Traditional) Big5 Hong Kong

The Region and Language Setting also determines your date format. For all other languages not listed above, the default format is <year-month-day> <time in 24 hours>.

Language	Date Format
English (US)	Quarantine Summary 9/14/2006 5:00 PM
English (UK)	Quarantine Summary 14/09/2006 16:00
German	Quarantäne-Übersicht 14.09.2006 15:45
Spanish	Resumen de Cuarentena 14/09/2006 17:00
Japanese	2006/9/14 16:00
Dutch	Opsomming quarantaine 14-9-2006 15:45
Chinese	2006-9-14 16:00
All other languages	2006-9-14 16:00

Index

A

Attachment Manager Fields

- at_notify_on 312
- bounce_fragments 323
- qtine_redir_out_atq 383

B

batch processing 15

- command syntax 18
- procedure 16
- submitting commands 16
- validation 16
- when to use 15

Building a batch file

- Using a List batch command 19
- Using Download Users/Settings 21

C

CIDR format 212, 216, 218, 220, 222

Command Quick Reference

- Adding 92
- Deleting 93
- Displaying and Reporting 95
- Domain Management 97
- IM Security 98
- IP Locking 100
- Listing 100
- Message Archiving 101
- Message Encryption 102
- Modifying 103
- Notification 104
- Organization Management 105
- Provisional User Management 106
- Spooling 107
- Testing 107
- User Management 108

Command Reference page syntax notations 135

Commands

- addalias 137
- adddomain 140
- addorg 142
- adduser 144, 548, 550

archive_settings display 148

archive_settings modify 150, 564

blockprovuser 152, 562

checklatency 153

checkroute 155

deletealias 157

deletedomain 160

deleteorg 161

deleteprovuser 163, 562

deleteuser 164

displaydomain 168, 550

displayorg 170, 538, 550, 553, 560

displayprovuser 173, 562

displayspool 175

displayuser 178, 550, 553

domain_tls add 180

domain_tls delete 182

domain_tls display 184

domain_tls modify 186

encryption display_org 188

encryption display_user 190

encryption list_users 191

encryption modify_org 193

encryption modify_user 195

getorgreport 197

help 202

im add 204

im delete 206

im display 207

im list 209

im listforuser 211

iplock add_range 212

iplock delete_range 218

iplock display 220

iplock set_disposition 222

iplockdelete 216

listdomain 224

listdomains 550

listorgs 229, 550

listprovusers 234, 560, 562

listusers 238, 538, 550, 553, 566

modifydomain 244

modifyorg 246, 563
 modifyuser 249, 538, 541, 550
 notification display 252
 notification modify 256
 org_im_settings display 261, 566
 org_im_settings modify 263, 566
 password force_update 265
 password reset 267
 password_policy display 269
 password_policy update 271
 promotprovuser 275, 562
 resetuser 276, 553
 setorgsubstripping 278
 showallowedips 280
 suspenduser 282
 testfirewall 285
 testmail 286
 testmx 289
 unblockprovuser 292, 562
 user_im_settings add 293
 user_im_settings delete 295
 user_im_settings display 297
 user_im_settings modify 299

Comments in Batch Files 17

C

Common Tasks

- Adding Users and Domains to Sender Lists 555
- Changing a user's spam settings 538
- Editing a PMP Password 541
- Editing General Notification Settings 543
- Editing Message Archiving Settings 564
- Editing Message Center Access and Settings 538
- Editing Message Encryption Settings 565
- Editing the Localization Language Setting 563
- Editing Your Mail Handling Policies 562
- Editing Your Message Limit Policies 559
- Example Syntax 535
- Listing the Organizational Hierarchy 550
- Listing User Aliases and Primary Addresses 566
- Receiving a Welcome Notification 547
- Resending the Welcome Notification 548
- Resetting Users 553
- Setting a Virus Notification Interval 549
- Viewing and Editing an Org's IM Settings 566
- Viewing Authentication and Password Settings 540
- Viewing General Notification Settings 542
- Viewing Mail Handling Policies 560
- Viewing Message Center Settings 536
- Viewing Message Limit Policies 558
- Viewing Your Organization's Sender Lists 554

Connection Manager Field

- async_bounce 311

D

documentation, related 14

Domain Commands

- adddomain 140
- deletedomain 160
- displaydomain 168
- domain_tls add 180
- domain_tls delete 182

domain_tls display 184
 domain_tls modify 186
 listdomains 224
 modifydomain 244
 setorgsubstripping 278

Domain Field Reference page syntax notations 463

Domain Field Syntax Quick Reference 49

Domain Fields

- alias 464
- aliasedfrom 465
- aliasedto 465
- created_ts 468
- customername 489
- domainid 469
- domainname 470
- org 471
- primary_did 472
- primary_dom 473
- sub_strip 475
- substrip 474

Domain Fields Quick Reference 113

E

EZCommand

- About EZCommand 22
- calling commands 23
- command reference 24
- Commands
- addalias 137
- adduser 144
- deletealias 157
- deleteuser 164
- modifyuser 249
- suspenduser 282
- example 24
- remotecmd_secret 391
- response codes 24
- setting up 22

I

IM Security Commands

- im add 204
- im delete 206
- im display 207
- im list 209
- im listforuser 211
- listusers 238
- modifyorg 246
- org_im_settings display 261
- org_im_settings modify 263
- user_im_settings add 293
- user_im_settings delete 295
- user_im_settings display 297
- user_im_settings modify 299

IM Security Fields

- file_transfer_receive 337
- file_transfer_send 338
- im_enable 342
- im_external_enable 344

im_proto_enable 345

IM Security Tasks

- Viewing and Editing an Org's IM Settings 566

IP Range Commands

- iplock add_delete 216
- iplock add_range 212
- iplock delete_range 218
- iplock display 220
- iplock set_disposition 222
- showallowedips 280

L

Languages and Timezones

- lang_locale (for orgs) 350
- lang_locale (for users) 435
- Reference 569

M

Message Archiving Commands

- archive_settings display 148
- archive_settings modify 150

Message Archiving Fields

- archive 308
- archive_enable 309, 564
- journaling 348, 564
- mail_flow 352, 564
- retention_months 392

Message Archiving Tasks

- Editing Message Archiving Settings 564

Message Center Tasks

- Editing a PMP Password 541
- Editing Message Center Access and Settings 538
- Viewing Authentication and Password Settings 540
- Viewing Message Center Settings 536

Message Encryption Commands

- encryption display_user 190
- encryption list_users 191
- encryption modify_org 193
- encryption modify_user 195

Message Encryption Manager Commands

- encryption display_org 188

Message Encryption Task

- Editing Message Encryption Settings 565

N

Notification Tasks

- Editing General Notification Settings 543
- Receiving a Welcome Notification 547
- Resending the Welcome Notification 548
- Setting a Virus Notification Interval 549
- Viewing General Notification Settings 542

Notifications, getting session status 16

O

Org Commands

- addorg 142
- deleteorg 161
- displayorg 170
- listorgs 229
- modifyorg 246
- notification display 252

notification modify 256

org_im_settings display 261

org_im_settings modify 263

setorgsubstripping 278

Org Field Reference page syntax notations 303

Org Fields

- antivirus_sensitivity 304
- approved_senders 306, 555
- archive 308
- archive_enable 309
- async_bounce 311, 560
- at_notify_on 312, 542, 543
- atine_redir_out_virus 384
- authentication_data 314, 540, 560
- authentication_type 316, 540, 560
- autocreate_smtp 560
- autocreate_web 318, 560
- blatant_spam 319
- blocked_senders 321, 555
- bounce_fragments 323
- company_name 324, 542, 543
- create_method 325
- created_date 326
- creator 327
- custom_journal 328
- default_message_limit 330, 558, 559
- default_user 332, 538, 550, 553
- disable_first_spam 333, 542, 543, 548
- disposition_virus 335
- ext_encrypt 565
- file_transfer_receive 337
- file_transfer_send 338
- footer_on 340
- iid 341
- im_enable 342
- im_external_enable 344
- im_proto_enable 345
- is_email_config 347, 550
- journaling 348
- lang_locale 350, 563
- lastmod_date 351
- mail_flow 352
- max_message_size 353, 558, 559
- message_encrypt 355
- message_encryption_criteria 356
- ndr 358, 560
- non_account_bounce 359, 560
- non_account_virus_scan 361
- nullsender_disposition 363, 365
- orgname 367
- orgtag 369
- out_at_notify_on 370, 542, 543
- outbound_max_message_size 372, 558
- outbound_max_message-size 559
- outbound_virus 373
- outbound_virus_disposition 375
- parent_org 376
- qsum_actionable 378
- qsum_enable 379
- qtine_redir_atq 380

qtine_redir_ndr 382
 qtine_redir_out_atq 383
 qtine_redir_spam 386
 qtine_redir_virus 387
 quarantine_links 388, 564
 quarsum_links 389, 564
 remotecmd_secret 391
 retention_months 392
 spam_notify_on 393, 542, 543
 standard_journal 394
 support_contact 396, 542, 543
 tagonly_spam 398
 timezone 399
 tls_notify_admin 400
 tls_notify_on 402
 virus_clean 403
 virus_notify 404, 542, 543, 549
 welcome_on 406, 542
 zero_hour_notify_on 407
 zero_hour_scan 409

Org Settings Tasks

- Adding Users and Domains to Sender Lists 555
- Editing Your Mail Handling Policies 562
- Editing Your Message Limit Policies 559
- Listing the Organizational Hierarchy 550
- Resetting Users 553
- Viewing Mail Handling Policies 560
- Viewing Message Limit Policies 558
- Viewing Your Organization's Sender Lists 554

Organization Field Syntax Quick Reference 52

Organization Fields Quick Reference

- Attachment Manager 111
- Default User 112
- Email Config 114
- General Settings 116
- IM Security 118
- Message Archiving 119
- Message Limits 120
- Notifications 121
- Outbound Compliance Footer 121
- Sender List 126
- Spam Filtering 127
- System Testing 128
- User Access 129
- Virus Blocking 133

P

PMP Commands

- password force_update 265
- password reset 267
- password_policy display 269
- password_policy update 271

Policy-Enforced TLS Commands

- domain_tls add 180
- domain_tls delete 182
- domain_tls display 184
- domain_tls modify 186

Provisional User Commands

- blockprovuser 152
- deleteprovuser 163

displayprovuser 173
 listprovusers 234
 promotprovuser 275
 unblockprovuser 292

Q

Quarantine Summary Task

- Editing the Localization Language Setting 563

Quick Reference Summaries

- Command and Field Syntax 27
- Command Quick Reference 91
- Field Quick Reference 111

R

related documentation 14

Report Command

- getorgreport 197

Report Field Reference page syntax notation 477

Report Field Syntax Quick Reference 70

Report Fields

- acc_messages 478
- account 479
- bad_isp 480
- bad_sender 481
- bulk 482
- bytes 483
- clean_failures 486
- cleanings 485
- commerce 487
- customerid 488
- deliveries 490
- inf_deliveries 491
- messages 492
- mmf 494
- naughty 495
- num_bh_messages 496
- num_bytes 497
- num_f_messages 498
- num_messages 499
- num_q_messages 500
- num_spams 502
- num_viruses 503
- pct_bh_bytes 504
- pct_bh_messages 505
- pct_f_bytes 506
- pct_f_messages 507
- pct_q_bytes 508
- pct_q_messages 509
- productid 510
- racial 511
- recip 513
- sellerid 514
- ssb 515
- stored_size 516
- users 518

Reporting Fields Quick Reference

- Spam 122
- Traffic 123
- Usage 124
- Virus 125

S

SmartCreate, See Provisional User Commands
Spool Command
 displayspool 175
Spool Field Reference page syntax notations 521
Spool Field Syntax Quick Reference 78
Spool Fields
 auto_unspool 522
 despool_max_connections 523
 duration 524
 org 525
 quota 526
 spool_delay 528
 spool_mech 529
 status 531
 used_pct 532
 used_size 533

T

Testing Commands
 checklatency 153
 checkroute 155
 testfirewall 285
 testmail 286
 testmx 289
troubleshooting batch processing 26

U

User Commands
 addalias 137
 adduser 144
 deletealias 157
 deleteuser 164
 displayuser 178
 im_listforuser 211
 listusers 238
 modifyuser 249
 resetuser 276
 suspenduser 282
 user_im_settings add 293
 user_im_settings delete 295
 user_im_settings display 297
 user_im_settings modify 299

User Field Reference page syntax notations 411

User Field Syntax Quick Reference 80

User Fields

 active 412, 536, 547
 address 413
 approved_recipients 414, 536
 approved_senders 416, 536
 blocked_senders 419, 536
 create_method 421
 created_date 422
 created_ts 423
 filter_adult 424, 538
 filter_bulk 426, 538
 filter_getrich 427, 538
 filter_offers 428, 538
 filter_racial 430, 538
 im_name 431

initial_password 432, 540
junkmail_filter 434, 538
lang_locale 435, 538
lastmod_date 436
message_count 437, 558, 559
message_encrypt 438
message_limit 440, 558, 559
message_limited 441, 558, 559
notice_address 442, 538
orgid 444
password 445, 540, 541
primary 447
primary_add 448
timezone 449, 538
TS1 451
TS3 452
u_id 454
uid 453
user_id 455
virus_notify 456, 549
virus_state 458
weblocked 459, 538
welcome_count 460, 542, 547
welcome_on 547
wireless_state 461, 538

User Fields Quick Reference

General Settings 130, 133
Message Limits 120
Quarantine 121
Sender List 126
Spam Filter 127
Virus Blocking 134

User Tasks

 Listing User Aliases and Primary Addresses 566